CISSP.exam.724q

Number: CISSP
Passing Score: 800
Time Limit: 120 min

CISSP

Certified Information Systems Security Professional

Sections

1. Security and Risk Management
2. Asset Security
3. Security Engineering

4. Communication and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

Exam A

QUESTION 1
Regarding risk reduction, which of the following answers is BEST defined by the process of giving only just enough access to information necessary for them to perform their job functions?

A. Least Privilege Principle
B. Minimum Privilege Principle
C. Mandatory Privilege Requirement
D. Implicit Information Principle

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more. If an individual has excessive permissions and rights, it could open the door to abuse of access and put the company at more risk than is necessary. For example, if Dusty is a technical writer for a company, he does not necessarily need to have access to the company's source code. So, the mechanisms that control Dusty's access to resources should not let him access source code. This would properly fulfill operations security controls that are in place to protect resources.

Incorrect Answers:
B: Minimum Privilege Principle is not the term defined by the process of giving only just enough access to information necessary for them to perform their job functions.
C: Mandatory Privilege Requirement is not the term defined by the process of giving only just enough access to information necessary for them to perform their job functions.
D: Implicit Information Principle is not the term defined by the process of giving only just enough access to information necessary for them to perform their job

functions.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1236

QUESTION 2
Which term BEST describes a practice used to detect fraud for users or a user by forcing them to be away from the workplace for a while?

A. Mandatory Vacations
B. Least Privilege Principle
C. Obligatory Separation
D. Job Rotation

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Employees in sensitive areas should be forced to take their vacations, which is known as a mandatory vacation. While they are on vacation, other individuals fill their positions and thus can usually detect any fraudulent errors or activities. Two of the many ways to detect fraud or inappropriate activities would be the discovery of activity on someone's user account while they're supposed to be away on vacation, or if a specific problem stopped while someone was away and not active on the network. These anomalies are worthy of investigation. Employees who carry out fraudulent activities commonly do not take vacations because they do not want anyone to figure out what they are doing behind the scenes. This is why they must be forced to be away from the organization for a period of time, usually two weeks.

Incorrect Answers:
B: Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more. This is not what is described in the question.
C: Obligatory Separation is not a term for the process used to detect fraud for users or a user by forcing them to be away from the workplace for a while. D: Job rotation in the workplace is a system where employees work at several jobs in a business, performing each job for a relatively short period of time. This could be used to detect fraud for users or a user by forcing them to be away from the workplace for a while. However, this question is asking for the BEST answer and Mandatory Vacations are for this specific purpose.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 127, 1235-1236

QUESTION 3
Which of the following is a fraud detection method whereby employees are moved from position to position?

A. Job Rotation

B. Mandatory Rotation
C. Mandatory Vacations
D. Mandatory Job Duties

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Job rotation is a detective administrative control to detect fraud.
Job rotation means that, over time, more than one person fulfills the tasks of one position within the company. This enables the company to have more than one person who understands the tasks and responsibilities of a specific job title, which provides backup and redundancy if a person leaves the company or is absent. Job rotation also helps identify fraudulent activities, and therefore can be considered a detective type of control. If Keith has performed David's position, Keith knows the regular tasks and routines that must be completed to fulfill the responsibilities of that job. Thus, Keith is better able to identify whether David does something out of the ordinary and suspicious.

Incorrect Answers:
B: Job Rotation, not Mandatory Rotation is the fraud detection method whereby employees are moved from position to position.
C: Mandatory vacations are a way of detecting fraud. If a fraudulent activity stops while an employee is on vacation, it is easy to determine who was committing the fraud. Mandatory vacations force employees to take vacations rather than move them to another position.
D: Mandatory Job Duties would describe duties that must be performed as part of a role. It does not describe a fraud detection method whereby employees are moved from position to position.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 127, 1235-1236

QUESTION 4
The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:

A. preventive/physical.

B. detective/technical.
C. detective/physical.
D. detective/administrative.

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
The detective/physical controls help to identify an incident's activities and potentially an intruder using items put into place to protect facility, personnel, and resources. These items include motion detectors and closed-circuit TVs. Closed-circuit TVs are normally monitored by security guards to detect intruders.

Incorrect Answers:
A: Preventive/physical controls are meant to discourage a potential attacker using items put into place to protect facility, personnel, and resources. Sensors or cameras are not included in these items.
B: The detective/technical controls helps to identify an incident's activities and potentially an intruder using software or hardware components, which include Audit logs and IDS. Sensors or cameras are not included.
D: The detective/administrative controls helps to identify an incident's activities and potentially an intruder using management-oriented controls, which include monitoring and supervising, job rotation, and investigations. Sensors or cameras are not included.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 28-34

QUESTION 5
Controls such as job rotation, the sharing of responsibilities, and reviews of audit records are associated with:

A. preventive/physical.
B. detective/technical.
C. detective/physical.
D. detective/administrative.

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:

Examples of detective administrative controls include monitoring and supervising, job rotation, and investigations.

Incorrect Answers:
A: Examples of preventive/physical controls include locks, badge systems, security guards, biometric system, and mantrap doors.
B: Examples of detective/technical controls include audit logs and IDS.
C: Examples of detective/physical controls include motion detectors and closed-circuit TVs.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 28-34

QUESTION 6
In terms or Risk Analysis and dealing with risk, which of the four common ways listed below seek to eliminate involvement with the risk being evaluated?
A. Avoidance
B. Acceptance
C. Transference
D. Mitigation

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
If a company decides to terminate the activity that is introducing the risk, this is known as risk avoidance. For example, if a company allows employees to use instant messaging (IM), there are many risks surrounding this technology. The company could decide not to allow any IM activity by their users because there is not a strong enough business need for its continued use. Discontinuing this service is an example of risk avoidance.
By avoiding the risk, we can eliminate involvement with the risk.

Incorrect Answers:
B: Risk acceptance means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. This does not eliminate involvement with the risk.
C: Risk transference is where you assign the risk to someone else; for example, by purchasing insurance. This would transfer the risk to the insurance company. This does not eliminate involvement with the risk. D: Risk mitigation is to implement a countermeasure to protect against the
risk. This does not eliminate involvement with the risk.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

QUESTION 7

Of the multiple methods of handling risks which we must undertake to carry out business operations, which one involves using controls to reduce the risk?

A. Mitigation
B. Avoidance
C. Acceptance
D. Transference

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Risk mitigation is where the risk is reduced to a level considered acceptable enough to continue conducting business. The implementation of firewalls, training, and intrusion/detection protection systems or other control types represent types of risk mitigation efforts.

Incorrect Answers:
B: Risk avoidance is where a company removes the risk. For example, by disabling a service or removing an application deemed to be a risk. This is not the process of reducing risk by implementing controls.
C: Risk acceptance means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. This is not the process of reducing risk by implementing controls.
D: Risk transference is where you assign the risk to someone else; for example, by purchasing insurance. This would transfer the risk to the insurance company. This is not the process of reducing risk by implementing controls.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

QUESTION 8
There is no way to completely abolish or avoid risks, you can only manage them. A risk free environment does not exist. If you have risks that have been identified, understood and evaluated to be acceptable in order to conduct business operations. What is this this approach to risk management called?

A. Risk Acceptance
B. Risk Avoidance
C. Risk Transference
D. Risk Mitigation

Correct Answer: A
Section: Security and Risk Management

Explanation

Explanation/Reference:
Explanation:
Risk Acceptance means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. Many companies will accept risk when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the potential loss value.
Risk acceptance should be based on several factors. For example, is the potential loss lower than the countermeasure? Can the organization deal with the "pain" that will come with accepting this risk? This second consideration is not purely a cost decision, but may entail noncost issues surrounding the decision. For example, if we accept this risk, we must add three more steps in our production process. Does that make sense for us? Or if we accept this risk, more security incidents may arise from it, and are we prepared to handle those?

Incorrect Answers:
B: Risk avoidance is where a company removes the risk. For example, by disabling a service or removing an application deemed to be a risk. This does not refer to the accepting of known risks.
C: Risk transference is where you assign the risk to someone else; for example, by purchasing insurance. This would transfer the risk to the insurance company. This does not to the accepting of known risks.
D: Risk mitigation is to implement countermeasures to protect against the risk. This does not refer to the accepting of known risks.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

QUESTION 9
John is the product manager for an information system. His product has undergone under security review by an IS auditor. John has decided to apply appropriate security controls to reduce the security risks suggested by an IS auditor. Which of the following technique is used by John to treat the identified risk provided by an IS auditor?

A. Risk Mitigation
B. Risk Acceptance
C. Risk Avoidance
D. Risk transfer

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:

Risk mitigation is where the risk is reduced to a level considered acceptable enough to continue conducting business. The implementation of firewalls, training, and intrusion/detection protection systems or other control types represent types of risk mitigation efforts.

Incorrect Answers:
B: C: Risk acceptance means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. This is not the process of reducing risk by implementing controls.
C: Risk avoidance is where a company removes the risk. For example, by disabling a service or removing an application deemed to be a risk. This is not the process of reducing risk by implementing controls.
D: Risk transference is where you assign the risk to someone else; for example, by purchasing insurance. This would transfer the risk to the insurance company. This is not the process of reducing risk by implementing controls.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

QUESTION 10
Sam is the security Manager of a financial institute. Senior management has requested he performs a risk analysis on all critical vulnerabilities reported by an IS auditor. After completing the risk analysis, Sam has observed that for a few of the risks, the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred. What kind of a strategy should Sam recommend to the senior management to treat these risks?

A. Risk Mitigation
B. Risk Acceptance
C. Risk Avoidance
D. Risk transfer

Correct Answer: B
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Risk Acceptance means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. Many companies will accept risk when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the potential loss value.
Risk acceptance should be based on several factors. For example, is the potential loss lower than the countermeasure? Can the organization deal with the “pain” that will come with accepting this risk? This second consideration is not purely a cost decision, but may entail noncost issues surrounding the decision. For example, if we accept this risk, we must add three more steps in our production process. Does that make sense for us? Or if we accept this risk, more security incidents may arise from it, and are we prepared to handle those?

Incorrect Answers:
A: Risk mitigation is to implement countermeasures to protect against the risk. This does not refer to the accepting of known risks because the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred.
C: Risk avoidance is where a company removes the risk. For example, by disabling a service or removing an application deemed to be a risk. This does not refer to the accepting of known risks because the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred.
D: Risk transference is where you assign the risk to someone else; for example, by purchasing insurance. This would transfer the risk to the insurance company. This does not to the accepting of known risks because the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

QUESTION 11
Which of the following risk handling technique involves the practice of being proactive so that the risk in question is not realized?

A. Risk Mitigation
B. Risk Acceptance
C. Risk Avoidance
D. Risk transfer

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
If a company decides to terminate the activity that is introducing the risk, this is known as risk avoidance. For example, if a company allows employees to use instant messaging (IM), there are many risks surrounding this technology. The company could decide not to allow any IM activity by their users because there is not a strong enough business need for its continued use. Discontinuing this service is an example of risk avoidance.
By being proactive and removing the vulnerability causing the risk, we are avoiding the risk.

Incorrect Answers:
A: Risk mitigation is to implement a countermeasure to protect against the risk. Implementing controls is being proactive and would 'reduce' a risk, however, only risk avoidance 'removes' the risk or prevents the risk being realized in the first place.
B: Risk acceptance means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. This does not describe being proactive to remove the risk.
D: Risk transference is where you assign the risk to someone else; for example, by purchasing insurance. This would transfer the risk to the insurance company. This does not describe being proactive to remove the risk.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

QUESTION 12
Which of the following risk handling technique involves the practice of passing on the risk to another entity, such as an insurance company?

A. Risk Mitigation
B. Risk Acceptance
C. Risk Avoidance
D. Risk transfer

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Many types of insurance are available to companies to protect their assets. If a company decides the total risk is too high to gamble with, it can purchase insurance, which would transfer the risk to the insurance company.
Incorrect Answers:
A: Risk mitigation is where controls or countermeasures are implemented to ensure the risk is reduced to a level considered acceptable enough to continue conducting business. This is not the practice of passing on the risk to another entity, such as an insurance company.
B: Risk acceptance means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. This is not the practice of passing on the risk to another entity, such as an insurance company.
C: Risk avoidance is where a company removes a risk or does not implement something that could introduce a risk. For example, by disabling a service or removing an application deemed to be a risk or not implementing them in the first place. This is not the practice of passing on the risk to another entity, such as an insurance company.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

QUESTION 13
Which of the following pairings uses technology to enforce access control policies?

A. Preventive/Administrative
B. Preventive/Technical
C. Preventive/Physical
D. Detective/Administrative

Correct Answer: B
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Controls are implemented to mitigate risk and reduce the potential for loss. Controls can be preventive, detective, or corrective. Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful occurrences; corrective controls are used to restore systems that are victims of harmful attacks.
Technical controls are the software tools used to restrict subjects' access to objects. They are core components of operating systems, add-on security packages, applications, network hardware devices, protocols, encryption mechanisms, and access control matrices. These controls work at different layers within a network or system and need to maintain a synergistic relationship to ensure there is no unauthorized access to resources and that the resources' availability, integrity, and confidentiality are guaranteed. Technical controls protect the integrity and availability of resources by limiting the number of subjects that can access them and protecting the confidentiality of resources by preventing disclosure to unauthorized subjects.

Incorrect Answers:
A: Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Administrative controls do not use technology to enforce access control policies.
C: Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting. Physical controls do not use technology to enforce access control policies.
D: Detective controls are established to discover harmful occurrences after they have happened. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training.
Detective controls and administrative controls do not use technology to enforce access control policies.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 28, 245

QUESTION 14
Which type of risk assessment is the formula ALE = ARO x SLE used for?

A. Quantitative Analysis
B. Qualitative Analysis
C. Objective Analysis
D. Expected Loss Analysis

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
A quantitative risk analysis is used to assign monetary and numeric values to all elements of the risk analysis process. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks.
The most commonly used equations used in quantitative risk analysis are the single loss expectancy (SLE) and the annual loss expectancy (ALE).
The SLE is a dollar amount that is assigned to a single event that represents the company's potential loss amount if a specific threat were to take place.
The annualized rate of occurrence (ARO) is the value that represents the estimated frequency of a specific threat taking place within a 12-month timeframe.

Incorrect Answers:
B: Qualitative risk analysis quantifies the risk rather than assigning a monetary value to the impact of a risk. It does not use the ALE = ARO x SLE formula.
C: Objective Analysis is not one of the defined risk assessment methods and does not use the ALE = ARO x SLE formula.
D: Expected Loss Analysis is not one of the defined risk assessment methods. Expected loss is calculated using the quantitative risk analysis method.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 87

QUESTION 15
Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?

A. Confidentiality
B. Integrity
C. Availability
D. Accuracy

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Confidentiality ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure.
Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more.
We can keep data 'confidential' by providing access to information only to authorized and intended users.

Incorrect Answers:
B: Integrity ensures that data is unaltered. It does not restrict access to information only to authorized and intended users.

C: Availability ensures reliability and timely access to data and resources to authorized individuals. It does not restrict access to information only to authorized and intended users.
D: Accuracy is not one of the three CIA/AIC attributes (Confidentiality, Integrity, Availability) and does not restrict access to information only to authorized and intended users.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 22-23

QUESTION 16
You are a manager for a large international bank and periodically move employees between positions in your department. What is this process called?

A. Job Rotation
B. Separation of Duties
C. Mandatory Vacation
D. Dual Control

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Job rotation ensures that more than one person fulfills the tasks of one position within the company, over time. It, therefore, provides backup and redundancy if a person leaves the company or is absent.

Incorrect Answers:
B: Separation of Duties is a preventive administrative control that is used to make sure one person is unable to carry out a critical task alone.
C: Mandatory Vacation is when employees in sensitive areas are forced to take their vacations, allowing other individuals to fill their positions for the purpose of detecting any fraudulent errors or activities.

D: Dual Control is a variation of Separation of Duties.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 126-127

QUESTION 17
Which of the following is a CHARACTERISTIC of a decision support system (DSS) in regards to Threats and Risks Analysis?

A. DSS is aimed at solving highly structured problems.
B. DSS emphasizes flexibility in the decision making approach of users.
C. DSS supports only structured decision-making tasks.
D. DSS combines the use of models with non-traditional data access and retrieval functions.

Correct Answer: B
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
A Decision Support System (DSS) is a computer-based information system that supports business or organizational decision-making activities. DSSs serve the management, operations, and planning levels of an organization (usually mid and higher management) and help people make decisions about problems that may be rapidly changing and not easily specified in advance - i.e. Unstructured and Semi-Structured decision problems.
DSS emphasizes flexibility and adaptability to accommodate changes in the environment and the decision making approach of the user.
DSS tends to be aimed at the less well structured, underspecified problem that upper level managers typically face.
DSS attempts to combine the use of models or analytic techniques with traditional data access and retrieval functions.
DSS attempts to combine the use of models or analytic techniques with traditional data access and retrieval functions.

Incorrect Answers:
A: DSS is aimed at solving unstructured and semi-structured decision problems, not highly structured problems.
C: DSS does not support only structured decision-making tasks; it supports unstructured and semi-structured decision-making tasks.
D: DSS attempts to combine the use of models or analytic techniques with traditional (not non-traditional) data access and retrieval functions.

References:
https://en.wikipedia.org/wiki/Decision_support_system

QUESTION 18
Which of the following is covered under Crime Insurance Policy Coverage?

A. Inscribed, printed and Written documents

B. Manuscripts
C. Accounts Receivable
D. Money and Securities

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Crime Insurance policy protects organizations from loss of money, securities, or inventory resulting from crime.

Incorrect Answers:
A: Crime Insurance Policy does not protect Inscribed, printed and written documents. You would need Valuable paper insurance for that.
B: Crime Insurance Policy does not protect manuscripts. You would need Valuable paper insurance for that.
C: Crime Insurance Policy does not protect business records such as Accounts Receivable. You would need Valuable paper insurance for that.

References:
http://www.insurecast.com/html/crime_insurance.asp

QUESTION 19
It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?

A. security administrator
B. security analyst
C. systems auditor
D. systems programmer

Correct Answer: D
Section: Security and Risk Management
Explanation
Explanation/Reference:
Explanation:
Reason: The security administrator, security analysis, and the system auditor need access to portions of the security systems to accomplish their jobs. The system programmer does not need access to the working (AKA: Production) security systems.

Programmers should not be allowed to have ongoing direct access to computers running production systems (systems used by the organization to operate its business). To maintain system integrity, any changes they make to production systems should be tracked by the organization's change management control system.

Because the security administrator's job is to perform security functions, the performance of non-security tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users abusing their authority by taking actions outside of their assigned functional responsibilities.

Incorrect Answers:
A: The security administrator needs to access the software on systems implementing security to perform his job function.
B: The security analyst needs to access the software on systems implementing security to perform his job function.
C: The systems auditor needs to access the software on systems implementing security to perform his job function.

QUESTION 20
The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

A. Clipping level
B. Acceptance level
C. Forgiveness level
D. Logging level

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
The correct answer is "clipping level". This is the point at which a system decides to take some sort of action when an action repeats a preset number of times. In order to limit the amount of audit information flagged and reported by automated violation analysis and reporting mechanisms, clipping levels can be set. Using clipping levels refers to setting allowable thresholds on a reported activity. For example, a clipping level of three can be set for reporting failed log-on attempts at a workstation. Thus, three or fewer log-on attempts by an individual at a workstation will not be reported as a violation, thus eliminating the need for reviewing normal log-on entry errors.

Incorrect Answers:
B: Acceptance level is not the correct term for the number of violations that will be accepted or forgiven before a violation record is produced.
C: Forgiveness level is not the correct term for the number of violations that will be accepted or forgiven before a violation record is produced.
D: Logging level is a term used to describe what types of events are logged. It is not the correct term for the number of violations that will be accepted or forgiven before a violation record is produced.

References:

Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 50

QUESTION 21
Which of the following ensures that security is NOT breached when a system crash or other system failure occurs?

A. Trusted recovery
B. Hot swappable
C. Redundancy
D. Secure boot

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Trusted recovery ensures that security is not breached when a system crash or other system failure (sometimes called a “discontinuity”) occurs. It must ensure that the system is restarted without compromising its required protection scheme, and that it can recover and rollback without being compromised after the failure. Trusted recovery is required only for B3 and A1 level systems. A system failure represents a serious security risk because the security controls may be bypassed when the system is not functioning normally.
For example, if a system crashes while sensitive data is being written to a disk (where it would normally be protected by controls), the data may be left unprotected in memory and may be accessible by unauthorized personnel.
Trusted recovery has two primary activities — preparing for a system failure and recovering the system.

Incorrect Answers:
B: Hot swappable refers to computer components that can be swapped while the computer is running. This is not what is described in the question.
C: Redundancy refers to multiple instances of computer or network components to ensure that the system can remain online in the event of a component failure. This is not what is described in the question.
D: Secure Boot refers to a security standard that ensures that a computer boots using only software that is trusted. This is not what is described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p.

310

QUESTION 22
Which of the following ensures that a TCB is designed, developed, and maintained with formally controlled standards that enforces protection at each stage in the system's life cycle?

A. Life cycle assurance
B. Operational assurance
C. Covert timing assurance
D. Covert storage assurance

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
The Orange Book defines two types of assurance — operational assurance and life cycle assurance.
Life cycle assurance ensures that a TCB is designed, developed, and maintained with formally controlled standards that enforces protection at each stage in the system's life cycle. Configuration management, which carefully monitors and protects all changes to a system's resources, is a type of life cycle assurance.
The life cycle assurance requirements specified in the Orange Book are as follows:
▪ Security testing
▪ Design specification and testing
▪ Configuration management ▪
Trusted distribution

Incorrect Answers:
B: Operational assurance focuses on the basic features and architecture of a system. An example of an operational assurance would be a feature that separates a security-sensitive code from a user code in a system's memory. Operational assurance is not what is described in the question. C: Covert timing assurance is not one of the two defined types of assurance.
D: Covert storage assurance is not one of the two defined types of assurance.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, pp. 305-306

QUESTION 23
What is the MAIN objective of proper separation of duties?

A. To prevent employees from disclosing sensitive information.
B. To ensure access controls are in place.
C. To ensure that no single individual can compromise a system.
D. To ensure that audit trails are not tampered with.

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
The objective of separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. High-risk activities should be broken up into different parts and distributed to different individuals or departments. That way, the company does not need to put a dangerously high level of trust in certain individuals. For fraud to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity Job rotation in the workplace is a system where employees work at several jobs in a business, performing each job for a relatively short period of time.

Incorrect Answers:
A: Separation of duties does not prevent employees from disclosing sensitive information.
B: Separation of duties does not ensure access controls are in place.
D: Separation of duties does not ensure that audit trails are not tampered with.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 1235-1236

QUESTION 24
This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

A. Checkpoint level
B. Ceiling level
C. Clipping level
D. Threshold level

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.

The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).

If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.

Incorrect Answers:
A: Checkpoint level is not the correct term for the baseline described in the question.
B: Ceiling level is not the correct term for the baseline described in the question.
D: Threshold level is not the correct term for the baseline described in the question.

QUESTION 25
In order to enable users to perform tasks and duties without having to go through extra steps, it is important that the security controls and mechanisms that are in place have a degree of?

A. Complexity
B. Non-transparency
C. Transparency
D. Simplicity

Correct Answer: C
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
The security controls and mechanisms that are in place must have a degree of transparency.
This enables the user to perform tasks and duties without having to go through extra steps because of the presence of the security controls. Transparency also does not let the user know too much about the controls, which helps prevent him from figuring out how to circumvent them. If the controls are too obvious, an attacker can figure out how to compromise them more easily.

Security (more specifically, the implementation of most security controls) has long been a sore point with users who are subject to security controls. Historically, security controls have been very intrusive to users, forcing them to interrupt their work flow and remember arcane codes or processes (like long passwords or access codes), and have generally been seen as an obstacle to getting work done. In recent years, much work has been done to remove that stigma of security controls as a detractor from the work process adding nothing but time and money. When developing access control, the system must be as transparent as

possible to the end user. The users should be required to interact with the system as little as possible, and the process around using the control should be engineered so as to involve little effort on the part of the user.
For example, requiring a user to swipe an access card through a reader is an effective way to ensure a person is authorized to enter a room. However, implementing a technology (such as RFID) that will automatically scan the badge as the user approaches the door is more transparent to the user and will do less to impede the movement of personnel in a busy area.
In another example, asking a user to understand what applications and data sets will be required when requesting a system ID and then specifically requesting access to those resources may allow for a great deal of granularity when provisioning access, but it can hardly be seen as transparent. A more transparent process would be for the access provisioning system to have a role-based structure, where the user would simply specify the role he or she has in the organization and the system would know the specific resources that user needs to access based on that role. This requires less work and interaction on the part of the user and will lead to more accurate and secure access control decisions because access will be based on predefined need, not user preference.
When developing and implementing an access control system special care should be taken to ensure that the control is as transparent to the end user as possible and interrupts his work flow as little as possible.

Incorrect Answers:
A: The complexity of security controls is not what enables users to perform tasks and duties without having to go through extra steps. The controls can be complex or simple; as long as they have a degree of transparency, users will be able to perform tasks and duties without having to go through extra steps.
B: Non-transparent security controls do not enable users to perform tasks and duties without having to go through extra steps; this would be the opposite in that it would require the extra steps.
D: The simplicity of security controls is not what enables users to perform tasks and duties without having to go through extra steps. The controls can be complex or simple; as long as they have a degree of transparency, users will be able to perform tasks and duties without having to go through extra steps.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 1239-1240

QUESTION 26
Which of the following rules is LEAST likely to support the concept of least privilege?

A. The number of administrative accounts should be kept to a minimum.
B. Administrators should use regular accounts when performing routine operations like reading mail.
C. Permissions on tools that are likely to be used by hackers should be as restrictive as possible.
D. Only data to and from critical systems and applications should be allowed through the firewall.

Correct Answer: D
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:

Only data to and from critical systems and applications should be allowed through the firewall is a detractor. Critical systems or applications do not necessarily need to have traffic go through a firewall. Even if they did, only the minimum required services should be allowed. Systems that are not deemed critical may also need to have traffic go through the firewall.

Least privilege is a basic tenet of computer security that means users should be given only those rights required to do their jobs or tasks. Least privilege is ensuring that you have the minimum privileges necessary to do a task. An admin NOT using his admin account to check email is a clear example of this.

Incorrect Answers:
A: The number of administrative accounts should be kept to a minimum: this is good practice and supports the concept of least privilege.
B: Administrators should use regular accounts when performing routine operations like reading mail: this is good practice and supports the concept of least privilege.
C: Permissions on tools that are likely to be used by hackers should be as restrictive as possible: this is good practice and supports the concept of least privilege.

QUESTION 27
Complete the following sentence. A message can be encrypted, which provides:

A. Confidentiality
B. Non-Repudiation
C. Authentication
D. Integrity

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Confidentiality ensures that a message can only be read by the intended recipient. Encrypting a message provides confidentiality.
Different steps and algorithms provide different types of security services:
- A message can be encrypted, which provides confidentiality.
- A message can be hashed, which provides integrity
- A message can be digitally signed, which provides authentication, nonrepudiation, and integrity.
- A message can be encrypted and digitally signed, which provides confidentiality, authentication, nonrepudiation, and integrity

Incorrect Answers:
B: A digital signature is required to provide non-repudiation for a message. Encryption alone does not provide non-repudiation.
C: A digital signature is required to provide authentication for a message. Encryption alone does not provide authentication.
D: A hash is required to provide integrity for a message. Encryption alone does not provide integrity.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 829-830

QUESTION 28
A message can be encrypted and digitally signed, which provides:

A. Confidentiality, Authentication, Non-repudiation, and Integrity.
B. Confidentiality and AuthenticationC. Confidentiality and Non-repudiation
D. Confidentiality and Integrity.

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Confidentiality ensures that a message can only be read by the intended recipient. Encrypting a message provides confidentiality.
A digital signature provides Authentication, Non-repudiation, and Integrity**.**
The purpose of digital signatures is to detect unauthorized modifications of data, and to authenticate the identity of the signatories and non-repudiation. These functions are accomplished by generating a block of data that is usually smaller than the size of the original data. This smaller block of data is bound to the original data and to the identity of the sender. This binding verifies the **integrity** of data and provides non-repudiation. To quote the National Institute Standards and Technology (NIST) Digital Signature Standard (DSS): Digital signatures are used to detect unauthorized modifications to data and to **authenticate** the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory.

Different steps and algorithms provide different types of security services:
- A message can be encrypted, which provides confidentiality.
- A message can be hashed, which provides integrity
- A message can be digitally signed, which provides authentication, nonrepudiation, and integrity.
- A message can be encrypted and digitally signed, which provides confidentiality, authentication, nonrepudiation, and integrity

Incorrect Answers:
B: A digital signature provides Authentication, Non-repudiation, and Integrity; not just Authentication.
C: A digital signature provides Authentication, Non-repudiation, and Integrity; not just Non-repudiation.
D: A digital signature provides Authentication, Non-repudiation, and Integrity; not just Integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 829-830
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 151

QUESTION 29

There are basic goals of Cryptography. Which of the following most benefits from the process of encryption?

A. Confidentiality
B. Authentication
C. Integrity
D. Non-Repudiation

Correct Answer: A
Section: Security and Risk Management
Explanation

Explanation/Reference:
Explanation:
Confidentiality makes sure that the required level of secrecy is applied at each junction of data processing and prevents unauthorized disclosure. Encrypting data as it is stored and transmitted, enforcing strict access control and data classification, and teaching employees on the correct data protection procedures are ways in which Confidentiality can be provided.

Incorrect Answers:
B: Authentication refers to the verification of the identity of a user who is requesting the use of a system and/or access to network resources.
C: Integrity is upheld by providing assurance of the accuracy and reliability of information and systems and preventing any unauthorized modification.
D: Non-Repudiation makes sure that a sender is unable to deny sending a message.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 23-25, 162, 398

QUESTION 30
In Mandatory Access Control, sensitivity labels attached to objects contain what information?

A. The item's classification
B. The item's classification and category set
C. The item's category
D. The items' need to know

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Mandatory Access Control begins with security labels assigned to all resource objects on the system. These security labels contain two pieces of information - a classification (top secret, confidential etc.) and a category (which is essentially an indication of the management level, department or project to which the object is available).
Similarly, each user account on the system also has classification and category properties from the same set of properties applied to the resource objects. When a user attempts to access a resource under Mandatory Access Control the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's credentials match the MAC security label properties of the object access is allowed. It is important to note that both the classification and categories must match. A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object.

Incorrect Answers:
A: In Mandatory Access Control, the sensitivity labels attached to objects contain a category set as well as the item's classification.
C: In Mandatory Access Control, the sensitivity labels attached to objects contain the item's classification as well as a category.
D: An item's need to know is not something that is included in the sensitivity label. The categories portion of the label is used to enforce need-to-know rules.
References:
http://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control

QUESTION 31
The Orange Book describes four hierarchical levels to categorize security systems. Which of the following levels require mandatory protection?

A. A and B.
B. B and C.
C. A, B, and C.
D. B and D.

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal security
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Level B is the lowest level that requires mandatory protection. Level A, being a higher level also requires mandatory protection.

Incorrect Answers:
B: Mandatory protection is not required for level C. Level C is Discretionary protection.
C: Mandatory protection is not required for level C. Level C is Discretionary protection.
D: Mandatory protection is not required for level D. Level D is Minimal security.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-393

QUESTION 32
What mechanism does a system use to compare the security labels of a subject and an object?

A. Validation Module.
B. Reference Monitor.
C. Clearance Check.
D. Security Module.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The reference monitor is an abstract machine that mediates all access subjects have to objects, both to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification. For a system to achieve a higher level of trust, it must require subjects (programs, users, processes) to be fully authorized prior to accessing an object (file, program, resource). A subject must not be allowed to use a requested resource until the subject has proven it has been granted access privileges to use the requested object. The reference monitor is an access control concept, not an actual physical component, which is why it is normally referred to as the “reference monitor concept” or an “abstract machine.”

Incorrect Answers:
A: A Validation Module is not what the system uses to compare the security labels of a subject and an object.
C: A Clearance Check is not what the system uses to compare the security labels of a subject and an object.
D: A Security Module is not what the system uses to compare the security labels of a subject and an object.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 362

QUESTION 33

Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?

A. Degaussing
B. Parity Bit Manipulation
C. Zeroization
D. Buffer overflow

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.
Incorrect Answers:
B: Parity has to do with disk error detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the information that was sent.
C: Zeroization involves overwriting data to sanitize it. There is a drawback to this method. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. Degaussing is more effective than overwriting the sectors.
D: This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.

QUESTION 34
Which of the following is NOT a media viability control used to protect the viability of data storage media?

A. clearing
B. marking
C. handling
D. storage

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Clearing is not an example of a media viability control used to protect the viability of data storage media.
Media viability controls are implemented to preserve the proper working state of the media, particularly to facilitate the timely and accurate restoration of the system after a failure.
Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process: ▪ Marking. All data storage media should be accurately marked or labeled. The labels can be used to identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.

- Handling. Proper handling of the media is important. Some issues with the handling of media include cleanliness of the media and the protection from physical damage to the media during transportation to the archive sites.
- Storage. Storage of the media is very important for both security and environmental reasons. A proper heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust.

Incorrect Answers:
B: Marking is a media viability control used to protect the viability of data storage media.
C: Handling is a media viability control used to protect the viability of data storage media.
D: Storage is a media viability control used to protect the viability of data storage media.
References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p.

324

QUESTION 35
An electrical device (AC or DC) which can generate coercive magnetic force for the purpose of reducing magnetic flux density to zero on storage media or other magnetic media is called:

A. a magnetic field.
B. a degausser.
C. magnetic remanence.
D. magnetic saturation.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

Incorrect Answers:
A: A magnetic field is not the electrical device described in the question.
C: Magnetic remanence is not the electrical device described in the question.
D: Magnetic saturation is not the electrical device described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 1282

QUESTION 36
What is the most secure way to dispose of information on a CD-ROM?

A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The information stored on a CDROM is not in electro-magnetic format, so a degausser would be ineffective.
The only way to dispose of information on a CD-ROM is to physically destroy the CD-ROM.

Incorrect Answers:
A: You cannot sanitize read-only media such as a CDROM.
B: Physical damage is not the MOST secure way to dispose of information on a CD-ROM. Data could still be recovered from the undamaged part of the CD-ROM. Only complete destruction of the CD-ROM will suffice.
C: Degaussing does not work on read-only media such as a CDROM.

QUESTION 37
Which of the following refers to the data left on the media after the media has been erased?

A. remanence

B. recovery
C. sticky bits
D. semi-hidden

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Data Remanence is the problem of residual information remaining on the media after erasure, which may be subject to restoration by another user, thereby resulting in a loss of confidentiality. Diskettes, hard drives, tapes, and any magnetic or writable media are susceptible to data remanence. Retrieving the bits and pieces of data that have not been thoroughly removed from storage media is a common method of computer forensics, and is often used by law enforcement personnel to preserve evidence and to construct a trail of misuse. Anytime a storage medium is reused (and also when it is discarded), there is the potential for the media's information to be retrieved. Methods must be employed to properly destroy the existing data to ensure that no residual data is available to new users. The "Orange Book" standard recommends that magnetic media be formatted seven times before discard or reuse.

Incorrect Answers:
B: Recovery is not the term that refers to the data left on the media after the media has been erased.
C: Sticky bits is not the term that refers to the data left on the media after the media has been erased.
D: Semi-hidden is not the term that refers to the data left on the media after the media has been erased.
References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 477

QUESTION 38
What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?

A. Data fiddling
B. Data diddling
C. Salami techniques
D. Trojan horses

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
Salami techniques: A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. In this case, the employee has been shaving off pennies from multiple accounts in the hope that no one notices. Shaving pennies from an account is the small crime in this example. However, the cumulative effect of the multiple 'small crimes' is that a larger amount of money is stolen in total.

Incorrect Answers:
A: Data fiddling is not a defined attack type. The term could refer to entering incorrect data in a similar way to data diddling. However, it is not the term used to describe a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account.
B: Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20. This is not what is described in the question.
D: A Trojan Horse is a program that is disguised as another program. This is not what is described in the question.

References:
S Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1059

QUESTION 39
Which of the following logical access exposures involvers changing data before, or as it is entered into the computer?

A. Data diddling
B. Salami techniques
C. Trojan horses
D. Viruses

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20.
This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.

Incorrect Answers:

B: Salami techniques: A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. This is not what is described in the question.
C: A Trojan Horse is a program that is disguised as another program. This is not what is described in the question.
D: A Virus is a small application or a string of code that infects applications. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1059

QUESTION 40
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).

There are three general methods of purging media: overwriting, degaussing, and destruction.

There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.

Incorrect Answers:
A: It is not true that clearing completely erases the media or that purging only removes file headers, allowing the recovery of files.
C: Clearing does not involve rewriting the media.
D: It is not true that clearing renders information unrecoverable against a laboratory attack or purging renders information unrecoverable to a keyboard attack.

QUESTION 41
Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

A. Degaussing
B. Overwrite every sector of magnetic media with pattern of 1's and 0's
C. Format magnetic media
D. Delete File allocation table

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Degaussing is the most effective method out of all the provided choices to erase sensitive data on magnetic media.
A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information.
Specialized hardware devices known as degaussers can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degausser is of sufficient strength to meet object reuse requirements when erasing data. If a degausser is used with insufficient coercivity, then a remanence of the data will exist.
Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degaussers can destroy drives. The security professional should exercise caution when recommending or using degaussers on media for reuse.

Incorrect Answers:
B: Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There is a drawback to using overwrite

software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. Degaussing is more effective than overwriting the sectors.
C: Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply removes the pointers to the information.
D: Deleting the File allocation table will not erase all data. The data can be recoverable using software tools.

QUESTION 42
Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

A. SSH (Secure Shell)
B. S/MIME (Secure MIME)
C. SET (Secure Electronic Transaction)
D. SSL (Secure Sockets Layer)

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. SET has been waiting in the wings for full implementation and acceptance as a standard for quite some time. Although SET provides an effective way of transmitting credit card information, businesses and users do not see it as efficient because it requires more parties to coordinate their efforts, more software installation and configuration for each entity involved, and more effort and cost than the widely used SSL method.
SET is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet. The following entities would be involved with a SET transaction, which would require each of them to upgrade their software, and possibly their hardware:
- Issuer (cardholder's bank) The financial institution that provides a credit card to the individual.
- Cardholder The individual authorized to use a credit card.
- Merchant The entity providing goods.
- Acquirer (merchant's bank) The financial institution that processes payment cards. ▪

Payment gateway This processes the merchant payment. It may be an acquirer.

Incorrect Answers:
A: SSH is a network protocol that allows for a secure connection to a remote system. Developed to replace Telnet and other insecure remote shell methods. This is not what is described in the question.
B: S/MIME stands for Secure/Multipurpose Internet Mail Extensions, which outlines how public key cryptography can be used to secure MIME data types. This is not what is described in the question.

D: SSL (Secure Sockets Layer) is most commonly used to Internet connections and e-commerce transactions. It is used instead of SET but is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 856

QUESTION 43
In Mandatory Access Control, sensitivity labels attached to object contain what information?

A. The item's classification
B. The item's classification and category set
C. The item's category
D. The item's need to know

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A sensitivity label is required for every subject and object when using the Mandatory Access Control (MAC) model. The sensitivity label is made up of a classification and different categories.

Incorrect Answers:
A: The item's classification on its own is incorrect. It has to have a category as well.
C: The item's category on its own is incorrect. It has to have a classification as well.
D: Need-to-know rules are applied by the categories section of the label.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 223
http://en.wikipedia.org/wiki/Mandatory_Access_Control

QUESTION 44
Which of the following European Union (EU) principles pertaining to the protection of information on private individuals is incorrect?

A. Data collected by an organization can be used for any purpose and for as long as necessary, as long as it is never communicated outside of the organization by which it was collected.
B. Individuals have the right to correct errors contained in their personal data.
C. Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited.
D. Records kept on an individual should be accurate and up to date.

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
EU's Data Protection Data Integrity states that Data must be relevant and reliable for the purpose it was collected for.

Incorrect Answers:
B: EU's Data Protection Directive includes the access directive which states that individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
C: EU's Data Protection Directive includes the Onward Transfer directive which states that transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
D: EU's Data Protection Directive includes the Data Integrity directive which states that Data must be relevant and reliable for the purpose it was collected for.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1064-1065

QUESTION 45
Who should DECIDE how a company should approach security and what security measures should be implemented?

A. Senior management
B. Data owner
C. Auditor
D. The information security specialist

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Computers and the information processed on them usually have a direct relationship with a company's critical missions and objectives. Because of this level of importance, senior management should make protecting these items a high priority and provide the necessary support, funds, time, and resources to ensure that systems, networks, and information are protected in the most logical and cost-effective manner possible.
For a company's security plan to be successful, it must start at the top level and be useful and functional at every single level within the organization. Senior management needs to define the scope of security and identify and decide what must be protected and to what extent.

Incorrect Answers:

B: The data owner can grant access to the data. However, the data owner should not decide how a company should approach security and what security measures should be implemented.
C: Systems Auditors ensure the appropriate security controls are in place. However, they should not decide how a company should approach security and what security measures should be implemented.
D: The information security specialist may be the ones who implement the security measures. However, they should not decide how a company should approach security and what security measures should be implemented.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 101

QUESTION 46
The Telecommunications Security Domain of information security is also concerned with the prevention and detection of the misuse or abuse of systems, which poses a threat to the tenets of:

A. Confidentiality, Integrity, and Entity (C.I.E.).
B. Confidentiality, Integrity, and Authenticity (C.I.A.).
C. Confidentiality, Integrity, and Availability (C.I.A.).
D. Confidentiality, Integrity, and Liability (C.I.L.).

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Fundamental Principles of Security which are to provide confidentiality, availability, and integrity, and Confidentiality (the CIA triad).

Incorrect Answers:
A: The three tenets do not include Entity.
B: The three tenets do not include Authenticity.
D: The three tenets do not include Liability.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 22

QUESTION 47
Controlling access to information systems and associated networks is necessary for the preservation of their:

A. Authenticity, confidentiality and availability

B. Confidentiality, integrity, and availability.
C. Integrity and availability.
D. Authenticity, confidentiality, integrity and availability.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Information security is made up of the following main attributes:
- Availability - Prevention of loss of, or loss of access to, data and resources
- Integrity - Prevention of unauthorized modification of data and resources
- Confidentiality - Prevention of unauthorized disclosure of data and resources

Incorrect Answers:
A: Authenticity is an attribute that stems from the three main attributes.
C: Information security is made up of three main attributes, which includes confidentiality.
D: Authenticity is an attribute that stems from the three main attributes.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 298, 299

QUESTION 48
What security model is dependent on security labels?

A. Discretionary access control
B. Label-based access control
C. Mandatory access control
D. Non-discretionary access control

Correct Answer: C
Section: Asset Security
Explanation
Explanation/Reference:
Explanation:

Mandatory Access Control begins with security labels assigned to all resource objects on the system. These security labels contain two pieces of information - a classification (top secret, confidential etc.) and a category (which is essentially an indication of the management level, department or project to which the object is available).
Similarly, each user account on the system also has classification and category properties from the same set of properties applied to the resource objects. When a user attempts to access a resource under Mandatory Access Control the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's credentials match the MAC security label properties of the object access is allowed. It is important to note that both the classification and categories must match. A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object.

Incorrect Answers:
A: Discretionary access control is not dependent on security labels.
B: Label-based access control is not one of the defined access control types.
D: Non-discretionary access control is not dependent on security labels.

References:
http://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control

QUESTION 49
At which temperature does damage start occurring to magnetic media?

A. 100 degrees Fahrenheit or 37.7 degrees Celsius
B. 125 degrees Fahrenheit or 51.66 degrees Celsius
C. 150 degrees Fahrenheit or 65.5 degrees Celsius
D. 175 degrees Fahrenheit or 79.4 degrees Celsius

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Maintaining appropriate temperature and humidity is important in any facility, especially facilities with computer systems. Improper levels of either can cause damage to computers and electrical devices.
Lower temperatures can cause mechanisms to slow or stop, and higher temperatures can cause devices to use too much fan power and eventually shut down. Damage can start to occur on magnetic media at 100 degrees Fahrenheit or 37'7º Celsius.

Incorrect Answers:
B: Damage can start to occur on magnetic media at 100 degrees Fahrenheit, not 125 degrees Fahrenheit. Therefore, this answer is incorrect.

C: Damage can start to occur on magnetic media at 100 degrees Fahrenheit, not 150 degrees Fahrenheit. Therefore, this answer is incorrect.
D: Damage can start to occur on magnetic media at 100 degrees Fahrenheit, not 175 degrees Fahrenheit. Damage can start to occur in computer systems and peripheral devices at 175 degrees Fahrenheit. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 466

QUESTION 50
Which of the following access control models requires defining classification for objects?

A. Role-based access control
B. Discretionary access control
C. Identity-based access control
D. Mandatory access control

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Mandatory access control (MAC) is an access policy that restricts access to objects based on the security clearance of a subject and the classification of an object.

Incorrect Answers:
A: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.
B: Access in a DAC model is restricted based on the authorization granted to the users.
C: Identity-based access control is a type of DAC system that allows or prevents access based on the identity of the subject.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 51
In which of the following security models is the subject's clearance compared to the object's classification such that specific rules can be applied to control how the subject-to-object interactions take place?

A. Bell-LaPadula model
B. Biba model
C. Access Matrix model

D. Take-Grant model
Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels. The level at which information is classified determines the handling procedures that should be used. The BellLaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. **The subject's clearance is compared to the object's classification and then specific rules are applied to control how subjectto-object interactions can take place.**
This model uses subjects, objects, access operations (read, write, and read/write), and security levels. Subjects and objects can reside at different security levels and will have relationships and rules dictating the acceptable activities between them.

Incorrect Answers:
B: The Biba Model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. This is not what is described in the question.
C: An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. This is not what is described in the question.
D: The take-grant protection model is used to establish or disprove the safety of a given computer system that follows specific rules. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 229

QUESTION 52
Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

A. B
B. A
C. C
D. D

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal protection
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Level B: Mandatory Protection: Mandatory access control is enforced by the use of security labels. The architecture is based on the Bell-LaPadula security model, and evidence of reference monitor enforcement must be available.

Incorrect Answers:
B: Level A is defined as verified protection, not mandatory protection.
C: Level C is defined as discretionary protection, not mandatory protection.
D: Level D is defined as minimal security, not mandatory protection.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392, 395

QUESTION 53
Which of the following classes is defined in the TCSEC (Orange Book) as discretionary protection?

A. C
B. B
C. A
D. D

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal protection
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Level C: Discretionary Protection: The C rating category has two individual assurance ratings within it. The higher the number of the assurance rating, the greater the protection.

Incorrect Answers:
B: Level B is defined as mandatory protection, not discretionary protection.
C: Level A is defined as verified protection, not discretionary protection.
D: Level D is defined as minimal security, not discretionary protection.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392, 394

QUESTION 54
Which of the following division is defined in the TCSEC (Orange Book) as minimal protection?

A. Division D
B. Division C
C. Division B
D. Division A

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal protection
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Division D: Minimal Protection: There is only one class in Division D. It is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions.

Incorrect Answers:
B: Level C is defined as discretionary protection, not minimal protection.
C: Level B is defined as mandatory protection, not minimal protection.
D: Level A is defined as verified protection, not mandatory minimal.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392, 395

QUESTION 55
Which of the following establishes the minimal national standards for certifying and accrediting national security systems?

A. NIACAP
B. DIACAP
C. HIPAA
D. TCSEC

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
National Information Assurance Certification and Accreditation Process (NIACAP), establishes the minimum national standards for certifying and accrediting national security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site. This process focuses on an enterprise-wide view of the information system (IS) in relation to the organization's mission and the IS business case.

Incorrect Answers:
B: The DoD Information Assurance Certification and Accreditation Process (DIACAP) is a United States Department of Defense (DoD) process that means to ensure that companies and organizations apply risk management to information systems (IS). This is not what is described in the question.
C: HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs. This is not what is described in the question.
D: Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. This is not what is described in the question.

References:
http://infohost.nmt.edu/~sfs/Regs/nstissi_1000.pdf

QUESTION 56
Which of the following places the Orange Book classifications in order from MOST secure to LEAST secure?

A. A, B, C, D
B. D, C, B, A

C. D, B, A, C

D. C, D, B, A

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal security
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Incorrect Answers:
B: Classification A represents the highest level of assurance, and D represents the lowest level of assurance.
C: Classification A represents the highest level of assurance, and D represents the lowest level of assurance.
D: Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-393

QUESTION 57
What would BEST define a covert channel?

A. An undocumented backdoor that has been left by a programmer in an operating system
B. An open system port that should be closed.
C. A communication channel that allows transfer of information in a manner that violates the system's security policy.
D. A Trojan horse.

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system's security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:

- Improper oversight in the development of the product
- Improper implementation of access controls within the software
- Existence of a shared resource between the two entities which are not properly controlled

Incorrect Answers:
A: An undocumented backdoor that has been left by a programmer in an operating system could be used in a covert channel. However, this is not the BEST definition of a covert channel.
B: An open system port that should be closed could be used in a covert channel. However, an open port is not the definition of a covert channel.
D: A Trojan horse could be used in a covert channel. However, a Trojan horse is not the definition of a covert channel.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 378-379

QUESTION 58
Which of the following Orange Book ratings represents the highest level of trust?

A. B1
B. B2
C. F6
D. C2

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal security
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.
Each division can have one or more numbered classes with a corresponding set of requirements that must be met for a system to achieve that particular rating.

The classes with higher numbers offer a greater degree of trust and assurance. So B2 would offer more assurance than B1, and C2 would offer more assurance than C1.

Incorrect Answers:
A: B1 has a lower level of trust than B2.
C: F6 is not a valid rating.
D: Division C has a lower level of trust than division B.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-393

QUESTION 59
What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

A. A
B. D
C. E
D. F

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protection
D. Minimal security

Classification A represents the highest level of assurance, and D represents the lowest level of assurance. Each division can have one or more numbered classes with a corresponding set of requirements that must be met for a system to achieve that particular rating.
There is only one class in Division D. It is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions.

Incorrect Answers:
A: Division A is the highest level.

C: The lowest division/level (reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions) is D, not E.
D: The lowest division/level (reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions) is D, not F.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-393

QUESTION 60
Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D
B. C
C. B
D. A

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protection
D. Minimal security

C1: Discretionary Security Protection: Discretionary access control is based on individuals and/or groups. It requires a separation of users and information, and identification and authentication of individual entities. Some type of access control is necessary so users can ensure their data will not be accessed and corrupted by others. The system architecture must supply a protected execution domain so privileged system processes are not adversely affected by lower-privileged processes. There must be specific ways of validating the system's operational integrity. The documentation requirements include design documentation, which shows that the system was built to include protection mechanisms, test documentation (test plan and results), a facility manual (so companies know how to install and configure the system correctly), and user manuals.

Incorrect Answers:
A: Division C, not D deals with discretionary protection.
C: Division C, not B deals with discretionary protection.
D: Division C, not A deals with discretionary protection.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-394

QUESTION 61

Which of the following computer crime is MORE often associated with INSIDERS?

A. IP spoofing
B. Password sniffing
C. Data diddling
D. Denial of service (DoS)

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20.
This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.

Incorrect Answers:
A: IP Spoofing attacks are more commonly performed by outsiders.
B: Password sniffing can be performed by insiders or outsiders. However, Data Diddling is MORE commonly performed by insiders.
D: Most Denial of service attacks occur over the internet and are performed by outsiders.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1059

QUESTION 62

Which of the following groups represents the leading source of computer crime losses?

A. Hackers
B. Industrial saboteurs
C. Foreign intelligence officers
D. Employees

Correct Answer: D
Section: Asset Security
Explanation
Explanation/Reference:
Explanation:
Employees represent the leading source of computer crime losses. This can be through hardware theft, data theft, physical damage and interruptions to services. Laptop theft is increasing at incredible rates each year. They have been stolen for years, but in the past they were stolen mainly to sell the hardware. Now laptops are also being stolen to gain sensitive data for identity theft crimes. Since employees use laptops as they travel, they may have extremely sensitive company or customer data on their systems that can easily fall into the wrong hands.

Incorrect Answers:
A: Losses caused by hackers can be high. However, this is rare in comparison to losses caused by employees.
B: Losses caused by industrial saboteurs can be high. However, this is very rare in comparison to losses caused by employees.
C: Foreign intelligence officers are not a cause of computer crime losses.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 457

QUESTION 63
Which of the following term BEST describes a weakness that could potentially be exploited?

A. Vulnerability
B. Risk
C. Threat
D. Target of evaluation (TOE)

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A vulnerability is the absence of a countermeasure or a weakness in an in-place countermeasure, and can therefore be exploited.

Incorrect Answers:
B: A risk is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact.
C: A threat is any potential danger that is associated with the exploitation of a vulnerability.
D: Target Of Evaluation (TOE) refers to the product or system that is the subject of the evaluation.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 26
https://en.wikipedia.org/wiki/Common_Criteria

QUESTION 64
Which of the following BEST describes an exploit?

A. An intentional hidden message or feature in an object such as a piece of software or a movie.
B. A chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software.
C. An anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer.
D. A condition where a program (either an application or part of the operating system) stops performing its expected function and also stops responding to other parts of the system.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
An exploit refers to a piece of software or data, or a sequence of commands that takes advantage of a bug or vulnerability with the aim of causing unplanned or unexpected behavior to take place on computerized hardware, or its software.

Incorrect Answers:
A: An intentional hidden message, in-joke, or feature in a work such as a computer program, web page, video game, movie, book, or crossword is known as a virtual Easter egg.
C: The anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer is known as buffer overflow.
D: In computing, a condition where a program (either an application or part of the operating system) stops performing its expected function and also stops responding to other parts of the system is known as a crash.

References: https://en.wikipedia.org/wiki/Exploit_%28computer_security%29 https://www.quora.com/topic/Easter-Eggs-media https://en.wikipedia.org/wiki/Buffer_overflow http://www.article-buzz.com/Article/Avoiding-Data-Loss---A-Guide-To-The-Best-Online-Data-Storage-Websites/328757#.Vjc757crKHu

QUESTION 65
Virus scanning and content inspection of S/MIME encrypted e-mail without doing any further processing is:

A. Not possible
B. Only possible with key recovery scheme of all user keys

C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
E-mail encryption solutions such as S/MIME have been available for a long time. These encryption solutions have seen varying degrees of adoption in organizations of different types. However, such solutions present some challenges:
Inability to apply messaging policies: Organizations also face compliance requirements that require inspection of messaging content to make sure it adheres to messaging policies. However, messages encrypted with most client-based encryption solutions, including S/MIME, prevent content inspection on the server. Without content inspection, an organization can't validate that all messages sent or received by its users comply with messaging policies.
Decreased security: Antivirus software is unable to scan encrypted message content, further exposing an organization to risk from malicious content such as viruses and worms. Encrypted messages are generally considered to be trusted by most users, thereby increasing the likelihood of a virus spreading throughout your organization.

Incorrect Answers:
B: Virus scanning and content inspection of S/MIME encrypted e-mail is not possible even with a key recovery scheme of all user keys.
C: Virus scanning and content inspection of S/MIME encrypted e-mail is not possible even if X509 Version 3 certificates are used.
D: Using "brute force" decryption on S/MIME encrypted e-mail for the purpose of virus scanning and content inspection is not practical and unlikely to be successful.

References: https://technet.microsoft.com/en-us/library/dd638122(v=exchg.150).aspx

QUESTION 66
What can be defined as secret communications where the very existence of the message is hidden?

A. Clustering
B. Steganography
C. Cryptology
D. Vernam cipher

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
Steganography is a method of hiding data in another media type so the very existence of the data is concealed.
Only the sender and receiver are supposed to be able to see the message because it is secretly hidden in a graphic, wave file, document, or other type of media.
The message is not encrypted, just hidden. Encrypted messages can draw attention because it tells the bad guy, “This is something sensitive.” A message hidden in a picture of your grandmother would not attract this type of attention, even though the same secret message can be embedded into this image. Steganography is a type of security through obscurity.

Incorrect Answers:
A: Clustering describes multiple instances of a component working together as a single unit. This is not what is described in the question.
C: Cryptology is the study of cryptography and cryptanalysis. This is not what is described in the question.
D: Vernam cipher is another name for one-time pad because one-time pad was invented by Gilbert Vernam. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 774-775

QUESTION 67
Which of the following terms can be described as the process to conceal data into another file or media in a practice known as security through obscurity?

A. Steganography
B. ADS - Alternate Data Streams
C. Encryption
D. NTFS ADS

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Steganography allows you to hide data in another media type, concealing the very existence of the data.

Incorrect Answers:
B, D: Alternate data stream (ADS) is a feature of Windows New Technology File System (NTFS) that includes metadata for locating a specific file by author or title.
C: Encryption is a method of transforming readable data into a form that appears to be random and unreadable.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 774

http://searchsecurity.techtarget.com/definition/alternate-data-stream

QUESTION 68
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

A. Steganography
B. Digital watermarking
C. Digital enveloping
D. Digital signature

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Digital watermarking is defined as “Computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data -- text, graphics, images, video, or audio -- and for detecting or extracting the marks later.”
A "digital watermark", i.e., the set of embedded bits, is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. Depending on the particular technique that is used, digital watermarking can assist in proving ownership, controlling duplication, tracing distribution, ensuring data integrity, and performing other functions to protect intellectual property rights.

Incorrect Answers:
A: Steganography is a method of hiding data in another media type so the very existence of the data is concealed. Digital Watermarking is considered to be a type of steganography. However, steganography is not what is described in the question.
C: A digital envelope is another term used to describe hybrid cryptography where a message is encrypted with a symmetric key and the symmetric key is encrypted with an asymmetric key. This is not what is described in the question.
D: A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. This is not what is described in the question.

References:
http://tools.ietf.org/html/rfc4949

QUESTION 69
What is Dumpster Diving?

A. Going through dust bin
B. Running through another person's garbage for discarded document, information and other various items that could be used against that person or company
C. Performing media analysis

D. performing forensics on the deleted items

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Dumpster diving refers to the concept of rummaging through a company or individual's garbage for discarded documents, information, and other precious items that could then be used in an attack against that company or person.

Incorrect Answers:
A: Dumpster Diving is more specific than going through dust bins.
C: Dumpster Diving does not refer to media analysis.
D: Dumpster Diving does not refer to forensics on deleted items.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1060

QUESTION 70
The control of communications test equipment should be clearly addressed by security policy for which of the following reasons?

A. Test equipment is easily damaged.
B. Test equipment can be used to browse information passing on a network.
C. Test equipment is difficult to replace if lost or stolen.
D. Test equipment must always be available for the maintenance personnel.

Correct Answer: B

Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A Protocol Analyzer (also known as a packet sniffer) is a useful tool for testing or troubleshooting network communications.
A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing packets sent from a computer system is known as packet sniffing.
The ability to browse information passing on a network is a security risk which means access to a protocol analyzer should be carefully managed and therefore addressed by security policy.

Incorrect Answers:
A: Damage to test equipment is not a 'security' risk so does not need to be addressed by security policy.
C: Test equipment is generally not difficult to replace if lost or stolen. Even if it was, that would not constitute a 'security' risk so it would not need to be addressed by security policy.
D: The need for test equipment to always be available for the maintenance personnel would not constitute a 'security' risk so it would not need to be addressed by security policy.

QUESTION 71
Which of the following would BEST be defined as an absence or weakness of safeguard that could be exploited?

A. A threat.
B. A vulnerability.
C. A risk.
D. An exposure.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A vulnerability is defined as "the absence or weakness of a safeguard that could be exploited".
A vulnerability is a lack of a countermeasure or a weakness in a countermeasure that is in place. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 26

QUESTION 72
Which of the following could be BEST defined as the likelihood of a threat agent taking advantage of a vulnerability?

A. A risk.
B. A residual risk.
C. An exposure.
D. A countermeasure.

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A risk is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact. If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method. If users are not educated on processes and procedures, there is a higher likelihood that an employee will make an unintentional mistake that may destroy data. If an intrusion detection system (IDS) is not implemented on a network, there is a higher likelihood an attack will go unnoticed until it is too late. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.

Incorrect Answers:
B: Residual risk is the risk that remains after countermeasures have been implemented.
C: An exposure is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages.
D: A countermeasure is a step taken to mitigate a risk.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 26

QUESTION 73
Which of the following is responsible for MOST of the security issues?

A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure

Correct Answer: C

Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Personnel represent the leading source of computer crime losses. This can be through hardware theft, data theft, physical damage and interruptions to services. Laptop theft is increasing at incredible rates each year. They have been stolen for years, but in the past they were stolen mainly to sell the hardware. Now laptops are also being stolen to gain sensitive data for identity theft crimes. Since employees use laptops as they travel, they may have extremely sensitive company or customer data on their systems that can easily fall into the wrong hands.

Incorrect Answers:
A: Losses caused by industrial outside espionage can be high. However, this is very rare in comparison to losses caused by personnel.
B: Losses caused by hackers can be high. However, this is rare in comparison to losses caused by personnel.
D: Equipment failure can be a cause of security issues. However, security issues caused by personnel are more common.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 457

QUESTION 74
Passwords can be required to change monthly, quarterly, or at other intervals:

A. depending on the criticality of the information needing protection.
B. depending on the criticality of the information needing protection and the password's frequency of use.
C. depending on the password's frequency of use.
D. not depending on the criticality of the information needing protection but depending on the password's frequency of use.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A password that is the same for each log-on is called a static password. A password that changes with each log-on is termed a dynamic password. The changing of passwords can also fall between these two extremes. Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password’s frequency of use. Obviously, the more times a password is used, the more chance there is of it being compromised.

Incorrect Answers:
A: This answer is not complete. Passwords can also be required to change depending on the password's frequency of use.

C: This answer is not complete. Passwords can also be required to change depending on the criticality of the information needing protection.
D: Passwords CAN be required to change depending on the criticality of the information needing protection.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 57

QUESTION 75
Computer security should be first and foremost which of the following?

A. Cover all identified risks
B. Be cost-effective.
C. Be examined in both monetary and non-monetary terms.
D. Be proportionate to the value of IT systems.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Each organization is different in its size, security posture, threat profile, and security budget. One organization may have one individual responsible for information risk management (IRM) or a team that works in a coordinated manner. The overall goal of the team is to ensure the company is protected in the most cost-effective manner.

Incorrect Answers:
A: Not all identified risks are mitigated. Some risks are accepted.
C: It is not true that computer security should be first and foremost examined in both monetary and non-monetary terms.
D: It is not true that computer security should be first and foremost proportionate to the value of IT systems. The value of IT systems does not necessarily mean that more or less security is required.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 87

QUESTION 76
IT security measures should:

A. be complex.
B. be tailored to meet organizational security goals.
C. make sure that every asset of the organization is well protected.

D. not be developed in a layered fashion.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The National Institute of Standards and Technology (NIST) defines 33 IT Security principles.
Principle 8 states:
"Implement tailored system security measures to meet organizational security goals."
In general, IT security measures are tailored according to an organization's unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used – implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.

Incorrect Answers:
A: According to the NIST IT security principles, IT security measures should strive for simplicity not be complex.
C: According to the NIST IT security principles, you should not implement unnecessary security mechanisms. Protecting 'every' asset may be unnecessary.
D: According to the NIST IT security principles, IT security measures should be developed in a layered fashion.
References: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf, p.10

QUESTION 77
The absence of a safeguard, or a weakness in a system that may possibly be exploited is called a(n)?

A. Threat
B. Exposure
C. Vulnerability
D. Risk

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A vulnerability is defined as "the absence or weakness of a safeguard that could be exploited".

A vulnerability is a lack of a countermeasure or a weakness in a countermeasure that is in place. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

Incorrect Answers:
A: A threat is any potential danger that is associated with the exploitation of a vulnerability.
B: An exposure is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages.
D: A risk is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 26

QUESTION 78
What can be defined as an event that could cause harm to the information systems?

A. A risk
B. A threat
C. A vulnerability
D. A weakness

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A threat is any potential danger that is associated with the exploitation of a vulnerability. The threat is that someone, or something, will identify a specific vulnerability and use it against the company or individual. The entity that takes advantage of a vulnerability is referred to as a threat agent. A threat agent could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy, a tornado wiping out a facility, or an employee making an unintentional mistake that could expose confidential information.

Incorrect Answers:
A: A risk is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact.
C: A vulnerability is the absence or weakness of a safeguard that could be exploited.
D: A weakness is the state of something being weak. For example, a weak security measure would be a vulnerability. A weakness is not what is described in this question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 26

QUESTION 79
Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?

A. Business and functional managers
B. IT Security practitioners
C. System and information owners
D. Chief information officer

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Both the system owner and the information owner (data owner) are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data.
The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner. The data owner (information owner) is usually a member of management who is in charge of a specific business unit, and who is ultimately responsible for the protection and use of a specific subset of information. The data owner has due care responsibilities and thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data she is responsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers.

Incorrect Answers:
A: Business and functional managers are not responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data.
B: IT Security practitioners implement the security controls. However, they are not ultimately responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data.
D: The Chief Information Officer (CIO) is responsible for the strategic use and management of information systems and technology within the organization. The CIO is not responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 121

QUESTION 80

Which of the following BEST defines add-on security?

A. Physical security complementing logical security measures.
B. Protection mechanisms implemented as an integral part of an information system.
C. Layer security.
D. Protection mechanisms implemented after an information system has become operational.

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Add-on security is defined as “Security protection mechanisms that are hardware or software retrofitted to a system to increase that system’s protection level.”
Incorrect Answers:
A: Add-on security can be physical security (hardware) but it is often software as well.
B: An add-on is something ‘added’ to an existing system; it is not an integral part of a system.
C: Add-on security can be a layer of security. However, layered security does not refer specifically to security add-ons.

QUESTION 81
Which of the following is BEST practice to employ in order to reduce the risk of collusion?

A. Least Privilege
B. Job Rotation
C. Separation of Duties D. Mandatory Vacations

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The objective of separation of duties is to ensure that one person acting alone cannot compromise the company’s security in any way. High-risk activities should be broken up into different parts and distributed to different individuals or departments. That way, the company does not need to put a dangerously high level of trust in certain individuals. For fraud to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity Job rotation in the workplace is a system where employees work at several jobs in a business, performing each job for a relatively short period of time. Job rotation in the workplace is a system where employees work at several jobs in a business, performing each job for a relatively short period of time. By moving people willing to collude to commit fraud, we can reduce the risk of collusion.

Incorrect Answers:
A: Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more. It is not the best control for reducing collusion.
C: Separation of Duties prevents one person being able to commit fraud. With separation of duties, collusion between two or more people would be required to commit the fraud. However, separation of duties does not prevent the collusion.
D: Mandatory vacations are a way of detecting fraud. If a fraudulent activity stops while an employee is on vacation, it is easy to determine who was committing the fraud. Mandatory vacations do not prevent the collusion.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1235-1236

QUESTION 82
What are the four domains that make up CobiT?

A. Plan and Organize, Maintain and Implement, Deliver and Support, and Monitor and Evaluate
B. Plan and Organize, Acquire and Implement, Support and Purchase, and Monitor and Evaluate
C. Acquire and Implement, Deliver and Support, Monitor, and Evaluate
D. Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The Control Objectives for Information and related Technology (CobiT) is a framework and set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs. CobiT is broken down into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

Incorrect Answers:
A: Maintain and Implement is not one of the four domains; it should be Acquire and Implement.
B: Support and Purchase is not one of the four domains; it should be Deliver and Support.
C: This answer is missing the first domain, Plan and Organize.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 55

QUESTION 83

CobiT was developed from the COSO framework. Which of the choices below best describe the COSO's main objectives and purpose?

A. COSO main purpose is to help ensure fraudulent financial reporting cannot take place in an organization
B. COSO main purpose is to define a sound risk management approach within financial companies.
C. COSO addresses corporate culture and policy development.
D. COSO is risk management system used for the protection of federal systems.

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
COSO is a model for corporate governance, and CobiT is a model for IT governance. COSO deals more at the strategic level, while CobiT focuses more at the operational level. You can think of CobiT as a way to meet many of the COSO objectives, but only from the IT perspective. COSO deals with non-IT items also, as in company culture, financial accounting principles, board of director responsibility, and internal communication structures. COSO was formed to provide sponsorship for the National Commission on Fraudulent Financial Reporting, an organization that studies deceptive financial reports and what elements lead to them.
There have been laws in place since the 1970s that basically state that it was illegal for a corporation to cook its books (manipulate its revenue and earnings reports), but it took the Sarbanes–Oxley Act (SOX) of 2002 to really put teeth into those existing laws. SOX is a U.S. federal law that, among other things, could send executives to jail if it was discovered that their company was submitting fraudulent accounting findings to the Security Exchange Commission (SEC). SOX is based upon the COSO model, so for a corporation to be compliant with SOX, it has to follow the COSO model. Companies commonly implement ISO/IEC 27000 standards and CobiT to help construct and maintain their internal COSO structure.

Incorrect Answers:
B: It is not the main purpose of COSO to define a sound risk management approach within financial companies.
C: It is not the main purpose of COSO to address corporate culture and policy development.
D: COSO is not a risk management system used for the protection of federal systems.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 59

QUESTION 84
What are the three MOST important functions that Digital Signatures perform?

A. Integrity, Confidentiality and Authorization
B. Integrity, Authentication and Nonrepudiation
C. Authorization, Authentication and Nonrepudiation

D. Authorization, Detection and Accountability

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Digital Signatures can be used to provide Integrity, Authentication and Nonrepudiation.

A digital signature is a hash value that has been encrypted with the sender's private key.
If Kevin wants to ensure that the message he sends to Maureen is not modified and he wants her to be sure it came only from him, he can digitally sign the message. This means that a one-way hashing function would be run on the message, and then Kevin would encrypt that hash value with his private key. When Maureen receives the message, she will perform the hashing function on the message and come up with her own hash value. Then she will decrypt the sent hash value (digital signature) with Kevin's public key. She then compares the two values, and if they are the same, she can be sure the message was not altered during transmission. She is also sure the message came from Kevin because the value was encrypted with his private key. The hashing function ensures the integrity of the message, and the signing of the hash value provides authentication and nonrepudiation.

Incorrect Answers:
A: Digital signatures do not provide Confidentiality or Authorization.
C: Digital signatures do not provide Authorization.
D: Digital signatures do not provide Authorization, Detection or Accountability.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 829

QUESTION 85
Which of the following results in the most devastating business interruptions?
A. Loss of Hardware/Software
B. Loss of Data
C. Loss of Communication Links
D. Loss of Applications

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

Data loss often lead to business failure. Data loss has the most negative impact on business functions.

Incorrect Answers:
A: Software can be reinstalled and hardware can replaced, and are therefore less critical compared to loss of data.
C: Communication links can quite easily put back again, compared to loss of data.
D: Loss of applications is Critical as they can be reinstalled.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 957

QUESTION 86
Which one of the following is used to provide authentication and confidentiality for e-mail messages?

A. Digital signature
B. PGP
C. IPSEC AH
D. MD4

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Incorrect Answers:
A: Digital signature is used only to ensure the origin, but cannot do any authentication.
C: IPSec can provide encryption and authentication, but work on packets not on email messages.
D: MD4 is an algorithm used to verify data integrity, but it cannot be used to provide authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 850-851

QUESTION 87
Which of the following access control models is based on sensitivity labels?

A. Discretionary access control

B. Mandatory access control
C. Rule-based access control
D. Role-based access control

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Mandatory Access control is considered nondiscretionary and is based on a security label system

Incorrect Answers:
A: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
C: Rule-based access control is considered nondiscretionary because the users cannot make access decisions based upon their own discretion.
D: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 88
Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?

A. Discretionary Access Control
B. Mandatory Access Control
C. Sensitive Access Control
D. Role-based Access Control
Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.

Incorrect Answers:

B: Mandatory Access control is considered nondiscretionary and is based on a security label system
C: Sensitive access control is not a valid access control.
D: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 89
Which of the following countermeasures would be the most appropriate to prevent possible intrusion or damage from wardialing attacks?

A. Monitoring and auditing for such activity
B. Require user authentication
C. Making sure only necessary phone numbers are made public
D. Using completely different numbers for voice and data accesses

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers - malicious hackers who specialize in computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network.
To prevent possible intrusion or damage from wardialing attacks, you should configure the system to require authentication before a network connection can be established. This will ensure that an attacker cannot gain access to the network without knowing a username and password.

Incorrect Answers:
A: Monitoring wardialing attacks would not prevent an attacker gaining access to the network. It would just tell you that at attack has happened.
C: Making sure only necessary phone numbers are made public will not protect against intrusion. An attacker would still be able to gain access through one of the 'necessary' phone numbers.
D: Using completely different numbers for voice and data accesses will not protect against intrusion. An attacker would still be able to gain access through one of the data access phone numbers.

References:
http://en.wikipedia.org/wiki/War_dialing

QUESTION 90
Which of the following access control models introduces user security clearance and data classification?

A. Role-based access control
B. Discretionary access control
C. Non-discretionary access control
D. Mandatory access control

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Mandatory access control (MAC) is an access policy that restricts access to objects based on the security clearance of a subject and the classification of an object.

Incorrect Answers:
A: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.
B: Access in a DAC model is restricted based on the authorization granted to the users.
C: Non-discretionary access control is when the system administrator or a single management body within an organization centrally controls access to all resources for everybody on a network.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228
http://www.answers.com/Q/What_is_Non_discretionary_access_control

QUESTION 91
Kerberos can prevent which one of the following attacks?

A. Tunneling attack.
B. Playback (replay) attack.
C. Destructive attack.
D. Process attack.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
In a Kerberos implementation that is configured to use an authenticator, the user sends to the server her identification information, a timestamp, as well as sequence number encrypted with the session key that they share. The server then decrypts this information and compares it with the identification data the KDC sent to it regarding this requesting user. The server will allow the user access if the data is the same. The timestamp is used to help fight against replay attacks.

Incorrect Answers:
A: Tunneling attack is not a valid type of attack with regards to Kerberos.
C: Destructive attack is not a valid type of attack with regards to Kerberos.
D: Process attack is not a valid type of attack with regards to Kerberos.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 212

QUESTION 92
Which of the following attacks could capture network user passwords?

A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Password sniffing sniffs network traffic with the hope of capturing passwords being sent between computers.
Incorrect Answers:
A: Data diddling refers to the alteration of existing data.
C: Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.
D: Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 599, 1059, 1060

QUESTION 93
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):

A. active attack.
B. outside attack.
C. inside attack.
D. passive attack.

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
An attack by an authorized user is known as an inside attack.
An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access.
Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.
An insider attack is also known as an insider threat.

Incorrect Answers:
A: In an active attack, the attacker attempts to make changes to data on the target or data as it is transmitted to the target. An attack by an authorized user could be an active type of attack but it is not known as an active attack. B: An attack by an authorized user is not known as an outside attack.
D: In a passive attack, the attacker attempts to learn information but does not affect resources. An attack by an authorized user could be passive in nature but it is not known as a passive attack.

References: https://www.techopedia.com/definition/26217/insider-attack

QUESTION 94
MOST access violations are:

A. Accidental
B. Caused by internal hackers C. Caused by external hackers
D. Related to Internet

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
In security circles, people are often the weakest link. Either accidentally through mistakes or lack of training, or intentionally through fraud and malicious intent, personnel cause more serious and hard-to-detect security issues than hacker attacks, outside espionage, or equipment failure.
A common accidental access violation is a user discovering a feature of an application that they should not be accessing.

Incorrect Answers:
B: Most access violations are not caused by internal hackers.
C: Most access violations are not caused by external hackers.
D: Most access violations are not related to Internet.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 129

QUESTION 95
Which of the following tools is less likely to be used by a hacker?

A. l0phtcrack
B. Tripwire
C. OphCrack
D. John the Ripper

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Tripwire is a tool that detects when files have been altered by regularly recalculating hashes of them and storing the hashes in a secure location. The product triggers when changes to the files have been detected. By using cryptographic hashes, tripwire is often able to detect subtle changes. Contrast: The simplistic form of tripwire is to check file size and last modification time. l0phtcrack, OphCrack and John the Ripper are password cracking tools and are therefore more likely to be used by hackers than Tripwire.
Incorrect Answers:
A: l0phtcrack is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, hybrid attacks, and rainbow tables. It is more likely to be used by a hacker than Tripwire.
C: Ophcrack is a free Windows password cracker based on rainbow tables. It is more likely to be used by a hacker than Tripwire.
D: John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS. It is more likely to be used by a hacker than Tripwire.

References:

http://linux.about.com/cs/linux101/g/tripwire.htm

QUESTION 96
What refers to legitimate users accessing networked services that would normally be restricted to them?

A. Spoofing
B. Piggybacking
C. Eavesdropping
D. Logon abuse

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Logon abuse refers to legitimate users accessing networked services that would normally be restricted to them. Unlike network intrusion, this type of abuse focuses primarily on those users who may be internal to the network, legitimate users of a different system, or users who have a lower security classification.

Incorrect Answers:
A: Spoofing refers to an attacker deliberately inducing a user (subject) or device (object) into taking an incorrect action by giving it incorrect information. This is not what is described in the question.
B: Piggy-backing refers to an attacker gaining unauthorized access to a system by using a legitimate user's connection. A user leaves a session open or incorrectly logs off, enabling an attacker to resume the session. This is not what is described in the question.
C: Eavesdropping is the unauthorized interception of network traffic. This is not what is described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 173

QUESTION 97
This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill. What BEST describes this scenario?
A. Excessive Rights
B. Excessive Access
C. Excessive Permissions
D. Excessive Privileges

Correct Answer: D

Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Privilege is a term used to describe what a user can do on a computer or system. It covers rights, access and permissions. A user who has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill is said to have 'excessive privileges'.

Incorrect Answers:
A: Rights are just one aspect of what a user can do with a computer or system. Access and permissions are other aspects. Privileges cover all three.
B: Access is just one aspect of what a user can do with a computer or system. Rights and permissions are other aspects. Privileges cover all three.
C: Permissions are just one aspect of what a user can do with a computer or system. Access and rights are other aspects. Privileges cover all three.

QUESTION 98
Which answer BEST describes information access permissions where, unless the user is specifically given access to certain data they are denied any access by default?

A. Implicit Deny
B. Explicit Deny
C. Implied Permissions
D. Explicit Permit

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Implicit Deny means that a user is denied access by default. To be given access, the user must (explicitly) be permitted access to the resource.

Incorrect Answers:
B: Explicit Deny means the user has been denied access to the data. It does not mean the user is denied by default.
C: Implied Permissions does not describe information access permissions where, unless the user is specifically given access to certain data they are denied any access by default.
D: Explicit Permit means that a user is specifically given access to the data. However, it does not mean that the user is denied by default.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 205

QUESTION 99
Who is responsible for implementing user clearances in computer-based information systems at the B3 level of the TCSEC rating?

A. Security administrators
B. Operators
C. Data owners
D. Data custodians

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Typical security administrator functions may include the following:
- Setting user clearances, initial passwords, and other security characteristics for new users
- Changing security profiles for existing users
- Setting or changing file sensitivity labels
- Setting the security characteristics of devices and communications channels
- Reviewing audit data

Incorrect Answers:
B: System operators provide day-to-day operations of computer systems. They do not perform the tasks listed in the question.
C: Data owners are primarily responsible for determining the data's sensitivity or classification levels. They can also be responsible for maintaining the information's accuracy and integrity. They do not perform the tasks listed in the question.
D: Data custodians are delegated the responsibility of protecting data by its owner. They do not perform the tasks listed in the question.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 211

QUESTION 100
Which of the following should NOT be performed by an operator?

A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.

System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs.

Incorrect Answers:
A: Implementing the initial program load is a function that should be performed by an operator.
B: Monitoring execution of the system is a function that should be performed by an operator.
D: Controlling job flow is a function that should be performed by an operator.

QUESTION 101
Which of the following should be performed by an operator?

A. Changing profiles
B. Approving changes
C. Adding and removal of users
D. Installing system software

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment.

Incorrect Answers:
A: Changing profiles should not be performed by an operator; this should be performed by a security administrator.
B: Approving changes should not be performed by an operator; this should be performed by a change control analyst or panel.
C: Adding and removal of users should not be performed by an operator; this should be performed by a security administrator.

QUESTION 102
Which of the following is NOT appropriate in addressing object reuse?

A. Degaussing magnetic tapes when they're no longer needed.
B. Deleting files on disk before reusing the space.
C. Clearing memory blocks before they are allocated to a program or data.
D. Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Object reuse requirements, applying to systems rated TCSEC C2 and above, are used to protect files, memory, and other objects in a trusted system from being accidentally accessed by users who are not authorized to access them.
Deleting files on disk before reusing the space does not meet this requirement and is therefore not appropriate in addressing object reuse.
Deleting files on disk merely erases file headers in a directory structure. It does not clear data from the disk surface, thus making files still recoverable. All other options involve clearing used space, preventing any unauthorized access.

Incorrect Answers:
A: Degaussing magnetic tapes when they're no longer needed protects files from unauthorized access by destroying the data on the tapes. This is a valid method of addressing object reuse.
C: Clearing memory blocks before they are allocated to a program or data removes any residual data from the memory thus preventing unauthorized access. This is a valid method of addressing object reuse.
D: Clearing buffered pages, documents, or screens from the local memory of a terminal or printer removes any residual data from the memory thus preventing unauthorized access. This is a valid method of addressing object reuse.

QUESTION 103
What security problem is most likely to exist if an operating system permits objects to be used sequentially by multiple users without forcing a refresh of the objects?

A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.
C. Data leakage through covert channels.
D. Denial of service through a deadly embrace.
Correct Answer: A

Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Allowing objects to be used sequentially by multiple users without a refresh of the objects can lead to disclosure of residual data. It is important that steps be taken to eliminate the chance for the disclosure of residual data.

Object reuse refers to the allocation or reallocation of system resources to a user or, more appropriately, to an application or process. Applications and services on a computer system may create or use objects in memory and in storage to perform programmatic functions. In some cases, it is necessary to share these resources between various system applications. However, some objects may be employed by an application to perform privileged tasks on behalf of an authorized user or upstream application. If object usage is not controlled or the data in those objects is not erased after use, they may become available to unauthorized users or processes.

Disclosure of residual data and Unauthorized obtaining of a privileged execution state are both a problem with shared memory and resources. Not clearing the heap/stack can result in residual data and may also allow the user to step on somebody's session if the security token/identify was maintained in that space. This is generally more malicious and intentional than accidental though. The MOST common issue would be Disclosure of residual data.

Incorrect Answers:
B: Unauthorized obtaining of a privileged execution state is not a problem with Object Reuse.
C: A covert channel is a communication path. Data leakage would not be a problem created by Object Reuse. In computer security, a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. The term, originated in 1973 by Lampson is defined as "(channels) not intended for information transfer at all, such as the service program's effect on system load." to distinguish it from Legitimate channels that are subjected to access controls by COMPUSEC.
D: Denial of service through a deadly embrace is not a problem with Object Reuse.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 424 https://www.fas.org/irp/nsa/rainbow/tg018.htm http://en.wikipedia.org/wiki/Covert_channel

QUESTION 104
Which of the following categories of hackers poses the greatest threat?

A. Disgruntled employees
B. Student hackers
C. Criminal hackers
D. Corporate spies

Correct Answer: A

Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Employee sabotage can become an issue if an employee is knowledgeable enough about the IT infrastructure of an organization, has sufficient access.

Incorrect Answers:
B: Student hackers are a lesser threat as a disgruntled employee already has access to the system.
C: A disgruntled employee is a larger threat compared to a criminal hacker as the employee already has access to the system.
D: A disgruntled employee is a larger threat compared to a corporate spy as the employee already has access to the system.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 602

QUESTION 105
The copyright law ("original works of authorship") protects the right of the owner in all of the following except?

A. The public distribution of the idea
B. Reproduction of the idea
C. The idea itself
D. Display of the idea

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Copyright law does not product the idea itself. Copyright law protects the right of an author to control the public distribution, reproduction, display, and adaptation of his original work.

Incorrect Answers:
A: Copyright law protects the right of an author to control the public distribution of his original work.
B: Copyright law protects the right of an author to control the reproduction of his original work.
D: Copyright law protects the right of an author to control the display of his original work.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1000

QUESTION 106

Which of the following is biggest factor that makes Computer Crimes possible?

A. The fraudster obtaining advanced training & special knowledge.
B. Victim carelessness.
C. Collusion with others in information processing.
D. System design flaws.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
Human-unintentional threats represent the most common source of disasters. Examples of human unintentional threats are primarily those that involve inadvertent errors and omissions, in which the person, through lack of knowledge, laziness, or carelessness, serves as a source of disruption.

Incorrect Answers:
A: A more knowledgeable fraudster would increase the risk of Computer Crimes, but it is less of a factor compared to human carelessness.
C: Collusion makes computer crimes possible, but human carelessness is the main factor.
D: System design flaws makes computer crimes possible, but human carelessness is the main factor.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 347

QUESTION 107

Which of the following questions is less likely to help in assessing physical and environmental protection?

A. Are entry codes changed periodically?
B. Are appropriate fire suppression and prevention devices installed and working?
C. Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
D. Is physical access to data transmission lines controlled?

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information are technical controls, not physical controls.

Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Locks and access control systems are examples of physical controls. Asking about the entry codes of an access control system will help in assessing physical and environmental protection. Therefore, this answer is incorrect.
B: Fire suppression and prevention devices are examples of physical controls. Asking if they are installed and working will help in assessing physical and environmental protection. Therefore, this answer is incorrect.
D: Physical access to data transmission lines is an example of physical control. Asking if this is physical access is controlled will help in assessing physical and environmental protection. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28

QUESTION 108
Which of the following would MOST likely ensure that a system development project meets business objectives?

A. Development and tests are run by different individuals
B. User involvement in system specification and acceptance
C. Development of a project plan identifying all development activities
D. Strict deadlines and budgets

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Early in a system development project, there is a requirements gathering phase when everyone involved attempts to understand why the project is needed and what the scope of the project entails. During this phase, the team examines the software’s requirements and proposed functionality, brainstorming sessions take place, and obvious restrictions are reviewed.

As end users will be the people using the system, they are most likely to have the most valuable input into the system requirements definition. When the requirements are determined and the system is developed, user testing will ensure the system meets the requirements defined in the early project stages.

Incorrect Answers:
A: This question is asking for the answer that will MOST likely ensure that a system development project meets business objectives. Tests run by different individuals will provide a better test to ensure system meets the requirements. However, user involvement in system requirements and specification stage will make it more likely that the system is developed to meet the requirements.
C: Development of a project plan identifying all development activities will not ensure the system meets business objectives if the initial design of the system is not what is required.
D: Strict deadlines and budgets will ensure the project is completed on time and within budget. However, it will have no effect on whether the system meets business objectives.

QUESTION 109
In which phase of the System Development Lifecycle (SDLC) is Security Accreditation Obtained?

A. Functional Requirements Phase
B. Testing and evaluation control
C. Acceptance Phase
D. Postinstallation Phase

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Within the SDLC framework Security Accreditation is obtained during the Implementation Phase, more specifically during Testing and evaluation control.

Incorrect Answers:
A: Security Accreditation is not used during the Functional Requirements Phase. It is used later during the Implementation phase.
C: Security Accreditation is not used during the Acceptance Phase. It is used earlier during the Implementation phase.
D: Security Accreditation is not used during the Postinstallation Phase. It is used earlier during the Implementation phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1088

QUESTION 110
Which of the following would be the MOST serious risk where a systems development life cycle methodology is inadequate?

A. The project will be completed late.
B. The project will exceed the cost estimates.
C. The project will be incompatible with existing systems.
D. The project will fail to meet business and user needs.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The systems development life cycle (SDLC), also referred to as the application development life-cycle, is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system. The systems development life-cycle concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both. The most important stages of the systems development life cycle are the early requirement gathering and design phases. If the system requirements are not correctly determined, the system will not meet the needs of the business and users.

A: This question is asking for the MOST serious risk. A project completed late is inconvenient but a system that fails to meet business and user needs is a more serious risk.
B: This question is asking for the MOST serious risk. A project that exceeds cost estimates is a pain but a system that fails to meet business and user needs is a more serious risk.
C: This question is asking for the MOST serious risk. A project that is incompatible with existing systems is not good but new systems could be deployed. However, a system that fails to meet business and user needs is no good to anyone.

References:
https://en.wikipedia.org/wiki/Systems_development_life_cycle

QUESTION 111
In which of the following phases of system development life cycle (SDLC) is contingency planning most important?

A. Initiation
B. Development/acquisition
C. Implementation
D. Operation/maintenance

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The system development life cycle (SDLC) is the process of developing an information system. The SDLC includes the Initiation, Development and Acquisition, Implementation, Operation and Maintenance and Disposal phases.
The initiation phase includes determining the system's goals and feasibility. The systems feasibility includes its system requirements and how well they match with operational processes. The requirements of a contingency plan should be analyzed based on the system's requirements and design.
Incorrect Answers:
B: Contingency planning is most important in the initiation phase, not the Development/acquisition phase. It is important to create a contingency plan in the earliest possible stage of a project.
C: Contingency planning is most important in the initiation phase, not the Implementation phase. The contingency plan should be created before the system is implemented.
D: Contingency planning is most important in the initiation phase, not the operation/maintenance phase. It is important to create a contingency plan in the earliest possible stage of a project, not after the system has been deployed.

References:
EC-Council, *Disaster Recovery*, Cengage Learning, Andover, 2010, pp 4-11

QUESTION 112
Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?

A. Development/acquisition
B. Implementation
C. Operation/Maintenance
D. Initiation

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In the Operation/maintenance phase the system is used and cared for. Proper authentication of the users and processes must be developed in this phase.

Incorrect Answers:
A: In the Acquisition/development the new system is either created or purchased. The main concern of this phase is not the authentication of users and processes.
B: In the implementation phase the new system is installed into production environment. The main concern of this phase is not the authentication of users and processes.
D: In the Initiation phase the need for a new system is defined. Authentication of users and processes is not a major concern of this phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1087

QUESTION 113
What can be defined as: It confirms that users' needs have been met by the supplied solution?

A. Accreditation
B. Certification
C. Assurance
D. Acceptance

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Acceptance testing is used to ensure that the code meets customer requirements. If this testing is passed the user's needs have been met.

Incorrect Answers:
A: The final stage is accreditation, which is management's, but not the users', formal approval.
B: Certification involves testing the newly purchased product within the company's environment. Certification does not confirm that the users' need have been met.
C: Assurance is a measurement of confidence in the level of protection that a specific security control delivers and the degree to which it enforces the security policy.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1105

QUESTION 114
Which of the following fire extinguishing systems incorporating a detection system is currently the most recommended water system for a computer room?

A. Wet pipe
B. Dry pipe
C. Deluge
D. Preaction

Correct Answer: D
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
Preaction systems are similar to dry pipe systems in that the water is not held in the pipes, but is released when the pressurized air within the pipes is reduced. Once this happens, the pipes are filled with water, but it is not released right away. A thermal-fusible link on the sprinkler head has to melt before the water is released. The purpose of combining these two techniques is to give people more time to respond to false alarms or to small fires that can be handled by other means. Putting out a small fire with a handheld extinguisher is better than losing a lot of electrical equipment to water damage. These systems are usually used only in data processing environments rather than the whole building, because of the higher cost of these types of systems.

Incorrect Answers:
A: Wet pipe systems always contain water in the pipes and are usually discharged by temperature control–level sensors. This type is not the most recommended water system for a computer room because this system provides no time to respond to false alarms or to small fires that can be handled by other means. Therefore, this answer is incorrect.
B: In dry pipe systems, the water is not actually held in the pipes. The water is contained in a “holding tank” until it is released. This type is not the most recommended water system for a computer room because this system provides no time to respond to false alarms or to small fires that can be handled by other means. Therefore, this answer is incorrect.
C: A deluge system has its sprinkler heads wide open to allow a larger volume of water to be released in a shorter period. Because the water being released is in such large volumes, these systems are usually not used in data processing environments. This type is not the most recommended water system for a computer room. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 474-475

QUESTION 115
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:

A. Concern that the laser beam may cause eye damage.
B. The iris pattern changes as a person grows older.
C. There is a relatively high rate of false accepts.

D. The optical unit must be positioned so that the sun does not shine into the aperture.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The optical unit of the iris pattern biometric system must be positioned so that the sun does not shine into the aperture.

Incorrect Answers:
A: Iris recognition systems do not use laser like beams.
B: With iris scans, the kind of errors that can occur during the authentication process is reduced because the iris remains constant through adulthood.
C: Extreme resistance to false matching is an advantage of iris recognition.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 191
https://en.wikipedia.org/wiki/Iris_recognition

QUESTION 116
Which of the following is not classified as "Security and Audit Frameworks and Methodologies"?

A. Bell LaPadula
B. Committee of Sponsoring Organizations of the Treadway Commission (COSO)
C. IT Infrastructure Library (ITIL)
D. Control Objectives for Information and related Technology (COBIT)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Bell-LaPadula model is a security model, not a Security and Audit Frameworks and Methodology. The Bell-LaPadula model is a subject-to-object model. An example would be how you (subject) could read a data element (object) from a specific database and write data into that database. The Bell-LaPadula model focuses on ensuring that subjects are properly authenticated—by having the necessary security clearance, need to know, and formal access approval—before accessing an object.

The Control Objectives for Information and related Technology (CobiT) is a framework and set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs.
CobiT was derived from the COSO framework, developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission in 1985 to deal with fraudulent financial activities and reporting.
The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management. ITIL is a customizable framework that is provided in a set of books or in an online format.

Incorrect Answers:
B: Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a Security and Audit Frameworks and Methodology.
C: IT Infrastructure Library (ITIL) is a Security and Audit Frameworks and Methodology.
D: Control Objectives for Information and related Technology (COBIT) is a Security and Audit Frameworks and Methodology.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 55-60, 369

QUESTION 117
At which of the basic phases of the System Development Life Cycle are security requirements formalized?

A. Disposal
B. System Design Specifications
C. Development and Implementation
D. Functional Requirements Definition

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Requirements, including security requirements, are formalized in the Functional Requirements Definition phase.

Incorrect Answers:
A: Disposal activities need to ensure that an orderly termination of the system takes place and that all necessary data are preserved. Security requirements are not formalized at the disposal phase.
B: Within the Systems Development Life Cycle (DSLC) model the design phase, also known as the System Design Specifications phase, transforms requirements, including the security requirements, into a complete System Design Document.
C: In the implementation phase the system is implemented into a product production environment. The security requirements have already been developed long before this phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1095

QUESTION 118
During which phase of an IT system life cycle are security requirements developed?

A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Within the Systems Development Life Cycle (DSLC) model the design phase, also known as the security requirement phase, transforms requirements, including the security requirements, into a complete System Design Document.

Incorrect Answers:
A: The operation phase describes tasks to operate in a production environment, and is not concerned with development of security requirements.
B: The initiation phase starts when a sponsor identifies a need or an opportunity. During this phase a Concept Proposal, but no security requirements, is created.
D: In the implementation phase the system is implemented into a product production environment. The security requirements have already been developed long before this phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1095

QUESTION 119
Which of the following phases of a system development life-cycle is most concerned with establishing a good security policy as the foundation for design?

A. Development/acquisition
B. Implementation
C. Initiation
D. Maintenance

Correct Answer: C

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Within the SDLC model during the initiation phase the need for a new system is defined. The initiation phase includes security categorization and preliminary risk assessment including a security policy.
The security policy is a documentation that describes senior management's directives toward the role that security plays within the organization. It provides a framework within which an organization establishes needed levels of information security to achieve the desired confidentiality, availability, and integrity goals.

Incorrect Answers:
A: The Development/acquisition phase does not establish a good security policy; instead it includes risk assessment and risk analysis.
B: The implementation phase includes security certification and security accreditation. Establishing a good security policy is not included in the implementation phase.
D: The maintenance phase include continuous monitoring, and configuration management and control. It does include creation of a security policy.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 1088, 1422

QUESTION 120
When considering an IT System Development Life-cycle, security should be:
A. Mostly considered during the initiation phase.
B. Mostly considered during the development phase.
C. Treated as an integral part of the overall system design.
D. Added once the design is completed.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Within the System Development Life-cycle (SDLC) model, security is critical in each phase of the life cycle.

Incorrect Answers:
A: Security is critical to each phase of the SDLC model, not only the initiation phase.
B: Security is critical to each phase of the SDLC model, not only the development phase.
D: Security is critical to each phase of the SDLC model, and is not added when the design is completed.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1087

QUESTION 121
Risk reduction in a system development life-cycle should be applied:

A. Mostly to the initiation phase.
B. Mostly to the development phase.
C. Mostly to the disposal phase.
D. Equally to all phases.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Risk reduction should be applied equally to the initiation phase, the development phase, and to the disposal phase.
Within the initiation phase a preliminary risk assessment should be carried out to develop an initial description of the confidentiality, integrity, and availability requirements of the system.
The development phase include formal risk assessment which identifies vulnerabilities and threats in the proposed system and the potential risk levels as they pertain to confidentiality, integrity, and availability. This builds upon the initial risk assessment carried out in the previous phase (the initiation phase). The results of this assessment help the team build the system's security plan.
Disposal activities need to ensure that an orderly termination of the system takes place and that all necessary data are preserved. The storage medium of the system may need to be degaussed, put through a zeroization process, or physically destroyed.

Incorrect Answers:
A: Risk reduction should be applied to all phases equally, not mostly to the initiation phase.
B: Risk reduction should be applied to all phases equally, not mostly to the development phase.
C: Risk reduction should be applied to all phases equally, not mostly to the disposal phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 1091-1093

QUESTION 122
Who developed one of the first mathematical models of a multilevel-security computer system?

A. Diffie and Hellman.
B. Clark and Wilson.
C. Bell and LaPadula.

D. Gasser and Lipner.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Bell-LaPadula model was the first mathematical model of a multilevel security policy used to define the concept of a secure state machine and modes of access, and outlined rules of access.

Incorrect Answers:
A: Diffie and Hellman developed the first asymmetric key agreement algorithm, not the first multilevel security policy computer system.
B: The question asks for the developers of the first mathematical models of a multilevel-security computer system. This was Bell and LaPadula, not Clark and Wilson.
D: The question asks for the developers of the first mathematical models of a multilevel-security computer system. This was Bell and LaPadula, not Gasser and Lipner.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 369, 812

QUESTION 123
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?

A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The mechanism that automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters is known as an auxiliary station alarm.

Alarm systems may have auxiliary alarms that ring at the local fire or police stations. Most central station systems include this feature, which requires permission form the local authorities before implementation.

Incorrect Answers;
A: Central Station Systems are operated and monitored around the clock by private security firms. The central stations are signaled by detectors over leased lines. Most central station systems include auxiliary alarms that ring at the local fire or police stations. However, the name of the alarm system that rings at the local fire or police stations is 'auxiliary alarm'. Therefore, this answer is incorrect.
B: Proprietary Systems are similar to the central station systems, except that the monitoring system is owned and operated by the customer. Proprietary alarm is not name of the alarm that rings at the local fire or police stations. Therefore, this answer is incorrect.
C: A remote station alarm is not the alarm that rings at the local fire or police stations. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 474

QUESTION 124
Which security model introduces access to objects only through programs?

A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model

Correct Answer: C
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
With the Clark–Wilson model, users are unable to modify critical data (CDI) directly. Users have to be authenticated to a piece of software, and the software procedures (TPs) will carry out the operations on behalf of the user.

Incorrect Answers:
A: The Biba model allows access to sensitive data based on a lattice of integrity levels.
B: The Bell-LaPadula model allows access to sensitive data based on a lattice of security levels.
D: The information flow model, on which both the Bell-LaPadula and Biba models are based, allows direct access to data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 369-378 https://en.wikipedia.org/wiki/Clark-Wilson_model

QUESTION 125
Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

A. The Take-Grant model
B. The Biba integrity model
C. The Clark Wilson integrity model
D. The Bell-LaPadula integrity model

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
When an application uses the Clark-Wilson model, it separates data into one subset that needs to be highly protected, which is referred to as a constrained data item (CDI), and another subset that does not require a high level of protection, which is called an unconstrained data item (UDI). Users cannot modify critical data (CDI) directly. Instead, the subject (user) must be authenticated to a piece of software, and the software procedures (Transformation Procedures) will carry out the operations on behalf of the user. For example, when Kathy needs to update information held within her company's database, she will not be allowed to do so without a piece of software controlling these activities. First, Kathy must authenticate to a program, which is acting as a front end for the database, and then the program will control what Kathy can and cannot do to the information in the database.

Incorrect Answers:
A: The take-grant protection model is used to establish or disprove the safety of a given computer system that follows specific rules. This is not what is described in the question.
B: The Biba Model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. However, it does not define a constrained data item and a transformation procedure.
C: The Bell-LaPadula model does not deal with integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 374

QUESTION 126
The BIGGEST difference between System High Security Mode and Dedicated Security Mode is:

A. The clearance required
B. Object classification
C. Subjects cannot access all objects
D. Need-to-know

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A system is operating in a dedicated security mode if all users have a clearance for, and a formal need-to-know about, all data processed within the system. All users have been given formal access approval for all information on the system and have signed nondisclosure agreements (NDAs) pertaining to this information. The system can handle a single classification level of information.
A system is operating in system high-security mode when all users have a security clearance to access the information but not necessarily a need-to-know for all the information processed on the system. So, unlike in the dedicated security mode, in which all users have a need-to-know pertaining to all data on the system, in system high-security mode, all users have a need-to-know pertaining to some of the data. This mode also requires all users to have the highest level of clearance required by any and all data on the system. However, even though a user has the necessary security clearance to access an object, the user may still be restricted if he does not have a need-to-know pertaining to that specific object.

Incorrect Answers:
A: The clearance required is not the difference between the two. All users have clearance in both systems. However, in high-security mode, access is further restricted by need-to-know.
B: Object classification is not the difference between the two. The classification of objects can be the same or it can be different; however, high-security mode is further restricted by need-to-know.
C: Subjects cannot access all objects is not the difference between the two. All subjects CAN access all objects providing they have the 'need-to-know'.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 4th Edition, McGraw-Hill, New York, 2007, p. 387

QUESTION 127
For competitive reasons, the customers of a large shipping company called the "Integrated International Secure Shipping Containers Corporation" (IISSCC) like to keep private the various cargos that they ship. IISSCC uses a secure database system based on the Bell-LaPadula access control model to keep this information private. Different information in this database is classified at different levels. For example, the time and date a ship departs is labeled Unclassified, so customers can estimate when their cargos will arrive, but the contents of all shipping containers on the ship are labeled Top Secret to keep different shippers from viewing each other's cargos.

An unscrupulous fruit shipper, the "Association of Private Fruit Exporters, Limited" (APFEL) wants to learn whether or not a competitor, the "Fruit Is Good Corporation" (FIGCO), is shipping pineapples on the ship "S.S. Cruise Pacific" (S.S. CP). APFEL can't simply read the top secret contents in the IISSCC database because of the access model. A smart APFEL worker, however, attempts to insert a false, unclassified record in the database that says that FIGCO is shipping pineapples on the S.S. CP, reasoning that if there is already a FIGCO-pineapple-SSCP record then the insertion attempt will fail. But the attempt does not fail, so APFEL can't be sure whether or not FIGCO is shipping pineapples on the S.S. CP.

What is the name of the access control model property that prevented APFEL from reading FIGCO's cargo information? What is a secure database technique that could explain why, when the insertion attempt succeeded, APFEL was still unsure whether or not FIGCO was shipping pineapples?

A. *-Property and Polymorphism
B. Strong *-Property and Polyinstantiation
C. Simple Security Property and Polymorphism
D. Simple Security Property and Polyinstantiation

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level. Simple Security Property is the name of the access control model property that prevented APFEL from reading FIGCO's cargo information.

The secure database technique that could explain why, when the insertion attempt succeeded, APFEL was still unsure whether or not FIGCO was shipping pineapples is Polyinstantiation. Polyinstantiation enabled the false record to be created.
Polyinstantiation enables a table that contains multiple tuples with the same primary keys, with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects must be restricted from it. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking the information actually means something else.

Incorrect Answers:
A: The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. This is not the access control model property that prevented APFEL from reading FIGCO's cargo information.
Polymorphism takes place when different objects respond to the same command, input, or message in different ways. This is not the secure database technique used in this question.
B: The strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal. This is not the access control model property that prevented APFEL from reading FIGCO's cargo information.
C: Polymorphism takes place when different objects respond to the same command, input, or message in different ways. This is not the secure database technique used in this question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 4th Edition, McGraw-Hill, New York, 2007, pp. 370, 1186

QUESTION 128
Which security model uses an access control triple and also requires separation of duty?

A. DAC
B. Lattice

C. Clark-Wilson
D. Bell-LaPadula

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Clark-Wilson model enforces the three goals of integrity by using access triple (subject, software [TP], object), separation of duties, and auditing. This model enforces integrity by using well-formed transactions (through access triple) and separation of duties.
When an application uses the Clark-Wilson model, it separates data into one subset that needs to be highly protected, which is referred to as a constrained data item (CDI), and another subset that does not require a high level of protection, which is called an unconstrained data item (UDI). Users cannot modify critical data (CDI) directly. Instead, the subject (user) must be authenticated to a piece of software, and the software procedures (TPs) will carry out the operations on behalf of the user. For example, when Kathy needs to update information held within her company's database, she will not be allowed to do so without a piece of software controlling these activities. First, Kathy must authenticate to a program, which is acting as a front end for the database, and then the program will control what Kathy can and cannot do to the information in the database.
This is referred to as access triple: subject (user), program (TP), and object (CDI). A user cannot modify CDI without using a TP.
The Clark-Wilson security model uses division of operations into different parts and requires different users to perform each part. This is known as Separation of Duties.
The Clark-Wilson model outlines how to incorporate separation of duties into the architecture of an application. If a customer needs to withdraw over $10,000, the application may require a supervisor to log in and authenticate this transaction. This is a countermeasure against potential fraudulent activities. The model provides the rules that the developers must follow to properly implement and enforce separation of duties through software procedures.

Incorrect Answers:
A: DAC (Discretionary Access Control) is not a security model that uses an access control triple and requires separation of duty.
B: Lattice-based access control model A mathematical model that allows a system to easily represent the different security levels and control access attempts based on those levels. It is not a security model that uses an access control triple and requires separation of duty.
D: The Bell–LaPadula Model is a state machine model used for enforcing access control in government and military applications. It is not a security model that uses an access control triple and requires separation of duty.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 370-377

QUESTION 129
You have been approached by one of your clients. They are interested in doing some security re-engineering. The client is looking at various information security models. It is a highly secure environment where data at high classifications cannot be leaked to subjects at lower classifications. Of primary concern to them, is the identification of potential covert channel. As an Information Security Professional, which model would you recommend to the client?

A. Information Flow Model combined with Bell LaPadula

B. Bell LaPadula
C. Biba
D. Information Flow Model

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Bell-LaPadula model focuses on preventing information from flowing from a high security level to a low security level. Information Flow Model deals with covert channels.

Subjects can access files. Processes can access memory segments. When data are moved from the hard drive's swap space into memory, information flows. Data are moved into and out of registers on a CPU. Data are moved into different cache memory storage devices. Data are written to the hard drive, thumb drive, CDROM drive, and so on. Properly controlling all of these ways of how information flows can be a very complex task. This is why the information flow model exists—to help architects and developers make sure their software does not allow information to flow in a way that can put the system or data in danger. One way that the information flow model provides this type of protection is by ensuring that covert channels do not exist in the code.

Incorrect Answers:
B: The Bell LaPadula model on its own is not sufficient because it does not deal with the identification of covert channels.
C: The Biba model is an integrity model. It will not prevent information from flowing from a high security level to a low security level or identify covert channels.
D: The Information Flow model on its own is not sufficient because it will not prevent information from flowing from a high security level to a low security level.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 377-378

QUESTION 130
Which of the following security models introduced the idea of mutual exclusivity which generates dynamically changing permissions?

A. Biba
B. Brewer & Nash
C. Graham-Denning
D. Clark-Wilson

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Brewer and Nash model, also called the Chinese Wall model, was created to provide access controls that can change dynamically depending upon a user's previous actions. The main goal of the model is to protect against conflicts of interest by users' access attempts.
Under the Brewer and Nash model, company sensitive information is categorized into mutually disjointed conflict-of-interest categories. If you have access to one set of data, you cannot access the other sets of data.

Incorrect Answers:
A: The Biba model deals with integrity. It does not use dynamically changing permissions.
C: The Graham-Denning model shows how subjects and objects should be securely created and deleted. It also addresses how to assign specific access rights. It does not use dynamically changing permissions.
D: The Clark-Wilson model deals with integrity. It does not use dynamically changing permissions.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 383

QUESTION 131
Which of the following was the FIRST mathematical model of a multilevel security policy used to define the concepts of a security state and mode of access, and to outline rules of access?

A. Biba
B. Bell-LaPadula
C. Clark-Wilson
D. State machine

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In the 1970s, the U.S. military used time-sharing mainframe systems and was concerned about the security of these systems and leakage of classified information. The Bell-LaPadula model was developed to address these concerns. It was the first mathematical model of a multilevel security policy used to define the concept of a secure state machine and modes of access, and outlined rules of access. Its development was funded by the U.S. government to provide a framework for computer systems that would be used to store and process sensitive information. The model's main goal was to prevent secret information from being accessed in an unauthorized manner.
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels.

Incorrect Answers:
A: The Biba Model is an integrity model. This is not what is described in the question.
C: The Clark-Wilson Model is an integrity model. This is not what is described in the question.
D: State machine is not a specific model; it is a type of model. For example, the Bell-LaPadula model is a state machine model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 369

QUESTION 132
Which of the following answers BEST describes the Bell La-Padula model of storage and access control of classified information?

A. No read up and No write down
B. No write up, no read down
C. No read over and no write up
D. No reading from higher classification levels

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Three main rules are used and enforced in the Bell-LaPadula model:
The simple security (SS) rule, the *-property (star property) rule, and the strong star property rule. The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level.
The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. The simple security rule is referred to as the “no read up” rule, and the *-property rule is referred to as the “no write down” rule.
The third rule, the strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal.

Incorrect Answers:
B: No write up, no read down is not the best description of the Bell-LaPadula model.
C: No read over and no write up is not the best description of the Bell-LaPadula model.
D: No reading from higher classification levels is not the best description of the Bell-LaPadula model.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 369-370

QUESTION 133
Individual accountability does not include which of the following?

A. unique identifiers
B. policies and procedures
C. access rules
D. audit trails

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Accountability would not include policies & procedures because while important on an effective security program they cannot be used in determining accountability.

References:
A: Accountability would include unique identifiers so that you can identify the individual.
C: Accountability would include access rules to define access violations.
D: Accountability would include audit trails to be able to trace violations or attempted violations.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 248-250

QUESTION 134
Which of the following components are considered part of the Trusted Computing Base?

A. Trusted hardware and firmware.
B. Trusted hardware and software.
C. Trusted hardware, software and firmware.
D. Trusted computer operators and system managers.

Correct Answer: C
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
The trusted computing base (TCB) is a collection of all the hardware, software, and firmware components within a system that provide some type of security and enforce the system's security policy. The TCB does not address only operating system components, because a computer system is not made up of only an operating system. Hardware, software components, and firmware components can affect the system in a negative or positive manner, and each has a

responsibility to support and enforce the security policy of that particular system. Some components and mechanisms have direct responsibilities in supporting the security policy, such as firmware that will not let a user boot a computer from a USB drive, or the memory manager that will not let processes overwrite other processes' data. Then there are components that do not enforce the security policy but must behave properly and not violate the trust of a system. Examples of the ways in which a component could violate the system's security policy include an application that is allowed to make a direct call to a piece of hardware instead of using the proper system calls through the operating system, a process that is allowed to read data outside of its approved memory space, or a piece of software that does not properly release resources after use.

To assist with the evaluation of secure products, TCSEC introduced the idea of the Trusted Computing Base (TCB) into product evaluation. In essence, TCSEC starts with the principle that there are some functions that simply must be working correctly for security to be possible and consistently enforced in a computing system. For example, the ability to define subjects and objects and the ability to distinguish between them is so fundamental that no system could be secure without it. The TCB then are these fundamental controls implemented in a given system, whether that is in hardware, software, or firmware. Each of the TCSEC levels describes a different set of fundamental functions that must be in place to be certified to that level.

Incorrect Answers:
A: Software is also considered part of the Trusted Computing Base.
B: Firmware is also considered part of the Trusted Computing Base.
D: Trusted computer operators and system managers are not considered part of the Trusted Computing Base.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 360
https://www.freepracticetests.org/documents/TCB.pdf

QUESTION 135
The high availability of multiple all-inclusive, easy-to-use hacking tools that do NOT require much technical knowledge has brought a growth in the number of which type of attackers?

A. Black hats
B. White hats
C. Script kiddies
D. Phreakers

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

Script kiddies are hackers who do not necessarily have the skill to carry out specific attacks without the tools provided for them on the Internet and through friends. Since these people do not necessarily understand how the attacks are actually carried out, they most likely do not understand the extent of damage they can cause.

Incorrect Answers:
A: Black hats are malicious, skilled hackers. Easy-to-use hacking tools have not brought a growth in black hats.
B: White hats are security professionals; ethical hackers who hack systems to test their security. Easy-to-use hacking tools have not brought a growth in white hats. D: Phreakers are telephone/PBX (private branch exchange) hackers. Easy-to-use hacking tools have not brought a growth in Phreakers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 986

QUESTION 136
Which is the last line of defense in a physical security sense?

A. people
B. interior barriers
C. exterior barriers
D. perimeter barriers

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In terms of physical security, people are the last line of defense for your company's assets. If an intruder gets past the perimeter barriers, then the external barriers and finally the internal barriers, there are no more physical defenses remaining other than people in the facility.

Incorrect Answers:
B: Interior barriers are behind external barriers and perimeter barriers in terms of physical security. However, internal barriers are not the last line of defense; people are. Therefore, this answer is incorrect.
C: Exterior barriers are between perimeter barriers and internal barriers in terms of physical security. Therefore, they are not the last line of defense so this answer is incorrect.
D: Perimeter barriers are the first line of defense; not the last line of defense. Therefore, this answer is incorrect.

QUESTION 137
What is an error called that causes a system to be vulnerable because of the environment in which it is installed?

A. Configuration error
B. Environmental error
C. Access validation error
D. Exceptional condition handling error

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Environmental errors include utility failure, service outage, natural disasters, or neighboring hazards. Any issue with the environment in which a system is installed is known as an environmental error.
Maintaining appropriate temperature and humidity is important in any facility, especially facilities with computer systems. Improper levels of either can cause damage to computers and electrical devices. High humidity can cause corrosion, and low humidity can cause excessive static electricity. This static electricity can short out devices, cause the loss of information, or provide amusing entertainment for unsuspecting employees. Lower temperatures can cause mechanisms to slow or stop, and higher temperatures can cause devices to use too much fan power and eventually shut down.

Incorrect Answers:
A: A configuration error is a problem caused by the configuration of the settings in a system, not the environment in which the system is installed.
C: An access validation error is a problem caused a user not having the correct permissions or access rights to the system. An access validation error is not caused by the environment in which the system is installed.
D: An exceptional condition handling error is a problem caused by the software code of the system, not the environment in which the system is installed.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 466

QUESTION 138
Devices that supply power when the commercial utility power system fails are called which of the following?

A. power conditioners
B. uninterruptible power supplies
C. power filters
D. power dividers

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
An uninterruptible power supply (UPS) is an electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries, supercapacitors, or flywheels. The on-battery runtime of most uninterruptible power sources is relatively short (often only a few minutes) but sufficient to start a standby power source or properly shut down the protected equipment.

Incorrect Answers:
A: A power conditioner is a device intended to improve the quality of the power that is delivered to electrical equipment. It does not supply power when the commercial utility power system fails. Therefore, this answer is incorrect.
C: A power filter is similar to a power conditioner in that it is intended to improve the quality of the power that is delivered to electrical equipment. It does not supply power when the commercial utility power system fails. Therefore, this answer is incorrect.
D: Power dividers are used in radio technology. They do not supply power when the commercial utility power system fails. Therefore, this answer is incorrect.

References:
https://en.wikipedia.org/wiki/Uninterruptible_power_supply

QUESTION 139
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:

A. specify what users can do.
B. specify which resources they can access.
C. specify how to restrain hackers.
D. specify what operations they can perform on a system.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Access controls are security features that control how users and systems communicate and interact with other systems and resources. Access controls give organization the ability to control, restrict, monitor, and protect resource availability, integrity and confidentiality.
Access controls do not enable management to specify how to restrain hackers. Access controls can only prevent hackers accessing a system.

Incorrect Answers:
A: Access control does enable managers of a system to specify what users can do within the system.
B: Access control does enable managers of a system to specify which resources they can access.

D: Access control does enable managers of a system to specify what operations they can perform on a system.

References:
https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems

QUESTION 140
Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?

A. SESAME
B. RADIUS
C. KryptoKnight
D. TACACS+

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support.

Incorrect Answers:
B: RADIUS is a network protocol that allows for client/server authentication and authorization, and audits remote users. It was not developed to address some of the weaknesses in Kerberos.
C: KryptoKnight provides authentication and key distribution services to applications and communicating entities in a network environment. It was not developed to address some of the weaknesses in Kerberos.
D: TACACS+ is a network protocol that allows for client/server authentication and authorization. It was not developed to address some of the weaknesses in Kerberos.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 214, 234-236
http://www.eurecom.fr/~nsteam/Papers/kryptoknight.pdf

QUESTION 141
Which of the following is NOT a system-sensing wireless proximity card?

A. magnetically striped card

B. passive device
C. field-powered device
D. transponder

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A system sensing device recognizes the presence of a card and communicates with it without the user needing to carry out any activity.
A magnetically striped card is a card with a magnetic strip along one edge of the card. Credit cards today still have magnetic strips although they are rarely used for reading the card. To obtain information from the card by using the magnetic strip, the card needs to be 'swiped' through a card reader. The physical contact required between the card and the card reader means that a magnetically striped card is not a wireless proximity card.
System sensing access control readers, also called transponders, recognize the presence of an approaching object within a specific area. This type of system does not require the user to swipe the card through the reader. The reader sends out interrogating signals and obtains the access code from the card without the user having to do anything.

Incorrect Answers:
B: A passive device is a wireless proximity card. Passive devices contain no battery or power on the card, but sense the electromagnetic field transmitted by the reader and transmit at different frequencies using the power field of the reader. Therefore, this answer is incorrect.
C: A field-powered device is a wireless proximity card. They contain active electronics, a radio frequency transmitter, and a power supply circuit on the card. Therefore, this answer is incorrect.
D: A transponder is a wireless proximity card. The reader and card communicate directly. The card and reader have a receiver, transmitter, and battery. The reader sends signals to the card to request information. The card sends the reader an access code. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 484

QUESTION 142
Which of the following is the most costly countermeasure to reducing physical security risks?

A. Procedural Controls
B. Hardware Devices
C. Electronic Systems
D. Security Guards

Correct Answer: D

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
One drawback of security guards is that the cost of maintaining a guard function either internally or through an external service is expensive.
With common physical security risk countermeasures such as door entry control systems or perimeter fencing, there is typically a one-off cost when the countermeasure is implemented. With security guards, you have the ongoing cost of paying the salary of the security guard.
Incorrect Answers:
A: Procedural controls consist of approved written policies, procedures, standards and guidelines. The cost of implement procedural controls is not more costly than the ongoing costs associated with security guards. Therefore, this answer is incorrect.
B: Hardware Devices typically have a one-off cost when they are implemented and they may have a small cost for maintenance. However, this cost not more costly than the ongoing costs associated with security guards. Therefore, this answer is incorrect.
C: Electronic Systems typically have a one-off cost when they are implemented and they may have a small cost for maintenance. However, this cost not more than the ongoing costs associated with security guards. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 535

QUESTION 143
Which one of the following authentication mechanisms creates a problem for mobile users?

A. Mechanisms based on IP addresses B.
Mechanism with reusable passwords
C. One-time password mechanism.
D. Challenge response mechanism.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Authentication mechanisms based on IP addresses are useful if a user has a fixed IP address. This could be a fixed IP address at work or even a fixed IP address at home. With authentication mechanisms based on IP addresses, a user can access a resource only from a defined IP address.
However, authentication mechanisms based on IP addresses are a problem for mobile users. This is because mobile users will connect to different networks on their travels such as different WiFi networks or different mobile networks. This means that the public IP address that the mobile user will be connecting from will change frequently.

Incorrect Answers:
B: Authentication mechanisms with reusable passwords are not a problem for mobile users. As long as the mobile user knows the password, he can access the resource.
C: One-time password authentication mechanisms are not a problem for mobile users. The mobile user will have a token device that provides the one-time password which will enable the user to access the resource.
D: Challenge response authentication mechanisms are not a problem for mobile users. As long as the user has network connectivity to the authenticating server (usually over the Internet) the challenge-response authentication will succeed.

QUESTION 144
In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?

A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In this question, the attacker is trying to obtain the key from several “encrypted messages”. When the attacker has only encrypted messages to work from, this is known as a Ciphertext-only attack.

Cryptanalysis is the act of obtaining the plaintext or key from the ciphertext. Cryptanalysis is used to obtain valuable information and to pass on altered or fake messages in order to deceive the original intended recipient. This attempt at “cracking” the cipher is also known as an attack.
The following are example of some common attacks:
Chosen Ciphertext. Portions of the ciphertext are selected for trial decryption while having access to the corresponding decrypted plaintext
Known Plaintext. The attacker has a copy of the plaintext corresponding to the ciphertext
Chosen Plaintext. Chosen plaintext is encrypted and the output ciphertext is obtained
Ciphertext Only. Only the ciphertext is available

Incorrect Answers:
A: With a Known Plaintext attack, the attacker has a copy of the plaintext corresponding to the ciphertext. This is not what is described in the question.
C: With a Chosen-Ciphertext attack, the attacker has a copy of the plaintext corresponding to the ciphertext. This is not what is described in the question.
D: With a Plaintext-only attack, the attacker does not have the encrypted messages as stated in the question.

References:

Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 154

QUESTION 145
The RSA algorithm is an example of what type of cryptography?

A. Asymmetric Key.
B. Symmetric Key.
C. Secret Key.
D. Private Key.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RSA is a public key algorithm that is an example of asymmetric key algorithms. RSA is used for encryption, digital signatures, and key distribution.

Incorrect Answers:
B: RSA is not an example of symmetric key algorithms.
C: Secret Key cryptography is an encryption system where a common key is used to encrypt and decrypt the message. This is not the case in RSA.
D: RSA uses Private Keys for decryption, but it is not an example of Private Key cryptography.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 815, 831
http://www.webopedia.com/TERM/S/symmetric_key_cryptography.html

QUESTION 146
What algorithm was DES derived from?

A. Twofish.
B. Skipjack.
C. Brooks-Aldeman.
D. Lucifer.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Lucifer was adopted and modified by the U.S. National Security Agency (NSA) to establish the U.S. Data Encryption Standard (DES) in 1976.

Incorrect Answers:
A: Twofish is a symmetric block cipher, which was a candidate for being the basis of the Advanced Encryption Standard (AES). B: Skipjack is an algorithm that was used by Clipper Chip, which was used in the Escrowed Encryption Standard (EES). C: Brooks-Aldeman is not a valid algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 764, 809
Conrad, Eric, Seth Misenar, Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 250

QUESTION 147
What is a characteristic of using the Electronic Code Book mode of DES encryption?

A. A given block of plaintext and a given key will always produce the same ciphertext.
B. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
C. Individual characters are encoded by combining output from earlier encryption routines with plaintext.
D. The previous DES output is used as input.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
With Electronic Code Book (ECB) Mode, a 64-bit data block is entered into the algorithm with a key, and a block of ciphertext is produced. The same block of ciphertext will always result from a given block of plaintext and a given key.

Incorrect Answers:
B: This option refers to Cipher Block Chaining (CBC).
C: This option is not a characteristic of using the Electronic Code Book mode of DES encryption, as ECB allows for ciphertext to be produced from a given block of plaintext and a given key.
D: This option refers to Cipher Block Chaining (CBC).

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 800-807

QUESTION 148

Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use Hybrid Encryption Methods. What does this mean?

A. Use of public key encryption to secure a secret key, and message encryption using the secret key.
B. Use of the recipient's public key for encryption and decryption based on the recipient's private key.
C. Use of software encryption assisted by a hardware encryption accelerator.
D. Use of elliptic curve encryption.

Correct Answer: A
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
For large quantities of sensitive information, symmetric key encryption (using a secret key) is more efficient.
Public key cryptography uses two keys (public and private) generated by an asymmetric algorithm for protecting encryption keys and key distribution, and a secret key is generated by a symmetric algorithm and used for bulk encryption. Then there is a hybrid use of the two different algorithms: asymmetric and symmetric. Each algorithm has its pros and cons, so using them together can be the best of both worlds.
In the hybrid approach, the two technologies are used in a complementary manner, with each performing a different function. A symmetric algorithm creates keys used for encrypting bulk data, and an asymmetric algorithm creates keys used for automated key distribution.
When a symmetric key is used for bulk data encryption, this key is used to encrypt the message you want to send. When your friend gets the message you encrypted, you want him to be able to decrypt it, so you need to send him the necessary symmetric key to use to decrypt the message. You do not want this key to travel unprotected, because if the message were intercepted and the key were not protected, an evildoer could intercept the message that contains the necessary key to decrypt your message and read your information. If the symmetric key needed to decrypt your message is not protected, there is no use in encrypting the message in the first place. So we use an asymmetric algorithm to encrypt the symmetric key. Why do we use the symmetric key on the message and the asymmetric key on the symmetric key? The reason is that the asymmetric algorithm takes longer because the math is more complex. Because your message is most likely going to be longer than the length of the key, we use the faster algorithm (symmetric) on the message and the slower algorithm (asymmetric) on the key.

Incorrect Answers:
B: For large quantities of sensitive information, symmetric key encryption (using a secret key) is more efficient. Using public and private keys for encryption and decryption is asymmetric key encryption.
C: Software encryption is not an answer on its own. We need to determine what type of software encryption to use.
D: Elliptical curve cryptography (ECC) is a public key encryption technique. Symmetric key encryption is more efficient for large amounts of data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 793

QUESTION 149

Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.
B. The channels through which the information flows are secure.
C. The recipient's identity can be positively verified by the sender.
D. The sender of the message is the only other person with access to the recipient's private key.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
When information is encrypted using a public key, it can only be decrypted by using the associated private key. As the recipient is the only person with the private key, the recipient is the only person who can decrypt the message. This provides a form of authentication in that the recipient's identity can be positively verified by the sender. If the receiver replies to the message, the sender knows that the intended recipient received the message.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 784-785

QUESTION 150
Kerberos depends upon what encryption method?

A. Public Key cryptography.
B. Secret Key cryptography.
C. El Gamal cryptography.
D. Blowfish cryptography.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
During the Kerberos Authentication Process, the user and the KDC share a secret key, while the service and the KDC share a different secret key. Kerberos is, therefore, dependent on Secret Key cryptography.

Incorrect Answers:
A: Kerberos is dependent on Secret Key cryptography, not Public Key cryptography.
C: El Gamal is a public key algorithm that can be used for digital signatures, encryption, and key exchange. Kerberos is not, however, dependent on it.
D: Blowfish is a block cipher that works on 64-bit blocks of data. Kerberos is not, however, dependent on it.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213, 810, 818

QUESTION 151
Which of the following statements is TRUE about data encryption as a method of protecting data?

A. It should sometimes be used for password files
B. It is usually easily administered
C. It makes few demands on system resources
D. It requires careful key management

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The main challenge brought by improved security is that introducing encryption software also introduces management complexity, and in particular this means dealing with encryption keys.
An encryption key applies a set of complex algorithms to data and translates it into streams of seemingly random alphanumeric characters. There are two main types – private key (or symmetric) encryption and public key (or asymmetric) encryption.
In symmetric encryption, all users have access to one private key, which is used to encrypt and decrypt data held in storage media such as backup tapes and disk drives. Although considered generally secure, the downside is that there is only one key, which has to be shared with others to perform its function. Asymmetric encryption comprises two elements: a public key to encrypt data and a private key to decrypt data. The public key is used by the owner to encrypt information and can be given to third parties running a compatible application to enable them to send encrypted messages back.
Managing encryption keys effectively is vital. Unless the creation, secure storage, handling and deletion of encryption keys is carefully monitored, unauthorized parties can gain access to them and render them worthless. And if a key is lost, the data it protects becomes impossible to retrieve.

Incorrect Answers:
A: Data encryption should not 'sometimes' be used for password files; it should always be used.
B: It is not true that data encryption is usually easily administered; it is complicated.
C: It is not true that data encryption makes few demands on system resources; encrypting data requires significant processing power.

References:
http://www.computerweekly.com/feature/Encryption-key-management-is-vital-to-securing-enterprise-data-storage

QUESTION 152
Which type of algorithm is considered to have the highest strength per bit of key length of any of the asymmetric algorithms?

A. Rivest, Shamir, Adleman (RSA)
B. El Gamal
C. Elliptic Curve Cryptography (ECC)
D. Advanced Encryption Standard (AES)

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An elliptic curve cryptosystem (ECC) provides much of the same functionality RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency. ECC is more efficient than RSA and any other asymmetric algorithm.
Some devices have limited processing capacity, storage, power supply, and bandwidth, such as wireless devices and cellular telephones. With these types of devices, efficiency of resource use is very important. ECC provides encryption functionality, requiring a smaller percentage of the resources compared to RSA and other algorithms, so it is used in these types of devices.
In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device.

Incorrect Answers:
A: Elliptic Curve Cryptography (ECC) has a higher strength per bit of key length than RSA.
B: Elliptic Curve Cryptography (ECC) has a higher strength per bit of key length than El Gamal.
D: Elliptic Curve Cryptography (ECC) has a higher strength per bit of key length than AES.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 818-819

QUESTION 153
How many bits is the effective length of the key of the Data Encryption Standard algorithm?

A. 168
B. 128
C. 56
D. 64

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Data Encryption Standard (DES) has had a long and rich history within the computer community. NIST invited vendors to submit data encryption algorithms to be used as a cryptographic standard. IBM had already been developing encryption algorithms to protect financial transactions. In 1974, IBM's 128-bit algorithm, named Lucifer, was submitted and accepted. The NSA modified this algorithm to use a key size of 64 bits (with 8 bits used for parity, resulting in an effective key length of 56 bits) instead of the original 128 bits, and named it the Data Encryption Algorithm (DEA).
NOTE DEA is the algorithm that fulfills DES, which is really just a standard. So DES is the standard and DEA is the algorithm, but in the industry we usually just refer to it as DES. The CISSP exam may refer to the algorithm by either name, so remember both.

Incorrect Answers:
A: The Data Encryption Standard algorithm has an effective key length of 56 bits, not 168 bits.
B: The Data Encryption Standard algorithm has an effective key length of 56 bits, not 128 bits.
D: The Data Encryption Standard algorithm has an effective key length of 56 bits, not 64 bits.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 800

QUESTION 154
The primary purpose for using one-way hashing of user passwords within a password file is which of the following?

A. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
B. It prevents an unauthorized person from reading the password.
C. It minimizes the amount of storage required for user passwords.
D. It minimizes the amount of processing time used for encrypting passwords.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A one-way hash function performs a mathematical encryption operation on a password that cannot be reversed. This prevents an unauthorized person from reading the password.
Some systems and applications send passwords over the network in cleartext, but a majority of them do not anymore. Instead, the software performs a one-way hashing function on the password and sends only the resulting value to the authenticating system or service. The authenticating system has a file containing all users' password hash values, not the passwords themselves, and when the authenticating system is asked to verify a user's password, it compares the hashing value sent to what it has in its file.

Incorrect Answers:
A: One-way hashing of user passwords does not prevent an unauthorized person from trying multiple passwords in one logon attempt. This is not the purpose of one-way hashing.
C: One-way hashing of user passwords does not minimize the amount of storage required for user passwords; it increases it because a hashed password is typically much longer than the password itself.
D: One-way hashing of user passwords does not minimize the amount of processing time used for encrypting passwords.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1059

QUESTION 155
Which of the following issues is not addressed by digital signatures?

A. nonrepudiation
B. authentication
C. data integrity
D. denial-of-service

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Digital signatures offer no protection against denial-of-service attacks.
A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

A digital signature is a hash value that has been encrypted with the sender's private key.
If Kevin wants to ensure that the message he sends to Maureen is not modified and he wants her to be sure it came only from him, he can digitally sign the message. This means that a one-way hashing function would be run on the message, and then Kevin would encrypt that hash value with his private key. When Maureen receives the message, she will perform the hashing function on the message and come up with her own hash value. Then she will decrypt the sent hash value (digital signature) with Kevin's public key. She then compares the two values, and if they are the same, she can be sure the message was not altered during transmission. She is also sure the message came from Kevin because the value was encrypted with his private key. The hashing function ensures the integrity of the message, and the signing of the hash value provides authentication and nonrepudiation.

Incorrect Answers:
A: Digital signatures can be used to address the issue of nonrepudiation.
B: Digital signatures can be used to address the issue of authentication.
D: Digital signatures can be used to address the issue of data integrity.

References:
https://www.techopedia.com/definition/24841/denial-of-service-attack-dos
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 829

QUESTION 156
Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?
A. The use of good key generators.
B. The use of session keys.
C. Nothing can defend you against a brute force crypto key attack.
D. Algorithms that are immune to brute force key attacks.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
A session key is a single-use symmetric key that is used to encrypt messages between two users during a communication session.
If Tanya has a symmetric key she uses to always encrypt messages between Lance and herself, then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using encryption. However, using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If, on the other hand, a new symmetric key were generated each time Lance and Tanya wanted to communicate, it would be used only during their one dialogue and then destroyed. If they wanted to communicate an hour later, a new session key would be created and shared.
A session key provides more protection than static symmetric keys because it is valid for only one session between two computers. If an attacker were able to capture the session key, she would have a very small window of time to use it to try to decrypt messages being passed back and forth.

Incorrect Answers:
A: A strong encryption key offers no protection against brute force attacks. If the same key is always used, once an attacker obtains the key, he would be able to decrypt the data.
C: It is not true that nothing can defend you against a brute force crypto key attack. Using a different key every time is a good defense.
D: There are no algorithms that are immune to brute force key attacks. This is why it is a good idea to use a different key every time.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 798-799

QUESTION 157
The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?

A. 64 bits of data input results in 56 bits of encrypted output
B. 128 bit key with 8 bits used for parity
C. 64 bit blocks with a 64 bit total key length
D. 56 bits of data input results in 56 bits of encrypted output

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
DES is a symmetric block encryption algorithm. When 64-bit blocks of plaintext go in, 64-bit blocks of ciphertext come out. It is also a symmetric algorithm, meaning the same key is used for encryption and decryption. It uses a 64-bit key: 56 bits make up the true key, and 8 bits are used for parity.
When the DES algorithm is applied to data, it divides the message into blocks and operates on them one at a time. The blocks are put through 16 rounds of transposition and substitution functions. The order and type of transposition and substitution functions depend on the value of the key used with the algorithm. The result is 64-bit blocks of ciphertext

Incorrect Answers:
A: When 64-bit blocks of plaintext go in, 64-bit blocks of encrypted data come out.
B: DES uses a 64-bit key (not 128-bit): 56 bits make up the true key, and 8 bits are used for parity.
D: DES uses 64-bit blocks, not 56-bit.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 801

QUESTION 158
PGP uses which of the following to encrypt data?

A. An asymmetric encryption algorithm B.
A symmetric encryption algorithm
C. A symmetric key distribution system
D. An X.509 digital certificate

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Pretty Good Privacy (PGP) was designed by Phil Zimmerman as a freeware e-mail security program and was released in 1991. It was the first widespread public key encryption program.
PGP is a complete cryptosystem that uses cryptographic protection to protect e-mail and files. It can use RSA public key encryption for key management and use IDEA symmetric cipher for bulk encryption of data, although the user has the option of picking different types of algorithms for these functions.
PGP can provide confidentiality by using the IDEA encryption algorithm, integrity by using the MD5 hashing algorithm, authentication by using the public key certificates, and nonrepudiation by using cryptographically signed messages. PGP uses its own type of digital certificates rather than what is used in PKI, but they both have similar purposes.

Incorrect Answers:
A: PGP uses a symmetric encryption algorithm, not an asymmetric encryption algorithm to encrypt data.
C: PGP does not use a symmetric 'key distribution system' to encrypt data.
D: An X.509 digital certificate is used in asymmetric cryptography. PGP does not use asymmetric cryptography.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 850

QUESTION 159

A public key algorithm that does both encryption and digital signature is which of the following?

A. RSA
B. DES
C. IDEA
D. Diffie-Hellman

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RSA, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a public key algorithm that is the most popular when it comes to asymmetric algorithms. RSA is a worldwide de facto standard and can be used for digital signatures, key exchange, and encryption. It was developed in 1978 at MIT and provides authentication as well as key encryption.
One advantage of using RSA is that it can be used for encryption and digital signatures. Using its one-way function, RSA provides encryption and signature verification, and the inverse direction performs decryption and signature generation.

Incorrect Answers:
B: DES is a symmetric block encryption algorithm. It is not a public key algorithm.
C: IDEA is a symmetric block encryption algorithm. It is not a public key algorithm.
D: Diffie-Hellman is used for key distribution. It is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 815

QUESTION 160
Which of the following is NOT true of Secure Sockets Layer (SSL)?

A. By convention it uses 's-http://' instead of 'http://'.
B. Is the predecessor to the Transport Layer Security (TLS) protocol.
C. It was developed by Netscape.
D. It is used for transmitting private information, data, and documents over the Internet.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
By convention Secure Sockets Layer (SSL) uses “https://”. It does not use “s-http://”.

Incorrect Answers:
B: It is true that Secure Sockets Layer (SSL) is the predecessor to the Transport Layer Security (TLS) protocol.
C: It is true that Secure Sockets Layer (SSL) was developed by Netscape.
D: It is true that Secure Sockets Layer (SSL) is used for transmitting private information, data, and documents over the Internet.

QUESTION 161
The Physical Security domain focuses on three areas that are the basis to physically protecting enterprise's resources and sensitive information. Which of the following is NOT one of these areas?

A. Threats
B. Countermeasures
C. Vulnerabilities
D. Risks

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
“Risks” is not one of the three areas that the Physical Security domain focuses on.
The Physical Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise’s resources and sensitive information. These resources include personnel, the facility in which they work, and the data, equipment, support systems, and media with which they work. Physical security often refers to the measures taken to protect systems, buildings, and their related supporting infrastructure against threats that are associated with the physical environment.

Incorrect Answers:
A: Threats is one of the three areas that the Physical Security domain focuses on. Therefore, this answer is incorrect.
B: Countermeasures is one of the three areas that the Physical Security domain focuses on. Therefore, this answer is incorrect.
C: Vulnerabilities is one of the three areas that the Physical Security domain focuses on. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 451

QUESTION 162

Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard?

A. Twofish
B. Serpent
C. RC6
D. Rijndael

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
After DES was used as an encryption standard for over 20 years and it was cracked in a relatively short time once the necessary technology was available, NIST decided a new standard, the Advanced Encryption Standard (AES), needed to be put into place. In January 1997, NIST announced its request for AES candidates and outlined the requirements in FIPS PUB 197. AES was to be a symmetric block cipher supporting key sizes of 128, 192, and 256 bits. The following five algorithms were the finalists:

- MARS Developed by the IBM team that created Lucifer
- RC6 Developed by RSA Laboratories
- Serpent Developed by Ross Anderson, Eli Biham, and Lars Knudsen
- Twofish Developed by Counterpane Systems
- Rijndael Developed by Joan Daemen and Vincent Rijmen

Out of these contestants, Rijndael was chosen. The block sizes that Rijndael supports are 128, 192, and 256 bits.
Rijndael works well when implemented in software and hardware in a wide range of products and environments. It has low memory requirements and has been constructed to easily defend against timing attacks.
Rijndael was NIST's choice to replace DES. It is now the algorithm required to protect sensitive but unclassified U.S. government information.

Incorrect Answers:
A: Twofish was a finalist; however, Rijndael was selected by NIST for the new Advanced Encryption Standard.
B: Serpent was a finalist; however, Rijndael was selected by NIST for the new Advanced Encryption Standard.
C: RC6 was a finalist; however, Rijndael was selected by NIST for the new Advanced Encryption Standard.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 809

QUESTION 163
Compared to RSA, which of the following is true of Elliptic Curve Cryptography (ECC)?

A. It has been mathematically proved to be more secure.

B. It has been mathematically proved to be less secure.
C. It is believed to require longer key for equivalent security.
D. It is believed to require shorter keys for equivalent security.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An elliptic curve cryptosystem (ECC) provides much of the same functionality RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency. ECC is more efficient than RSA and any other asymmetric algorithm.
Some devices have limited processing capacity, storage, power supply, and bandwidth, such as wireless devices and cellular telephones. With these types of devices, efficiency of resource use is very important. ECC provides encryption functionality, requiring a smaller percentage of the resources compared to RSA and other algorithms, so it is used in these types of devices.
In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device.

Incorrect Answers:
A: ECC is not more secure than RSA; it just requires a shorter key length to provide equivalent security.
B: ECC is not less secure than RSA; it just requires a shorter key length to provide equivalent security.
C: ECC requires a shorter key length to provide equivalent security.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 818-819

QUESTION 164
Which of the following algorithms does NOT provide hashing?

A. SHA-1
B. MD2
C. RC4
D. MD5
Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
RC4 is a stream cipher; it does not provide hashing.
RC4 is one of the most commonly implemented stream ciphers. It has a variable key size, is used in the SSL protocol, and was (improperly) implemented in the 802.11 WEP protocol standard. RC4 was developed in 1987 by Ron Rivest and was considered a trade secret of RSA Data Security, Inc., until someone posted the source code on a mailing list. Since the source code was released nefariously, the stolen algorithm is sometimes implemented and referred to as ArcFour or ARC4 because the title RC4 is trademarked. The algorithm is very simple, fast, and efficient, which is why it became so popular. But because it has a low diffusion rate, it is subject to modification attacks. This is one reason that the new wireless security standard (IEEE 802.11i) moved from the RC4 algorithm to the AES algorithm.

Incorrect Answers:
A: SHA (Secure Hash Algorithm) produces a 160-bit hash value, or message digest. SHA was improved upon and renamed SHA-1.
B: MD2 (Message Digest 2) is a one-way hash function designed by Ron Rivest that creates a 128-bit message digest value.
D: MD5 (Message Digest 5) was also created by Ron Rivest and is the newer version of MD4. It still produces a 128-bit hash, but the algorithm is more complex, which makes it harder to break.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 810

QUESTION 165
Which of the following protocols that provide integrity and authentication for IPSec, can also provide non-repudiation in IPSec?

A. Authentication Header (AH)
B. Encapsulating Security Payload (ESP)
C. Secure Sockets Layer (SSL)
D. Secure Shell (SSH-2)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
IPSec is a standard that provides encryption, access control, non-repudiation, and authentication of messages over an IP.
The two main protocols of IPSec are the Authentication Header (AH) and the Encapsulating Security Payload (ESP.) The AH provides integrity, authentication, and non-repudiation. An ESP primarily provides encryption, but it can also provide limited authentication.
Incorrect Answers:
B: ESP provides encryption; it does not provide integrity, authentication or non-repudiation.
C: Secure Sockets Layer (SSL) is not part of IPSec.
D: Secure Shell (SSH-2) is not part of IPSec.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 161

QUESTION 166
Which of the following is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet?

A. Secure Electronic Transaction (SET)
B. MONDEX
C. Secure Shell (SSH-2)
D. Secure Hypertext Transfer Protocol (S-HTTP)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. SET has been waiting in the wings for full implementation and acceptance as a standard for quite some time. Although SET provides an effective way of transmitting credit card information, businesses and users do not see it as efficient because it requires more parties to coordinate their efforts, more software installation and configuration for each entity involved, and more effort and cost than the widely used SSL method.
SET is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet. The following entities would be involved with a SET transaction, which would require each of them to upgrade their software, and possibly their hardware:
▪ Issuer (cardholder's bank) The financial institution that provides a credit card to the individual. ▪
Cardholder The individual authorized to use a credit card.
▪ Merchant The entity providing goods.
▪ Acquirer (merchant's bank) The financial institution that processes payment cards. ▪
Payment gateway This processes the merchant payment. It may be an acquirer.

Incorrect Answers:
B: MONDEX is a payment system that uses currency stored on smart cards. This is not what is described in the question.
C: Secure Shell (SSH-2) was not developed to send encrypted credit card numbers over the Internet.
D: Secure Hypertext Transfer Protocol (S-HTTP) is an early standard for encrypting HTTP documents. S-HTTP was overtaken by SSL. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 856

QUESTION 167

Which of the following cryptographic attacks describes when the attacker has a copy of the plaintext and the corresponding ciphertext?

A. known plaintext
B. brute force
C. ciphertext only
D. chosen plaintext

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Cryptanalysis is the act of obtaining the plaintext or key from the ciphertext. Cryptanalysis is used to obtain valuable information and to pass on altered or fake messages in order to deceive the original intended recipient. This attempt at “cracking” the cipher is also known as an attack.
The following are example of some common attacks:
▪ Brute Force. Trying every possible combination of key patterns — the longer the key length, the more difficult it is to find the key with this method ▪
Known Plaintext. The attacker has a copy of the plaintext corresponding to the ciphertext
▪ Chosen Plaintext. Chosen plaintext is encrypted and the output ciphertext is obtained ▪
Ciphertext Only. Only the ciphertext is available

Incorrect Answers:
B: A Brute Force attack involves trying every possible combination of key patterns. This is not what is described in the question.
C: With a Ciphertext Only attack, only the ciphertext is available. The plaintext is not available.
D: In a Chosen Plaintext attack, chosen plaintext is encrypted and the output ciphertext is obtained. This is not what is described in the question.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 154

QUESTION 168
Which of the following is NOT a true statement regarding the implementation of the 3DES modes?

A. DES-EEE1 uses one key
B. DES-EEE2 uses two keys
C. DES-EEE3 uses three keys
D. DES-EDE2 uses two keys
Correct Answer: A

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
It is not true that DES-EEE1 uses one key.
3DES can work in different modes, and the mode chosen dictates the number of keys used and what functions are carried out:
- DES-EEE3 uses three different keys for encryption, and the data are encrypted, encrypted, encrypted.
- DES-EDE3 uses three different keys for encryption, and the data are encrypted, decrypted, encrypted.
- DES-EEE2 is the same as DES-EEE3, but uses only two keys, and the first and third encryption processes use the same key.
- DES-EDE2 is the same as DES-EDE3, but uses only two keys, and the first and third encryption processes use the same key.

Incorrect Answers:
B: It is true that DES-EEE2 uses two keys.
C: It is true that DES-EEE3 uses three keys.
D: It is true that DES-EDE2 uses two keys.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 808

QUESTION 169
Which one of the following is a key agreement protocol used to enable two entities to agree and generate a session key (secret key used for one session) over an insecure medium without any prior secrets or communications between the entities? The negotiated key will subsequently be used for message encryption using Symmetric Cryptography.

A. RSA
B. PKI
C. Diffie_Hellmann
D. 3DES

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Diffie–Hellman key exchange (D–H) is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such

as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Incorrect Answers:
A: RSA is not the key agreement protocol described in the question.
B: PKI is not the key agreement protocol described in the question.
D: 3DES is not the key agreement protocol described in the question.

References:
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

QUESTION 170
Which of the following ciphers is a subset on which the Vigenere polyalphabetic cipher was based on?

A. Caesar
B. The Jefferson disks
C. Enigma
D. SIGABA

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Julius Caesar (100–44 B.C.) developed a simple method of shifting letters of the alphabet. He simply shifted the alphabet by three positions.
Today, this technique seems too simplistic to be effective, but in the time of Julius Caesar, not very many people could read in the first place, so it provided a high level of protection. The Caesar cipher is an example of a monoalphabetic cipher. Once more people could read and reverse-engineer this type of encryption process, the cryptographers of that day increased the complexity by creating polyalphabetic ciphers.
In the 16th century in France, Blaise de Vigenere developed a polyalphabetic substitution cipher for Henry III. This was based on the Caesar cipher, but it increased the difficulty of the encryption and decryption process

Incorrect Answers:
B: The Vigenere polyalphabetic cipher is based on the Caesar cipher, not the Jefferson disks.
C: The Vigenere polyalphabetic cipher is based on the Caesar cipher, not Enigma.
D: The Vigenere polyalphabetic cipher is based on the Caesar cipher, not SIGABA.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 761-762

QUESTION 171
In a known plaintext attack, the cryptanalyst has knowledge of which of the following?
A. the ciphertext and the key
B. the plaintext and the secret key
C. both the plaintext and the associated ciphertext of several messages
D. the plaintext and the algorithm

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Cryptanalysis is the act of obtaining the plaintext or key from the ciphertext. Cryptanalysis is used to obtain valuable information and to pass on altered or fake messages in order to deceive the original intended recipient. This attempt at “cracking” the cipher is also known as an attack.

In a Known Plaintext attack, the attacker has both the plaintext and the associated ciphertext of several messages.

Incorrect Answers:
A: In a known plaintext attack, the attacker does not have the key.
B: In a known plaintext attack, the attacker does not have the secret key.
D: In a known plaintext attack, the attacker does not have the algorithm.

Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 154

QUESTION 172
What is the length of an MD5 message digest?

A. 128 bits B.
160 bits
C. 256 bits
D. varies depending upon the message size.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

MD5 is a message digest algorithm that was developed by Ronald Rivest in 1991. MD5 takes a message of an arbitrary length and generates a 128-bit message digest. In MD5, the message is processed in 512-bit blocks in four distinct rounds.
Incorrect Answers:
B: MD5 generates a 128-bit message digest, not 160-bit.
C: MD5 generates a 128-bit message digest, not 256-bit.
D: MD5 generates a 128-bit message digest regardless of the message size.

Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 153

QUESTION 173
The Secure Hash Algorithm (SHA-1) creates:

A. a fixed length message digest from a fixed length input message.
B. a variable length message digest from a variable length input message.
C. a fixed length message digest from a variable length input message.
D. a variable length message digest from a fixed length input message.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
SHA-1 was designed by NSA and published by NIST to be used with the Digital Signature Standard (DSS).
The Secure Hash Algorithm (SHA-1) computes a fixed length message digest from a variable length input message. This message digest is then processed by the DSA to either generate or verify the signature.
SHA-1 produces a message digest of 160 bits when any message less than 264 bits is used as an input.
SHA-1 has the following properties:
- It is computationally infeasible to find a message that corresponds to a given message digest.
- It is computationally infeasible to find two different messages that produce the same message digest.

For SHA-1, the length of the message is the number of bits in a message. Padding bits are added to the message to make the total length of the message, including padding, a multiple of 512.

Incorrect Answers:
A: SHA-1 creates a fixed length message digest from a variable length input message, not from a fixed length input message.
B: SHA-1 creates a fixed length message digest, not a variable length message digest.
D: SHA-1 creates a fixed length message digest, not a variable length message digest. The fixed length message digest is created from a variable length input message, not from a fixed length input message.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 152

QUESTION 174
The RSA Algorithm uses which mathematical concept as the basis of its encryption?

A. Geometry
B. 16-round ciphers
C. PI (3.14159...)
D. Two large prime numbers

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RSA is derived from the last names of its inventors, Rivest, Shamir, and Addleman.
This algorithm is based on the difficulty of factoring a number, N, which is the product of two large prime numbers. These numbers may be 200 digits each. Thus, the difficulty in obtaining the private key from the public key is a hard, one-way function that is equivalent to the difficulty of finding the prime factors of N.
In RSA, public and private keys are generated as follows:
▪ Choose two large prime numbers, p and q, of equal length, compute p3q 5 n, which is the public modulus.
▪ Choose a random public key, e, so that e and (p – 1)(q – 1) are relatively prime.
▪ Compute e x d = 1 mod (p – 1)(q – 1), where d is the private key. ▪
Thus, d = e–1 mod [(p – 1)(q – 1)]

From these calculations, (d, n) is the private key and (e, n) is the public key.

Incorrect Answers:
A: The RSA Algorithm does not use Geometry as the basis of its encryption.
B: The RSA Algorithm does not use 16-round ciphers as the basis of its encryption.
C: The RSA Algorithm does not use PI as the basis of its encryption.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 148

QUESTION 175
The Clipper Chip utilizes which concept in public key cryptography?

A. Substitution

B. Key Escrow
C. An undefined algorithm
D. Super strong encryption

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Clipper chip was a chipset that was developed and promoted by the United States National Security Agency (NSA) as an encryption device, with a built-in backdoor, intended to be adopted by telecommunications companies for voice transmission. It was announced in 1993 and by 1996 was entirely defunct.
The Clipper chip used a data encryption algorithm called Skipjack to transmit information and the Diffie-Hellman key exchange-algorithm to distribute the cryptokeys between the peers.
At the heart of the concept was key escrow. In the factory, any new telephone or other device with a Clipper chip would be given a cryptographic key, that would then be provided to the government in escrow. If government agencies "established their authority" to listen to a communication, then the key would be given to those government agencies, who could then decrypt all data transmitted by that particular telephone. The newly formed Electronic Frontier Foundation preferred the term "key surrender" to emphasize what they alleged was really occurring.

Incorrect Answers:
A: Substitution is not the concept used by the Clipper Chip.
C: Clipper chip does not use an undefined algorithm although the Skipjack algorithm was initially classed as ‘Secret’ by the NSA.
D: The Clipper chip does not use ‘Super Strong’ encryption. The encryption key was 80-bit.

References:
https://en.wikipedia.org/wiki/Clipper_chip

QUESTION 176
Which of the following are suitable protocols for securing VPN connections at the lower layers of the OSI model?

A. S/MIME and SSH
B. TLS and SSL
C. IPsec and L2TP
D. PKCS#10 and X.509

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Layer 2 Tunneling Protocol (L2TP) is a combination of PPTP and the earlier Layer 2 Forwarding Protocol (L2F) that works at the Data Link Layer like PPTP. It has become an accepted tunneling standard for VPNs.
IPSec operates at the Network Layer and it enables multiple and simultaneous tunnels. IPSec has the functionality to encrypt and authenticate IP data. It is built into the new IPv6 standard, and is used as an add-on to the current IPv4. While PPTP and L2TP are aimed more at dial-up VPNs, IPSec focuses more on network-tonetwork connectivity.

Incorrect Answers:
A: S/MIME and SSH run in the application layer (layer 7) of the OSI model. This is the highest level, not a lower level.
B: TLS runs in layer 6 of the OSI model and SSL runs in layer 4. L2TP and IPSEC run in layers 2 and 3 respectively.
D: PKCS#10 and X.509 alone do not provide VPN connections; they are used by other protocols.

QUESTION 177
What is the role of IKE within the IPsec protocol?

A. peer authentication and key exchange
B. data encryption
C. data signature
D. enforcing quality of service

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The main protocols that make up the IPSec suite and their basic functionality are as follows:
▪ Authentication Header (AH) provides data integrity, data origin authentication, and protection from replay attacks.
▪ Encapsulating Security Payload (ESP) provides confidentiality, data-origin authentication, and data integrity.
▪ Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for security association creation and key exchange. ▪ Internet Key Exchange (IKE) provides authenticated keying material for use with ISAKMP

Incorrect Answers:
B: The IPsec protocol uses Encapsulating Security Payload (ESP) for encryption, not IKE.
C: The IPSec protocol uses data signatures to provide data integrity. IKE is not used for signing the data packets.
D: The IPsec protocol does not enforce quality of service.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 705

QUESTION 178
In which phase of Internet Key Exchange (IKE) protocol is peer authentication performed?

A. Pre Initialization Phase

B. Phase 1
C. Phase 2
D. No peer authentication is performed

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
When two computers (peers) use IPsec to communicate, they create two kinds of security associations. In the first, called main mode or phase one, the peers mutually authenticate themselves to each other, thus establishing trust between the computers. In the second, called quick mode or phase two, the peers will negotiate the particulars of the security association, including how they will digitally sign and encrypt traffic between them.

Incorrect Answers:
A: The phase in which peer authentication is performed is not known as the Pre Initialization Phase. C: Peer authentication is performed in phase 1, not phase 2. D: It is not true that no peer authentication is performed.

References:
https://technet.microsoft.com/en-us/library/cc512617.aspx

QUESTION 179
What is NOT an authentication method within IKE and IPsec?

A. CHAP
B. Pre shared key
C. certificate based authentication
D. Public key authentication

Correct Answer: A

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
CHAP (Challenge Handshake Authentication Protocol) is not used within IKE and IPSec.
Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication - either pre-shared or distributed using DNS and a Diffie–Hellman key exchange - to set up a shared session secret from which cryptographic keys are derived.
IKE phase one's purpose is to establish a secure authenticated communication channel by using the Diffie–Hellman key exchange algorithm to generate a shared secret key to encrypt further IKE communications. This negotiation results in one single bi-directional ISAKMP Security Association (SA). The authentication can be performed using either pre-shared key (shared secret), signatures, or public key encryption.

Incorrect Answers:
B: Pre-shared key is an authentication method that can be used within IKE and IPsec.
C: Certificate-based authentication is an authentication method that can be used within IKE and IPsec.
D: Public key authentication is an authentication method that can be used within IKE and IPsec.

References:
https://en.wikipedia.org/wiki/Internet_Key_Exchange

QUESTION 180
What is NOT true with pre shared key authentication within IKE / IPsec protocol?

A. Pre shared key authentication is normally based on simple passwords
B. Needs a Public Key Infrastructure (PKI) to work
C. IKE is used to setup Security Associations
D. IKE builds upon the Oakley protocol and the ISAKMP protocol.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A pre-shared key is simply a string of characters known to both parties. When configuring a VPN using IPSec with pre-shared keys for authentication, the preshared key is entered into the configuration of the VPN device at each end of the VPN.
IKE can use certificate-based authentication using certificates from a PKI *or* it can use pre-shared keys. When using pre-shared keys, you do not need a PKI.

Incorrect Answers:
A: It is true that pre-shared key authentication is normally based on simple passwords.
C: It is true that IKE is used to setup Security Associations.
D: It is true that IKE builds upon the Oakley protocol and the ISAKMP protocol.

References:
https://en.wikipedia.org/wiki/Internet_Key_Exchange

QUESTION 181
In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?
A. Subordinate CA
B. Top Level CA
C. Big CA
D. Master CA

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Public key infrastructure (PKI) consists of programs, data formats, procedures, communication protocols, security policies, and public key cryptographic mechanisms working in a comprehensive manner to enable a wide range of dispersed people to communicate in a secure and predictable fashion. In other words, a PKI establishes a level of trust within an environment. PKI is an ISO authentication framework that uses public key cryptography and the X.509 standard. Each person who wants to participate in a PKI requires a digital certificate, which is a credential that contains the public key for that individual along with other identifying information. The certificate is created and signed (digital signature) by a trusted third party, which is a certificate authority (CA).
The certificate authority (CA) is the entity that issues the certificates. CA's are often organized into hierarchies with the root CA at the top of the hierarchy and intermediate or subordinate CA's below the root. As the root CA is 'top of the tree', it is often referred to as the Top-Level CA.

Incorrect Answers:
A: A Subordinate CA is below the root or top-level CA.
C: A Root CA is not known as a Big CA.
D: A Root CA is not known as a Master CA.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 833

QUESTION 182
What is the primary role of cross certification?

A. Creating trust between different PKIs
B. Build an overall PKI hierarchy
C. set up direct trust to a second root CA
D. Prevent the nullification of user certificates by CA certificate revocation

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
More and more organizations are setting up their own internal PKIs. When these independent PKIs need to interconnect to allow for secure communication to take place (either between departments or between different companies), there must be a way for the two root CAs to trust each other. The two CAs do not have a CA above them they can both trust, so they must carry out cross certification. A cross certification is the process undertaken by CAs to establish a trust relationship in which they rely upon each other's digital certificates and public keys as if they had issued them themselves. When this is set up, a CA for one company can validate digital certificates from the other company and vice versa.

Incorrect Answers:
B: Building an overall PKI hierarchy is not the primary purpose of cross certification. Cross certification is used to create a trust between different PKIs or PKI hierarchies.
C: Cross certification does not set up a direct trust to a second root CA; it creates trusts between two PKIs (this includes all CA's in each hierarchy).
D: Preventing the nullification of user certificates by CA certificate revocation is not the purpose of cross certification. Certificate revocation should nullify user certificates or at least render them untrusted.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 835

QUESTION 183
What kind of encryption is realized in the S/MIME-standard?

A. Asymmetric encryption scheme
B. Password based encryption scheme
C. Public key based, hybrid encryption scheme
D. Elliptic curve based encryption

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Secure MIME (S/MIME) is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions. S/MIME extends the MIME standard by allowing for the encryption of e-mail and attachments. The encryption and hashing algorithms can be specified by the user of the mail package, instead of having it dictated to them. S/MIME follows the Public Key Cryptography Standards (PKCS). S/MIME provides confidentiality through encryption algorithms, integrity through hashing algorithms, authentication through the use of X.509 public key certificates, and nonrepudiation through cryptographically signed message digests.
A user that sends a message with confidential information can keep the contents private while it travels to its destination by using message encryption. For message encryption, a symmetric algorithm (DES, 3DES, or in older implementations RC2) is used to encrypt the message data. The key used for this process is a one-time bulk key generated at the email client. The recipient of the encrypted message needs the same symmetric key to decrypt the data, so the key needs to be communicated to the recipient in a secure manner. To accomplish that, an asymmetric key algorithm (RSA or Diffie-Hellman) is used to encrypt and securely exchange the symmetric key. The key used for this part of the message encryption process is the recipient's public key. When the recipient receives the encrypted message, he will use his private key to decrypt the symmetric key, which in turn is used to decrypt the message data.
As you can see, this type of message encryption uses a hybrid system, which means it uses both symmetric and asymmetric algorithms. The reason for not using the public key system to encrypt the data directly is that it requires a lot of CPU resources; symmetric encryption is much faster than asymmetric encryption. Only the content of a message is encrypted; the header of the message is not encrypted so mail gateways can read addressing information and forward the message accordingly.

Incorrect Answers:
A: The S/MIME-standard does not use asymmetric encryption to encrypt the message; for message encryption, a symmetric algorithm is used. Asymmetric encryption is used to encrypt the symmetric key.
B: The S/MIME-standard does not use a password based encryption scheme.
D: The S/MIME-standard does not use Elliptic curve based encryption.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 850
http://www.techexams.net/technotes/securityplus/emailsecurity.shtml

QUESTION 184
What is the main problem of the renewal of a root CA certificate?

A. It requires key recovery of all end user keys
B. It requires the authentic distribution of the new root CA certificate to all PKI participants
C. It requires the collection of the old root CA certificates from all the users
D. It requires issuance of the new root CA certificate

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Every entity (user, computer, application, network device) that has a certificate from a PKI trusts other entities with certificates issued by the same PKI because they all trust the root Certificate Authority (CA). This trust is ensured because every entity has a copy of the root CA's public certificate.
If you want to change or renew the root CA certificate, to maintain the trust, the new certificate must be distributed to every entity that has a certificate from the PKI.

Incorrect Answers:
A: Renewing a root CA certificate does not require key recovery of all end user keys.
C: Renewing a root CA certificate does not require the collection of the old root CA certificates from all the users; the root certificates will just be invalid because they will be out-of-date.
D: Issuance of the new root CA certificate is not a problem; it is not a difficult procedure. The distribution of the certificate to all PKI participants is more of a challenge.

QUESTION 185
Critical areas should be lighted:

A. Eight feet high and two feet out.
B. Eight feet high and four feet out.
C. Ten feet high and four feet out.
D. Ten feet high and six feet out.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Critical areas should be lighted eight feet high and two feet out.
The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high and use two foot-candles, which is a unit that represents the illumination power of an individual light.

Incorrect Answers:
A: Critical areas should be lighted eight feet high and two feet out, not eight feet high and four feet out. Therefore, this answer is incorrect.
B: Critical areas should be lighted eight feet high and two feet out, not ten feet high and four feet out. Therefore, this answer is incorrect.
D: Critical areas should be lighted eight feet high and two feet out, not ten feet high and six feet out. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1365

QUESTION 186
What attribute is included in a X.509-certificate?

A. Distinguished name of the subject
B. Telephone number of the department
C. secret key of the issuing CA
D. the key pair of the certificate holder

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
An X.509 certificate contains information about the identity to which a certificate is issued and the identity that issued it. Standard information in an X.509 certificate includes:
- Version – which X.509 version applies to the certificate (which indicates what data the certificate must include)
- Serial number – the identity creating the certificate must assign it a serial number that distinguishes it from other certificates
- Algorithm information – the algorithm used by the issuer to sign the certificate
- Issuer distinguished name – the name of the entity issuing the certificate
- Validity period of the certificate – start/end date and time
- Subject distinguished name – the name of the identity the certificate is issued to
- Subject public key information – the public key associated with the identity

Extensions (optional)

Incorrect Answers:
B: The telephone number of the department is not included in an X509 certificate.
C: The secret key of the issuing CA is not included in an X509 certificate. The secret key is the private key which is never distributed.
D: The key pair of the certificate holder is not included in an X509 certificate. A key pair includes a private key which is kept private.

References:
http://searchsecurity.techtarget.com/definition/X509-certificate

QUESTION 187
Which of the following choices is a valid Public Key Cryptography Standard (PKCS) addressing RSA?

A. PKCS #17799
B. PKCS-RSA

C. PKCS#1
D. PKCS#11

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In cryptography, PKCS #1 is the first of a family of standards called Public-Key Cryptography Standards (PKCS), published by RSA Laboratories. It provides the basic definitions of and recommendations for implementing the RSA algorithm for public-key cryptography. It defines the mathematical properties of public and private keys, primitive operations for encryption and signatures, secure cryptographic schemes, and related ASN.1 syntax representations.

Incorrect Answers:
A: PKCS #17799 is not a valid Public Key Cryptography Standard (PKCS) addressing RSA.
B: PKCS-RSA is not a valid Public Key Cryptography Standard (PKCS) addressing RSA.
D: PKCS#11 is not a valid Public Key Cryptography Standard (PKCS) addressing RSA.
References:
https://en.wikipedia.org/wiki/PKCS_1

QUESTION 188
The environment that must be protected includes all personnel, equipment, data, communication devices, power supply and wiring. The necessary level of protection depends on the value of the data, the computer systems, and the company assets within the facility. The value of these items can be determined by what type of analysis?

A. Critical-channel analysis
B. Covert channel analysis
C. Critical-path analysis
D. Critical-conduit analysis

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The value of items to be protected can be determined by a critical-path analysis. The critical-path analysis lists all pieces of an environment and how they interact.

Incorrect Answers:

A: Critical-channel analysis is not the correct term for the analysis described in the question. Therefore, this answer is incorrect.
B: A covert channel is a way for an entity to receive information in an unauthorized manner. Covert channel analysis is used to determine where covert channels exist. This is not the analysis described in the question. Therefore, this answer is incorrect.
D: Critical-conduit analysis is not the correct term for the analysis described in the question. Therefore, this answer is incorrect.

QUESTION 189
The DES algorithm is an example of what type of cryptography?

A. Secret Key
B. Two-key
C. Asymmetric Key
D. Public Key

Correct Answer: A
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
DES is a symmetric algorithm. This means that the same key is used for encryption and decryption. This is also a definition for Secret Key cryptography.

Incorrect Answers:
B: This is not a valid cryptography term.
C: DES is a symmetric algorithm, and can therefore not be an example of Asymmetric Key cryptography.
D: Public Key cryptography makes use of asymmetric key algorithms, whereas DES is a symmetric algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 801, 831

QUESTION 190
Which of the following encryption methods is known to be unbreakable?

A. Symmetric ciphers.
B. DES codebooks.
C. One-time pads.
D. Elliptic Curve Cryptography.

Correct Answer: C

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
- The one-time pad encryption scheme is considered unbreakable only if:
- The pad is used only one time.
- The pad is as long as the message.
- The pad is securely distributed and protected at its destination.

The pad is made up of truly random values.

Incorrect Answers:
A, B: Symmetric ciphers and DES electronic code books are part of symmetric encryption, which are susceptible to brute force and cryptanalysis attacks.
D: Elliptic curve cryptography is not known to be unbreakable, as it is susceptible to a modified Shor's algorithm for solving the discrete logarithm problem on elliptic curves.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 771-773
http://www.encryptionanddecryption.com/encryption/symmetric_encryption.html
https://en.wikipedia.org/wiki/Elliptic_curve_cryptography#Security

QUESTION 191
Which of the following questions is LESS likely to help in assessing physical access controls?

A. Does management regularly review the list of persons with physical access to sensitive facilities?
B. Is the operating system configured to prevent circumvention of the security software and application controls?
C. Are keys or other access devices needed to enter the computer room and media library?
D. Are visitors to sensitive areas signed in and escorted?

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Configuring an operating system to prevent circumvention of the security software and application controls is an example of configuring technical controls, not physical controls.

Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Physical access to facilities is a physical control. Asking about regularly reviews of the list of persons with physical access to sensitive facilities will help in assessing physical access controls. Therefore, this answer is incorrect.
C: Keys and access devices are examples of physical controls. Asking if they are required to enter the computer room and media library will help in assessing physical access controls. Therefore, this answer is incorrect.
D: Escorting a visitor is an example of a physical control. Asking if this is required to enter sensitive areas will help in assessing physical access controls. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28

QUESTION 192
Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

A. Wave pattern motion detectors
B. Capacitance detectors
C. Field-powered devices
D. Audio detectors

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A capacitance detector, emits a measurable magnetic field. The detector monitors this magnetic field, and an alarm sounds if the field is disrupted. These devices are usually used to protect specific objects (artwork, cabinets, or a safe) versus protecting a whole room or area.
An electrostatic IDS creates an electrostatic magnetic field, which is just an electric field associated with static electric charges. All objects have a static electric charge. They are all made up of many subatomic particles, and when everything is stable and static, these particles constitute one holistic electric charge. This means there is a balance between the electric capacitance and inductance. Now, if an intruder enters the area, his subatomic particles will mess up this balance in the electrostatic field, causing a capacitance change, and an alarm will sound.

Incorrect Answers:

A: Wave pattern motion detectors are used overall room security monitoring. Therefore, this answer is incorrect.
C: Field-powered devices are not intrusion detection devices. Field-powered device refers to a type of system-sensing proximity card. Therefore, this answer is incorrect.
D: Audio detectors are used overall room security monitoring. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 496
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 850

QUESTION 193
Which of the following Kerberos components holds all users' and services' cryptographic keys?

A. The Key Distribution Service
B. The Authentication Service
C. The Key Distribution Center
D. The Key Granting Service

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Key Distribution Center (KDC) is the most important component within a Kerberos environment as it holds all users' and services' secret keys.

Incorrect Answers:
A: Key Distribution Service is not a valid Kerberos term.
B: The authentication service is a part of the KDC that authenticates a principal. It does not hold all users' and services' cryptographic keys
D: Key Granting Service is not a valid Kerberos term.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213

QUESTION 194
There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?

A. public keys
B. private keys

C. public-key certificates
D. private-key certificates

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Public Key describes a system that uses certificates or the underlying public key cryptography on which the system is based.
In the traditional public key model, clients are issued credentials or "certificates" by a Certificate Authority (CA). The CA is a trusted third party. Public key certificates contain the user's name, the expiration date of the certificate etc. The most common certificate format is X.509. Public key credentials in the form of certificates and public-private key pairs can provide a strong distributed authentication system.
The Kerberos and public key trust models are very similar. A Kerberos ticket is analogous to a public key certificate (a Kerberos ticket is supplied to provide access to resources). However, Kerberos tickets usually have lifetimes measured in days or hours rather than months or years.

Incorrect Answers:
A: Kerberos tickets do not actually contain public keys. They use symmetric cryptography which uses one shared key instead of asymmetric cryptography which uses public-private key pairs.
B: Kerberos tickets do not contain private keys. They use symmetric cryptography which uses one shared key instead of asymmetric cryptography which uses public-private key pairs.
D: Private-key certificates are always kept by the authentication provider; they are never distributed to subjects that require access to resources. The public key is given to the subject to provide access to a resource in a similar way to a Kerberos ticket.

References:
Tipton, Harold F. and Micki Krause, *Information Security Management Handbook*, 5th Edition, Auerbach Publications, Boca Raton, 2006, p. 1438

QUESTION 195
Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is NOT a component that achieves this type of security?

A. Administrative control mechanisms
B. Integrity control mechanisms
C. Technical control mechanisms
D. Physical control mechanisms

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Integrity controls are not one of the three defined security control types.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Security procedures are an example of administrative controls. Therefore, this answer is incorrect.
C: An intrusion detection system is an example of technical controls. Therefore, this answer is incorrect.
D: The facility construction, fire and water protection are examples of physical controls. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28

QUESTION 196
Which of the following is TRUE about digital certificate?

A. It is the same as digital signature proving Integrity and Authenticity of the data
B. Electronic credential proving that the person the certificate was issued to is who they claim to be.
C. You can only get digital certificate from Verisign, RSA if you wish to prove the key belong to a specific user.
D. Can't contain geography data such as country for example.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Each person who wants to participate in a PKI requires a digital certificate, which is a credential that contains the public key for that individual along with other identifying information. The certificate is created and signed (digital signature) by a trusted third party, which is a certificate authority (CA). When the CA signs the certificate, it binds the individual’s identity to the public key, and the CA takes liability for the authenticity of that individual. It is this trusted third party (the CA) that allows people who have never met to authenticate to each other and to communicate in a secure method. If Kevin has never met Dave but would like to communicate securely with him, and they both trust the same CA, then Kevin could retrieve Dave’s digital certificate and start the process.

Incorrect Answers:
A: A digital certificate is not the same as a digital signature proving Integrity and Authenticity of the data. A digital certificate binds a key to an identity.

C: It is not true that you can only get a digital certificate from Verisign, RSA if you wish to prove the key belong to a specific user; you can get a digital certificate from any CA. The CA needs to be trusted however for the certificate to be effective. The CA can be one of many 'public' CAs or it can be part of a private PKI.
D: A digital certificate can contain geography data such as country for example.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 834

QUESTION 197
What kind of encryption technology does SSL utilize?

A. Secret or Symmetric key
B. Hybrid (both Symmetric and Asymmetric)
C. Public Key
D. Private Key

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
SSL uses asymmetric encryption to securely share a key. That key is then used for symmetric encryption to encrypt the data.

IPsec and SSL use asymmetric encryption to establish the encryption protocol when the session starts and then to securely exchange a private key used during the session. This private key is similar to the single secret key used in symmetric encryption.

Asymmetric encryption uses a key pair -- both a public and a private one -- for encryption. The sender uses the receiver's public key to encrypt the data and the receiver uses their private key to decrypt it. The transmission is secure because the recipient always has the private key in their possession and never exposes it by sending it over a public connection, such as the Internet.
There is a catch to using asymmetric encryption. It runs about 1,000 times slower than symmetric encryption and eats up just as much processing power, straining already overburdened servers. That means asymmetric encryption is only used (by IPsec and SSL) to create an initial and secure encrypted connection to exchange a private key. Then, that key is used to create a shared secret, or session key, that is only good during the session when the two hosts are connected.

Incorrect Answers:
A: SSL uses both symmetric and asymmetric encryption, not just symmetric encryption.
C: SSL does not use only public key encryption; shared key (symmetric) encryption is also used.
D: SSL does not use private key encryption. Initially, encryption is performed using public keys and decryption is performed using private keys (asymmetric). Then both encryption and decryption are performed using a shared key (symmetric).

References:
http://searchsecurity.techtarget.com/answer/How-IPsec-and-SSL-TLS-use-symmetric-and-asymmetric-encryption

QUESTION 198
What is the name of a one way transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string? Such a transformation cannot be reversed.

A. One-way hash
B. DES
C. Transposition
D. Substitution

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data is often called the *message*, and the hash value is often called the *message digest* or simply the *digest*.
The ideal cryptographic hash function has four main properties:
▪ it is easy to compute the hash value for any given message ▪ it is infeasible to generate a message from its hash ▪ it is infeasible to modify a message without changing the hash ▪ it is infeasible to find two different messages with the same hash.
▪ Most cryptographic hash functions are designed to take a string of any length as input and produce a fixed-length hash value.

Incorrect Answers:
B: Data Encryption Standard (DES) is a symmetric block cipher. Data encrypted using DES can be decrypted using the symmetric key.
C: A transposition cipher does not replace the original text with different text, but rather moves the original values around. This encryption can be reversed and does not produce a fixed length output.
D: A substitution cipher replaces bits, characters, or blocks of characters with different bits, characters, or blocks. This encryption can be reversed and does not produce a fixed length output.

References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 199

Which of the following is NOT an asymmetric key algorithm?

A. RSA
B. Elliptic Curve Cryptosystem (ECC)
C. El Gamal
D. Data Encryption Standard (DES)

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Data Encryption Standard (DES) is not an asymmetric key algorithm; it's a symmetric key algorithm.
DES is a symmetric block encryption algorithm. When 64-bit blocks of plaintext go in, 64-bit blocks of ciphertext come out. It is also a symmetric algorithm, meaning the same key is used for encryption and decryption. It uses a 64-bit key: 56 bits make up the true key, and 8 bits are used for parity. When the DES algorithm is applied to data, it divides the message into blocks and operates on them one at a time. The blocks are put through 16 rounds of transposition and substitution functions. The order and type of transposition and substitution functions depend on the value of the key used with the algorithm. The result is 64-bit blocks of ciphertext.

Incorrect Answers:
A: RSA is an asymmetric key algorithm.
B: Elliptic Curve Cryptosystem (ECC) is an asymmetric key algorithm.
C: El Gamal is an asymmetric key algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 801

QUESTION 200
Which of the following is NOT a symmetric key algorithm?
A. Blowfish
B. Digital Signature Standard (DSS)
C. Triple DES (3DES)
D. RC5

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Digital Signature Standard (DSS) is not a symmetric key algorithm; it is an asymmetric key algorithm.
Because digital signatures are so important in proving who sent which messages, the U.S. government decided to establish standards pertaining to their functions and acceptable use. In 1991, NIST proposed a federal standard called the Digital Signature Standard (DSS). It was developed for federal departments and agencies, but most vendors also designed their products to meet these specifications. The federal government requires its departments to use DSA, RSA, or the elliptic curve digital signature algorithm (ECDSA) and SHA. SHA creates a 160-bit message digest output, which is then inputted into one of the three mentioned digital signature algorithms. SHA is used to ensure the integrity of the message, and the other algorithms are used to digitally sign the message. This is an example of how two different algorithms are combined to provide the right combination of security services. RSA and DSA are the best known and most widely used digital signature algorithms. DSA was developed by the NSA. Unlike RSA, DSA can be used only for digital signatures, and DSA is slower than RSA in signature verification. RSA can be used for digital signatures, encryption, and secure distribution of symmetric keys.

Incorrect Answers:
A: Blowfish is a block symmetric cipher that uses 64-bit block sizes and variable-length keys.
C: Triple DES is a symmetric cipher that applies DES three times to each block of data during the encryption process.
D: RC5 is a block symmetric cipher that uses variable block sizes (32, 64, 128) and variable-length key sizes (0–2040).

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 832

QUESTION 201
Which of the following asymmetric encryption algorithms is based on the difficulty of factoring LARGE numbers?

A. El Gamal
B. Elliptic Curve Cryptosystems (ECCs)
C. RSA
D. International Data Encryption Algorithm (IDEA)

Correct Answer: C
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
RSA is derived from the last names of its inventors, Rivest, Shamir, and Addleman.
This algorithm is based on the difficulty of factoring a number, N, which is the product of two large prime numbers. These numbers may be 200 digits each. Thus, the difficulty in obtaining the private key from the public key is a hard, one-way function that is equivalent to the difficulty of finding the prime factors of N.
In RSA, public and private keys are generated as follows:
- Choose two large prime numbers, p and q, of equal length, compute p3q 5 n, which is the public modulus.
- Choose a random public key, e, so that e and (p – 1)(q – 1) are relatively prime.

▪ Compute e x d = 1 mod (p – 1)(q – 1), where d is the private key. ▪
Thus, d = e–1 mod [(p – 1)(q – 1)]

From these calculations, (d, n) is the private key and (e, n) is the public key.

Incorrect Answers:
A: El Gamal is based not on the difficulty of factoring large numbers but on calculating discrete logarithms in a finite field.
B: Elliptic Curve Cryptosystems (ECCs) are not based on the difficulty of factoring large numbers.
D: International Data Encryption Algorithm (IDEA) is not based on the difficulty of factoring large numbers.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 148

QUESTION 202
The Diffie-Hellman algorithm is primarily used to provide which of the following?

A. Confidentiality
B. Key Agreement
C. Integrity
D. Non-repudiation

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Diffie–Hellman key exchange (D–H) is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
Incorrect Answers:
A: The Diffie-Hellman algorithm is not primarily used to provide confidentiality.
C: The Diffie-Hellman algorithm is not primarily used to provide integrity.
D: The Diffie-Hellman algorithm is not primarily used to provide non-repudiation.

References:
https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

QUESTION 203
FIPS-140 is a standard for the security of which of the following?

A. Cryptographic service providers
B. Smartcards
C. Hardware and software cryptographic modules
D. Hardware security modules

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The National Institute of Standards and Technology (NIST) issues the 140 Publication Series to coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government. FIPS 140 does not purport to provide sufficient conditions to guarantee that a module conforming to its requirements is secure, still less that a system built using such modules is secure. The requirements cover not only the cryptographic modules themselves but also their documentation and (at the highest security level) some aspects of the comments contained in the source code.

Incorrect Answers:
A: FIPS-140 is not a standard for cryptographic service providers.
B: FIPS-140 is not a standard for smartcards.
D: FIPS-140 is not a standard for hardware security modules.

References:
https://en.wikipedia.org/wiki/FIPS_140

QUESTION 204

Which of the following can best define the "revocation request grace period"?

A. The period of time allotted within which the user must make a revocation request upon a revocation reason
B. Minimum response time for performing a revocation by the CA
C. Maximum response time for performing a revocation by the CA
D. Time period between the arrival of a revocation request and the publication of the revocation information

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Occasionally, a certificate authority needs to revoke a certificate. This might occur for one of the following reasons: ▪
The certificate was compromised.
▪ The certificate was erroneously issued.
▪ The details of the certificate changed. ▪
The security association changed.

The revocation request grace period is the maximum response time within which a CA will perform any requested revocation. This is defined in the certificate practice statement (CPS). The CPS states the practices a CA employs when issuing or managing certificates.

Incorrect Answers:
A: The revocation request grace period is not the period of time allotted within which the user must make a revocation request upon a revocation reason.
B: The revocation request grace period is the maximum response time, not the minimum response time within which a CA will perform any requested revocation.
D: The revocation request grace period is not the period of time between the arrival of a revocation request and the publication of the revocation information. Publication of a certificate revocation list does not always happen as soon as a certificate has been revoked.

QUESTION 205
Which is NOT a suitable method for distributing certificate revocation information?

A. CA revocation mailing list
B. Delta CRL
C. OCSP (online certificate status protocol)
D. Distribution point CRL

Correct Answer: A

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A CA revocation mailing list is NOT a suitable method for distributing certificate revocation information.
There are several mechanisms to represent revocation information; RFC 2459 defines one such method. This method involves each CA periodically issuing a signed data structure called a certificate revocation list (CRL). A CRL is a time stamped list identifying revoked certificates, which is signed by a CA and made freely available in a public repository.
There are several types of CRLs: full CRLs (also known as base CRLs), delta CRLs, and CRL Distribution Points (CDPs). Full CRLs contain the status of all certificates. Delta CRLs contain only the status of all certificates that have changed status between the issuance the last Base CRL.
CRL Distribution Point (CDP) is a certificate extension that indicates where the certificate revocation list for a CA can be retrieved. This extension can contain multiple HTTP, FTP, File or LDAP URLs for the retrieval of the CRL.
Online Certificate Status Protocol (OCSP) is a protocol that allows real-time validation of a certificate's status by having the CryptoAPI make a call to an OCSP responder and the OCSP responder providing an immediate validation of the revocation status for the presented certificate. Typically, the OCSP responder uses CRLs for retrieving certificate status information.

Incorrect Answers:
B: A Delta CRL is a suitable method for distributing certificate revocation information.
C: OCSP (online certificate status protocol) is a suitable method for distributing certificate revocation information.
D: Distribution point CRL is a suitable method for distributing certificate revocation information.

References:
https://technet.microsoft.com/en-us/library/cc700843.aspx

QUESTION 206
Which encryption algorithm is BEST suited for communication with handheld wireless devices?

A. ECC (Elliptic Curve Cryptosystem)
B. RSA
C. SHA
D. RC4

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An elliptic curve cryptosystem (ECC) provides much of the same functionality RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency. ECC is more efficient than RSA and any other asymmetric algorithm.
Some devices have limited processing capacity, storage, power supply, and bandwidth, such as wireless devices and cellular telephones. With these types of devices, efficiency of resource use is very important. ECC provides encryption functionality, requiring a smaller percentage of the resources compared to RSA and other algorithms, so it is used in these types of devices.
In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device.

Incorrect Answers:
B: RSA is less efficient than ECC which makes RSA less suited for communication with handheld wireless devices.
C: SHA is a hashing algorithm; it is not an encryption algorithm suited for communication with handheld wireless devices.
D: RC4 is a symmetric algorithm whereas ECC is asymmetric which makes ECC more suited for communication with handheld wireless devices.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 818-819

QUESTION 207
Which of the following keys has the SHORTEST lifespan?

A. Secret key
B. Public key
C. Session key
D. Private key

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A session key is a single-use symmetric key that is used to encrypt messages between two users during a single communication session.
If Tanya has a symmetric key she uses to always encrypt messages between Lance and herself, then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using encryption. However, using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If, on the other hand, a new symmetric key were generated each time Lance and Tanya wanted to communicate, it would be used only during their one dialogue and then destroyed. If they wanted to communicate an hour later, a new session key would be created and shared.
A session key provides more protection than static symmetric keys because it is valid for only one session between two computers. If an attacker were able to capture the session key, she would have a very small window of time to use it to try to decrypt messages being passed back and forth.

Incorrect Answers:
A: A secret key is static in nature. It has no fixed lifespan and is used until someone decides to change the key. Session keys are used for single communication sessions so they have a much shorter lifespan.
B: A public key is issued by a CA and typically has a lifespan of one or two years. Session keys are used for single communication sessions so they have a much shorter lifespan.
D: A private key is issued by a CA and typically has a lifespan of one or two years. Session keys are used for single communication sessions so they have a much shorter lifespan.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 798-799

QUESTION 208
What is the RESULT of a hash algorithm being applied to a message?

A. A digital signature
B. A ciphertext
C. A message digest
D. A plaintext

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. The input data is often called the message, and the hash value is often called the message digest or simply the digest.

Incorrect Answers:
A: To create a digital signature, a message digest is calculated (by the hash algorithm being applied to the message) then it is encrypted with the sender's private key. However, the digital signature is not the direct output of the hash algorithm being applied to the message.
B: A ciphertext is the output of an encryption algorithm, not a hash algorithm being applied to data.
D: A plaintext is the message 'before' the hash algorithm is applied to the message; it is the input to the hash algorithm, not the output.

References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 151

QUESTION 209

Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?

A. Message non-repudiation.
B. Message confidentiality.
C. Message interleave checking.
D. Message integrity.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communications security over a computer network.
The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.
A message authentication code (MAC) is a short piece of information used to authenticate a message—in other words, to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin.
A MAC algorithm, sometimes called a keyed (cryptographic) hash function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

Incorrect Answers:
A: Secure Sockets Layer (SSL) does not use a Message Authentication Code (MAC) for message non-repudiation.
B: Secure Sockets Layer (SSL) does not use a Message Authentication Code (MAC) for message confidentiality; it uses symmetric cryptography for that.
C: Secure Sockets Layer (SSL) does not use a Message Authentication Code (MAC) for message interleave checking.

References:
https://en.wikipedia.org/wiki/Transport_Layer_Security
https://en.wikipedia.org/wiki/Message_authentication_code

QUESTION 210
Which of the following services is NOT provided by the digital signature standard (DSS)?

A. Encryption
B. Integrity
C. Digital signatureD. Authentication

Correct Answer: A
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
Digital signatures do not provide encryption.
The purpose of digital signatures is to detect unauthorized modifications of data, and to authenticate the identity of the signatories and non-repudiation. These functions are accomplished by generating a block of data that is usually smaller than the size of the original data. This smaller block of data is bound to the original data and to the identity of the sender. This binding verifies the **integrity** of data and provides non-repudiation. To quote the National Institute Standards and Technology (NIST) Digital Signature Standard (DSS): Digital signatures are used to detect unauthorized modifications to data and to **authenticate** the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory.

Incorrect Answers:
B: Digital signatures do provide integrity.
C: The digital signature standard (DSS) as its name suggests is all about digital signatures.
D: Digital signatures do provide authentication.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 151

QUESTION 211
What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?

A. Key collision
B. Key clustering
C. Hashing
D. Ciphertext collision

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In cryptography, key clustering is said to occur when two different keys generate the same ciphertext from the same plaintext, using the same cipher algorithm. A good cipher algorithm, using different keys on the same plaintext, should generate a different ciphertext, irrespective of the key length.

Incorrect Answers:

A: Key collision is not the correct term to describe an instance of two different keys generating the same ciphertext from the same plaintext.
C: Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. This is not what is described in the question.
D: Ciphertext collision is not the correct term to describe an instance of two different keys generating the same ciphertext from the same plaintext.
References:
https://en.wikipedia.org/wiki/Key_clustering

QUESTION 212
Which of the following is TRUE about link encryption?

A. Each entity has a common key with the destination node.
B. Encrypted messages are only decrypted by the final node.
C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
D. Only secure nodes are used in this type of transmission.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
With Link Encryption each entity has keys in common with its two neighboring nodes in the transmission chain. Thus, a node receives the encrypted message from its predecessor (the neighboring node), decrypts it, and then re-encrypts it with another key that is common to the successor node. Then, the encrypted message is sent on to the successor node where the process is repeated until the final destination is reached. Obviously, this mode does not provide protection if the nodes along the transmission path can be compromised.

Incorrect Answers:
A: It is not true that each entity has a common key with the destination node. Each entity has keys in common with only its two neighboring nodes.
B: It is not true that encrypted messages are only decrypted by the final node. Every node in the chain (except the original sending node) decrypts the message.
D: It is not true that only secure nodes are used in this type of transmission. The data is encrypted for security; the nodes themselves can be insecure.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 126

QUESTION 213
What uses a key of the same length as the message where each bit or character from the plaintext is encrypted by a modular addition?

A. Running key cipher
B. One-time pad

C. Steganography
D. Cipher block chaining

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, then the resulting ciphertext will be impossible to decrypt or break. However, practical problems have prevented one-time pads from being widely used.

The "pad" part of the name comes from early implementations where the key material was distributed as a pad of paper, so that the top sheet could be easily torn off and destroyed after use.

The one-time pad has serious drawbacks in practice because it requires:
- Truly random (as opposed to pseudorandom) one-time pad values, which is a non-trivial requirement.
- Secure generation and exchange of the one-time pad values, which must be at least as long as the message. (The security of the one-time pad is only as secure as the security of the one-time pad exchange).
- Careful treatment to make sure that it continues to remain secret, and is disposed of correctly preventing any reuse in whole or part—hence "one time".

Because the pad, like all shared secrets, must be passed and kept secure, and the pad has to be at least as long as the message, there is often no point in using one-time padding, as one can simply send the plain text instead of the pad (as both can be the same size and have to be sent securely).
Distributing very long one-time pad keys is inconvenient and usually poses a significant security risk. The pad is essentially the encryption key, but unlike keys for modern ciphers, it must be extremely long and is much too difficult for humans to remember. Storage media such as thumb drives, DVD-Rs or personal digital audio players can be used to carry a very large one-time-pad from place to place in a non-suspicious way, but even so the need to transport the pad physically is a burden compared to the key negotiation protocols of a modern public-key cryptosystem, and such media cannot reliably be erased securely by any means short of physical destruction (e.g., incineration).
The key material must be securely disposed of after use, to ensure the key material is never reused and to protect the messages sent. Because the key material must be transported from one endpoint to another, and persist until the message is sent or received, it can be more vulnerable to forensic recovery than the transient plaintext it protects.

Incorrect Answers:
A: Running key cipher does not use a key of the same length as the message.
C: Steganography is a method of hiding data in another media type so the very existence of the data is concealed. This is not what is described in the question.
D: Cipher block chaining is an encryption method where each block of text, the key, and the value based on the previous block are processed in the algorithm and applied to the next block of text. This is not what is described in the question.

References:
https://en.wikipedia.org/wiki/One-time_pad

QUESTION 214
Guards are appropriate whenever the function required by the security program involves which of the following?

A. The use of discriminating judgment
B. The use of physical force
C. The operation of access control devices
D. The need to detect unauthorized access

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Guards are appropriate whenever immediate discriminating judgement is required by the security entity.
Guards are the oldest form of security surveillance. Guards still have a very important primary function in the physical security process, particularly in perimeter control. Because of a human's ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment, a guard can make determinations that hardware or automated security devices cannot make.

Incorrect Answers:
B: The use of physical force is not the most appropriate reason to use security guards. Therefore, this answer is incorrect.
C: The operation of access control devices typically does not require the use of security guards. Most access control devices are automatic electrical and mechanical devices that unlock and lock doors as required. Therefore, this answer is incorrect.
D: Security guards are not required to detect unauthorized access. There are many systems that can detect unauthorized access such as motion sensors etc. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 535

QUESTION 215
What is the maximum number of different keys that can be used when encrypting with Triple DES?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Triple DES (3DES) can use a maximum of three keys.
3DES can work in different modes, and the mode chosen dictates the number of keys used and what functions are carried out:
- DES-EEE3 Uses three different keys for encryption, and the data are encrypted, encrypted, encrypted.
- DES-EDE3 Uses three different keys for encryption, and the data are encrypted, decrypted, encrypted.
- DES-EEE2 The same as DES-EEE3, but uses only two keys, and the first and third encryption processes use the same key.
- DES-EDE2 The same as DES-EDE3, but uses only two keys, and the first and third encryption processes use the same key.

Incorrect Answers:
A: A maximum of 3, not 1 different keys can be used when encrypting with Triple DES.
B: A maximum of 3, not 2 different keys can be used when encrypting with Triple DES.
D: A maximum of 3, not 4 different keys can be used when encrypting with Triple DES.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 808

QUESTION 216
What algorithm has been selected as the AES algorithm, replacing the DES algorithm?

A. RC6
B. Twofish
C. Rijndael
D. Blowfish

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
After DES was used as an encryption standard for over 20 years and it was cracked in a relatively short time once the necessary technology was available, NIST decided a new standard, the Advanced Encryption Standard (AES), needed to be put into place. In January 1997, NIST announced its request for AES candidates and outlined the requirements in FIPS PUB 197. AES was to be a symmetric block cipher supporting key sizes of 128, 192, and 256 bits. The following five algorithms were the finalists:

- MARS Developed by the IBM team that created Lucifer
- RC6 Developed by RSA Laboratories
- Serpent Developed by Ross Anderson, Eli Biham, and Lars Knudsen
- Twofish Developed by Counterpane Systems
- Rijndael Developed by Joan Daemen and Vincent Rijmen

Out of these contestants, Rijndael was chosen. The block sizes that Rijndael supports are 128, 192, and 256 bits.
Rijndael works well when implemented in software and hardware in a wide range of products and environments. It has low memory requirements and has been constructed to easily defend against timing attacks.
Rijndael was NIST's choice to replace DES. It is now the algorithm required to protect sensitive but unclassified U.S. government information.

Incorrect Answers:
A: RC6 was a finalist; however, Rijndael was selected by NIST as the AES algorithm.
B: Twofish was a finalist; however, Rijndael was selected by NIST as the AES algorithm.
B: Blowfish was not selected by NIST as the AES algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 809

QUESTION 217
Which of the following is a symmetric encryption algorithm?

A. RSA
B. Elliptic Curve
C. RC5
D. El Gamal

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RC5 is a symmetric-key block cipher notable for its simplicity. Designed by Ronald Rivest in 1994, RC stands for "Rivest Cipher", or alternatively, "Ron's Code".
The Advanced Encryption Standard (AES) candidate RC6 was based on RC5.
RC5 has a variety of parameters it can use for block size, key size, and the number of rounds used. It was created by Ron Rivest and analyzed by RSA Data Security, Inc. The block sizes used in this algorithm are 32, 64, or 128 bits, and the key size goes up to 2,048 bits. The number of rounds used for encryption and decryption is also variable. The number of rounds can go up to 255.

Incorrect Answers:
A: RSA is an asymmetric key algorithm.
B: Elliptic Curve Cryptosystem (ECC) is an asymmetric key algorithm.
D: El Gamal is an asymmetric key algorithm.

References:
https://en.wikipedia.org/wiki/RC5
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 810

QUESTION 218
Which of the following protocols would BEST mitigate threats of sniffing attacks on web application traffic?

A. SSL or TLS
B. 802.1X
C. ARP Cache Security
D. SSH - Secure Shell

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
SSL and TLS encrypt web application traffic to mitigate threats of sniffing attacks.
The SSL protocol was developed by Netscape in 1994 to secure Internet client-server transactions. The SSL protocol authenticates the server to the client using public key cryptography and digital certificates. In addition, this protocol also provides for optional client to server authentication. It supports the use of RSA public key algorithms, IDEA, DES and 3DES private key algorithms, and the MD5 hash function. Web pages using the SSL protocol start with HTTPs. SSL 3.0 and its successor, the Transaction Layer Security (TLS) 1.0 protocol are defacto standards. TLS implements confidentiality, authentication, and integrity above the Transport Layer, and it resides between the application and TCP layer. Thus, TLS, as with SSL, can be used with applications such as Telnet, FTP, HTTP, and email protocols. Both SSL and TLS use certificates for public key verification that are based on the X.509 standard.

Incorrect Answers:
B: The 802.1X standard is a port-based network access control that ensures a user cannot make a full network connection until he is properly authenticated. 802.1X is not used to encrypt web application traffic.
C: ARP Cache Security can prevent ARP Cache poisoning attacks. However, it is not used to encrypt web application traffic.
D: SSH (Secure Shell) is a set of protocols that are primarily used for remote access over a network by establishing an encrypted tunnel between an SSH client and an SSH server. SSH is not used to encrypt web application traffic.

References:

Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 160

QUESTION 219
What type of key would you find within a browser's list of trusted root CAs?

A. Private key
B. Symmetric key
C. Recovery key
D. Public key

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.
In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company which charges customers to issue certificates for them.
If you trust the Root CA, you'll trust all certificates issued by the CA. All web browsers come with an extensive built-in list of trusted root certificates, many of which are controlled by organizations that may be unfamiliar to the user. The built-in list of trusted root certificates is a collection of Public Key certificates from the CAs.

Incorrect Answers:
A: The private key is always retained by the owner (in this case, a CA); it is never distributed.
B: You would not find a symmetric key within a browser's list of trusted root CAs.
C: You would not find a recovery key within a browser's list of trusted root CAs.

References:
https://en.wikipedia.org/wiki/Public_key_certificate

QUESTION 220
What can be defined as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate?

A. A public-key certificate
B. An attribute certificate

C. A digital certificate
D. A descriptive certificate

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The US American National Standards Institute (ANSI) X9 committee developed the concept of attribute certificate as a data structure that binds some attributes values with the identification information about its holder.
According to RFC 2828 [24], an attribute certificate is “a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate.
One of the advantages of attribute certificate is that it can be used for various other purposes. It may contain group membership, role clearance, or any other form of authorization.

Incorrect Answers:
A: An attribute certificate can be used to supplement a public-key certificate by storing additional information or attributes. However, an attribute certificate, not a public-key certificate is what is described in the question.
C: A digital certificate is another name for a public key certificate. It is an electronic document used to prove ownership of a public key. This is not what is described in the question.
D: A descriptive certificate is not a defined certificate type.

QUESTION 221
What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?

A. Certificate revocation list
B. Certificate revocation tree
C. Authority revocation list
D. Untrusted certificate list

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

An Authority Revocation List (ARL) is a list of serial numbers for public key certificates issued to certificate authorities that have been revoked, and therefore should not be relied upon.

Incorrect Answers:
A: A certificate revocation list (CRL) is a list of serial numbers for certificates that have been revoked, and should therefore, no longer trust entities presenting them.
B: A certificate revocation tree is a mechanism for distributing notices of certificate revocations, but is not supported in X.509.
D: A list of untrusted certificates is known as an untrusted CTL. It does not contain revoked certificates, but untrusted ones.

References:
https://en.wikipedia.org/wiki/Revocation_list
http://zvon.org/comp/r/ref-Security_Glossary.html#Terms~certificate_revocation_tree
https://technet.microsoft.com/en-us/library/dn265983.aspx

QUESTION 222
Who vouches for the binding between the data items in a digital certificate?
A. Registration authority
B. Certification authority
C. Issuing authority
D. Vouching authority

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A certification authority issues digital certificates that include a public key and the identity of the owner. The matching private key is not publicly available, but kept secret by the end user who created the key pair. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A certification authority's duty in such schemes is to verify an applicant's credentials, so that users and relying parties are able to trust the information in the CA's certificates.

Incorrect Answers:
A: A registration authority (RA) confirms user requests for a digital certificate and informs the certificate authority (CA) to distribute it.
C: An issuing authority does not vouch for the binding between the data items in a digital certificate.
D: A vouching authority does not vouch for the binding between the data items in a digital certificate.

References:

https://en.wikipedia.org/wiki/Certificate_authority
http://searchsecurity.techtarget.com/definition/registration-authority

QUESTION 223
What enables users to validate each other's certificate when they are certified under different certification hierarchies?

A. Cross-certification
B. Multiple certificates
C. Redundant certification authorities
D. Root certification authorities

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Cross certification allows entities in one public key infrastructure (PKI) to trust entities in another PKI. This mutual trust relationship is typically supported by a crosscertification agreement between the certification authorities (CAs) in each PKI. This agreement determines the responsibilities and liability of each party. A mutual trust relationship between two CAs requires that each CA issue a certificate to the other to establish the relationship in both directions. The path of trust is not hierarchal even though the separate PKIs may be certificate hierarchies.

Incorrect Answers:
B: Multiple certificates will not allow users to validate each other's certificate when they are certified under different certification hierarchies.
C: Redundant certification authorities will not allow users to validate each other's certificate when they are certified under different certification hierarchies.
D: A root certification authority is identified by a root certificate, which is an unsigned or a self-signed public key certificate.

References:
https://msdn.microsoft.com/en-us/library/windows/desktop/bb540800(v=vs.85).aspx
https://en.wikipedia.org/wiki/Root_certificate

QUESTION 224
Which of the following would best define a digital envelope?

A. A message that is encrypted and signed with a digital certificate.
B. A message that is signed with a secret key and encrypted with the sender's private key.
C. A message encrypted with a secret key attached with the message. The secret key is encrypted with the public key of the receiver.
D. A message that is encrypted with the recipient's public key and signed with the sender's private key.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Hybrid cryptography is the combined use of symmetric and asymmetric algorithms where the symmetric key encrypts data and an asymmetric key encrypts the symmetric key.
A digital envelope is another term used to describe hybrid cryptography.
When a message is encrypted with a symmetric key (secret key) and the symmetric key is encrypted with an asymmetric key, it is collectively known as a digital envelope.

Incorrect Answers:
A: A message that is encrypted and signed with a digital certificate is not the correct definition of a digital envelope. The message would have to be encrypted with a symmetric key and the symmetric key is encrypted with an asymmetric key to be a digital envelope. This answer does not specify what type of encryption is used. B: A message that is signed with a secret key and encrypted with the sender's private key is not the correct definition of a digital envelope. A private key is an asymmetric key. In a digital envelope, the message is encrypted with a symmetric key and the symmetric key is encrypted with an asymmetric key.
D: A message that is encrypted with the recipient's public key and signed with the sender's private key is not the correct definition of a digital envelope. A public key is an asymmetric key. In a digital envelope, the message is encrypted with a symmetric key and the symmetric key is encrypted with an asymmetric key.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 811

QUESTION 225
What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity?

A. A digital envelope
B. A cryptographic hash
C. A Message Authentication Code
D. A digital signature

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A digital signature is a hash value that is encrypted with the sender’s private key. The hashing function guarantees the integrity of the message, while the signing of the hash value offers authentication and nonrepudiation.

Incorrect Answers:
A: When a message is encrypted with a symmetric key and the symmetric key is encrypted with an asymmetric key, it is collectively known as a digital envelope.
B: A cryptographic hash can be used in digital signatures, but signatures are not part of the hash function.
C: Message authentication code (MAC) is a keyed cryptographic hash function that is used for data integrity and data origin authentication. It does not, however, require a signature.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 811, 829, 832
https://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 226
The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated up to?

A. Illuminated at nine feet high with at least three foot-candles
B. Illuminated at eight feet high with at least three foot-candles
C. Illuminated at eight feet high with at least two foot-candles
D. Illuminated at nine feet high with at least two foot-candles

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A foot-candle (fc) is an illuminance measurement equal to one lumen per square foot.
The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high and use two foot-candles, which is a unit that represents the illumination power of an individual light.

Incorrect Answers:
A: The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high and use two foot-candles, not nine feet high with at least three foot-candles. Therefore, this answer is incorrect.
B: The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high and use two foot-candles, not eight feet high with at least three foot-candles. Therefore, this answer is incorrect.
D: The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high and use two foot-candles, not nine feet high with at least two foot-candles. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1365

QUESTION 227
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?

A. OAKLEY
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. IPsec Key exchange (IKE)

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
ISAKMP defines actions and packet formats to establish, negotiate, modify and delete Security Associations. It is distinct from key exchange protocols with the intention of cleanly separating the details of security association management and key management from the details of key exchange.

Incorrect Answers:
A: The Oakley Key Determination Protocol is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection by making use of the Diffie–Hellman key exchange algorithm.
C: Simple Key-management for Internet Protocols (SKIP) was a protocol developed by the IETF Security Working Group for the sharing of encryption keys.
D: Internet Key Exchange (IKE) provides authenticated keying material for use with ISAKMP.

References:
https://en.wikipedia.org/wiki/Internet_Security_Association_and_Key_Management_Protocol https://en.wikipedia.org/wiki/Oakley_protocol https://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 863

QUESTION 228
Which of the following is defined as a key establishment protocol based on the Diffie-Hellman algorithm proposed for IPsec but superseded by IKE?

A. Diffie-Hellman Key Exchange Protocol
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. OAKLEY

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Oakley Key Determination Protocol is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection by making use of the Diffie–Hellman key exchange algorithm. It formed the basis for the more widely used Internet key exchange protocol.

Incorrect Answers:
A: The Diffie-Hellman algorithm proposed for IPsec is the Diffie-Hellman Key Exchange Protocol.
B: Internet Key Exchange (IKE) provides authenticated keying material for use with ISAKMP. It has not superseded ISAKMP.
C: SKIP is a distribution protocol, not a key establishment protocol.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 863
https://en.wikipedia.org/wiki/Oakley_protocol
https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange https://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

QUESTION 229
Which of the following is defined as an Internet, IPsec, key-establishment protocol, partly based on OAKLEY, that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations?
A. Internet Key exchange (IKE)
B. Security Association Authentication Protocol (SAAP)
C. Simple Key-management for Internet Protocols (SKIP)
D. Key Exchange Algorithm (KEA)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
With IPsec, Key management can be dealt with manually or automatically via a key management protocol. The genuine standard for IPSec is to make use of Internet Key Exchange (IKE), which is a permutation of the ISAKMP and OAKLEY protocols.

Incorrect Answers:
B: Security Association Authentication Protocol(SAAP) is not a valid term.

C: Simple Key-management for Internet Protocols (SKIP) was a protocol developed by the IETF Security Working Group for the sharing of encryption keys.
D: Key Exchange Algorithm includes Diffie-Hellman and RSA, but is not based on OAKLEY.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 863
https://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol
https://technet.microsoft.com/en-us/library/cc962035.aspx

QUESTION 230
Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys? This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?

A. Internet Security Association and Key Management Protocol (ISAKMP)
B. Simple Key-management for Internet Protocols (SKIP)
C. Diffie-Hellman Key Distribution Protocol
D. IPsec Key exchange (IKE)

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Simple Key-management for Internet Protocols (SKIP) was a protocol developed by the IETF Security Working Group for the sharing of encryption keys. It is a hybrid Key distribution protocol.

Incorrect Answers:
A: Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for security association creation and **key exchange**. C: Diffie–Hellman key exchange (D–H) is a specific method of securely **exchanging** cryptographic keys via a public channel D: Internet Key Exchange (IKE) provides authenticated keying material for use with ISAKMP.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 863
https://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol
https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

QUESTION 231
Which of the following can best be defined as a key recovery technique for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that only certain third parties can perform the decryption operation to retrieve the stored key?

A. Key escrow
B. Fair cryptography
C. Key encapsulation
D. Zero-knowledge recovery

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
According to RFC 4949, key encapsulation is a key recovery technique for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that only certain third parties called "recovery agents" can perform the decryption operation to retrieve the stored key. Key encapsulation typically permits direct retrieval of a secret key used to provide data confidentiality.

Incorrect Answers:
A: A key recovery technique for storing knowledge of a cryptographic key or parts thereof in the custody of one or more third parties called "escrow agents", so that the key can be recovered and used in specified circumstances. This is not what is described in the question. B: Fair cryptography is not a valid answer.
D: Zero-knowledge recovery is not a valid answer.

References:
http://tools.ietf.org/html/rfc4949

QUESTION 232
Which of the following can best be defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs?

A. A known-plaintext attack
B. A known-algorithm attack
C. A chosen-ciphertext attack
D. A chosen-plaintext attack

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

In this question, the attacker is trying to obtain the key from several “some plaintext-ciphertext pairs”. When the attacker has a copy of the plaintext corresponding to the ciphertext, this is known as a known-plaintext attack.

Cryptanalysis is the act of obtaining the plaintext or key from the ciphertext. Cryptanalysis is used to obtain valuable information and to pass on altered or fake messages in order to deceive the original intended recipient. This attempt at “cracking” the cipher is also known as an attack.
The following are example of some common attacks:
- Known Plaintext. The attacker has a copy of the plaintext corresponding to the ciphertext
- Chosen Ciphertext. Portions of the ciphertext are selected for trial decryption while having access to the corresponding decrypted plaintext
- Chosen Plaintext. Chosen plaintext is encrypted and the output ciphertext is obtained - Ciphertext Only. Only the ciphertext is available

Incorrect Answers:
B: A known-algorithm attack is not a defined type of attack.
C: With a Chosen-Ciphertext attack, the attacker has a copy of the plaintext corresponding to the ciphertext. This is not what is described in the question.
D: With a chosen-plaintext attack, chosen plaintext is encrypted and the output ciphertext is obtained. This is not what is described in the question.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 154

QUESTION 233
Which of the following is NOT a property of a one-way hash function?

A. It converts a message of a fixed length into a message digest of arbitrary length.
B. It is computationally infeasible to construct two different messages with the same digest.
C. It converts a message of arbitrary length into a message digest of a fixed length.
D. Given a digest value, it is computationally infeasible to find the corresponding message.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Cryptographic hash functions are designed to take a string of any length as input and produce a fixed-length message digest, not a message digest of arbitrary length.

A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data is often called the *message*, and the hash value is often called the *message digest* or simply the *digest*.

The ideal cryptographic hash function has four main properties: ▪ it is easy to compute the hash value for any given message ▪ it is infeasible to generate a message from its hash ▪ it is infeasible to modify a message without changing the hash ▪ it is infeasible to find two different messages with the same hash.

Incorrect Answers:
B: It is true that it is computationally infeasible to construct two different messages with the same digest.
C: It is true that it converts a message of arbitrary length into a message digest of a fixed length.
D: It is true that given a digest value, it is computationally infeasible to find the corresponding message.

References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 234
The Data Encryption Algorithm performs how many rounds of substitution and permutation?

A. 4
B. 16C. 54
D. 64

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
International Data Encryption Algorithm (IDEA) is a block cipher and operates on 64-bit blocks of data, which is divided into 16 smaller blocks, and each has eight rounds of mathematical functions performed on it.

Incorrect Answers:
A: This is the size of one of the smaller blocks.
C: This is not a valid block size for block ciphers.
D: This is incorrect as it is the initial size of the block.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 809, 810

QUESTION 235

Which of the following statements is MOST accurate regarding a digital signature?

A. It is a method used to encrypt confidential data.
B. It is the art of transferring handwritten signature to electronic media.
C. It allows the recipient of data to prove the source and integrity of data.
D. It can be used as a signature system and a cryptosystem.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The purpose of digital signatures is to detect unauthorized modifications of data, and to authenticate the identity of the signatories and non-repudiation. These functions are accomplished by generating a block of data that is usually smaller than the size of the original data. This smaller block of data is bound to the original data and to the identity of the sender. This binding verifies the integrity of data and provides non-repudiation. To quote the National Institute Standards and Technology (NIST) Digital Signature Standard (DSS): Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory.

Incorrect Answers:
A: Digital signatures do not provide encryption.
B: A digital signature is not the art of transferring handwritten signature to electronic media.
D: A digital signature cannot be used as a signature system and a cryptosystem.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 151

QUESTION 236
The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as "_____," RSA is quite feasible for computer use.

A. computing in Galois fields
B. computing in Gladden fields
C. computing in Gallipoli fields
D. computing in Galbraith fields

Correct Answer: A

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as computing in Galois fields, RSA is quite feasible for computer use.

A Galois field is a finite field.

Incorrect Answers:
B: A finite field is not called a Gladden field. Gladden fields are not used in RSA.
C: A finite field is not called a Gallipoli field. Gallipoli fields are not used in RSA.
D: A finite field is not called a Galbraith field. Galbraith fields are not used in RSA.

QUESTION 237
Which of the following concerning the Rijndael block cipher algorithm is NOT true?

A. The design of Rijndael was strongly influenced by the design of the block cipher Square.
B. A total of 25 combinations of key length and block length are possible C. Both block size and key length can be extended to multiples of 64 bits.
D. The cipher has a variable block length and key length.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
It is false that both block size and key length can be extended to multiples of 64 bits; they can be extended in multiples of 32 bits.
Rijndael is a block symmetric cipher that was chosen to fulfill the Advanced Encryption Standard. It uses a 128-bit block size and various key lengths (128, 192, 256).
The Rijndael specification is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

Incorrect Answers:
A: It is true that the design of Rijndael was strongly influenced by the design of the block cipher Square.
B: It is true that a total of 25 combinations of key length and block length are possible.
D: It is true that the cipher has a variable block length and key length.

References:
http://searchsecurity.techtarget.com/definition/Rijndael
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 145

QUESTION 238
This type of attack is generally most applicable to public-key cryptosystems, what type of attack am I?

A. Chosen-Ciphertext attack
B. Ciphertext-only attack
C. Plaintext Only Attack
D. Adaptive-Chosen-Plaintext attack

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A chosen-ciphertext attack is one in which a cryptanalyst may choose a piece of ciphertext and attempt to obtain the corresponding decrypted plaintext. This type of attack is generally most applicable to public-key cryptosystems.

Incorrect Answers:
B: A Ciphertext-Only attack is one which the cryptanalyst obtains a sample of ciphertext without the plaintext associated with it. This data is relatively easy to obtain in many scenarios, but a successful ciphertext-only attack is generally difficult and requires a very large ciphertext sample. This attack is not generally most applicable to public-key cryptosystems.
C: Plaintext Only Attack it not a defined attack type.
D: An Adaptive-Chosen-Plaintext attack is a special case of chosen-plaintext attack in which the cryptanalyst is able to choose plaintext samples dynamically and alter his or her choices based on the results of previous encryptions. This attack is not generally most applicable to public-key cryptosystems.

QUESTION 239
What is NOT true about a one-way hashing function?
A. It provides authentication of the message
B. A hash cannot be reverse to get the message used to create the hash
C. The results of a one-way hash is a message digest
D. It provides integrity of the message

Correct Answer: A

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
One-way hashing does not provide confidentiality or authentication.

Incorrect Answers:
B: One-way hash functions are never used in reverse.
C: With one-way hashing, the sender puts a message through a hashing algorithm that results in a message digest (MD) value.
D: One-way hashing does not provide confidentiality or authentication, but it does provide integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 821, 825

QUESTION 240
You've decided to authenticate the source who initiated a particular transfer while ensuring integrity of the data being transferred. You can do this by:

A. having the sender encrypt the message with his private key.
B. having the sender encrypt the hash with his private key.
C. having the sender encrypt the message with his symmetric key.
D. having the sender encrypt the hash with his public key.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
A hash will ensure the integrity of the data being transferred. A private key will authenticate the source (sender). Only the sender has a copy of the private key. If the recipient is able to decrypt the hash with the public key, then the recipient will know that the hash was encrypted with the private key of the sender.

A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. The input data is often called the *message*, and the hash value is often called the *message digest* or simply the *digest*. ▪
The ideal cryptographic hash function has four main properties:
▪ it is easy to compute the hash value for any given message ▪ it is infeasible to generate a message from its hash ▪ it is infeasible to modify a message without changing the hash ▪ it is infeasible to find two different messages with the same hash.

Incorrect Answers:
A: Having the sender encrypt the message with his private key would authenticate the sender. However, is would not ensure the integrity of the message. A hash is required to ensure the integrity of the message.
C: Having the sender encrypt the message with his symmetric key will not authenticate the sender or ensure the integrity of the message. A hash is required to ensure the integrity of the message and the hash should be encrypted with the sender's private key.
D: Having the sender encrypt the hash with his public key will not authenticate the sender. Anyone could have a copy of the sender's public key. The hash should be encrypted with the sender's private key as the sender is the only person in possession of the private key.

References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 241
Which of the following type of lock uses a numeric keypad or dial to gain entry?

A. Bolting door locks
B. Cipher lock
C. Electronic door lock
D. Biometric door lock

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Cipher locks, also known as programmable locks, are keyless and use keypads to control access into an area or facility. The lock requires a specific combination to be entered into the keypad and possibly a swipe card. They cost more than traditional locks, but their combinations can be changed, specific combination sequence values can be locked out, and personnel who are in trouble or under duress can enter a specific code that will open the door and initiate a remote alarm at the same time. Thus, compared to traditional locks, cipher locks can provide a much higher level of security and control over who can access a facility.

Incorrect Answers:
A: A bolting door lock is not the name for the type of lock that uses a numeric keypad or dial to gain entry. Therefore, this answer is incorrect.
C: Locks that use a numeric keypad or dial to gain entry are often electronic locks. However, they can also be mechanical (non-electronic) locks. Therefore, this answer is incorrect.
D: Biometric door locks do not use a numeric keypad or dial to gain entry; they use biometric scanners such as fingerprint or retina scanners. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 480

QUESTION 242
In a dry pipe system, there is no water standing in the pipe - it is being held back by what type of valve?

A. Relief valve
B. Emergency valve
C. Release valve
D. Clapper valve

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In a dry pipe system, there is no water standing in the pipe — it is being held back by a clapper valve. In the event of a fire, the valve opens, the air is blown out of the pipe, and the water flows.

Incorrect Answers:
A: The valve used in a dry pipe system is called a clapper valve, not a relief valve. Therefore, this answer is incorrect.
B: The valve used in a dry pipe system is called a clapper valve, not an emergency valve. Therefore, this answer is incorrect.
C: The valve used in a dry pipe system is called a clapper valve, not a release valve. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 463

QUESTION 243
The most prevalent cause of computer center fires is which of the following?

A. AC equipment
B. Electrical distribution systems
C. Heating systems
D. Natural causes

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
The most prevalent cause of computer center fires is electrical distribution systems.
Most computer circuits use only two to five volts of direct current, which usually cannot start a fire. If a fire does happen in a computer room, it will most likely be an electrical fire caused by overheating of wire insulation or by overheating components that ignite surrounding plastics. Prolonged smoke usually occurs before combustion.

Incorrect Answers:
A: AC equipment is not the most prevalent cause of computer center fires. Therefore, this answer is incorrect.
C: Heating systems are not the most prevalent cause of computer center fires. Computer centers use cooling systems, not heating systems. Therefore, this answer is incorrect.
D: Natural causes are not the most prevalent cause of computer center fires. Computer centers are typically protected against natural causes. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 469

QUESTION 244
Under what conditions would the use of a Class C fire extinguisher be preferable to a Class A extinguisher?

A. When the fire involves paper products
B. When the fire is caused by flammable products
C. When the fire involves electrical equipment
D. When the fire is in an enclosed area

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Class C fire extinguishers are used for fires involving electrical equipment.
Class C fires are electrical fires which that may occur in electrical equipment or wiring. Class C fire extinguishers use gas, CO2 or dry powders. These extinguishing agents are non-conductive.
Class A fire extinguishers use water or foam. Water or foam used on an electrical fire would conduct the electricity and make the fire worse. Therefore, for an electrical fire, a Class C fire extinguisher is preferable to a Class A fire extinguisher.

Incorrect Answers:
A: For a paper fire, a Class A fire extinguisher that uses water or foam is preferred. Therefore, this answer is incorrect.

B: All products that are burning in a fire are 'flammable'. The specific type of product needs to be determined to determine which fire extinguisher to use. Therefore, this answer is incorrect.
D: For a fire in an enclosed area, a Class A fire extinguisher that uses water or foam is preferred (unless the elements of the fire require a different fire extinguisher). This is because other fire extinguishers can use gases that can be harmful to life. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 472

QUESTION 245
Examples of types of physical access controls include all EXCEPT which of the following?

A. badges
B. locks
C. guards
D. passwords

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Access control needs to be enforced through physical and technical components when it comes to physical security. Physical access controls use mechanisms to identify individuals who are attempting to enter a facility or area. They make sure the right individuals get in and the wrong individuals stay out, and provide an audit trail of these actions.
A physical security control is a physical item put into place to protect facility, personnel, and resources. Examples of physical access controls include badges, locks, guards, fences, barriers, RFID cards etc. A password is not a physical object; it is something you know. Therefore, a password is not an example of a physical access control.

Incorrect Answers:
A: A badge is a physical object. Therefore, this answer is incorrect.
B: A lock is a physical object. Therefore, this answer is incorrect.
C: A guard is a physical object; a person working as a guard counts as a physical access control. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 476

QUESTION 246
Which of the following statements pertaining to fire suppression systems is TRUE?

A. Halon is today the most common choice as far as agents are concerned because it is highly effective in the way that it interferes with the chemical reaction of the elements within a fire.
B. Gas masks provide an effective protection against use of CO2 systems. They are recommended for the protection of the employees within data centers.
C. CO2 systems are NOT effective because they suppress the oxygen supply required to sustain the fire.
D. Water Based extinguishers are NOT an effective fire suppression method for class C (electrical) fires.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Class C fires are electrical fires which that may occur in electrical equipment or wiring. Class C fire extinguishers use gas, CO2 or dry powders. These extinguishing agents are non-conductive.
Class A fire extinguishers use water or foam. Water or foam used on an electrical fire would conduct the electricity and make the fire worse. Therefore, it is TRUE that water-based extinguishers are NOT an effective fire suppression method for class C (electrical) fires.

Incorrect Answers:
A: Halon is NOT the most common choice as far as agents are concerned. Halon is now known to be dangerous and no longer produced. Therefore, this answer is incorrect.
B: Gas masks DO NOT provide an effective protection against use of CO2 systems. CO2 systems work by removing the oxygen from the air. Therefore, this answer is incorrect.
C: CO2 systems ARE effective because they suppress the oxygen supply required to sustain the fire. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 472

QUESTION 247
How should a doorway of a manned facility with automatic locks be configured?

A. It should be configured to be fail-secure.
B. It should be configured to be fail-safe.
C. It should have a door delay cipher lock.
D. It should not allow piggybacking.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Doorways with automatic locks can be configured to be fail-safe or fail-secure. A fail-safe setting means that if a power disruption occurs that affects the automated locking system, the doors default to being unlocked. Fail-safe deals directly with protecting people. If people work in an area and there is a fire or the power is lost, it is not a good idea to lock them in. A fail-secure configuration means that the doors default to being locked if there are any problems with the power. If people do not need to use specific doors for escape during an emergency, then these doors can most likely default to fail-secure settings.

Incorrect Answers:
A: The doorway should be configured to be fail-safe, not fail-secure. A fail-secure configuration could lock people in the building if a power disruption occurs that affects the automated locking system. Therefore, this answer is incorrect.
C: A door delay cipher lock will sound an alarm if the door is held open for too long. This is not a requirement for a doorway of a manned facility. Therefore, this answer is incorrect.
D: Piggybacking is when an individual gains unauthorized access by using someone else's legitimate credentials or access rights. Usually an individual just follows another person closely through a door without providing any credentials. It is not a requirement for a doorway of a manned facility to not allow piggybacking. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 451

QUESTION 248
Which of the following is a proximity identification device that does not require action by the user and works by responding with an access code to signals transmitted by a reader?

A. A passive system sensing device
B. A transponder
C. A card swipe
D. A magnetic card

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
System sensing access control readers, also called transponders, recognize the presence of an approaching object within a specific area. This type of system does not require the user to swipe the card through the reader. The reader sends out interrogating signals and obtains the access code from the card without the user having to do anything.

Incorrect Answers:

A: A passive system sensing device contains no battery or power on the card, but senses the electromagnetic field transmitted by the reader and transmits at different frequencies using the power field of the reader. This device does not send an access code. Therefore, this answer is incorrect.
C: A swipe card requires the action from the user; the user has to swipe the card. Therefore, this answer is incorrect.
D: A magnetic card requires the action from the user; the user has to swipe the card. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 484
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 471

QUESTION 249
According to ISC^2, what should be the fire rating for the internal walls of an information processing facility?

A. All walls must have a one-hour minimum fire rating.
B. All internal walls must have a one-hour minimum fire rating, except for walls to adjacent rooms where records such as paper and media are stored, which should have a two-hour minimum fire rating.
C. All walls must have a two-hour minimum fire rating.
D. All walls must have a two-hour minimum fire rating, except for walls to adjacent rooms where records such as paper and media are stored, which should have a three-hour minimum fire rating.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The internal walls of your processing facility must be a floor to ceiling slab with a one-hour minimum fire rating. Any adjacent walls where records such as paper, media, etc. must have a two-hour minimum fire rating.
There are different regulations that exist for external walls from state to state.

Incorrect Answers:
A: Walls to adjacent rooms where records such as paper and media are stored should have a two-hour minimum fire rating, not a one-hour fire rating. Therefore, this answer is incorrect.
C: It is not necessary for all walls to have a two-hour minimum fire rating. Therefore, this answer is incorrect.
D: It is not necessary for the internal walls to have a two-hour fire rating and it is not necessary for walls to adjacent rooms where records such as paper and media are stored should have a three-hour minimum fire rating. Therefore, this answer is incorrect.

QUESTION 250
Which of the following statements pertaining to air conditioning for an information processing facility is TRUE?

A. The AC units must be controllable from outside the area.
B. The AC units must keep negative pressure in the room so that smoke and other gases are forced out of the room.
C. The AC units must be on the same power source as the equipment in the room to allow for easier shutdown.
D. The AC units must be dedicated to the information processing facility.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The AC units used in an information processing facility must be dedicated and controllable from within the area. They must be on an independent power source from the rest of the room and have a dedicated Emergency Power Off switch. It is positive, not negative pressure that forces smoke and other gases out of the room.

Incorrect Answers:
A: The AC units must be controllable from inside the area, not outside the area. Therefore, this answer is incorrect.
B: The AC units must keep positive pressure in the room, not negative pressure so that smoke and other gases are forced out of the room. Therefore, this answer is incorrect.
C: The AC units must be on a different power source as the equipment in the room to allow for easier shutdown. Therefore, this answer is incorrect.

QUESTION 251
Which of the following statements pertaining to secure information processing facilities is NOT true?

A. Walls should have an acceptable fire rating.
B. Windows should be protected with bars.
C. Doors must resist forcible entry.
D. Location and type of fire suppression systems should be known.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The following statements pertaining to secure information processing facilities are correct: ▪
Walls should have an acceptable fire rating.
▪ Doors must resist forcible entry.
▪ Location and type of fire suppression systems should be known.
▪ Flooring in server rooms and wiring closets should be raised to help mitigate flooding damage.
▪ Separate AC units must be dedicated to the information processing facilities. ▪
Backup and alternate power sources should exist.

The statement “windows should be protected with bars” is tricky. You could argue that they windows should be protected with bars. However, in a ‘secure’ information processing facility, there should be no windows.

Incorrect Answers:
A: It is true that walls should have an acceptable fire rating. Therefore, this answer is incorrect.
C: It is true that doors must resist forcible entry. Therefore, this answer is incorrect.
D: It is true that the location and type of fire suppression systems should be known. Therefore, this answer is incorrect.

QUESTION 252
What is a common problem when using vibration detection devices for perimeter control?

A. They are vulnerable to non-adversarial disturbances.
B. They can be defeated by electronic means.
C. Signal amplitude is affected by weather conditions.
D. They must be buried below the frost line.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A common problem when using vibration detection devices for perimeter control is false alarms. For example, someone could lean on the fence and trigger an alarm.

Perimeter Intrusion Detection and Assessment System (PIDAS) is a type of fencing that has sensors located on the wire mesh and at the base of the fence. It is used to detect if someone attempts to cut or climb the fence. It has a passive cable vibration sensor that sets off an alarm if an intrusion is detected. PIDAS is very sensitive and can cause many false alarms.

Incorrect Answers:
B: Vibration detection devices for perimeter control are not commonly defeated by electronic means. Therefore, this answer is incorrect.
C: Signal amplitude being affected by weather conditions is not common problem when using vibration detection devices for perimeter control. Therefore, this answer is incorrect.
D: It is not true that vibration detection devices for perimeter control must be buried below the frost line. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 487

QUESTION 253

Under what conditions would the use of a "Class C" hand-held fire extinguisher be preferable to the use of a "Class A" hand-held fire extinguisher?

A. When the fire is in its incipient stage.
B. When the fire involves electrical equipment.
C. When the fire is located in an enclosed area.
D. When the fire is caused by flammable products.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Class C fire extinguishers are used for fires involving electrical equipment.
Class C fires are electrical fires which that may occur in electrical equipment or wiring. Class C fire extinguishers use non-conductive agents such as gas, CO2 or dry powders.
Class A fire extinguishers use water or foam. Water or foam used on an electrical fire would conduct the electricity and make the fire worse. Therefore, for an electrical fire, a Class C fire extinguisher is preferable to a Class A fire extinguisher.

Incorrect Answers:
A: A fire being in its incipient stage (just starting) is not a reason to use a Class C fire extinguisher. Therefore, this answer is incorrect.
C: For a fire in an enclosed area, a Class A fire extinguisher that uses water or foam is preferred (unless the elements of the fire require a different fire extinguisher). This is because other fire extinguishers can use gases that are harmful to life. Therefore, this answer is incorrect.
D: All products that are burning in a fire are ‘flammable’. The specific type of product needs to be determined to determine which fire extinguisher to use. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 472

QUESTION 254
To be in compliance with the Montreal Protocol, which of the following options can be taken to refill a Halon flooding system in the event that Halon is fully discharged in the computer room?

A. Order an immediate refill with Halon 1201 from the manufacturer. B.
Contact a Halon recycling bank to make arrangements for a refill.
C. Order a Non-Hydrochlorofluorocarbon compound from the manufacturer.
D. Order an immediate refill with Halon 1301 from the manufacturer.
Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Halon is a gas that was widely used in the past to suppress fires because it interferes with the chemical combustion of the elements within a fire. It mixes quickly with the air and does not cause harm to computer systems and other data processing devices. It was used mainly in data centers and server rooms. It was discovered that halon has chemicals (chlorofluorocarbons) that deplete the ozone and that concentrations greater than 10 percent are dangerous to people. Halon used on extremely hot fires degrades into toxic chemicals, which is even more dangerous to humans.
Halon has not been manufactured since January 1, 1992, by international agreement. The Montreal Protocol banned halon in 1987, and countries were given until 1992 to comply with these directives. The most effective replacement for halon is FM-200, which is similar to halon but does not damage the ozone. By law, companies that have halon extinguishers do not have to replace them, but the extinguishers cannot be refilled. So, companies that have halon extinguishers do not have to replace them right away, but when the extinguisher's lifetime runs out, FM-200 extinguishers or other EPA-approved chemicals should be used.

Incorrect Answers:
A: You cannot refill a fire extinguisher with Halon 1201. Therefore, this answer is incorrect.
B: You cannot refill a fire extinguisher with Halon. Therefore, this answer is incorrect.
D: You cannot refill a fire extinguisher with Halon 1301. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 473

QUESTION 255
Within Crime prevention through Environmental Design (CPTED) the concept of territoriality is BEST described as:

A. ownership.
B. protecting specific areas with different measures.

C. localized emissions.
D. compromise of the perimeter.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Crime Prevention Through Environmental Design ("CPTED") is the design, maintenance, and use of the built environment in order to enhance quality of life and to reduce both the incidence and fear of crime.
Territoriality means providing clear designation between public, private, and semi-private areas and makes it easier for people to understand, and participate in, an area's intended use. Territoriality communicates a sense of active "ownership" of an area that can discourage the perception that illegal acts may be committed in the area without notice or consequences. The use of see-through screening, low fencing, gates, signage, different pavement textures, or other landscaping elements that visually show the transition between areas intended for different uses are examples of the principle of territoriality.

Incorrect Answers:
B: Protecting specific areas with different measures is not a description of the CPTED concept of territoriality. Therefore, this answer is incorrect.
C: Localized emissions are not a description of the CPTED concept of territoriality. Therefore, this answer is incorrect.
D: Compromise of the perimeter is not a description of the CPTED concept of territoriality. Therefore, this answer is incorrect.

References:
https://www.portlandoregon.gov/oni/article/320548

QUESTION 256
In the physical security context, a security door equipped with an electronic lock configured to ignore the unlock signals sent from the building emergency access control system in the event of an issue (fire, intrusion, power failure) would be in which of the following configuration?

A. Fail Soft
B. Fail Open
C. Fail Safe
D. Fail Secure

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

Doorways with automatic locks can be configured to be fail-safe or fail-secure. A fail-safe setting means that if a power disruption occurs that affects the automated locking system, the doors default to being unlocked. Fail-safe deals directly with protecting people. If people work in an area and there is a fire or the power is lost, it is not a good idea to lock them in.
A fail-secure configuration means that the doors default to being locked if there are any problems with the power. If people do not need to use specific doors for escape during an emergency, then these doors can most likely default to fail-secure settings.

Incorrect Answers:
A: Doorways with automatic locks can be configured to be fail-safe or fail-secure. “Fail-soft” is not a valid term when talking about doorways with automatic locks. Therefore, this answer is incorrect.
B: A fail-safe setting means that if a power disruption occurs that affects the automated locking system, the doors default to being unlocked. “Fail-open” is essentially the same as fail-safe although fail-safe is the more commonly used terminology. In a fail-safe or fail-open system, the doors do not remain locked. Therefore, this answer is incorrect.
C: A fail-safe setting means that if a power disruption occurs that affects the automated locking system, the doors default to being unlocked; the doors do not remain locked. Therefore, this answer is incorrect.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 451

QUESTION 257
An employee ensures all cables are shielded, builds concrete walls that extend from the true floor to the true ceiling and installs a white noise generator. What attack is the employee trying to protect against?

A. Emanation Attacks
B. Social Engineering
C. Object reuse
D. Wiretapping

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Shielding is used to protect against electromagnetic emanation by reducing the size and strength of the propagated field. This makes shielding an effective method for decreasing or eliminating the interference and crosstalk. White noise is also used to protect against electromagnetic emanation. It achieves this by drowning out the small signal emanations that could normally be identified and used by unauthorized users to steal data.

Incorrect Answers:
B: Shielding and white noise are not countermeasures to Social Engineering.

C: To protect against object reuse issues, you should wipe data from the subject media before reuse.
D: Shielding and white noise are not countermeasures to Wiretapping.

References:
Miller, David R, *CISSP Training Kit*, O'Reilly Media, 2013, Sebastopol, pp. 261, 262, 689
https://en.wikipedia.org/wiki/Social_engineering_(security)
http://people.howstuffworks.com/wiretapping.htm

QUESTION 258
Electrical systems are the lifeblood of computer operations. The continued supply of clean, steady power is required to maintain the proper personnel environment as well as to sustain data operations. Which of the following is not an element that can threaten power systems?

A. Transient Noise
B. Faulty Ground
C. Brownouts
D. UPS

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
An uninterruptible power supply (UPS) helps to ensure the continued supply of clean, steady power; it does not threaten it.
An uninterruptible power supply (UPS) is an electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries, supercapacitors, or flywheels. The on-battery runtime of most uninterruptible power sources is relatively short (only a few minutes) but sufficient to start a standby power source or properly shut down the protected equipment.

Incorrect Answers:
A: Transient Noise is an element that can threaten power systems. Therefore, this answer is incorrect.
B: Faulty Ground is an element that can threaten power systems. Therefore, this answer is incorrect.
C: A brownout is a prolonged period of lower than expected voltage; this an element that can threaten power systems. Therefore, this answer is incorrect.

References:
https://en.wikipedia.org/wiki/Uninterruptible_power_supply

QUESTION 259

The ideal operating humidity range is defined as 40 percent to 60 percent. High humidity (greater than 60 percent) can produce what type of problem on computer parts?

A. Static electricity
B. Corrosion
C. Energy-plating
D. Element-plating

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
High humidity means extra water in the air. This extra water can cause corrosion to computer parts.
It is important to maintain the proper temperature and humidity levels within data centers, which is why an HVAC system should be implemented specifically for this room. Too high a temperature can cause components to overheat and turn off; too low a temperature can cause the components to work more slowly. If the humidity is high, then corrosion of the computer parts can take place; if humidity is low, then static electricity can be introduced. Because of this, the data center must have its own temperature and humidity controls, which are separate from the rest of the building.

Incorrect Answers:
A: Static electricity is caused by low humidity, not high humidity. Therefore, this answer is incorrect.
C: Energy-plating is not caused by high humidity. Therefore, this answer is incorrect.
D: Element-plating is not caused by high humidity. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 456

QUESTION 260
Which of the following provides coordinated procedures for minimizing loss of life, injury, and property damage in response to a physical threat?

A. Business continuity plan
B. Incident response plan
C. Disaster recovery plan
D. Occupant emergency plan

Correct Answer: D

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The occupant emergency plan (OEP) provides the “response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Such events would include a fire, hurricane, criminal attack, or a medical emergency.”

Incorrect Answers:
A: A business continuity plan provides procedures for sustaining essential business operations while recovering from a significant disruption, while occupant emergency plan provides coordinated procedures for minimizing loss of life or injury and protecting properly damage in response to a physical threat.
B: Incident response plan focuses on malware, hackers, intrusions, attacks, and other security issues. It outlines procedures for incident response. C: A Disaster recovery plan provides detailed procedures to facilitate recovery of capabilities at an alternate site, while occupant emergency plan provides coordinated procedures for minimizing loss of life or injury and protecting properly damage in response to a physical threat.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 369-370

QUESTION 261
The main risks that physical security components combat are all of the following EXCEPT:

A. SYN flood
B. Physical damage
C. Theft
D. Tailgating

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A SYN flood is a type of software attack on system. The defense against a SYN flood is also software-based, not a physical component.
If an attacker sends a target system SYN packets with a spoofed address, then the victim system replies to the spoofed address with SYN/ACK packets. Each time the victim system receives one of these SYN packets it sets aside resources to manage the new connection. If the attacker floods the victim system with SYN packets, eventually the victim system allocates all of its available TCP connection resources and can no longer process new requests. This is a type of DoS that is referred to as a SYN flood. To thwart this type of attack you can use SYN proxies, which limit the number of open and abandoned network connections. The SYN proxy is a piece of software that resides between the sender and receiver and only sends on TCP traffic to the receiving system if the TCP handshake process completes successfully.

Incorrect Answers:
B: Physical damage is carried out by a person or people. Physical security components can reduce the risk of physical damage. Therefore, this answer is incorrect.
C: Theft is carried out by a person or people. Physical security components can reduce the risk of theft. Therefore, this answer is incorrect.
D: Tailgating is carried out by a person or people. Physical security components can reduce the risk of tailgating. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 539

QUESTION 262
A momentary power outage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Interference interrupts the flow of an electrical current, and fluctuations can actually deliver a different level of voltage than what was expected. Each fluctuation can be damaging to devices and people.
The following explains the different types of voltage fluctuations possible with electric power:
Power excess:
▪ Spike Momentary high voltage ▪
Surge Prolonged high voltage

Power loss:
▪ Fault Momentary power outage
▪ Blackout Prolonged, complete loss of electric power

Power degradation:
▪ Sag/dip Momentary low-voltage condition, from one cycle to a few seconds
▪ Brownout Prolonged power supply that is below normal voltage ▪ In-
rush current Initial surge of current required to start a load

Incorrect Answers:
A: A spike is a momentary high voltage, not a momentary power outage. Therefore, this answer is incorrect.
B: A blackout is a prolonged complete loss of power, not a momentary loss of power. Therefore, this answer is incorrect.
C: A surge is prolonged high voltage, not a momentary power outage. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 462-463

QUESTION 263
A momentary high voltage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Interference interrupts the flow of an electrical current, and fluctuations can actually deliver a different level of voltage than what was expected. Each fluctuation can be damaging to devices and people.
The following explains the different types of voltage fluctuations possible with electric power:
Power excess:
▪ Spike Momentary high voltage ▪
Surge Prolonged high voltage

Power loss:
▪ Fault Momentary power outage
▪ Blackout Prolonged, complete loss of electric power

Power degradation:
▪ Sag/dip Momentary low-voltage condition, from one cycle to a few seconds
▪ Brownout Prolonged power supply that is below normal voltage ▪ In-rush current Initial surge of current required to start a load

Incorrect Answers:

B: A blackout is a prolonged complete loss of power, not a momentary high voltage. Therefore, this answer is incorrect.
C: A surge is prolonged high voltage, not a momentary high voltage. Therefore, this answer is incorrect.
D: A fault is a momentary power outage, not a momentary high voltage. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 462-463

QUESTION 264
What can be defined as a momentary low voltage?

A. spike
B. blackout
C. sag
D. fault

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Interference interrupts the flow of an electrical current, and fluctuations can actually deliver a different level of voltage than what was expected. Each fluctuation can be damaging to devices and people.
The following explains the different types of voltage fluctuations possible with electric power:
Power excess:
- Spike Momentary high voltage
- Surge Prolonged high voltage

Power loss:
- Fault Momentary power outage
- Blackout Prolonged, complete loss of electric power

Power degradation:
- Sag/dip Momentary low-voltage condition, from one cycle to a few seconds
- Brownout Prolonged power supply that is below normal voltage
- In-rush current Initial surge of current required to start a load

Incorrect Answers:
A: A spike is a momentary high voltage, not a momentary low voltage. Therefore, this answer is incorrect.

B: A blackout is a prolonged complete loss of power, not a momentary low voltage. Therefore, this answer is incorrect.
D: A fault is a momentary power outage, not a momentary low voltage. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 462-463

QUESTION 265
A prolonged high voltage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A surge is a prolonged rise in voltage from a power source. Surges can cause a lot of damage very quickly. A surge is one of the most common power problems and is controlled with surge protectors. These protectors use a device called a metal oxide varistor, which moves the excess voltage to ground when a surge occurs. Its source can be from a strong lightning strike, a power plant going online or offline, a shift in the commercial utility power grid, and electrical equipment within a business starting and stopping.

Incorrect Answers:
A: A spike is a momentary high voltage, not a prolonged high voltage. Therefore, this answer is incorrect.
B: A blackout is a prolonged complete loss of power, not a prolonged high voltage. Therefore, this answer is incorrect.
D: A fault is a momentary power outage, not a prolonged high voltage. Therefore, this answer is incorrect.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 462-463

QUESTION 266
A prolonged complete loss of electric power is a:

A. brownout
B. blackout
C. surge

D. fault

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A blackout is when the voltage drops to zero. This can be caused by lightning, a car taking out a power line, storms, or failure to pay the power bill. It can last for seconds or days. This is when a backup power source is required for business continuity.

Incorrect Answers:
A: A brownout is a prolonged low voltage, not a prolonged complete loss of power. Therefore, this answer is incorrect.
C: A surge is a prolonged high voltage, not a prolonged power outage. Therefore, this answer is incorrect.
D: A fault is a momentary power outage, not a prolonged power outage. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 462-463

QUESTION 267
A prolonged electrical power supply that is below normal voltage is a:

A. brownout
B. blackout
C. surge
D. fault

Correct Answer: A
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
When power companies are experiencing high demand, they frequently reduce the voltage in an electrical grid, which is referred to as a brownout. Constant voltage transformers can be used to regulate this fluctuation of power. They can use different ranges of voltage and only release the expected 120 volts of alternating current to devices.

Interference interrupts the flow of an electrical current, and fluctuations can actually deliver a different level of voltage than what was expected. Each fluctuation can be damaging to devices and people.
The following explains the different types of voltage fluctuations possible with electric power:

Power excess:
▪ Spike Momentary high voltage ▪
Surge Prolonged high voltage

Power loss:
▪ Fault Momentary power outage
▪ Blackout Prolonged, complete loss of electric power

Power degradation:
▪ Sag/dip Momentary low-voltage condition, from one cycle to a few seconds
▪ Brownout Prolonged power supply that is below normal voltage ▪ In-
rush current Initial surge of current required to start a load

Incorrect Answers:
B: A blackout is a prolonged complete loss of power, not a prolonged low voltage. Therefore, this answer is incorrect.
C: A surge is a prolonged high voltage, not a prolonged low voltage. Therefore, this answer is incorrect.
D: A fault is a momentary power outage, not a prolonged low voltage. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 462-463

QUESTION 268
While referring to physical security, what does positive pressurization means?

A. The pressure inside your sprinkler system is greater than zero.
B. The air goes out of a room when a door is opened and outside air does not go into the room.
C. Causes the sprinkler system to go off.
D. A series of measures that increase pressure on employees in order to make them more productive.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Ventilation has several requirements that must be met to ensure a safe and comfortable environment. A closed-loop recirculating air-conditioning system should be installed to maintain air quality. “Closed-loop” means the air within the building is reused after it has been properly filtered, instead of bringing outside air in. Positive pressurization and ventilation should also be implemented to control contamination. Positive pressurization means that when an employee opens a door,

the air goes out, and outside air does not come in. If a facility were on fire, you would want the smoke to go out the doors instead of being pushed back in when people are fleeing.

Incorrect Answers:
A: Positive pressurization does not mean the pressure inside your sprinkler system is greater than zero. Therefore, this answer is incorrect.
C: Positive pressurization does not cause the sprinkler system to go off. Therefore, this answer is incorrect.
D: Positive pressurization is not a series of measures that increase pressure on employees in order to make them more productive. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 467

QUESTION 269
Because ordinary cable introduces a toxic hazard in the event of fire, special cabling is required in a separate area provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. This area is referred to as the:

A. smoke boundary area.
B. fire detection area.
C. plenum area.
D. intergen area.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Wiring and cables are strung through plenum areas, such as the space above dropped ceilings, the space in wall cavities, and the space under raised floors. Plenum areas should have fire detectors. Also, only plenum-rated cabling should be used in plenum areas, which is cabling that is made out of material that does not let off hazardous gases if it burns.

Incorrect Answers:
A: A smoke boundary area is not the area described in the question. Therefore, this answer is incorrect.
B: A fire detection area is not the area described in the question. Therefore, this answer is incorrect.
D: An Intergen area is not the area described in the question. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 473

QUESTION 270
Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are some of the examples of:

A. administrative controls.
B. logical controls.
C. technical controls.
D. physical controls.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are examples of physical security controls. These are all items put into place to protect facility, personnel, and resources.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are examples of physical security controls, not administrative controls. Therefore, this answer is incorrect.
B: Guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are examples of physical security controls, not logical controls. Therefore, this answer is incorrect.
C: Guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are examples of physical security controls, not technical controls. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28

QUESTION 271
To mitigate the risk of fire in your new data center, you plan to implement a heat-activated fire detector. Your requirement is to have the earliest warning possible of a fire outbreak. Which type of sensor would you select and where would you place it?

A. Rate-of-rise temperature sensor installed on the side wall

B. Variable heat sensor installed above the suspended ceiling
C. Fixed-temperature sensor installed in the air vent
D. Rate-of-rise temperature sensor installed below the raised floors

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Heat-activated detectors provide the earliest warning possible of a fire outbreak. They should be placed below the raised floors as this is where the cabling most likely to cause an electrical fire is.
Heat-activated detectors can be configured to sound an alarm either when a predefined temperature (fixed temperature) is reached or when the temperature increases over a period of time (rate-of-rise). Rate-of-rise temperature sensors usually provide a quicker warning than fixed-temperature sensors because they are more sensitive, but they can also cause more false alarms. The sensors can either be spaced uniformly throughout a facility, or implemented in a line type of installation, which is operated by a heat-sensitive cable.
It is not enough to have these fire and smoke detectors installed in a facility; they must be installed in the right places. Detectors should be installed both on and above suspended ceilings and raised floors, because companies run many types of wires in both places that could start an electrical fire. No one would know about the fire until it broke through the floor or dropped ceiling if detectors were not placed in these areas.

Incorrect Answers:
A: A side wall is not the best location for the sensor. If cabling under a raised floor starts a fire, it will be some time before the wall mounted heat sensor is triggered.
Therefore, this answer is incorrect.
B: A variable heat sensor is not the best type of sensor to provide the earliest warning possible of a fire outbreak. Therefore, this answer is incorrect.
C: Fixed-temperature sensors are triggered when a defined temperature is reached. This is not the best type of sensor to provide the earliest warning possible of a fire outbreak. The air vent is also not the best location for the sensor. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 470

QUESTION 272
Which type of fire extinguisher is MOST appropriate for a digital information processing facility?

A. Type A
B. Type B
C. Type C
D. Type D

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The most likely type of fire in a digital information processing facility is an electrical fire. Class C fire extinguishers are used for fires involving electrical equipment. Class C fires are electrical fires which that may occur in electrical equipment or wiring. Class C fire extinguishers use gas, CO2 or dry powders as these extinguishing agents are non-conductive.

Incorrect Answers:
A: Type A fire extinguishers use water or foam. These should not be used on an electrical fire. Therefore, this answer is incorrect.
B: Type B fires are liquid fires such as gasoline. Some Type B fire extinguishers use CO2 which could be used on an electrical fire. However, Type B fire extinguishers can also use foam which should not be used on electrical fires. Therefore, this answer is incorrect.
D: Type D fires are combustible metals such as magnesium, sodium or potassium. Type D fire extinguishers use dry powders designed for combustible metals and should not be used on electrical fires. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 472

QUESTION 273
Which of the following controls related to physical security is NOT an administrative control?

A. Personnel controls
B. Alarms
C. Training
D. Emergency response and procedures

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Alarms are an example of a physical control type, not an administrative control.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in

firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Personnel controls are an example of an administrative control. Therefore, this answer is incorrect.
C: Training is an example of an administrative control. Therefore, this answer is incorrect.
D: Emergency response and procedures are an example of an administrative control. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28

QUESTION 274
Which of the following is related to physical security and is NOT considered a technical control?

A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Locks are an example of a physical control type, not a technical control.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Access control Mechanisms are an example of a technical control. Therefore, this answer is incorrect.
B: Intrusion Detection Systems are an example of a technical control. Therefore, this answer is incorrect.
C: Firewalls are an example of a technical control. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28

QUESTION 275
Which of the following floors would be MOST appropriate to locate information processing facilities in a 6-stories building?
A. Basement
B. Ground floor
C. Third floor
D. Sixth floor

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Because data centers usually hold expensive equipment and the company's critical data, their protection should be thoroughly thought out before implementation. Data centers should not be located on the top floors because it would be more difficult for an emergency crew to access it in a timely fashion in case of a fire. By the same token, data centers should not be located in basements where flooding can affect the systems. And if a facility is in a hilly area, the data center should be located well above ground level. Data centers should be located at the core of a building so if there is some type of attack on the building, the exterior walls and structures will absorb the hit and hopefully the data center will not be damaged.

Incorrect Answers:
A: The information processing facilities should not be in the basement because of the risk of flooding. Therefore, this answer is incorrect.
B: The information processing facilities should not be on the ground floor because of the risk of flooding. Therefore, this answer is incorrect.
D: The information processing facilities should not be on the top floor because it would be more difficult for an emergency crew to access it in a timely fashion in case of a fire. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 454

QUESTION 276
Which of the following type of traffic can easily be filtered with a stateful packet filter by enforcing the context or state of the request?

A. ICMP
B. TCP
C. UDP
D. IP

Correct Answer: B

Section: Communication and Network Security
Explanation
Explanation/Reference:
Explanation:
The TCP protocol is stateful. In a TCP connection, the sender sends a SYN packet, the receiver sends a SYN/ACK, and then the sender acknowledges that packet with an ACK packet. A stateful firewall understands these different steps and will not allow packets to go through that do not follow this sequence. So, if a stateful firewall receives a SYN/ACK and there was not a previous SYN packet that correlates with this connection, the firewall understands this is not right and disregards the packet. This is what stateful means—something that understands the necessary steps of a dialog session. And this is an example of context-dependent access control, where the firewall understands the context of what is going on and includes that as part of its access decision.

Incorrect Answers:
A: The ICMP protocol is stateless, not stateful.
C: The UDP protocol is stateless, not stateful.
D: The IP protocol is stateless, not stateful.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 232

QUESTION 277
When referring to the data structures of a packet, the term Protocol Data Unit (PDU) is used, what is the proper term to refer to a single unit of TCP data at the transport layer?

A. TCP segment.
B. TCP datagram.
C. TCP frame.
D. TCP packet.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In the OSI model layer 4 is the transport layer. In the TCP/IP model, Application Layer data is encapsulated in a Layer 4 TCP segment. That TCP segment is encapsulated in a Layer 3 IP packet. Data, segments, and packets are examples of Protocol Data Units (PDUs).

Incorrect Answers:
B: TCP datagrams is not a notion that is used in the TCP/IP model.

C: The TCP frame is at the Layer 2 Ethernet layer, not at the transport level which is layer 4.
D: A TCP packet is at the application layer, not at the transport level.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 70

QUESTION 278
How do you distinguish between a bridge and a router?

A. A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to.
B. "Bridge" and "router" are synonyms for equipment used to join two networks.
C. The bridge is a specific type of router used to connect a LAN to the global Internet.
D. The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Bridges and routers both connect networks. While bridges works only up to the data link layer, routers work at the network layer.

Incorrect Answers:
A: Both bridges and routers connect multiple networks. A router examines each packet to determine which network to forward it, but bridges can also examine packets by using filters to determine if the data should be forwarded or not. B: Bridge and router are not synonyms as they work at different network layers.
C: A bridge is not one type of router. A bridge cannot connect a LAN to the Internet as it only working at the data link layer, and you need to work at the network layer to connect a LAN to the Internet.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 615

QUESTION 279
ICMP and IGMP belong to which layer of the OSI model?

A. Datagram Layer.
B. Network Layer.
C. Transport Layer.
D. Data Link Layer.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
ICMP and IGMP work at the network layer of the OSI model.

Incorrect Answers:
A: There is no Datagram Layer in the OSI model.
C: ICMP and IGMP do not belong to the Transport layer of the OSI model. TCP and UDP are examples of protocols working at the transport layer.
D: ICMP and IGMP do not belong to the Transport layer of the OSI model. ARP, OSOF, and MAC are examples of protocols workings at the data link layer.

References:
https://en.wikipedia.org/wiki/Network_layer

QUESTION 280
What is a limitation of TCP Wrappers?

A. It cannot control access to running UDP services.
B. It stops packets before they reach the application layer, thus confusing some proxy servers.
C. The hosts.* access control system requires a complicated directory tree.
D. They are too expensive.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TCP Wrappers allows you to restrict access to TCP services, but not to UDP services.
A TCP wrapper is an application that can serve as a basic firewall by restricting access to ports and resources based on user IDs or system IDs. Using TCP wrappers is a form of port – based access control.

Incorrect Answers:
B: The problem with TCP wrappers is not that confuse proxy servers. The problem is that they do not filter UDP traffic.
C: The hosts.* access control system does not require a complicated directory tree. In the simplest configuration, daemon connection policies are set to either permit or block, depending on the options in file /etc/hosts.allow. The default configuration in FreeBSD is to allow all connections to the daemons started with inetd.

D: In a UNIX/Linux system the TCP wrappers are included in the distribution and come at no cost.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 118

QUESTION 281
The IP header contains a protocol field. If this field contains the value of 1, what type of data is contained within the IP datagram?
A. TCP.
B. ICMP.
C. UDP.
D. IGMP.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The IP header protocol field value for ICMP is 1.

Incorrect Answers:
A: The IP header protocol field value for TCP is 6, not 1.
C: IP header protocol field value for UDP is 17, not 1.
D: The IP header protocol field value for IGMP is 2, not 1.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 122

QUESTION 282
The IP header contains a protocol field. If this field contains the value of 2, what type of data is contained within the IP datagram?

A. TCP.
B. ICMP.
C. UDP.
D. IGMP.

Correct Answer: D

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The IP header protocol field value for IGMP is 2.

Incorrect Answers:
A: The IP header protocol field value for TCP is 6, not 2.
B: The IP header protocol field value for ICMP is 1, not 2.
C: IP header protocol field value for UDP is 17, not 2.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 123

QUESTION 283
What is the proper term to refer to a single unit of IP data?

A. IP segment.
B. IP datagram.
C. IP frame.
D. IP fragment.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. The Internet Protocol is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks.

Incorrect Answers:
A: There is nothing called IP segment within the OSI model. The TCP protocol uses segments, while the IP protocol uses datagrams.
C: The network layer (layer 2) of the OSI model handles data link frames, but there are no IP frames in the OSI model. IP datagrams are the network layer (layer 3).
D: There is nothing called IP fragment within the OSI model.

References:
https://en.wikipedia.org/wiki/Internet_Protocol

QUESTION 284
Tim's day to day responsibilities include monitoring health of devices on the network. He uses a Network Monitoring System supporting SNMP to monitor the devices for any anomalies or high traffic passing through the interfaces.

Which of the protocols would be BEST to use if some of the requirements are to prevent easy disclosure of the SNMP strings and authentication of the source of the packets?
A. UDP B.
SNMP V1 C.
SNMP V3
D. SNMP V2

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Simple Network Management Protocol (SNMP) was released to the networking world in 1988 to help with the growing demand of managing network IP devices. Companies use many types of products that use SNMP to view the status of their network, traffic flows, and the hosts within the network.
SNMP uses agents and managers. Agents collect and maintain device-oriented data, which are held in management information bases. Managers poll the agents using community string values for authentication purposes.
SNMP versions 1 and 2 send their community string values in cleartext, but with SNMP version 3, cryptographic functionality has been added, which provides encryption, message integrity, and authentication security. So any sniffers that are installed on the network cannot sniff SNMP traffic.

Incorrect Answers:
A: UDP is not a protocol used to monitor network devices.
B: SNMP versions 1 and 2 send their community string values in cleartext. This does not prevent easy disclosure of the SNMP strings and authentication of the source of the packets.
D: SNMP versions 1 and 2 send their community string values in cleartext. This does not prevent easy disclosure of the SNMP strings and authentication of the source of the packets.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 587
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

QUESTION 285

In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class C network?

A. The first bit of the IP address would be set to zero.
B. The first bit of the IP address would be set to one and the second bit set to zero.
C. The first two bits of the IP address would be set to one, and the third bit set to zero.
D. The first three bits of the IP address would be set to one.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Class C was defined with the 3 high-order bits set to 1, 1, and 0, and designating the next 21 bits to number the networks. This translates to the IP address range of a class C network of 192.0.0.0 to 223.255.255.255.

Incorrect Answers:
A: Class C was defined with three fixed bits, not just one single bit.
B: Class C was defined with three fixed bits, not just two bits.
D: Class C was defined with the first bits set to 1, 1, and 0. Not to 1, 1, and 1.

References:
https://en.wikipedia.org/wiki/Classful_network

QUESTION 286
Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?

A. 192.168.42.5 B. 192.166.42.5
C. 192.175.42.5
D. 192.1.42.5

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:

Explanation:
The IP address 192.168.42.5 is in the private Class C IP address range.
The private IP address ranges are:
- 10.0.0.0–10.255.255.255 (Class A network)
- 172.16.0.0–172.31.255.255 (Class B networks)
- 192.168.0.0–192.168.255.255 (Class C networks)

Incorrect Answers:
B: 192.166.42.5 is not a private IP address. If the first octet is 192 then the second octet must be 168 for the address to be private.
C: 192.175.42.5 is not a private IP address. If the first octet is 192 then the second octet must be 168 for the address to be private.
D: 192.1.42.5 is not a private IP address. If the first octet is 192 then the second octet must be 168 for the address to be private.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 605

QUESTION 287
In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class A network?

A. The first bit of the IP address would be set to zero.
B. The first bit of the IP address would be set to one and the second bit set to zero.
C. The first two bits of the IP address would be set to one, and the third bit set to zero.
D. The first three bits of the IP address would be set to one.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Class A contains all addresses in which the most significant bit is zero. The address range of Class A is 0.0.0.0 - 127.255.255.255.

Incorrect Answers:
B: Class A contains only one single fixed bit, not two.
C: Class A contains only one single fixed bit, not three.
D: Class A contains only one single fixed bit, not three.

References:
https://en.wikipedia.org/wiki/Classful_network

QUESTION 288
Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?

A. 10.0.42.5
B. 11.0.42.5
C. 12.0.42.5
D. 13.0.42.5

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The IP address 10.0.42.5 is in the private Class A IP address range.
The private IP address ranges are:
- 10.0.0.0–10.255.255.255 (Class A network)
- 172.16.0.0–172.31.255.255 (Class B networks)
- 192.168.0.0–192.168.255.255 (Class C networks)

Incorrect Answers:
B: 11.0.42.5 is not a private IP address. The first octet must be 10 (or 172, or 192), not 11.
C: 12.0.42.5 is not a private IP address. The first octet must be 10 (or 172, or 192), not 12.
D: 13.0.42.5 is not a private IP address. The first octet must be 10 (or 172, or 192), not 13.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 605

QUESTION 289
Which of the following is NOT a way to secure a wireless network?

A. Disable broadcast of SSID within AP`s configuration
B. Change AP's default values
C. Put the access points (AP) in a location protected by a firewall
D. Give AP's descriptive names

Correct Answer: D

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A descriptive name of the Access Point is at best security neutral, but could decrease security as it makes it easier for an intruder might to gain some hints how the AP is used.

Incorrect Answers:
A: The SSID should not be seen as a reliable security mechanism because many APs broadcast their SSIDs, which can be easily sniffed and used by attackers. It is therefore prudent to disable the broadcast of SSIDs.
B: Keeping the default values, such as default passwords, for access points, could compromise the security.
C: The security of the Access Point can be increased by putting it behind a firewall.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 717

QUESTION 290
Which of the following media is MOST resistant to tapping?

A. Microwave.
B. Twisted pair.
C. Coaxial cable.
D. Fiber optic.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Because fiber-optic cable passes electrically non-conducting photons through a glass medium, it is very hard to wiretap.

Incorrect Answers:
A: As microwave signals passes through air, they are very easy to eavesdrop.
B: It is much easier to wiretap a twisted pair cable compared to fiber optic cable.
C: It is much easier to wiretap a coaxial cable compared to fiber optic cable.

QUESTION 291
Which of the following is a tool often used to reduce the risk to a local area network (LAN) that has external connections by filtering Ingress and Egress traffic?

A. A firewall.
B. Dial-up.
C. Passwords.
D. Fiber optics.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. TCP/IP packets that are being sent out of the internal network are examined via a router, firewall, or similar edge device.
Similarly, ingress filtering is used to ensure that incoming packets are actually from the networks from which they claim to originate.

Incorrect Answers:
B: Egress and ingress filtering can be implemented on a firewall, but not through dial-up.
C: Egress and ingress filtering can be implemented on a firewall, but not through passwords.
D: Egress and ingress filtering can be implemented on a firewall, but not fiber optics.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 631

QUESTION 292
Which one of the following is usually not a benefit resulting from the use of firewalls?

A. Reduces the risks of external threats from malicious hackers.
B. Prevents the spread of viruses.
C. Reduces the threat level on internal system.
D. Allows centralized management and control of services.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Firewalls can be useful in restricting the negative impacts of viruses, but an anti-virus program is the only way to prevent the spread of viruses.

Incorrect Answers:
A: Firewalls are used to restrict access to one network from another network. They reduce the risk of external threats such as hackers. C: Firewall increases the security on the internal network by restricting external access. D: Firewalls can be administered from a central location.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 628

QUESTION 293
Which of the following DoD Model layer provides non-repudiation services?

A. Network layer.
B. Application layer.
C. Transport layer.
D. Data link layer.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Non-repudiation is provided by applications such as PGP (Pretty Good Privacy). It is implemented in software and therefore run in the application layer.
Non-repudiation means that parties involved in a communication cannot deny having participated. It is a technique that assures genuine communication that cannot subsequently be refuted.
Implementing security at the application layer simplifies the provision of services such as non-repudiation by giving complete access to the data the user wants to protect.

Incorrect Answers:
A: Non-repudiation is implemented at application layer, not at the network layer.
C: Non-repudiation is implemented at application layer, not at the transport layer.
D: Non-repudiation is implemented at application layer, not at the data-link layer.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 249

QUESTION 294
What is the 802.11 standard related to?

A. Public Key Infrastructure (PKI)
B. Wireless network communications
C. Packet-switching technology
D. The OSI/ISO model

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
802.11 is a set specifications for implementing wireless local area network (WLAN) computer communication.

Incorrect Answers:
A: The 802.11 standard is not for PKI. It is a specification for wireless communication on a LAN.
C: The 802.11 standard does not concern packet-switching. It is a specification for wireless communication on a LAN.
D: The 802.11 standard is not related to the OSI model or the ISO model. The 802.11 standard relates to wireless communication on a LAN.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 715

QUESTION 295
Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer in a network. Within which OSI/ISO layer is RPC implemented?

A. Session layer
B. Transport layer
C. Data link layer
D. Network layer

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Session-layer services are commonly used in application environments that make use of remote procedure calls (RPCs).

Incorrect Answers:
B: RPC is implemented at the session layer, not at the transport layer.
C: RPC is implemented at the session layer, not at the data link layer.
D: RPC is implemented at the session layer, not at the network layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 524

QUESTION 296
Frame relay and X.25 networks are part of which of the following?

A. Circuit-switched services
B. Cell-switched services
C. Packet-switched services
D. Dedicated digital services

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Some examples of packet-switching technologies are the Internet, X.25, and frame relay.

Incorrect Answers:
A: X.25, and frame relay are packet switching services, not circuit-switching services.
B: X.25, and frame relay are packet switching services, not cell-switching services.
D: X.25, and frame relay are packet switching services, not dedicated digital services.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 674

QUESTION 297
Within the OSI model, at what layer are some of the SLIP, CSLIP, PPP control functions provided?

A. Data Link
B. Transport
C. Presentation
D. Application

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
PPP (Point-to-Point Protocol) is a data link protocol used to establish a direct connection between two nodes. PPP has replaced the older SLIP and CSLIP protocols.

Incorrect Answers:
B: SLIP, CSLIP, and PPP all work at the data link layer, not at the transport layer.
C: SLIP, CSLIP, and PPP all work at the data link layer, not at the presentation layer.
D: SLIP, CSLIP, and PPP all work at the data link layer, not at the application layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 683

QUESTION 298
In the Open Systems Interconnect (OSI) Reference Model, at what level are TCP and UDP provided?

A. Transport

B. Network
C. Presentation
D. Application

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TCP and UDP are examples of protocols working at the transport layer.

Incorrect Answers:
B: TCP and UDP work at the transport layer, not at the network layer.
C: TCP and UDP work at the transport layer, not at the presentation layer.
D: TCP and UDP work at the transport layer, not at the application layer.

References:
https://en.wikipedia.org/wiki/Network_layer

QUESTION 299
Which of the following is TRUE regarding Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)?

A. TCP is connection-oriented, UDP is not.
B. UDP provides for Error Correction, TCP does not.
C. UDP is useful for longer messages, rather than TCP.
D. TCP does not guarantee delivery of data, while UDP does guarantee data delivery.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TCP is a connection-oriented protocol, while UDP is a connectionless protocol.

Incorrect Answers:
B: TCP provides error corrections, while UDP does not. Not vice versa.
C: As UDP is a connectionless protocol it is less useful for longer messages, compared to the connection oriented protocol TCP.
D: As TCP is a connection-oriented protocol it guarantees delivery of data, while UDP does not guarantee data delivery as it is connectionless.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 525

QUESTION 300
The standard server port number for HTTP is which of the following?

A. 81
B. 80
C. 8080
D. 8180

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
HTTP uses port 80.

Incorrect Answers:
A: HTTP uses port 80, not port 81.
C: HTTP uses port 80, not port 8080.
D: HTTP uses port 80, not port 8180.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 537

QUESTION 301
Looking at the choices below, which ones would be the most suitable protocols/tools for securing e-mail?

A. PGP and S/MIME
B. IPsec and IKE
C. TLS and SSL
D. SSH

Correct Answer: A
Section: Communication and Network Security
Explanation
Explanation/Reference:
Explanation:
Secure MIME (S/MIME) is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions.
PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Incorrect Answers:
B: IPSec is not used to protect e-mails. IPsec is used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec can be implemented with the help of the IKE security architecture.
C: SSL and TLS are primarily used to protect HTTP traffic.
D: SSH is not used to protect e-mails. SSH allows remote login and other network services to operate securely over an unsecured network.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 850-851

QUESTION 302

Which conceptual approach to intrusion detection system is the MOST common?

A. Behavior-based intrusion detection
B. Knowledge-based intrusion detection
C. Statistical anomaly-based intrusion detection
D. Host-based intrusion detection

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
An IDS can detect malicious behavior using two common methods. One way is to use knowledge-based detection which is more frequently used. The second detection type is behavior-based detection.

Incorrect Answers:
A: behavior-based detection is less common compared to knowledge-based detection.
C: A Statistical anomaly-based IDS is a behavioral-based system.
D: Host-based intrusion detection is not a conceptual iDS approach. The two conventional approaches are knowledge-based detection and behavior-based detection.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 56

QUESTION 303
Which of the following is most affected by denial-of-service (DoS) attacks?

A. Confidentiality
B. Integrity
C. Accountability
D. Availability

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

Denial-of-service (DoS) attacks are attacks that prevent a system from processing or responding to legitimate traffic or requests for resources and objects. This type of attack makes the system unavailable.

Incorrect Answers:
A: Denial-of-service (DoS) attack main effect is not confidentiality, it is availability.
B: Denial-of-service (DoS) attack main effect is not integrity, it is availability.
C: Denial-of-service (DoS) attack main effect is not integrity, it is accountability.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 64

QUESTION 304
In this type of attack, the intruder re-routes data traffic from a network device to a personal machine. This diversion allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization. Pick the BEST choice below.

A. Network Address Translation
B. Network Address Hijacking
C. Network Address Supernetting
D. Network Address Sniffing

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Network address hijacking allows an attacker to reroute data traffic from a network device to a personal computer.

Also referred to as session hijacking, network address hijacking enables an attacker to capture and analyze the data addressed to a target system. This allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization.

Session hijacking involves assuming control of an existing connection after the user has successfully created an authenticated session. Session hijacking is the act of unauthorized insertion of packets into a data stream. It is normally based on sequence number attacks, where sequence numbers are either guessed or intercepted.

Incorrect Answers:
A: Network address translation (NAT) is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another. This is not what is described in the question.
C: Network Address Supernetting is forming an Internet Protocol (IP) network from the combination of two or more networks (or subnets) with a common Classless Inter-Domain Routing (CIDR) prefix. The new routing prefix for the combined network aggregates the prefixes of the constituent networks. This is not what is described in the question.
D: Network Address Sniffing: This is another bogus choice that sounds good but does not even exist. However, sniffing is a common attack to capture cleartext passwords and information unencrypted over the network. Sniffing is accomplished using a sniffer also called a Protocol Analyzer. A network sniffer monitors data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Also sometimes called "network probes" or "snoops," sniffers examine network traffic, making a copy of the data but without redirecting or altering it.

References:
http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm
http://wiki.answers.com/Q/What_is_network_address_hijacking
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 239

QUESTION 305
The Loki attack exploits a covert channel using which network protocol?

A. TCP
B. PPP
C. ICMP
D. SMTP

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The ICMP protocol was developed to send status messages, not to hold or transmit user data. But someone figured out how to insert some data inside of an ICMP packet, which can be used to communicate to an already compromised system. Loki is actually a client/server program used by hackers to set up back doors on

systems. The attacker targets a computer and installs the server portion of the Loki software. This server portion “listens” on a port, which is the back door an attacker can use to access the system. To gain access and open a remote shell to this computer, an attacker sends commands inside of ICMP packets. This is usually successful, because most routers and firewalls are configured to allow ICMP traffic to come and go out of the network, based on the assumption that this is safe because ICMP was developed to not hold any data or a payload.

Incorrect Answers:
A: A Loki attack uses ICMP, not TCP.
B: A Loki attack uses ICMP, not PPP.
D: A Loki attack uses ICMP, not SMTP.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 585

QUESTION 306
In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?

A. Peer-to-peer authentication
B. Only server authentication (optional)
C. Server authentication (mandatory) and client authentication (optional)
D. Role based authentication scheme

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
SSL and TLS both support server authentication (mandatory) and client authentication (optional).

Incorrect Answers:
A: Peer-to-peer authentication is not support by SSL/TLS.
B: Server authentication (optional) is not a supported SSL/TLS authentication mode.
D: Role based authentication is not supported by SSL/TLS.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 3rd Edition, Wiley & Sons, Indianapolis, 2005, p. 353

QUESTION 307

At which layer of ISO/OSI does the fiber optics work?

A. Network layer
B. Transport layer
C. Data link layer
D. Physical layer

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The physical layer consists of the basic networking hardware transmission technologies, such as fiber optics, of a network.

Incorrect Answers:
A: The network layer is responsible for packet forwarding including routing through intermediate routers.
B: The transport layer provide host-to-host communication services for applications. It provides services such as connection-oriented data stream support, reliability, flow control, and multiplexing.
C: The data link layer is responsible for media access control, flow control and error checking.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 530

QUESTION 308
Which of the following is TRUE of network security?

A. A firewall is a not a necessity in today's connected world.
B. A firewall is a necessity in today's connected world.
C. A whitewall is a necessity in today's connected world.
D. A black firewall is a necessity in today's connected world.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

Firewalls are used to restrict access to one network from another network. Most companies use firewalls to restrict access to their networks from the Internet. Using a firewall is today mandatory.

Incorrect Answers:
A: Today, as almost all computers are interconnected through the Internet, usage of firewall is necessary.
C: Whitewall is not a concept used in the IT security domain.
D: Black firewall is not a concept used in the IT security domain.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 628

QUESTION 309
Which of the following is NOT a correct notation for an IPv6 address?

A. 2001:0db8:0:0:0:0:1428:57ab
B. ABCD:EF01:2345:6789:
C. ABCD:EF01:2345:6789::1
D. 2001:DB8::8:800::417A

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The 128 bits of an IPv6 address are represented in 8 groups of 16 bits each. Each group is written as 4 hexadecimal digits and the groups are separated by colons (:).Consecutive sections of zeroes are replaced with a double colon (::).The double colon may only be used once in an address, as multiple use would render the address indeterminate. The address 2001:DB8::8:800::417A uses double colon twice, which is illegal.

Incorrect Answers:
A: 2001:0db8:0:0:0:0:1428:57ab is a well-formed IPv6 address with 8 groups of 16-bit hexadecimal numbers.
B: ABCD:EF01:2345:6789:1 is a well-formed IPv6 address with 8 groups of 16-bit hexadecimal numbers.
C: ABCD:EF01:2345:6789::1 is a well-formed IPv6 address with 8 groups of 16-bit hexadecimal numbers, and only one double colon.

References:
https://en.wikipedia.org/wiki/IPv6

QUESTION 310
Which of the following LAN devices only operates at the physical layer of the OSI/ISO model?

A. Switch
B. Bridge
C. Hub
D. Router

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A hub is a multiport repeater. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance.

Incorrect Answers:
A: Basic switches work at the data link layer. Layer 3, layer 4, and other layer switches have more enhanced functionality than layer 2 switches. B: A bridge is a LAN device used to connect LAN segments. It works at the data link layer. D: Routers work at the network layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 612

QUESTION 311
Which of the following technologies has been developed to support TCP/IP networking over low-speed serial interfaces?

A. ISDN
B. SLIP
C. xDSL
D. T1

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Serial Line Internet Protocol (SLIP) is an older technology developed to support TCP/IP communications over asynchronous serial connections, such as serial cables or modem dial - up.

Incorrect Answers:

A: ISDN can be considered a suite of digital services existing on layers 1, 2, and 3 of the OSI model. ISDN is digital, not serial.
C: xDSL is a digital technology. xDSL is the term for the Broadband Access technologies based on Digital Subscriber Line (DSL) technology
D: The T1 carrier is the most commonly used digital, not serial, transmission service.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 138

QUESTION 312
Which xDSL flavor, appropriate for home or small offices, delivers more bandwidth downstream than upstream and over longer distance?

A. VDSL B.
SDSL
C. ADSL
D. HDSL

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Asymmetric DSL (ADSL) provides data travel downstream faster than upstream. Upstream speeds are 128 Kbps to 384 Kbps, and downstream speeds can be as fast as 768 Kbps. Generally used by residential users. ADSL is appropriate for small offices.

Incorrect Answers:
A: VDSL is basically ADSL at much higher data rates (13 Mbps downstream and 2 Mbps upstream).
B: Symmetric DSL (SDSL) provides data travel upstream and downstream at the same rate.
D: High-Bit-Rate DSL (HDSL) provides T1 (1.544 Mbps) speeds over regular copper phone wire without the use of repeaters.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 699

QUESTION 313
Another name for a VPN is a:

A. tunnel
B. one-time password
C. pipeline

D. bypass

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A virtual private network (VPN) is a secure, private connection through an untrusted network. VPN technology requires a tunnel to work and it assumes encryption.

Incorrect Answers:
B: A one-time password is not the same as a VPN.
C: Tunnel, not pipeline, can be used as a name for a VPN.
D: Tunnel, not bypass, can be used as a name for a VPN.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 702

QUESTION 314
What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?

A. DS-0
B. DS-1
C. DS-2
D. DS-3

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Digital Signal Level 1 (DS - 1) provides 1.544 Mbps over a T1 line.

Incorrect Answers:
A: Digital Signal Level 0 (DS - 0) provides from 64 Kbps up to 1.544 Mbps on a Partial T1 line.
C: There is no framing specification named DS-2.
D: Digital Signal Level 3 (DS - 3) is a specification for T3, not for T1.
References:

Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 165

QUESTION 315
Which of the following is the BIGGEST concern with firewall security?

A. Internal hackers
B. Complex configuration rules leading to misconfiguration
C. Buffer overflows
D. Distributed denial of service (DDoS) attacks

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Firewalls filter traffic based on a defined set of rules. The rules must be configured correctly for the firewall to provide the intended security.

Incorrect Answers:
A: Firewalls main duty is to defend against external, not internal, threats.
C: Firewalls do not product from buffer overflows attacks.
D: Firewalls can help in defending from DDoS attacks, but the main concern with firewall is to configure them correctly.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 25

QUESTION 316
Which of the following is the SIMPLEST type of firewall?

A. Stateful packet filtering firewall
B. Packet filtering firewall
C. Dual-homed host firewall
D. Application gateway

Correct Answer: B
Section: Communication and Network Security

Explanation

Explanation/Reference:
Explanation:
Packet filtering was the first generation of firewalls and it is the most rudimentary type of all of the firewall technologies.

Incorrect Answers:
A: A stateful packet filtering firewall is more complicated compared to the Packet filtering firewall, since the latter is stateless.
C: Dual-homed is a firewall architecture, not a firewall type.
A Dual-homed firewall refers to a device that has two interfaces: one facing the external network and the other facing the internal network.
D: Application -level gateways are known as second generation firewalls, while packet filtering is a first generation firewall

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 317
Which of the following devices enables more than one signal to be sent out simultaneously over one physical circuit?

A. Router
B. Multiplexer
C. Channel service unit/Data service unit (CSU/DSU)
D. Wan switch

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
An electronic multiplexer makes it possible for several signals to share one device or resource. A multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line.

Incorrect Answers:
A: A router forwards data packets. A router does not handle signals.
C: A CSU/DSU is a digital-interface device used to connect a data terminal equipment (DTE), such as a router, to a digital circuit, such as a Digital Signal 1 (T1) line.
D: A switch forwards traffic at the data link layer of the OSI model. It does operate with multiple signals.

References:

https://en.wikipedia.org/wiki/Multiplexer

QUESTION 318
Which of the following is NOT an advantage that TACACS+ has over TACACS?

A. Event logging
B. Use of two-factor password authentication
C. User has the ability to change his password
D. Ability for security tokens to be resynchronized

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Event logging is available in both TACACS and TACACS+.

Incorrect Answers:
B: TACACS+ is XTACACS with extended two-factor user authentication.
C: TACACS uses fixed passwords for authentication, while TACACS+ allows users to employ dynamic (one-time) passwords, which provides more protection.
D: TACACS+ features security tokes, which is not included in TACACS.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 234

QUESTION 319
Which of the following remote access authentication systems is the MOST robust?

A. TACACS+
B. RADIUS
C. PAP
D. TACACS

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TACACS+ is more secure compared to TACACS, RADIUS, and PAP.
Incorrect Answers:
B: TACACS+ encrypts all of this data between the client and server and thus does not have the vulnerabilities inherent in the RADIUS protocol.
C: PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure.
D: TACACS uses fixed passwords for authentication, while TACACS+ allows users to employ dynamic (one-time) passwords, which provides more protection.
TACACS+ is XTACACS with extended two-factor user authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 234

QUESTION 320
Layer 2 of the OSI model has two sublayers. What are those sublayers, and what are two IEEE standards that describe technologies at that layer?

A. LLC and MAC; IEEE 802.2 and 802.3
B. LLC and MAC; IEEE 802.1 and 802.3
C. Network and MAC; IEEE 802.1 and 802.3
D. LLC and MAC; IEEE 802.2 and 802.3

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:

QUESTION 321
Which of the following protects Kerberos against replay attacks?

A. Tokens
B. Passwords
C. Cryptography
D. Time stamps

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
To protect against replay attacks, the Kerberos authentication protocol uses the concept of an authenticator. The authenticator includes the user identification information, a sequence number, and a timestamp. The timestamp is used to help fight against replay attacks.
Incorrect Answers:
A: Kerberos uses time stamps, not tokens, to defend against replay attacks.
B: Kerberos uses time stamps, not passwords, to defend against replay attacks.
C: Kerberos uses time stamps, not cryptography, to defend against replay attacks.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 212

QUESTION 322
Which of the following offers security to wireless communications?

A. S-WAP
B. WTLS
C. WSP
D. WDP

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Wireless Transport Layer Security (WTLS) provides security connectivity services similar to those of SSL or TLS.

Incorrect Answers:
A: There is no protocol named S-WAP
C: Wireless Session Protocol (WSP) does not provide security.
D: Wireless Datagram Protocol (WDP) does not provide security.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 103

QUESTION 323
Which of the following is a Wide Area Network that was originally funded by the Department of Defense, which uses TCP/IP for data interchange?

A. The Internet.
B. The Intranet.
C. The extranet.
D. The Ethernet.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Advanced Research Projects Agency Network (ARPANET), funded by the Department of Defense, was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet.

Incorrect Answers:
B: Intranets can use other protocols than TCP/IP. Intranet is not standard that was developed by the Department of Defense.
C: Intranet can use other protocols than TCP/IP. Extranet is not standard that was developed by the Department of Defense.
D: Ethernet can use other protocols than TCP/IP. Ethernet is not standard that was developed by the Department of Defense.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 549

QUESTION 324
An intranet is an Internet-like logical network that uses:

A. a firm's internal, physical network infrastructure.
B. a firm's external, physical network infrastructure.
C. a firm's external, physical netBIOS infrastructure.
D. a firm's internal, physical netBIOS infrastructure.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
When a company uses web-based technologies inside its networks, it is using an intranet, a private network. The company's internal physical network structure is used.

Incorrect Answers:
B: The internal, not the external, network structure is used.
C: The internal, not the external, network structure is used.
D: The physical structure, not the NetBIOS structure.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 661

QUESTION 325
An intranet provides more security and control than which of the following:

A. private posting on the Internet. B.
public posting on the Ethernet.
C. public posting on the Internet.
D. public posting on the Extranet.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A public posting on the internet is not secure. Compared to the internet, an intranet provides more control.

Incorrect Answers:
A: A private posting provides high security and control.
B: Ethernet is a link layer protocol in the TCP/IP stack. An Intranet is defined on the physical layer. The data link layer provides more control compared to the physical layer.
D: An extranet is a website that allows controlled access to partners, vendors and suppliers or an authorized set of customers - normally to a subset of the information accessible from an organization's intranet. As an extranet is a subset of an intranet is provides more security and control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 661

QUESTION 326
Which of the following Common Data Network Services is used to share data files and subdirectories on file servers?

A. File services.
B. Mail services.
C. Print services.

D. Client/Server services.

Correct Answer: A
Section: Communication and Network Security
Explanation
Explanation/Reference:
Explanation:
Files services, which are part of the Common Data Network Services, provides sharing of data files and subdirectories on file servers.

Incorrect Answers:
B: Mail services only provide sending and receiving email internally or externally through an email gateway device.
C: Print services only provide printing documents to a shared printer or a print queue/spooler.
D: Client/server services provide allocating computing power resources among workstations with some shared resources centralized in a file server.

References:
The CISSP and CAP Prep Guide: Mastering CISSP and CA (2007), page 138

QUESTION 327
Which of the following Common Data Network Services is used to send and receive email internally or externally through an email gateway device?

A. File services.
B. Mail services.
C. Print services.
D. Client/Server services.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Mail services, which are part of the Common Data Network Services, sends and receives email internally or externally through an email gateway device.

Incorrect Answers:
A: Files services provide sharing of data files and subdirectories on file servers.
C: Print services only prints documents to a shared printer or a print queue/spooler.
D: Client/server services allocate computing power resources among workstations with some shared resources centralized in a file server.

QUESTION 328

Asynchronous Communication transfers data by sending:

A. bits of data sequentially
B. bits of data sequentially in irregular timing patterns
C. bits of data in sync with a heartbeat or clock
D. bits of data simultaneously

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Asynchronous communication is the transmission sequencing technology that uses start and stop bits or similar encoding mechanism. Used in environments that transmits a variable amount of data in a periodic fashion.

Incorrect Answers:
A: Both asynchronous and synchronous communication sends bits of data sequentially.
C: Data bits transferred in sync with a heartbeat or clock is called synchronous communication.
D: Asynchronous Communication transfers one bit at a time, not multiple bits of data simultaneously.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 566

QUESTION 329
Communications devices must operate:

A. at different speeds to communicate. B.
at the same speed to communicate.
C. at varying speeds to interact.
D. at high speed to interact.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
It is preferable that both devices have the same speed when they are going to interoperate.

Incorrect Answers:
A: It is preferable that the devices have the same speed to interoperate well.
C: Communication is easier if the speeds of the devices do not change.
D: High speed is not a necessity for devices to be able to interact.

QUESTION 330
The basic language of modems and dial-up remote access systems is:

A. Asynchronous Communication.
B. Synchronous Communication.
C. Asynchronous Interaction.
D. Synchronous Interaction.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Asynchronous start-stop is the physical layer used to connect computers to modems for many dial-up Internet access applications, using a data link framing protocol.

Incorrect Answers:
B: Dial-up modems use Asynchronous, not synchronous, communication.
C: Dial-up modems connect to a remote system using communication, not interaction.
D: Dial-up modems connect to a remote system using communication, not interaction.

References:
https://en.wikipedia.org/wiki/Asynchronous_serial_communication

QUESTION 331
Which of the following Common Data Network Services is used to print documents to a shared printer or a print queue/spooler?

A. Mail services.
B. Print services.
C. Client/Server services.
D. Domain Name Service.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Print services, which are part of the Common Data Network Services, prints documents to a shared printer or a print queue/spooler.
Incorrect Answers:
A: Mail services only send and receive email internally or externally through an email gateway device.
C: Client/server services allocate computing power resources among workstations with some shared resources centralized in a file server.
D: Domain Name Service translates domain names into IP addresses.

QUESTION 332
Which of the following Common Data Network Services allocates computing power resources among workstations with some shared resources centralized on a server?

A. Print services
B. File services
C. Client/Server services
D. Domain Name Service

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Client/server services, which belongs to the Common Data Network Services, allocates computing power resources among workstations with some shared resources centralized in a file server.

Incorrect Answers:
A: Print services only print documents to a shared printer or a print queue/spooler.
B: Files services provide sharing of data files and subdirectories on file servers.
D: Domain Name Service translates domain names into IP addresses.

QUESTION 333
Domain Name Service is a distributed database system that is used to map:

A. Domain Name to IP addresses.

B. MAC addresses to domain names.
C. MAC Address to IP addresses.
D. IP addresses to MAC Addresses.

Correct Answer: A
Section: Communication and Network Security
Explanation
Explanation/Reference:
Explanation:
Domain Name Service translates domain names into IP addresses.

Incorrect Answers:
B: DNS is not used to map MAC addresses to domain names. DNS maps domain names into IP addresses.
C: The RARP protocol translates MAC Address to IP addresses.
D: The ARP protocol translates IP addresses to MAC Addresses.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 334
The Domain Name System (DNS) is a global network of:

A. servers that provide these Domain Name Services.
B. clients that provide these Domain Name Services.
C. hosts that provide these Domain Name Services.
D. workstations that provide these Domain Name Services.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Domain Name System is lists of domain names and IP addresses that are distributed on Domain Name System (DNS) Servers throughout the Internet in a hierarchy of authority.

Incorrect Answers:
B: The global Domain Name System (DNS) system consists of DNS servers, not DNS clients.

C: The global Domain Name System (DNS) system consists of DNS servers, not DNS hosts.
D: The global Domain Name System (DNS) system consists of DNS servers, not DNS workstations.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 591

QUESTION 335
The communications products and services, which ensure that the various components of a network (such as devices, protocols, and access methods) work together refers to:
A. Netware Architecture.
B. Network Architecture.
C. WAN Architecture.
D. Multiprotocol Architecture.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Network architecture is the design of a communication network. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, including protocols and access methods, as well as data formats used in its operation.

Incorrect Answers:
A: Novell Netware is specific to the vendor Novell.
C: WAN Architecture is not used for the various components of a network. It used for components that enables different local network to communicate with other networks.
D: The physical components must be included as well, not just the protocols.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 246

QUESTION 336
Unshielded Twisted Pair cabling is a:

A. four-pair wire medium that is used in a variety of networks.
B. three-pair wire medium that is used in a variety of networks.
C. two-pair wire medium that is used in a variety of networks.
D. one-pair wire medium that is used in a variety of networks.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Unshielded Twisted Pair cabling consists of an outer jacket and four pairs of twisted wire medium.

Incorrect Answers:
B: There are four pairs, not three.
C: There are four pairs, not two.
D: There are four pairs, not one.

References:
https://en.wikipedia.org/wiki/Twisted_pair#Unshielded_twisted_pair_.28UTP.29

QUESTION 337
In the UTP category rating, the tighter the wind:

A. the higher the rating and its resistance against interference and crosstalk.
B. the slower the rating and its resistance against interference and attenuation.
C. the shorter the rating and its resistance against interference and attenuation.
D. the longer the rating and its resistance against interference and attenuation.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
With Increased UTP category the better the signal is transmitted, that is the cable is more resistance against interference and crosstalk.
The lowest category is 1 and the highest is 8.2.

Incorrect Answers:
B: The UTP categories are just numbers from 1 to 8.2. They do not represent speed.
C: The UTP categories are just numbers. They do not represent length.
D: The UTP categories are just numbers. They do not represent speed.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 559

QUESTION 338
What works as an E-mail message transfer agent?

A. SMTP
B. SNMP
C. S-RPC
D. S/MIME

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In e-mail clients SMTP works as a message transfer agent and moves the message from the user's computer to the mail server when the user sends the e-mail message.

Incorrect Answers:
B: SNMP is used for monitoring the network, not for sending email messages.
C: S-RPC is used for remote procedure not calls, and not for sending email messages.
D: S/MIME is a standard for email encryption. It is not used to send email messages.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 339
Which of the following statements pertaining to packet switching is NOT true?

A. Most data sent today uses digital signals over network employing packet switching.
B. Messages are divided into packets.
C. All packets from a message travel through the same route.
D. Each network node or point examines each packet for routing.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet switching does not set up a dedicated virtual link, and packets from one connection can pass through a number of different individual devices, instead of all of them following one another through the same devices.

Incorrect Answers:
A: Most traffic over the Internet uses packet switching and the Internet is basically a connectionless network.
B: In a packet-switching network, the data are broken up into packets containing frame check sequence numbers.
D: The packet switching packets go through different network nodes, and their paths can be dynamically altered by a router or switch that determines a better route for a specific packet to take.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 674

QUESTION 340
All hosts on an IP network have a logical ID called a(n):

A. IP address.
B. MAC address.
C. TCP address.
D. Datagram address.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Each node on an IP network must have a unique IP address.

Incorrect Answers:
B: IP hosts use IP addresses, not MAC addresses.
C: There is no such thing as a TCP address in the TCP/IP model.
D: There is no such thing as a datagram address in the TCP/IP model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 541

QUESTION 341

An Ethernet address is composed of how many bits?

A. 48-bit address B.
32-bit address.
C. 64-bit address
D. 128-bit address

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Ethernet is a common LAN media access technology standardized by IEEE 802.3. Ethernet uses 48-bit MAC addressing, works in contention-based networks, and has extended outside of just LAN environments.

Incorrect Answers:
B: An Ethernet address has 48 bits, not 32 bits.
C: An Ethernet address has 48 bits, not 64 bits.
D: An Ethernet address has 48 bits, not 128 bits.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 578

QUESTION 342
Address Resolution Protocol (ARP) interrogates the network by sending out a?

A. broadcast.
B. multicast.
C. unicast.
D. semicast.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

ARP broadcasts a frame requesting the MAC address that corresponds with the destination IP address. Each computer on the subnet receives this broadcast frame, and all but the computer that has the requested IP address ignore it. The computer that has the destination IP address responds with its MAC address.

Incorrect Answers:
B: The ARP protocol uses broadcasts, not multicasts.
C: The ARP protocol uses broadcasts, not unicast.
D: The ARP protocol uses broadcasts, not semicast.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 581

QUESTION 343
When a station communicates on the network for the first time, which of the following protocol would search for and find the Internet Protocol (IP) address that matches with a known Ethernet address? A. Address Resolution Protocol (ARP).

B. Reverse Address Resolution Protocol (RARP).
C. Internet Control Message protocol (ICMP).
D. User Datagram Protocol (UDP).

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The RARP protocol translates MAC (Ethernet) Address to IP addresses.

Incorrect Answers:
A: The ARP protocol translates IP addresses to MAC Addresses. It is the wrong direction.
C: ICMP is not an address resolution protocol.
D: UDP is not an address resolution protocol. It is a transport protocol.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 584

QUESTION 344
Which protocol's primary function is to facilitate file and directory transfer between two machines?

A. Telnet.

B. File Transfer Protocol (FTP).
C. Trivial File Transfer Protocol (TFTP).
D. Simple Mail Transfer Protocol (SMTP)

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
FTP is a network application that supports an exchange of files between computers, and that requires anonymous or specific authentication.

Incorrect Answers:
A: Through Telnet users can access someone else's computer remotely.
C: TFTP is less capable compared to FTP. TFTP is used where user authentication and directory visibility are not required.
D: SMTP is used only for sending email messages.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 125

QUESTION 345
What is the primary reason why some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

A. It is too complex to manage user access restrictions under TFTP
B. Due to the inherent security risks
C. It does not offer high level encryption like FTP
D. It cannot support the Lightweight Directory Access Protocol (LDAP)

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TFTP is a network application that supports an exchange of fi les that does not require authentication. TFTP is not secure.

Incorrect Answers:
A: FTP is too insure, not too complex.

C: The difference between FTP and TFTP is that TFTP does not offer authentication.
D: Both FTP and TFTP support LDAP.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1276

QUESTION 346
Which protocol is used to send email?

A. File Transfer Protocol (FTP).
B. Post Office Protocol (POP).
C. Network File System (NFS).
D. Simple Mail Transfer Protocol (SMTP).

Correct Answer: D
Section: Communication and Network Security
Explanation
Explanation/Reference:
Explanation:
In e-mail clients SMTP works as a message transfer agent and moves the message from the user's computer to the mail server when the user sends the e-mail message.

Incorrect Answers:
A: FTP is a network application that supports an exchange of files between computers.
B: The Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve, not to send, e-mail from a remote server over a TCP/IP connection.
C: The Network File System (NFS) is a client/server application that lets a computer user view and optionally store and update file on a remote computer as though they were on the user's own computer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 347
Which of the following best describes the Secure Electronic Transaction (SET) protocol?

A. Originated by VISA and MasterCard as an Internet credit card protocol using Message Authentication Code.
B. Originated by VISA and MasterCard as an Internet credit card protocol using digital signatures.
C. Originated by VISA and MasterCard as an Internet credit card protocol using the transport layer.
D. Originated by VISA and American Express as an Internet credit card protocol using SSL.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. With SET an entity verifies a digital signature of the sender and digitally signs the information before it is sent to the next entity involved in the process.

Incorrect Answers:
A: SET uses digital signatures, not Message Authentication Codes.
C: SET uses digital signatures, not transport layer security.
D: Visa and Mastercard, not American Express, has proposed the SET protocol. The current security solution in use for credit cards transfers use SSL, but SET uses digital signatures.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 857

QUESTION 348
Which of the following protocols is designed to send individual messages securely?

A. Kerberos
B. Secure Electronic Transaction (SET).
C. Secure Sockets Layer (SSL).
D. Secure HTTP (S-HTTP).

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
S-HTTP provides protection for each message sent between two computers, but not the actual link.

Incorrect Answers:
A: Kerberos is a network authentication protocol. It is not used to secure messages.
B: SET is designed to provide secure credit card transactions, not to provide secure transfer of messages.
C: HTTPS protects the communication channel, not each individual message separately. HTTPS is HTTP that uses SSL for security purposes.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 873

QUESTION 349
Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at which layer of the OSI model?

A. Application Layer.
B. Transport Layer.
C. Session Layer.
D. Network Layer.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Both SET and S-HTTP provides application layer security.

Incorrect Answers:
B: SET and S-HTTP work at the application layer, not at the transportation layer.
C: SET and S-HTTP work at the session layer, not at the transportation layer.
D: SET and S-HTTP work at the network layer, not at the transportation layer.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 856

QUESTION 350
Why does fiber optic communication technology have significant security advantage over other transmission technology?

A. Higher data rates can be transmitted.
B. Interception of data traffic is more difficult.
C. Traffic analysis is prevented by multiplexing.
D. Single and double-bit errors are correctable.

Correct Answer: B

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Because fiber-optic cable passes electrically non-conducting photons through a glass medium, it is very hard to intercept or wiretap.

Incorrect Answers:
A: High data rates are an advantage of fiber options, but speed in itself does not significantly increase speed.
C: Multiplexing would not prevent traffic analysis. It would just make it harder.
D: Correctable bits are not an advantage of fiber optic communication.

QUESTION 351
Which of the following statements pertaining to IPSec is NOT true?

A. IPSec can help in protecting networks from some of the IP network attacks.
B. IPSec provides confidentiality and integrity to information transferred over IP networks through transport layer encryption and authentication.
C. IPSec protects against man-in-the-middle attacks.
D. IPSec protects against spoofing.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
IPSec works at the network layer, not at the transport layer.

Incorrect Answers:
A: IPSec protects networks by authenticating and encrypting each IP packet of a communication session.
C: IPSec protects against man-in-the-middle attacks by combining mutual authentication with shared, cryptography-based keys.
D: IPSec uses cryptography-based keys, shared only by the sending and receiving computers, to create a cryptographic checksum for each IP packet. The cryptographic checksum ensures that only the computers that have knowledge of the keys could have sent each packet. This products against spoofing.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1360

QUESTION 352
Which of the following is NOT a characteristic or shortcoming of packet filtering gateways?

A. The source and destination addresses, protocols, and ports contained in the IP packet header are the only information that is available to the router in making a decision whether or not to permit traffic access to an internal network. B. They don't protect against IP or DNS address spoofing.

C. They do not support strong user authentication.

D. They are appropriate for medium-risk environment.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering was the first generation of firewalls and it is the most rudimentary type of all of the firewall technologies. Packet filtering gateways/firewalls would be insufficient for a medium-risk environment.

Incorrect Answers:
A: Packet filtering gateways can make access decisions based upon the following basic criteria:
- Source and destination IP addresses
- Source and destination port numbers
- Protocol types
- Inbound and outbound traffic direction

B: Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa). On the other hand packet filtering gateways would not be able to protect against DNS spoofing. A stateful firewall is needed to protect against DNS spoofing C: Packet filter gateways cannot ensure strong user authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 353
In order to ensure the privacy and integrity of the data, connections between firewalls over public networks should use:

A. Screened subnets
B. Digital certificates
C. An encrypted Virtual Private Network
D. Encryption

Correct Answer: C
Section: Communication and Network Security

Explanation

Explanation/Reference:
Explanation:
A virtual private network (VPN) is a secure, private connection through an untrusted Network. It is a private connection because the encryption and tunneling protocols are used to ensure the confidentiality and integrity of the data in transit.

Incorrect Answers:
A: The main purpose of a screened subnet it to set up a demilitarized zone, not to protect connections over an insecure network.
B: A digital certificate provides identifying information. It is not used to protect connections over an insecure network.
D: Encryption can be used to protect connections over an insecure network, but it cannot protect the integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 701

QUESTION 354
Which of the following protocols does not operate at the data link layer (layer 2)?

A. PPP
B. RARP
C. L2F
D. ICMP

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
ICMP works at the network layer of the OSI model.

Incorrect Answers:
A: RARP is a data link layer protocol.
B: L2F is a data link layer protocol.
C: ICMP is a data link layer protocol.

References:
https://en.wikipedia.org/wiki/Network_layer

QUESTION 355

Which of the following protocols operates at the session layer (layer 5)?

A. RPC
B. IGMP
C. LPD
D. SPX

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Remote procedure call (RPC) works at the session layer of the OSI model.

Incorrect Answers:
B: ICMP works at the network layer of the OSI model.
C: LPD (Line Printer Daemon Protocol) is an application layer protocol.
D: SPX is a transport layer protocol.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 524 **QUESTION 356**
Which layer of the TCP/IP protocol stack corresponds to the ISO/OSI Network layer (layer 3)?

A. Host-to-host layer
B. Internet layer
C. Network access layer
D. Session layer

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The network layer of the OSI model corresponds to the Internet layer of the TCP/IP model.

Incorrect Answers:

A: The host-to-host layer of the TCP/IP model corresponds to the Transport layer of the OSI model.
C: The host-to-host layer of the TCP/IP model corresponds to the Data link layer of the OSI model.
D: The TCP/IP model does not have any session layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 518

QUESTION 357
Which layer of the OSI/ISO model handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control?

A. Physical
B. Data link
C. Network
D. Session

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The data link layer is responsible for proper communication within the network components and for changing the data into the necessary format (electrical voltage) for the physical layer. It is concerned with local delivery of frames between devices on the same LAN.

Incorrect Answers:
A: The physical layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes.
C: The session layer protocols set up connections between applications; maintain dialog control; and negotiate, establish, maintain, and tear down the communication channel.

D: The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e., a semi-permanent dialogue.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 528

QUESTION 358
The Logical Link Control sub-layer is a part of which of the following?

A. The ISO/OSI Data Link layer.
B. The Reference monitor.
C. The Transport layer of the TCP/IP stack model.
D. Change management control.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The ISO/OSI data link layer is divided into two functional sublayers: the Logical Link Control (LLC) and the Media Access Control (MAC).

Incorrect Answers:
B: Logical Link Control is a sublayer of the Data link layer, and not part of the Reference monitor.
C: Logical Link Control is a sublayer of the Data link layer, and not part of the Transport layer.
D: Logical Link Control is a sublayer of the Data link layer, and not part of the Change management control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 528

QUESTION 359
Which of the following services relies on UDP?

A. FTP
B. Telnet
C. DNS
D. SMTP

Correct Answer: C

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
DNS primarily uses User Datagram Protocol (UDP) on port number 53 to serve requests. DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.

Incorrect Answers:
A: FTP uses the TCP protocol.
B: Telnet uses the TCP protocol.
C: SMTP uses the TCP protocol.

References:
https://en.wikipedia.org/wiki/Domain_Name_System

QUESTION 360
Which of the following is NOT a common weakness of packet filtering firewalls?

A. Vulnerability to denial-of-service and related attacks.
B. Vulnerability to IP spoofing.
C. Limited logging functionality.
D. No support for advanced user authentication schemes.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).

Incorrect Answers:
A: Packet filtering firewalls, as they are stateless, are vulnerable to denial-of-service attacks. A stateful firewall would be able to handle these attacks better.
C: Logging is no problem when using packet filtering firewalls.
D: Packet filter gateways cannot ensure strong user authentication.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 361
Which Network Address Translation (NAT) is the MOST convenient and secure solution?

A. Hiding Network Address Translation
B. Port Address Translation
C. Dedicated Address Translation
D. Static Address Translation

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Port Address Translation (PAT) maps one internal IP address to an external IP address and port number combination. Thus, PAT can theoretically support 65,536 (2 16) simultaneous communications from internal clients over a single external leased IP address. A company can save a lot of money by using PAT, because the company needs to buy only a few public IP addresses, which are used by all systems in the network.

Incorrect Answers:
A: NAT maps one internal IP address to one external IP address. Compared to PAT this is pretty bad.
C: There is no NAT implementation called Dedicated Address Translation.
D: Static Address Translation is not convenient as it must be configured manually.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 606

QUESTION 362
What is the primary difference between FTP and TFTP?
A. Speed of negotiation
B. Authentication
C. Ability to automate
D. TFTP is used to transfer configuration files to and from network equipment.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TFTP is less capable compared to FTP. TFTP is used where user authentication and directory visibility are not required.

Incorrect Answers:
A: Both FTP and TFTP have ability to negotiate speedC:
There is ability to automate both FTP and TFTP.
D: TFTP can be used to transfer any files, not just configuration files between network equipment.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 125

QUESTION 363
Which of the following cable types is limited in length to 185 meters?

A. 10BaseT
B. RG8
C. RG58
D. 10Base5

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
RG-58 was once widely used in "thin" Ethernet (10BASE2), where it provides a maximum segment length of 185 meters.

Incorrect Answers:
A: 10BaseT has a maximal distance of 100 meters.
B: RG-8 has a maximal distance of 500 meters.
D: 10Base5 has a maximal distance of 500 meters.

References:
https://en.wikipedia.org/wiki/RG-58

QUESTION 364

In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
HTTP Secure (HTTPS) is HTTP running over SSL. The client browser generates a session key and encrypts it with the server's public key.

Incorrect Answers:
A: Only the client generates the key.
C: The client, not the server, generates the key.
D: The client, not a certification server, generates the key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 855

QUESTION 365
Which of the following statements pertaining to PPTP (Point-to-Point Tunneling Protocol) is NOT true?

A. PPTP allows the tunneling of any protocols that can be carried within PPP.
B. PPTP does not provide strong encryption.
C. PPTP does not support any token-based authentication method for users.
D. PPTP is derived from L2TP.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

PPTP is an encapsulation protocol based on PPP that works at OSI layer 2 (Data Link) and that enables a single point-to-point connection, usually between a client and a server. While PPTP depends on IP to establish its connection. As currently implemented, PPTP encapsulates PPP packets using a modified version of the generic routing encapsulation (GRE) protocol, which gives PPTP to the flexibility of handling protocols other than IP, such as IPX and NETBEUI over IP networks.
PPTP does have some limitations: It does not provide strong encryption for protecting data, nor does it support any token-based methods for authenticating users.
L2TP is derived from L2F and PPTP, not the opposite.

Incorrect Answers:
A: PPTP relies on the Point-to-Point Protocol (PPP) being tunneled to implement security functionality.
B: PPTP uses PPP for encryption. The PPP protocol has only the capability to encrypt data with 128-bit so it ensures low security.
C: The PPTP specification does not include authentication. In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, MSCHAP v1/v2 , but not with any token-based authentication scheme.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 708

QUESTION 366
During the initial stage of configuration of your firewall, which of the following rules appearing in an Internet firewall policy is inappropriate?

A. The firewall software shall run on a dedicated computer.
B. Appropriate firewall documentation and a copy of the rulebase shall be maintained on offline storage at all times.
C. The firewall shall be configured to deny all services not expressly permitted.
D. The firewall should be tested online first to validate proper configuration.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
For security reasons, the firewall should be tested offline.

Incorrect Answers:
A: A firewall may take the form of either software installed on a regular computer using a regular operating system or a dedicated hardware appliance that has its own operating system. The second choice is usually more secure.
B: It is important to make a backup of the configuration of the firewall.
C: All unneeded ports should be closed, and all unneeded services should be denied.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 643

QUESTION 367
SMTP can best be described as:

A. a host-to-host email protocol.
B. an email retrieval protocol.
C. a web-based e-mail reading protocol.
D. a standard defining the format of e-mail messages.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In e-mail clients SMTP works as a message transfer agent and moves the message from the user's computer to the mail server when the user sends the e-mail message.

Incorrect Answers:
B: SMTP is used only for sending, not retrieving, email messages.
C: SMTP is used only for sending, not reading, email messages.
D: SMTP is not a format of email messages. It is a protocol for sending email messages.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 368
Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?

A. SSL
B. FTP
C. SSH
D. S/MIME

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
SSL is primarily used to protect HTTP traffic. SSL capabilities are already embedded into most web browsers.

Incorrect Answers:
B: FTP is used to transfer files, not to secure data that are transferred.
C: S/MIME is not to protect data sent in web applications. S/MIME, more specifically, is used to secure email messages.
D: SSH is not used in a web based application. SSH allows remote login and other network services to operate securely over an unsecured network.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 846

QUESTION 369
What attack involves the perpetrator sending spoofed packet(s) which contains the same destination and source IP address as the remote host, the same port for the source and destination, having the SYN flag, and targeting any open ports that are open on the remote host?

A. Boink attack
B. Land attack
C. Teardrop attack
D. Smurf attack

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A land (Local Area Network Denial) attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address to an open port as both source and destination. This causes the machine to reply to itself continuously.

Incorrect Answers:
A: The Boink attack manipulates a field in TCP/IP packets, called a fragment offset. This field tells a computer how to reconstruct a packet that was broken up (fragmented) because it was too big to transmit in a whole piece. By manipulating this number, the Boink attack causes the target machine to reassemble a packet that is much too big to be reassembled. This causes the target computer to crash.
C: A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine.
D: The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 257

QUESTION 370
Which of the following is NOT a component of IPSec?

A. Authentication Header
B. Encapsulating Security Payload
C. Key Distribution Center
D. Internet Key Exchange

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A Key Distribution Center (KDC) is not used by IPSec. Kerberos uses a KDC for authentication.

Incorrect Answers:
A: The Authentication Header (AH) security protocol is used by IPSec.
B: The Encapsulating Security Payload (ESP) security protocol is used by IPSec.
D: The Internet Key Exchange (IKE) is the first phase of IPSec authentication, which accomplishes key management.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 861

QUESTION 371
Which of the following statements pertaining to IPSec is NOT true?

A. A security association has to be defined between two IPSec systems in order for bi-directional communication to be established.
B. Integrity and authentication for IP datagrams are provided by AH.
C. ESP provides for integrity, authentication and encryption to IP datagrams.
D. In transport mode, ESP only encrypts the data payload of each packet.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
One security association (SA) is not enough to establish bi-directional communication. Each device will have at least one security association (SA) for each secure connection it uses, so two security associations would be required.

Incorrect Answers:
B: AH provides authentication and integrity for the IP datagrams.
C: ESP provides authentication, integrity, and encryption for the IP datagrams.
D: In IPSec transport mode the payload, but not the routing and header information, of the message is protected.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 862

QUESTION 372
Which of the following statements pertaining to packet filtering is NOT true?

A. It is based on ACLs.
B. It is not application dependent.
C. It operates at the network layer.
D. It keeps track of the state of a connection.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering firewalls are stateless. They do not keep track of the state of a connection.

Incorrect Answers:
A: The device that is carrying out packet filtering processes is configured with ACLs, which dictate the type of traffic that is allowed into and out of specific networks.
B: Packet filtering firewalls are application dependent.
C: Packet filtering is a firewall technology that makes access decisions based upon network-level protocol header values.
D: Packet filtering works at the network and transport layers, not at the application layer. It is not application dependent.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 373
Which of the following is a method of multiplexing data where a communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams. This method allocates bandwidth dynamically to physical channels having information to transmit?

A. Time-division multiplexing
B. Asynchronous time-division multiplexing
C. Statistical multiplexing
D. Frequency division multiplexing

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Statistical time-division multiplexing (STDM) transmits several types of data simultaneously across a single transmission cable or line. The communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams.

Incorrect Answers:
A: Time-division multiplexing (TDM) is less complex compared to Statistical multiplexing. In its primary form, TDM is used communication with a fixed number of channels and constant bandwidth per channel.
B: Asynchronous time-division multiplexing (TDM) is similar to TDM. It uses a fixed number channels, not an arbitrary number of channels like STDM.
D: Frequency-division multiplexing (FDM) uses an available wireless spectrum, not a communication channel, to move data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 672

QUESTION 374
If an organization were to deploy only one Intrusion Detection System (IDS) sensor to protect its information system from the Internet:

A. It should be host-based and installed on the most critical system in the DMZ, between the external router and the firewall.
B. It should be network-based and installed in the DMZ, between the external router and the firewall.
C. It should be network-based and installed between the firewall to the DMZ and the intranet.
D. It should be host-based and installed between the external router and the Internet.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Network Intrusion Detection Systems (NIDS) are placed at a strategic point, such as between the internet-facing router and the firewall, within the network to monitor traffic to and from all devices on the network.

Incorrect Answers:
A: A host-based IDS is an IDS that is installed on a single computer and can monitor the activities on that computer only.
C: It is better to place the IDS between the DMZ and the internet.
D: A host-based IDS is an IDS that is installed on a single computer and can monitor the activities on that computer only.

References:
https://en.wikipedia.org/wiki/Intrusion_detection_system

QUESTION 375
Why is infrared generally considered to be more secure to eavesdropping than multidirectional radio transmissions?

A. Because infrared eavesdropping requires more sophisticated equipment.
B. Because infrared operates only over short distances.
C. Because infrared requires direct line-of-sight paths.
D. Because infrared operates at extra-low frequencies (ELF).

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Infrared communications require line-of-sight transmission. This makes infrared relative secure from electronic eavesdropping.

Incorrect Answers:
A: Infrared eavesdropping does not require more advanced transmissions.
B: Infrared operates over short distances, but this is not the main reason it is hard to eavesdrop. Compared to multidirectional radio transmission a direct line of sight is necessary.
D: Infrared operates at high frequencies around 430 THz.

QUESTION 376
Authentication Headers (AH) and Encapsulating Security Payload (ESP) protocols are the driving force of IPSec. Authentication Headers (AH) provides the following service except:

A. Authentication
B. Integrity
C. Replay resistance and non-repudiations
D. Confidentiality

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Integrity and authentication for IP datagrams are provided by AH, but AH does not provide Confidentiality.

Incorrect Answers:
A: Authentication is provided by AH.
B: Integrity is provided by AH.
C: Authentication Headers (AH) might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed. With nonrepudiations comes replay resistance.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 862

QUESTION 377
In IPSec, if the communication is to be gateway-to-gateway or host-to-gateway:

A. Tunnel mode of operation is required
B. Only transport mode can be used
C. Encapsulating Security Payload (ESP) authentication must be used
D. Both tunnel and transport mode can be used

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

In IPSec tunnel mode, the entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications.

Incorrect Answers:
B: Tunnel mode, not transport mode, must be used.
C: Tunnel mode, not ESP authentication, must be used.
D: Only tunnel mode can be used.

References:
https://en.wikipedia.org/wiki/IPsec#Tunnel_mode

QUESTION 378
Which of the following is NOT true about IPSec Tunnel mode?

A. Fundamentally an IP tunnel with encryption and authentication
B. Works at the Transport layer of the OSI model
C. Have two sets of IP headers
D. Established for gateway service

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
IPSec Tunnel mode works at the Internet layer, not at the Transport layer.

Incorrect Answers:
A: In IPSec tunnel mode, the entire IP packet is encrypted and/or authenticated.
C: In tunnel mode, the entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. That is, in tunnel mode, there are two sets of IP headers.
D: Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access or for gateway services) and host-to-host communications.

References:
https://en.wikipedia.org/wiki/IPsec#Tunnel_mode

QUESTION 379
Which of the following statements is NOT true of IPSec Transport mode?

A. It is required for gateways providing access to internal systems
B. Set-up when end-point is host or communications terminates at end-points
C. If used in gateway-to-host communication, gateway must act as host
D. When ESP is used for the security protocol, the hash is only applied to the upper layer protocols contained in the packet

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Tunnel mode, not transport mode, is required for gateway services.

Incorrect Answers:
B: Transport mode is allowed between two end hosts only.
C: As Transport mode only is allowed between two end hosts, the gateway must act as a host.
D: ESP operates directly on top of IP. The encryption is only applied to the upper layer protocols contained in the packet.

References:
https://tools.ietf.org/html/rfc3884

QUESTION 380
Which of the following statements pertaining to firewalls is NOT true?

A. Firewalls create bottlenecks between the internal and external network.
B. Firewalls allow for centralization of security services in machines optimized and dedicated to the task.
C. Firewalls protect a network at all layers of the OSI models.
D. Firewalls are used to create security checkpoints at the boundaries of private networks.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering firewalls work at the network level of the OSI model.
If you filter specific ports, you can say you're filtering at layer 4.

If your firewall inspects specific protocol states or data, you can say it operates at layer 7.
Firewalls do not work at layer 1, layer 2, or layer 3 of the OSI model.

Incorrect Answers:
A: Firewalls can create bottlenecks between the internal and external network.
B: Firewalls can be administered from a central location.
D: Firewall are most often placed at the boundaries of the private networks to implement a security checkpoint to restrict access from the Internet.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 628

QUESTION 381
Which of the following is an extension to Network Address Translation that permits multiple devices providing services on a local area network (LAN) to be mapped to a single public IP address?
A. IP Spoofing
B. IP subnetting
C. Port address translation
D. IP Distribution

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Port address translation (PAT) is an implementation of Network Address Translation. PAT is a mechanism for converting the internal private IP addresses found in packet headers into public IP addresses and port numbers for transmission over the Internet. PAT supports a many-to-one mapping of internal to external IP addresses by using ports.

Incorrect Answers:
A: IP Spoofing does not involve mapping of IP addresses. IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system B: IP subnetting is the practice of dividing a network into two or more networks. D: The distribution of IP addresses does not involve mapping of IP addresses.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 606

QUESTION 382
At which OSI/ISO layer is an encrypted authentication between a client software package and a firewall performed?

A. Network layer
B. Session layer
C. Transport layer
D. Data link layer

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Encrypted authentication is a firewall feature that allows users on an external network to authenticate themselves to prove that they are authorized to access resources on the internal network. Encrypted authentication is convenient because it happens at the transport layer between a client software and a firewall, allowing all normal application software to run without hindrance.

Incorrect Answers:
A: The firewall encrypted authentication feature is performed at the transport layer, not the network layer.
B: The firewall encrypted authentication feature is performed at the transport layer, not the session layer.
D: The firewall encrypted authentication feature is performed at the transport layer, not the data link layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1161

QUESTION 383
Which of the following attack is MOSTLY performed by an attacker to steal the identity information of a user such as credit card number, passwords, etc?

A. Smurf attack
B. Traffic analysisC. Pharming
D. Interrupt attack

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. At the fake site the user can be fooled into providing identity information such as passwords.

Incorrect Answers:
A: The aim of a smurf attack is not to steal information. A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service.
B: Traffic analysis is not mostly used to steal identity information.
D: The aim of an Interrupt attack is not to steal information. Interrupt Attacks are aimed to disrupt services.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 272

QUESTION 384
Which of the following was designed to support multiple network types over the same serial link?

A. Ethernet

B. SLIP
C. PPP
D. PPTP

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Point-to-Point Protocol (PPP) is a full - duplex protocol used for the transmission of TCP/IP packets over various non-LAN connections, such as modems, ISDN, VPNs, Frame Relay, and so on. PPP permits multiple network layer protocols to operate on the same communication link.

Incorrect Answers:
A: Ethernet is a link layer protocol in the TCP/IP stack, but Ethernet is not used for serial links.
B: SLIP is a predecessor of PPP which do not support multiple network types over a single link.
D: PPTP is a tunneling protocol which uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. PPTP tunnels do not handle network types.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 683

QUESTION 385
What is an IP routing table?

A. A list of IP addresses and corresponding MAC addresses.
B. A list of station and network addresses with corresponding gateway IP address.
C. A list of host names and corresponding IP addresses.
D. A list of current network interfaces on which IP routing is enabled.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A routing table is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. The routing table stores route information about directly connected and remote networks.

Incorrect Answers:
A: An IP Routing table does not contain MAC addresses.
B: There are not host names in IP routing tables.
D: A routing table does not include a list of network interface which are IP routing enabled. A routing table includes an Interface address, which is the outgoing network interface the device should use when forwarding the packet to the next hop or final destination.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 615

QUESTION 386
Which of the following should be allowed through a firewall to easy communication and usage by users?

A. RIP
B. IGRP
C. DNS
D. OSPF

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
DNS translates domain names into IP addresses, which enables us to use domain names instead of IP addresses.

Incorrect Answers:
A: RIP is a routing protocol. A routing protocol forwards routing information between routers, but does make it easier for users to communicate.
B: IGRP is a routing protocol. A routing protocol forwards routing information between routers, but does make it easier for users to communicate.
D: OSPF is a routing protocol. A routing protocol forwards routing information between routers, but does make it easier for users to communicate.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 387
Which of the following was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN?

A. DHCP
B. BootP
C. DNS
D. ARP

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
BOOTP has been used for Unix-like diskless workstations to obtain the network location of their boot image, in addition to the IP address assignment. Enterprises used it to roll out a pre-configured client (e.g., Windows) installation to newly installed PCs.

Incorrect Answers:
A: DHCP is a network protocol used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
C: DNS translates domain names into IP addresses, which enables us to use domain names instead of IP addresses.
D: The ARP protocol translates IP addresses to MAC Addresses.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 585

QUESTION 388
What is the greatest danger from DHCP?

A. An intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients.
B. Having multiple clients on the same LAN having the same IP address.
C. Having the wrong router used as the default gateway.

D. Having the organization's mail server unreachable.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The main security risk concerning DHCP is that unauthorized (rogue) DHCP servers offering IP configuration to DHCP clients. Rogue DHCP servers are often used in man in the middle or denial of service attacks for malicious purposes.

Incorrect Answers:
B: IP address collisions are not a major security risk.
C: Incorrect default gateway is not a major security problem compared to a rogue DHCP Server.
D: An unreachable mail server is not a main security concern compared to the damage a rogue DHCP server can do.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 598

QUESTION 389
Which of the following allows two computers to coordinate in executing software?

A. RSH
B. RPC
C. NFS
D. SNMP

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The programmer of a piece of software can write a function call that calls upon a subroutine. The subroutine could be local to the system or be on a remote system. If the subroutine is on a remote system, it is a Remote Procedure Call (RPC). The RPC request is carried over a session layer protocol. The result that the remote system provides is then returned to the requesting system over the same session layer protocol. With RPC a piece of software can execute components that reside on another system.

Incorrect Answers:

A: The remote shell (rsh) is a command line computer program that can execute shell commands as another user, and on another computer across a computer network. RSH is not used to remotely execute software.
C: The Network File System (NFS) is not used to execute software remotely. NFS is a client/server application that lets a computer user view and optionally store and update file on a remote computer as though they were on the user's own computer.
D: SNMP is used for monitoring the network, not for remote software execution.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 525

QUESTION 390
Which of the following should NOT normally be allowed through a firewall?

A. SNMP
B. SMTP
C. HTTP
D. SSH

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
SNMP is used for monitoring network traffic. SNMP would monitor the traffic on a single segment and there would be no reason to allow SNMP traffic through a firewall.

Incorrect Answers:
B: Users must be allowed to send email messages, so SMTP traffic must be allowed.
C: Users must be allowed to browse the internet, so HTTP traffic must be allowed.
D: Users must be allowed to log into a remote machine and execute commands, so SSH traffic must be allowed.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 587

QUESTION 391
Which of the following NAT firewall translation modes allows a large group of internal clients to share a single or small group of ROUTABLE IP addresses for the purpose of hiding their identities when communicating with external hosts?

A. Static translation

B. Load balancing translation
C. Network redundancy translation
D. Dynamic translation

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Port address translation (PAT) is a dynamic NAT translation. It maps one internal IP address to an external IP address and port number combination. Thus, PAT can theoretically support 65,536 (2 16) simultaneous communications from internal clients over a single external leased IP address.

Incorrect Answers:
A: With static translation each private address is statically mapped to a specific public address.
B: There is no NAT implementation named Load balancing translation.
C: There is no NAT implementation called Network redundancy translation.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 606

QUESTION 392
Which of the following NAT firewall translation modes offers no protection from hacking attacks to an internal host using this functionality?

A. Network redundancy translation
B. Load balancing translation
C. Dynamic translation
D. Static translation

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Static translation offers no protection against IP Spoofing.

Incorrect Answers:
A: There is no NAT firewall translation mode called Network redundancy translation.

B: There is no NAT firewall translation mode called Load balancing translation.
C: Port address translation (PAT) is a dynamic NAT translation. It maps one internal IP address to an external IP address and port number combination. With Dynamic NAT te internal IP address is hidden from external hackers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 606

QUESTION 393
Which of the following is the primary security feature of a proxy server?

A. Virus Detection
B. URL blocking
C. Route blocking
D. Content filtering

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A proxy firewall is a network security system that protects network resources by filtering messages at the application layer. The application-level proxy understands the packet as a whole and can make access decisions based on the content of the packets.

Incorrect Answers:
A: Firewalls does not detect viruses.
B: A proxy server firewall does not use URL blocking.
C: A proxy server firewall does not use route blocking.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 636

QUESTION 394
Which of the following is an advantage of proxies?

A. Proxies provide a single point of access, control, and logging.
B. Proxies must exist for each service.
C. Proxies create a single point of failure.
D. Proxies do not protect the base operating system.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Proxies provide services through a single access point. Proxies can be installed in order to eavesdrop upon the data-flow between client machines and the web. All content sent or accessed – including passwords submitted and cookies used – can be captured and analyzed by the proxy operator.

Incorrect Answers:
B: A proxy can handle many services, not only a single service. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. C: Proxies does not create a single point of failure.
D: Firewall proxies protect the base operating system.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 653

QUESTION 395
Which of the following packets should NOT be dropped at a firewall protecting an organization's internal network?

A. Inbound packets with Source Routing option set
B. Router information exchange protocols
C. Inbound packets with an internal address as the source IP address
D. Outbound packets with an external destination IP address

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Internal users access the internet will create outbound packets with external IP addresses. These legit packets should not be dropped.

Incorrect Answers:
A: Firewalls do not drop packet based on routing options.
B: Firewalls do not drop packet based on routing protocol information.
C: Inbound packets should have an external source address. If the inbound packet has an internal source address it must be dropped.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 396
A packet filtering firewall looks at the data packet to get information about the source and destination addresses of an incoming packet, the protocol (TCP, UDP, or ICMP), and the source and destination port for the:

A. desired service.
B. dedicated service.
C. delayed service.
D. distributed service.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering is a firewall technology that makes access decisions based upon network-level protocol header values. The filters can make access decisions based upon the following basic criteria:
▪ Source and destination port numbers (such as an application port or a service number) ▪
Protocol types
▪ Source and destination IP addresses
▪ Inbound and outbound traffic direction

Incorrect Answers:
B: A packet filtering firewall can grant access to desired services, not dedicated services, through source and destination numbers.
C: A packet filtering firewall can grant access to desired services, not delayed services, through source and destination numbers.
D: A packet filtering firewall can grant access to desired services, not distributed services, through source and destination numbers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 397
Frame relay uses a public switched network to provide:

A. Local Area Network (LAN) connectivity.
B. Metropolitan Area Network (MAN) connectivity.
C. Wide Area Network (WAN) connectivity.

D. World Area Network (WAN) connectivity.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Frame relay is a Wide Area Network (WAN) technology.

Incorrect Answers:
A: Frame relay is not used in local area networks. It is a WAN technology.
B: Frame relay is not used Metropolitan Area Network (MAN) networks. It is a WAN technology.
D: There is no connectivity technology named World Area Network (WAN).

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 677

QUESTION 398
Which of the following is a drawback of fiber optic cables?

A. It is affected by electromagnetic interference (EMI).
B. It can easily be tapped.
C. The expertise needed to install it.
D. The limited distance at high speeds.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Fiber-optic cable is expensive and difficult to work with.

Incorrect Answers:
A: Fiber optic cables are not affected by electromagnetic interference (EMI).
B: Fiber optic cables are hard to tap.
D: Fiber-optic cabling has higher transmission speeds that allow signals to travel over longer distances.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 560

QUESTION 399
Which of the following is the MOST secure firewall implementation?

A. Dual-homed host firewalls
B. Screened-subnet firewalls
C. Screened-host firewalls
D. Packet-filtering firewalls

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A screened-subnet architecture is the most secure solution as it adds another layer of security to the screened-host architecture, which in turn is more secure than both Dual-homed host firewalls and Packet-filtering firewalls.

Incorrect Answers:
A: Dual-homed host firewalls are less secure compared to screened-host firewall.
C: Screened-host firewalls are less secure compared to Screened-subnet firewalls, as the screened-subnet architecture is missing.
A screened host is a firewall that communicates directly with a perimeter router and the internal network.
D: A packet-filtering firewall is part of a screened-host firewall architecture, but is less secure as the screened-host firewall is missing.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 646

QUESTION 400
A Packet Filtering Firewall system is considered a:

A. first generation firewall.
B. second generation firewall.
C. third generation firewall.
D. fourth generation firewall.

Correct Answer: A

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering was the first generation of firewalls and it is the most rudimentary type of all of the firewall technologies.

Incorrect Answers:
B: Packet filtering is a first generation firewall, not a second generation firewall. Application -level gateways are known as second generation firewalls.
C: Packet filtering is a first generation firewall, not a third generation firewall.
D: Packet filtering is a first generation firewall, not a fourth generation firewall.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 401
Proxies work by transferring a copy of each accepted data packet from one network to another, thereby masking the:

A. data's payload.
B. data's details.
C. data's owner.
D. data's origin.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Proxy servers act as an intermediary between the clients that want access to certain services and the servers that provide those services. The proxy server sends an independent request to the destination on behalf of the user, thereby masking the origin of the data.

Incorrect Answers:
A: The proxy server transfer they payload data to the destination.
B: The proxy server transfer they payload data (the details of the data) to the destination.
C: The origin of the data, not the owner of the data, is masked by the proxy server.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 653

QUESTION 402
An application layer firewall is also called a:

A. Proxy
B. A Presentation Layer Gateway.
C. A Session Layer Gateway.
D. A Transport Layer Gateway.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A network-based application layer firewall is a computer networking firewall operating at the application layer of a protocol stack, and is also known as a proxybased or reverse-proxy firewall.

Incorrect Answers:
B: Application layer firewall works at the application layer, not at the presentation layer.
C: Application layer firewall works at the application layer, not at the session layer.
D: Application layer firewall works at the application layer, not at the transport layer.

References:
https://en.wikipedia.org/wiki/Application_firewall#Network-based_application_firewalls

QUESTION 403
Application Layer Firewalls operate at the:

A. OSI protocol Layer seven, the Application Layer.
B. OSI protocol Layer six, the Presentation Layer.
C. OSI protocol Layer five, the Session Layer.
D. OSI protocol Layer four, the Transport Layer.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:

Explanation:
Application layer firewall works at the application layer, which is layer 7 in the OSI model.

Incorrect Answers:
B: Application layer firewalls do not work at OSI layer 6, the presentation layer. They are at the Application layer, layer 7.
C: Application layer firewalls do not work at OSI layer 5, the session layer. They are at the Application layer, layer 7.
D: Application layer firewalls do not work at OSI layer 4, the session layer. They are at the Transport layer, layer 7.

References:
https://en.wikipedia.org/wiki/Application_firewall

QUESTION 404
One drawback of Application Level Firewall is that it reduces network performance due to the fact that it must analyze every packet and:

A. decide what to do with each application.
B. decide what to do with each user.
C. decide what to do with each port.
D. decide what to do with each packet.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The application firewall is typically built to control all network traffic on any OSI layer up to the application layer. At the lowest level the application firewall can examine each data packet. This slows down the performance.

Incorrect Answers:
A: Making decisions at the application level would not slow down the firewall.
B: An application firewall cannot make decisions based on the user.
C: Making decisions at the port level would not slow down the firewall, especially compared deciding what to do with each packet.

References:
https://en.wikipedia.org/wiki/Application_firewall

QUESTION 405
A circuit level proxy is _____ when compared to an application level proxy.

A. lower in processing overhead.
B. more difficult to maintain.
C. more secure.
D. slower.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A circuit level proxy works at the session layer of the OSI model and monitors traffic from a network-based view. This type of proxy cannot “look into” the contents of a packet like an application level proxy; thus, it does not carry out deep-packet inspection. This means that, compared to an application level proxy, A circuit level proxy is faster.

Incorrect Answers:
B: A circuit level proxy is easier to maintain as it is less flexible.
C: A circuit level proxy is less secure since it only works at the session layer, and cannot inspect data packets.
D: A circuit level proxy is faster, not slower.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 636

QUESTION 406
In a stateful inspection firewall, data packets are captured by an inspection engine that is operating at the:

A. Network or Transport Layer.
B. Application Layer.
C. Inspection Layer.
D. Data Link Layer.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A stateful firewall filters traffic based on OSI Layer 3 (Network layer) and Layer 4 (Transport layer).

Incorrect Answers:
B: A stateful firewall does not operate at the Application layer. It work at the Network or Transport Layer.
C: There is no inspection layer in the OSI model.
D: A stateful firewall does not operate at the Data link layer. It work at the Network or Transport Layer.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 63

QUESTION 407
When an outgoing request is made on a port number greater than 1023, this type of firewall creates an ACL to allow the incoming reply on that port to pass:

A. packet filtering
B. Circuit level proxy
C. Dynamic packet filtering
D. Application level proxy

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Ports up to 1023 are called well-known ports and are reserved for server-side services. The sending system must choose a dynamic port higher than 1023 when it sets up a connection with another entity. The dynamic packet-filtering firewall then creates an Access Control List (ACL) that allows the external entity to communicate with the internal system.

Incorrect Answers:
A: A Packet filtering firewall makes access decisions based upon network-level protocol header values. It does not use port numbers.
B: A Circuit level proxy works at the session layer and does not use ports.
D: An Application level proxy works at the packet level, not at the port level.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 640

QUESTION 408
A demilitarized zone is:

A. a part of a network perfectly safe from hackers
B. a militarized network segment
C. a firewall

D. the network segment between the Internet and a private network

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A demilitarized zone (DMZ) is a network segment located between the protected private network and unprotected public network (typically being the Internet).

Incorrect Answers:
A: A demilitarized zone is not safe from hackers as it connected to the Internet.
B: It is a demilitarized, not a militarized, zone.
C: A demilitarized zone is not a firewall. A demilitarized zone is shielded by two firewalls: one facing the Internet, and one facing the private network.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 628

QUESTION 409
A DMZ is located:

A. right behind your first Internet facing firewall
B. right in front of your first Internet facing firewall
C. right behind your first network active firewall
D. right behind your first network passive Internet http firewall

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A demilitarized zone is shielded by two firewalls: one right behind the first Internet facing the Internet, and one facing the private network.
Incorrect Answers:
B: A demilitarized zone is shielded by the Internet facing firewall. It is not placed outside this firewall.
C: A demilitarized zone is placed behind the first Internet facing firewall, not behind the first network active firewall.
D: A demilitarized zone does not need to be placed behind a network passive Internet http firewall. It just needs to be place behind the first Internet facing firewall.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 629

QUESTION 410
The DMZ does not normally contain:

A. encryption server
B. web server
C. external DNS server
D. mail relay

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The DMZ usually contains web servers, mail servers, and external DNS servers.

Incorrect Answers:
B: A web server is usually located in the DMZ.
C: An external web server is usually located in the DMZ.
D: A mail server is usually located in the DMZ.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 629

QUESTION 411
A DMZ is also known as a:
A. screened subnet.

B. three legged firewall.
C. place to attract hackers.
D. bastion host.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
With a screened subnet, two firewalls are used to create a DMZ.

Incorrect Answers:
B: The three legged model is just one way of implementing a DMZ. A DMZ can be implemented in different ways.
C: A place to attract hackers is called a honeypot, not a DMZ.
D: A bastion host is not a DMZ. It is a computer that is fully exposed to attack.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 646

QUESTION 412
Network-based Intrusion Detection systems:

A. commonly reside on a discrete network segment and monitor the traffic on that network segment.
B. commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
C. commonly reside on a discrete network segment and does not monitor the traffic on that network segment.
D. commonly reside on a host and monitor the traffic on that specific host.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A network - based IDS (Intrusion Detection systems) watches for questionable activity occurring on the network medium by inspecting packets and observing network traffic patterns.

Incorrect Answers:
B: The networked-based ISD must be present on the network segment it is monitoring.

C: The purpose of an Intrusion Detection system is to monitor the traffic.
D: A host-based, not a network-based, IDS watches for questionable activity on a single computer system.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 54

QUESTION 413
Which of the following are additional terms used to describe knowledge-based IDS and behavior-based IDS?

A. Signature-based IDS and statistical anomaly-based IDS, respectively.
B. Signature-based IDS and dynamic anomaly-based IDS, respectively.
C. Anomaly-based IDS and statistical-based IDS, respectively.
D. Signature-based IDS and motion anomaly-based IDS, respectively.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Knowledge-based detection is also called signature-based detection. In this case the IDS use a signature database and attempts to match all monitored events to its contents.
Behavior-based detection is also called statistical intrusion detection, anomaly detection, and heuristics-based detection.

Incorrect Answers:
B: Behavior-based IDS is not dynamical anomaly-based. Behavior-based IDS can be said to be statistical anomaly-based.
C: A knowledge-based IDS uses signatures, not anomalies.
D: Motion anomaly-based IDS is not a synonym for behavior-based IDS.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 56

QUESTION 414
Knowledge-based Intrusion Detection Systems (IDS) are more common than:

A. Network-based IDS
B. Host-based IDS

C. Behavior-based IDS
D. Application-Based IDS

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
An IDS can detect malicious behavior using two common methods. One way is to use knowledge-based detection which is more frequently used. The second detection type is behavior-based detection.

Incorrect Answers:
A: A Network-based IDS is not a type of Knowledge-based Intrusion Detection System.
B: A host-based IDS is not a type of Knowledge-based Intrusion Detection System.
D: An application-based IDS is not a type of Knowledge-based Intrusion Detection System.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 56

QUESTION 415
Which cable technology refers to the CAT3 and CAT5 categories?

A. Coaxial cables
B. Fiber Optic cables
C. Axial cables
D. Twisted Pair cables

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Twisted-pair cables are categorized into UTP categories CAT1, CAT2, CAT3, CAT4, CAT5, etc.

Incorrect Answers:
A: Coaxial cables do not have categories named CAT3 or CAT5.

B: Fiber optic cables do not have categories named CAT3 or CAT5.
C: Axial cables do not have categories named CAT3 or CAT5.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 559

QUESTION 416
The older coaxial cable has been widely replaced with twisted pair, which is extremely easy to work with, inexpensive, and also resistant to multiple host failure at once, especially when used in one of the following topology:

A. Token Passing Configuration.
B. Star Configuration.
C. Ring Configuration.
D. Point to Point Configuration.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In Star topologies twisted-pair cabling is the preferred cabling.

Incorrect Answers:
A: In a Token Passing configuration Coaxial cabling works fine.
C: In a Ring configuration Coaxial cabling works fine.
D: Twisted cable has not special advantage compared to other cabling in a point-to-point configuration.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 92

QUESTION 417
Which of the following was designed as a more fault-tolerant topology than Ethernet, and very resilient when properly implemented?

A. Token Link.
B. Token system.
C. Token Ring.
D. Duplicate ring.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Token Ring has a built in management and recovery system which makes it very fault tolerant.

Incorrect Answers:
A: Token link is not a network topology.
B: Token system is not a network topology.
D: Duplicate ring is not a network topology.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 570

QUESTION 418
Which of the following should be used as a replacement for Telnet for secure remote login over an insecure network?

A. S-Telnet
B. SSL
C. Rlogin
D. SSH

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Secure Shell (SSH) works as a type of tunneling mechanism that delivers terminal like access to remote computers. SSH should be used instead of Telnet, FTP, rlogin, rexec, or rsh, because it is more secure.

Incorrect Answers:
A: S-Telnet is only used for IBM 5250 data streams.
B: SSL is supported for Telnet implementations.
C: Rlogin is a software utility for Unix-like computer operating systems that enables users to log in on another host via a network. It is, however, less secure that SSH.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 860 https://en.wikipedia.org/wiki/Telnet https://en.wikipedia.org/wiki/Rlogin

QUESTION 419
Which of the following is LESS likely to be used today in creating a Virtual Private Network?

A. L2TP
B. PPTP
C. IPSec
D. L2F

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Layer 2 Forwarding Protocol (L2F) is rarely used today.
The following are the three most common VPN communications protocol standards:

- Point-to-Point Tunneling Protocol (PPTP). PPTP works at the Data Link Layer of the OSI model. Designed for individual client to server connections, it enables only a single point-to-point connection per session. This standard is very common with asynchronous connections that use Win9x or NT clients. PPTP uses native Point-to-Point Protocol (PPP) authentication and encryption services.
- Layer 2 Tunneling Protocol (L2TP). L2TP is a combination of PPTP and the earlier Layer 2 Forwarding Protocol (L2F) that works at the Data Link Layer like PPTP. It has become an accepted tunneling standard for VPNs. In fact, dial-up VPNs use this standard quite frequently. Like PPTP, this standard was designed for single point-topoint client to server connections. Note that multiple protocols can be encapsulated within the L2TP tunnel.
- IPSec. IPSec operates at the Network Layer and it enables multiple and simultaneous tunnels, unlike the single connection of the previous standards. IPSec has the functionality to encrypt and authenticate IP data. It is built into the new IPv6 standard, and is used as an add-on to the current IPv4. While PPTP and L2TP are aimed more at dial-up VPNs, IPSec focuses more on network-to-network connectivity.

Incorrect Answers:
A: L2TP and IPSec are commonly used together for VPNs today.
B: PPTP is not used as commonly as L2TP and IPSec but it is more common than L2F.
C: L2TP and IPSec are commonly used together for VPNs today.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 92

QUESTION 420

Which of the following answers presents the MOST significant threat to network based IDS or IPS systems?

A. Encrypted Traffic
B. Complex IDS/IPS Signature Syntax
C. Digitally Signed Network Packets
D. Segregated VLANs

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Encrypted network packets present the biggest threat to an effective IDS/IPS plan because the network traffic cannot easily be decoded and examined. Encrypted packets cannot be examined by the IDS to determine if there is a threat there so in most cases the traffic is just forwarded along with the potential threat.

There is an industry where a company provides examination services for your network traffic, acting like a proxy server for all your network traffic. You simply send them copies of your certificates so they can decode the traffic. This is common in the financial industry where violating federal law or being sued by federal investigators for insider trading can lead to business collapse.
The external company examines all the network traffic coming and going from your network for potential liabilities.

Incorrect Answers:
B: Complex IDS/IPS Signature syntax: IDS/IPS signatures can be complex but this is not the MOST significant threat to the functionality of an IDS/IPS system.
C: Digitally Signed Network Packets: This is not threat to IDS/IPS systems looking for dangerous network traffic.
D: Segregated VLANs are only a threat if the IDS/IPS system is not monitoring traffic on the segregated VLAN. VLANs can present barriers to IDS/IPS systems spotting dangerous traffic. There is an easy solution to VLANs and IDS/IPS systems and that would be simply placing an IDS/IPS sensor on that VLAN and set it up to send its traffic to the IDS/IPS management system.

QUESTION 421
Which of the following is NOT a countermeasure to traffic analysis?

A. Padding messages.
B. Eavesdropping.
C. Sending noise.
D. Faraday Cage

Correct Answer: B

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Eavesdropping is not a countermeasure, it is a type of attack where you are collecting traffic and attempting to see what is being sent between entities communicating with each other.
Traffic analysis, which is sometimes called trend analysis, is a technique employed by an intruder that involves analyzing data characteristics (message length, message frequency, and so forth) and the patterns of transmissions (rather than any knowledge of the actual information transmitted) to infer information that is useful to an intruder.
Countermeasures to traffic analysis are similar to the countermeasures to cryptoattacks:
- Padding messages. Creating all messages to be a uniform data size by filling empty space in the data.
- Sending noise. Transmitting non-informational data elements mixed in with real information to disguise the real message

Faraday cage can also be used as a countermeasure to traffic analysis as it prevents intruders from being able to access information emitted via electrical signals from network devices

Incorrect Answers:
A: Padding messages (creating all messages to be a uniform data size by filling empty space in the data) is a countermeasure to traffic analysis.
C: Sending noise (transmitting non-informational data elements mixed in with real information to disguise the real message) is a countermeasure to traffic analysis.
D: Faraday cage (preventing intruders from being able to access information emitted via electrical signals from network devices) is a countermeasure to traffic analysis.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 334

QUESTION 422
Which of the following describes the sequence of steps required for a Kerberos session to be established between a user (Principal P1), and an application server (Principal P2)?

A. Principals P1 and Principals P2 authenticate to the Key Distribution Center (KDC),
B. Principal P1 receives a Ticket Granting Ticket (TGT), and then Principal P2 requests a service ticket from the KDC.
C. Principal P1 authenticates to the Key Distribution Center (KDC), Principal P1 receives a Ticket Granting Ticket (TGT), and Principal P1 requests a service ticket from the Ticket Granting Service (TGS) in order to access the application server P2
D. Principal P1 authenticates to the Key Distribution Center (KDC),
E. Principal P1 requests a Ticket Granting Ticket (TGT) from the authentication server, and then Principal P1 requests a service ticket from the application server P2

F. Principals P1 and P2 authenticate to the Key Distribution Center (KDC), Principal P1 requests a Ticket Granting Ticket (TGT) from the authentication server, and application server P2 requests a service ticket from P1

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In the following sequence, the user (Principle P1) is Emily and the server (Principal P2) is a print server:

1. Emily comes in to work and enters her username and password into her workstation at 8:00 A.M. The Kerberos software on Emily's computer sends the username to the authentication service (AS) on the KDC, which in turn sends Emily a ticket granting ticket (TGT) that is encrypted with Emily's password (secret key).
2. If Emily has entered her correct password, then this TGT is decrypted and Emily gains access to her local workstation desktop.
3. When Emily needs to send a print job to the print server, her system sends the TGT to the ticket granting service (TGS), which runs on the KDC, and a request to access the print server. (The TGT allows Emily to prove she has been authenticated and allows her to request access to the print server.)
4. The TGS creates and sends a second ticket to Emily, which she will use to authenticate to the print server. This second ticket contains two instances of the same session key, one encrypted with Emily's secret key and the other encrypted with the print server's secret key. The second ticket also contains an authenticator, which contains identification information on Emily, her system's IP address, sequence number, and a timestamp.
5. Emily's system receives the second ticket, decrypts and extracts the embedded session key, adds a second authenticator set of identification information to the ticket, and sends the ticket on to the print server.
6. The print server receives the ticket, decrypts and extracts the session key, and decrypts and extracts the two authenticators in the ticket. If the print server can decrypt and extract the session key, it knows the KDC created the ticket, because only the KDC has the secret key used to encrypt the session key. If the authenticator information that the KDC and the user put into the ticket matches, then the print server knows it received the ticket from the correct principal.
7. Once this is completed, it means Emily has been properly authenticated to the print server and the server prints her document.

Incorrect Answers:
A: Principal P2 does not need to authenticate to the Key Distribution Center (KDC). There are more steps required than there are listed in this answer.
B: Principal P1 must authenticate first. Principal P2 does not request a service ticket from the KDC. There are more steps required than there are listed in this answer.
D: There are more steps required than there are listed in this answer.
E: Principal P1 must authenticate first. Principal P1 does not request a service ticket from the application server P2. There are more steps required than there are listed in this answer.
F: Principal P2 does not need to authenticate to the Key Distribution Center (KDC). Principal P2 does not request a service ticket from Principal P1. There are more steps required than there are listed in this answer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 210

QUESTION 423
A packet containing a long string of NOP's followed by a command is usually indicative of what?

A. A syn scan.
B. A half-port scan.
C. A buffer overflow attack.
D. A packet destined for the network's broadcast address.

Correct Answer: C
Section: Communication and Network Security
Explanation
Explanation/Reference:
Explanation:
In a carefully crafted buffer overflow attack, the stack is filled properly so the return pointer can be overwritten and control is given to the malicious instructions that have been loaded onto the stack instead of back to the requesting application. This allows the malicious instructions to be executed in the security context of the requesting application. In this example the buffer is filled with NOP's (No Operation) commands followed by the instruction that the attacker wants to be executed.

Incorrect Answers:
A: Syn scanning is not done by sending a packet with a long string of instructions. Syn scanning s is done by sending a SYN (synchronization) packet, as if to initiate a three-way handshake, to every port on the server.
B: A port scan is not done by sending a single packet with long string of instructions. A port scan, such as a half-port scan, is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides.
D: The purpose of sending this packet filled of instructions is likely to be a buffer-overflow attack, not that the packet is destined for the network's broadcast address.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 335

QUESTION 424
Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

A. Plan for implementing workstation locking mechanisms.
B. Plan for protecting the modem pool.
C. Plan for providing the user with his account usage information.
D. Plan for considering proper authentication options.

Correct Answer: D

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
LANs are typically protected from the Internet by firewalls. However, to allow external access to a LAN, you need to open ports on the firewall to allow the connections. With the firewall allowing external connections into the LAN, your last line of defense is authentication. You need to ensure that the remote user connecting to the LAN is who they say they are. Therefore, before allowing external access into a LAN, you should plan and implement proper authentication.

Incorrect Answers:
A: Workstation locking mechanisms are not the most important consideration when allowing external access to a LAN. Without the proper authentication mechanism in place, an intruder could connect to the LAN from an unlocked workstation.
B: Protecting the modem pool (if a modem pool is used to provide the remote access) is not the most important consideration when allowing external access to a LAN. Without the proper authentication mechanism in place, an intruder could connect to the LAN.
C: Providing the user with his account usage information is not the most important consideration when allowing external access to a LAN. Protecting LAN resources by ensuring only authorized people can connect to the LAN is far more important.

QUESTION 425
Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered. There are two basic IDS analysis methods that exist.

Which of the basic method is more prone to false positive?

A. Pattern Matching (also called signature analysis)
B. Anomaly Detection
C. Host-based intrusion detection
D. Network-based intrusion detection

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Anomaly Detection IDS learns about the normal activities and events on your system by watching and tracking what it sees. Once it has accumulated enough data about normal activity, it can detect abnormal and possibly malicious activities or events. There is a small risk that some non-harmful activity is classified as anomaly by mistake – false positives can occur.

Incorrect Answers:

A: A Pattern Matching IDS uses a signature database and attempts to match all monitored events to its contents. Only activities present in the database will be detected. There will be no false positives.
C: Host-based intrusion detection is not an IDS analysis method. It is a classification on information source.
A host - based IDS watches for questionable activity on a single computer system, especially by watching audit trails, event logs, and application logs.
D: Network-based intrusion detection is not an IDS analysis method. It is a classification on information course. Here the source is a network segment.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 56

QUESTION 426
You are part of a security staff at a highly profitable bank and each day, all traffic on the network is logged for later review. Every Friday when major deposits are made you're seeing a series of bits placed in the "Urgent Pointer" field of a TCP packet. This is only 16 bits which isn't much but it concerns you because:

A. This could be a sign of covert channeling in bank network communications and should be investigated.
B. It could be a sign of a damaged network cable causing the issue.
C. It could be a symptom of malfunctioning network card or drivers and the source system should be checked for the problem.
D. It is normal traffic because sometimes the previous fields 16 bit checksum value can over run into the urgent pointer's 16 bit field causing the condition.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Some Intrusion Detection System (IDS) evasion techniques involve deliberately violating the TCP or IP protocols in a way the target computer will handle differently from the IDS. For example, the TCP Urgent Pointer is handled differently on different operating systems and may not be handled correctly by the IDS.

Incorrect Answers:
B: It is very unlikely that a changed TCP Urgent pointer value is caused by a hardware problem, such as a damaged network cable.
C: It is very unlikely that a changed TCP Urgent pointer value is caused by a hardware problem, such as a damaged network card, or by a corrupt driver.
D: The TCP Urgent pointer field does not contain checksums.

References:
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

QUESTION 427
What would you call the process that takes advantages of the security provided by a transmission protocol by carrying one protocol over another?

A. Piggy Backing
B. Steganography
C. Tunneling
D. Concealing

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A tunneling protocol allows a network user to access or provide a network service that the underlying network does not support or provide directly. Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, one use of tunneling is to hide the nature of the traffic that is run through the tunnels.

Incorrect Answers:
A: Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge.
B: Steganography uses files, not protocols. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.
D: One protocol carrying another is called tunneling, not concealing.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 702

QUESTION 428
At which OSI layer does SSL reside in?

A. Application
B. Session
C. Transport
D. Network

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:

Explanation:
SSL encryption takes place at the transport layer.

Incorrect Answers:
A: SSL resides at transport layer, not at the application layer.
B: SSL resides at transport layer, not at the session layer.
D: SSL resides at transport layer, not at the network layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 846

QUESTION 429
A smart Card that has two chips with the Capability of utilizing both Contact and Contactless formats is called:

A. Contact Smart Cards
B. Contactless Smart Cards
C. Hybrid Cards
D. Combi Cards

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A smart Card that has two chips with the ability of utilizing both Contact and Contactless formats is called a combi card.

Incorrect Answers:
A: Contact Smart Cards are not configured for the Contactless format.
B: Contactless Smart Cards are not configured for the Contact format
C: The hybrid card makes use of two CPU chips for processing and includes both contact-oriented and contactless components.
D: The combi-card is similar to the hybrid card, but it only uses a single CPU chip for the processing.

References:
Miller, David R, *CISSP Training Kit*, O'Reilly Media, 2013, Sebastopol, p. 82
http://www.smartcardalliance.org/pages/smart-cards-intro-primer

QUESTION 430
The BEST technique to authenticate to a system is to:

A. establish biometric access through a secured server or Web site.
B. ensure the person is authenticated by something he knows and something he has.
C. maintain correct and accurate ACLs (access control lists) to allow access to applications.
D. allow access only through user ID and password.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
This is a tricky question. Normally, biometrics is the preferred answer as it is a more secure means of authentication than even multi-factor authentication. However, you would not establish biometric access through a secured server or Web site. Therefore, the answer must be “Ensure the person is authenticated by something he knows and something he has”. This is an example of two-factor authentication.

Incorrect Answers:
A: You would not establish biometric access through a secured server or Web site.
C: Maintain correct and accurate ACLs is always a good idea. However, this provides no authentication solution as required by the question.
D: A user ID and password is single-factor authentication. The user ID and the password are both “something you

QUESTION 431
Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

A. Palm Scan
B. Hand Geometry
C. Fingerprint
D. Retina scan

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A system that reads a person’s retina scans the blood-vessel pattern of the retina on the backside of the eyeball. This pattern has shown to be extremely unique between different people. A camera is used to project a beam inside the eye and capture the pattern and compare it to a reference file recorded previously. Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye.

Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

Incorrect Answers:
A: While requiring contact with a surface shared by others, a palm scan is generally considered more acceptable than sharing a surface with other parts of the anatomy. Therefore, this answer is incorrect.
B: A Hand Geometry scan is less accurate and more acceptable than a retina scan. Therefore, this answer is incorrect.
C: A fingerprint scan is more acceptable to users than a retina scan. Users are much more likely to prefer placing their fingers on a fingerprint scanner than looking into a retina scanner. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 60
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 191

QUESTION 432
Identity Management solutions include such technologies as Directories services, Single Sign-On and Web Access management. There are many reasons for management to choose an identity management solution.

Which of the following is a key management challenge regarding identity management solutions?

A. Increasing the number of points of failures.
B. Users will no longer be able to "recycle" their password for different applications.
C. Costs increase as identity management technologies require significant resources.
D. It must be able to scale to support high volumes of data and peak transaction rates.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identity management is the combination of business process and technology used to manage data on IT systems and applications about users. Managed data includes user objects, identity attributes, security entitlements and authentication factors.
Enterprises manage identity data about two broad kinds of users:
▪ Insiders: including employees and contractors. They often access multiple internal systems and their identity profiles are relatively complex. ▪
Outsiders: including customers, partners and vendors. There are normally many more outsiders than insiders.

One of the challenges presented by Identity management is scalability.
Enterprises manage user profile data for large numbers of people. There may be tens of thousands of insiders and hundreds of thousands of outsiders.
Any identity management system used in this environment must scale to support the data volumes and peak transaction rates produced by large user populations.

Incorrect Answers:
A: Increasing the number of points of failures is not key management challenge regarding identity management solutions. There should be no single points of failure but this would be more of a concern for the IT department than management.
B: Users not being able to “recycle” their password for different applications is not a concern for management.
C: A working scalable identity management system is more important to management than the cost. The resource requirement for identity management technologies is not that much when compared to the cost of other systems.

References:
http://hitachi-id.com/password-manager/docs/defining-enterprise-identity-management.html

QUESTION 433
When submitting a passphrase for authentication, the passphrase is converted into:

A. a virtual password by the system.
B. a new passphrase by the system.
C. a new passphrase by the encryption technology
D. a real password by the system which can be used forever.

Correct Answer: A
Section: Identity and Access Management
Explanation
Explanation/Reference:
Explanation:
A passphrase is a sequence of characters that is longer than a password. The user enters this phrase into an application, and the application transforms the value into a virtual password, making the passphrase the length and format that is required by the application. (For example, an application may require your virtual password to be 128 bits to be used as a key with the AES algorithm.) If a user wants to authenticate to an application, such as Pretty Good Privacy (PGP), he types in a passphrase, let’s say StickWithMeKidAndYouWillWearDiamonds. The application converts this phrase into a virtual password that is used for the actual authentication.
A passphrase is more secure than a password because it is longer, and thus harder to obtain by an attacker. In many cases, the user is more likely to remember a passphrase than a password.

Incorrect Answers:
B: The passphrase is not converted into a new passphrase by the system.
C: The passphrase is not converted into a new passphrase by the encryption technology.
D: The passphrase is not converted into a real password by the system which can be used forever.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 199
http://www.itl.nist.gov/fipspubs/fip112htm

QUESTION 434
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

A. Extensible Authentication Protocol
B. Challenge Handshake Authentication ProtocolC. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Extensible Authentication Protocol (EAP) is defined as:
A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences.

The Extensible Authentication Protocol (EAP) is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

Incorrect Answers:
B: The definition in the question does not describe Challenge Handshake Authentication Protocol.
C: The definition in the question does not describe Remote Authentication Dial-In User Service.
D: The definition in the question does not describe Multilevel Authentication Protocol.

References:
http://www.sans.org/security-resources/glossary-of-terms/?pass=e
http://searchsecurity.techtarget.com/definition/Extensible-Authentication-Protocol-EAP

QUESTION 435
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:

A. 100 subjects per minute.
B. 25 subjects per minute.C. 10 subjects per minute.
D. 50 subjects per minute.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a system. Acceptable throughput rates are in the range of 10 subjects per minute.

Incorrect Answers:
A: 100 subjects per minute is just over half a second per user. This is way faster than is necessary.
B: 25 subjects per minute is less than 3 seconds per user. This is faster than necessary as people using a biometric scanner would not use it that quickly.
D: 50 subjects per minute is just over one second per user. This is faster than necessary as people using a biometric scanner would not use it that quickly.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 59

QUESTION 436
Which of the following biometric parameters are better suited for authentication use over a long period of time?
A. Iris pattern
B. Voice pattern
C. Signature dynamics
D. Retina pattern

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Of the answers given, the iris is the least likely to change over a long period of time which makes the iris pattern better suited for authentication use over a long period of time.
The iris is the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas, and furrows. The uniqueness of each of these characteristics within the iris is captured by a camera and compared with the information gathered during the enrollment phase. Of the biometric systems, iris scans are the most accurate. The iris remains constant through adulthood, which reduces the type of errors that can happen during the authentication process.

Incorrect Answers:

B: A person's voice pattern is less suited for authentication use over a long period of time because the voice pattern can change over time.
C: A person's signature is less suited for authentication use over a long period of time because the signature can change over time.
D: A person's retina pattern is less suited for authentication use over a long period of time because the retina pattern can change over time and can be changed by illnesses such as Diabetes.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 191

QUESTION 437
Which of the following is NOT a disadvantage of Single Sign On (SSO)?

A. Support for all major operating system environment is difficult
B. The cost associated with SSO development can be significant
C. SSO could be single point of failure and total compromise of an organization asset
D. SSO improves an administrator's ability to manage user's account and authorization to all associated system

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Single sign-on (SSO) gives the administrator the ability to streamline user accounts and better control access rights. It, therefore, improves an administrator's ability to manage users and user configurations to all associated systems.

Incorrect Answers:
A: A disadvantage of SSO is that insufficient software solutions accommodate all major operating system environments. A mix of solutions must, therefore, be adapted to the enterprise's IT architecture and strategic direction.
B: A disadvantage of SSO is that considerable interface development and maintenance may be required, which could be costly.
C: SSO could be single point of failure and total compromise of an organization asset. This means that that if an attacker uncovers a credential set, the attacker would have access to every resource within the environment that the compromised account has access to.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 207-209

QUESTION 438
Another type of access control is lattice-based access control. In this type of control a lattice model is applied. How is this type of access control concept applied?

A. The pair of elements is the subject and object, and the subject has an upper bound equal or higher than the upper bound of the object being accessed.

B. The pair of elements is the subject and object, and the subject has an upper bound lower than the upper bound of the object being accessed.
C. The pair of elements is the subject and object, and the subject has no special upper or lower bound needed within the lattice.
D. The pair of elements is the subject and object, and the subject has no access rights in relation to an object.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A lattice is a mathematical construct that is built upon the notion of a group. The most common definition of the lattice model is "a structure consisting of a finite partially ordered set together with least upper and greatest lower bound operators on the set." Two methods are commonly used for applying mandatory access control:

- Rule-based (or label-based) access control: This type of control further defines specific conditions for access to a requested object. A Mandatory Access Control system implements a simple form of rule-based access control to determine whether access should be granted or denied by matching: - An object's sensitivity label
  - A subject's sensitivity label
- Lattice-based access control: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

Incorrect Answers:
B: The subject's upper bound must be equal or higher, not lower than the upper bound of the object being accessed.
C: The subject must have an upper bound.
D: The subject must have access rights determined by an upper bound.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 381
https://en.wikipedia.org/wiki/Computer_access_control http://en.wikipedia.org/wiki/Lattice-based_access_control

QUESTION 439
In the context of Biometric authentication, there is a quick way to compare the accuracy of devices. In general, the devices that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

A. the CER is used.
B. the FRR is used
C. the FAR is used
D. the FER is used

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three main performance measures in biometrics. These measures are as follows:
- False Rejection Rate (FRR) or Type I Error. The percentage of valid subjects that are falsely rejected.
- False Acceptance Rate (FAR) or Type II Error. The percentage of invalid subjects that are falsely accepted.
- Crossover Error Rate (CER). The percent in which the False Rejection Rate equals the False Acceptance Rate.

Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher FRR. Conversely, if the sensitivity is decreased, the FAR will increase. Thus, to have a valid measure of the system performance, the CER is used.

Incorrect Answers:
B: FRR is the percentage of valid subjects that are falsely rejected. It is not used to compare accuracy of biometric devices.
C: FAR is the percentage of invalid subjects that are falsely accepted. It is not used to compare accuracy of biometric devices.
D: FER is not used to compare accuracy of biometric devices.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 59
https://en.wikipedia.org/wiki/Biometrics

QUESTION 440
Which of the following biometric devices has the lowest user acceptance level?

A. Retina Scan
B. Fingerprint scan
C. Hand geometry
D. Signature recognition

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:

Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye.
Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

Incorrect Answers:
A: While requiring contact with a surface shared by others, a fingerprint scan is generally considered more acceptable than sharing a surface with other parts of the anatomy.
B: While requiring contact with a surface shared by others, a hand geometry scan is generally considered more acceptable than sharing a surface with other parts of the anatomy.
C: A signature does not involve contact with a surface shared by others and is therefore more acceptable than other biometric methods.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 60
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 191
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy

QUESTION 441
Which of the following would be an example of the BEST password?

A. golf001
B. Elizabeth
C. T1me4g0lF
D. password

Correct Answer: C
Section: Identity and Access Management
Explanation
Explanation/Reference:
Explanation:
The following four rules apply to what can be contained in a password. The more rules that are met by a password, the stronger the password is. Passwords should contain uppercase characters Passwords should contain lowercase characters
Passwords should contain base 10 digits (0 through 9)
Passwords should contain nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
Further to the list above, passwords should be at least eight characters long and not include names, usernames or dictionary words.

The password T1me4g0lF meets three of the above rules. It contains uppercase characters, numeric characters and lowercase characters. This is the strongest password of the options given.

Incorrect Answers:
A: golf001 meets only two of the password rules. It contains lowercase and numeric characters. This is not the strongest password.
B: Elizabeth meets only two of the password rules. It contains lowercase and numeric characters. Furthermore, the password is a name which makes it easier to guess. This is not the strongest password.
D: 'password' is a very weak password. It meets only one password rule (it contains lowercase letters). It is also one of the most easily guessed passwords there is.

References:
http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password

QUESTION 442
Which of the following does NOT apply to system-generated passwords?

A. Passwords are harder to remember for users.
B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
C. Passwords are more vulnerable to brute force and dictionary attacks.
D. Passwords are harder to guess for attackers.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Passwords that are generated by a system or a password generation tool are robust passwords in that they will contain a mix of uppercase characters, lowercase characters, numbers and non-alphanumeric characters.
One of the benefits of system-generated passwords is that they are LESS (not more) vulnerable to brute force and dictionary attacks.

Incorrect Answers:
A: It is true that system-generated passwords are harder to remember for users. This is due to the complexity of the password.
B: It is true that if the password-generating algorithm gets to be known, the entire system is in jeopardy. This is because it would be possible to crack the passwords by using the algorithm used to create the passwords.
D: It is true that system-generated passwords are harder to guess for attackers. This is due to the complexity of the password.

QUESTION 443
What is the MOST critical characteristic of a biometric identifying system?

A. Perceived intrusiveness
B. Storage requirements

C. Accuracy
D. Scalability

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Biometrics are based on the Type 3 authentication mechanism — something you are. Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
The most critical characteristic of a biometric identifying system (or any other identification and authentication system) is the accuracy of the system. The system needs to ensure that the identification of the person is correct.

Incorrect Answers:
A: The perceived intrusiveness of a biometric system is an important consideration. Users will not be happy to use a system which is perceived to be too intrusive. However, this is not as critical as the accuracy of the system.
B: The storage requirement of a biometric system is not an important consideration. Storage is cheap nowadays and biometric data does not require much storage space.
D: The scalability of a biometric system could be an important consideration if the company intends to expand in the future although most biometric systems are easily scalable. However, this is not as critical as the accuracy of the system.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 58

QUESTION 444
What is considered the MOST important type of error to avoid for a biometric access control system?

A. Type I Error
B. Type II Error
C. Combined Error Rate
D. Crossover Error Rate

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:

A Type II Error occurs when the system accepts impostors who should be rejected. This type of error is the most dangerous type, and therefore the most important to avoid.

Incorrect Answers:
A: A Type I Error is when a biometric system rejects an authorized individual. It is not as dangerous as a Type II Error, and therefore not the most important to avoid.
C: Combined Error Rate is not a valid type of biometric error.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate. It is the most important measurement when determining the system's accuracy.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 188

QUESTION 445
How can an individual/person BEST be identified or authenticated to prevent local masquerading attacks?

A. User Id and password
B. Smart card and PIN code
C. Two-factor authentication
D. Biometrics

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Masquerading is the term used when one user pretends to be another user. Strong authentication is the best defense against this. Authentication is based on the following three factor types: ▪ Type 1. Something you know, such as a PIN or password
▪ Type 2. Something you have, such as an ATM card or smart card
▪ Type 3. Something you are (physically), such as a fingerprint or retina scan

Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification.
A biometric authentication such as a fingerprint cannot be imitated which makes biometrics the best defense against masquerading attacks.

Incorrect Answers:

A: A user Id and password can be guessed by an attacker. This is not the best identification and authentication method to prevent local masquerading attacks.
B: A smart card can be stolen and the PIN guessed by an attacker. This is not the best identification and authentication method to prevent local masquerading attacks.
C: Two-factor authentication is more secure than other methods but still less secure than biometrics. Two-factor authentication could comprise of “something you have” and “something you know”. The “something you have” such as a smart card could be stolen by an attacker and the “something you know” such as a PIN could be guessed. This is not the best identification and authentication method to prevent local masquerading attacks.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 57
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 187

QUESTION 446
What are cognitive passwords?

A. Passwords that can be used only once.
B. Fact or opinion-based information used to verify an individual's identity.
C. Password generators that use a challenge response scheme.
D. Passphrases.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Cognitive passwords refer to fact-based or opinion-based information used to verify the identity of an individual. The cognitive password enrollment process requires the answering of some questions based on the user’s life experiences.

Incorrect Answers:
A: Passwords that can be used only once are known as one-time passwords (OTPs).
C: Password generators that use a challenge response scheme are known as asynchronous token devices.
D: A passphrase is a sequence of characters that is longer than a password.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 195-199

QUESTION 447
Which of the following biometrics devices has the highest Crossover Error Rate (CER)?

A. Iris scan
B. Hand geometry
C. Voice pattern
D. Fingerprints

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three main performance measures in biometrics. These measures are as follows:
- False Rejection Rate (FRR) or Type I Error. The percentage of valid subjects that are falsely rejected.
- False Acceptance Rate (FAR) or Type II Error. The percentage of invalid subjects that are falsely accepted.
- Crossover Error Rate (CER). The percent in which the False Rejection Rate equals the False Acceptance Rate.

Voice pattern biometrics have the highest Crossover Error Rate (CER). This is because voice patterns tend to change with the individual's mood and health. The common cold or flu, for instance, would alter the tone and pitch of a person's voice.

Incorrect Answers:
A: Iris scan biometric devices do not have the highest Crossover Error Rate (CER) due to the accuracy of an iris scan and the fact that the iris rarely changes. B: Hand geometry biometric devices do not have the highest Crossover Error Rate (CER) due to the accuracy of a hand geometry scan the fact that the hand rarely changes.
D: Fingerprint biometric devices do not have the highest Crossover Error Rate (CER) due to the accuracy of fingerprint scan the fact that the fingerprint rarely changes.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 59

QUESTION 448
What is the PRIMARY use of a password?

A. Allow access to files.
B. Identify the user.
C. Authenticate the user.
D. Segregate various users' accesses.

Correct Answer: C

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A protected string of characters, known as a password, is used to authenticate an individual.

Incorrect Answers:
A: The primary use of a password is not to allow access to files, it is to authenticate an individual.
B: The primary use of a password is not to identify an individual, it is to authenticate an individual.
D: The primary use of a password is not to divide various user's accesses, it is to authenticate an individual.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 192

QUESTION 449
The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:

A. you need.
B. you read.
C. you are.
D. you do.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three common factors that can be used for authentication:
- Something a person knows.
- Something a person has.
- Something a person is.

Incorrect Answers:
A, B, D: These answers are not valid classic authentication factors.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 162

QUESTION 450
An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?

A. Discretionary Access
B. Least Privilege
C. Mandatory Access
D. Separation of Duties

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more.

Incorrect Answers:
A: A: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
C: Mandatory Access control is based on a security label system
D: Separation of Duties is a preventive administrative control that is used to make sure one person is unable to carry out a critical task alone.

References:
https://en.wikipedia.org/wiki/Principle_of_least_privilege
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 126, 220-228

QUESTION 451
Pin, Password, Passphrases, Tokens, smart cards, and biometric devices are all items that can be used for Authentication. When one of these items listed above in conjunction with a second factor to validate authentication, it provides robust authentication of the individual by practicing which of the following?

A. Multi-party authentication
B. Two-factor authentication
C. Mandatory authentication
D. Discretionary authentication

Correct Answer: B
Section: Identity and Access Management
Explanation
Explanation/Reference:

Explanation:
Two-factor authentication provides identification of users via the combination of two different components, which could be something that the user knows, something that the user possesses or something that is inseparable from the user.

Incorrect Answers:
A: Multi-party authentication is not a valid term.
C: Mandatory authentication is not a valid term.
D: Discretionary authentication is not a valid term.

References:
https://en.wikipedia.org/wiki/Two-factor_authentication

QUESTION 452
Legacy single sign on (SSO) is:

A. Technology to allow users to authenticate to every application by entering the same user ID and password each time, thus having to remember only a single password.
B. Technology to manage passwords consistently across multiple platforms, enforcing policies such as password change intervals.
C. A mechanism where users can authenticate themselves once, and then a central repository of their credentials is used to launch various legacy applications.
D. Another way of referring to SESAME and KryptoKnight, now that Kerberos is the de-facto industry standard single sign on mechanism.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Legacy single sign on (SSO) is a mechanism where users can authenticate themselves once, and then a central repository of their credentials is used to launch various legacy applications.
An SSO solution may provide a bottleneck or single point of failure. If the SSO server goes down, users are unable to access network resources. This is why it's a good idea to have some type of redundancy or fail-over technology in place.

Incorrect Answers:
A: Legacy single sign on (SSO) enables users to sign on once; they do not have to sign on to every application.
B: Legacy single sign on (SSO) is not technology to manage passwords consistently across multiple platforms, enforcing policies such as password change intervals. This can be done with password synchronization.
D: Legacy single sign on (SSO) is not another way of referring to SESAME and KryptoKnight.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 177

QUESTION 453

Which type of password token involves time synchronization?

A. Static password tokens
B. Synchronous dynamic password tokens
C. Asynchronous dynamic password tokens
D. Challenge-response tokens

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:

Explanation:
Synchronous dynamic tokens make use of time or counters to synchronize a displayed token code with the code expected by the authentication server. Hence, the codes are synchronized.

Incorrect Answers:
A: Static passwords are reusable passwords that may or may not expire, and are normally user generated.
C: Asynchronous dynamic tokens are not synchronized with a central server.
D: Challenge-response tokens are asynchronous dynamic password tokens.

References:

Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 30-36

QUESTION 454

Which of the following would describe a type of biometric error refers to as FASLE rejection rate?

A. Type I error
B. Type II error
C. Type III error
D. CER error

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.

Incorrect Answers:
B: A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.
C: A Type III error does not exist in biometrics.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=93
https://pciguru.wordpress.com/2010/05/01/one-two-and-three-factor-authentication/

QUESTION 455
Which of the following statements pertaining to biometrics is FALSE?

A. Increased system sensitivity can cause a higher false rejection rate
B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
C. False acceptance rate is also known as Type II error.
D. Biometrics are based on the Type 2 authentication mechanism.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Type 2 authentication is based on something you have, like a token. Biometrics for part of Type 3 authentication, which is based on something you are. Something you are refers to an individual's physical traits.

Incorrect Answers:
A, B, C: These options are all TRUE with regards to biometrics.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 35-37
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 187-189

QUESTION 456

Which of the following statements pertaining to Kerberos is TRUE?

A. Kerberos does not address availability
B. Kerberos does not address integrity
C. Kerberos does not make use of Symmetric Keys
D. Kerberos cannot address confidentiality of information

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT. In Greek mythology, Kerberos is a three-headed dog that guards the entrance to the Underworld. Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network of which a client requires services.
Kerberos addresses the confidentiality and integrity of information. It does not address availability.

Incorrect Answers:
B: Kerberos does address integrity.
C: Kerberos does make use of Symmetric Keys.
D: Kerberos does address confidentiality of information.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 78

QUESTION 457
Which of the following BEST ensures accountability of users for the actions taken within a system or domain?

A. Identification
B. Authentication
C. Authorization
D. Credentials

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identification and authentication are the keystones of most access control systems. Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system. Identification establishes user accountability for the actions on the system. Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.
To 'ensure' accountability, the user must prove that they are who they say they are. This is the function of authentication. Therefore, authentication best ensures accountability of users for the actions taken within a system or domain.

Incorrect Answers:
A: Identification is the user saying who they are. However, to ensure accountability, you need authentication to prove that they are who they say they are.
C: Authorization is the rights and permissions granted to an individual which enable access to a computer resource. This does not ensure accountability because it does not ensure that the user accessing the system is who they say they are.
D: Credentials are the user's username and password combination. However, authentication is the process of validating the credentials. Credentials alone (without validation/authentication) do not ensure that the user accessing the system is who they say they are.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 57

QUESTION 458
Which of the following statements pertaining to biometrics is FALSE?

A. User can be authenticated based on behavior.
B. User can be authenticated based on unique physical attributes.
C. User can be authenticated by what he knows.
D. A biometric system's accuracy is determined by its crossover error rate (CER).

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Biometrics is based on "what you are" or "what you do". It is not based on what you know.

Incorrect Answers:
A: Behavioral (what you do), is one of the two categories that biometrics are divided into.
B: The physiological biometric category refers to traits that are physical attributes unique to a specific individual.
D: When determining a biometric system's accuracy, the CER metric is the most important measurement.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 187, 188

QUESTION 459
Which of the following biometric devices offers the LOWEST CER?

A. Keystroke dynamics
B. Voice verification
C. Iris scan
D. Fingerprint

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
According to the SANS Institute, an Iris scan has a lower CER than keystroke dynamics, voice verification, and fingerprint.

Incorrect Answers:
A, B, D: According to the SANS Institute, keystroke dynamics, voice verification, and fingerprint has a higher CER than iris scan.

References:
https://www.sans.org/reading-room/whitepapers/authentication/biometric-selection-body-parts-online-139

QUESTION 460
Which of the following is the WEAKEST authentication mechanism?

A. Passphrases
B. Passwords
C. One-time passwords
D. Token devices

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:

Passwords are considered one of the weakest security mechanisms available, because users generally select passwords that are easy to guess.

Incorrect Answers:
A: Because a passphrase is longer, it is said to be more secure than a password.
C: Once a one-time password is used, it is no longer valid. It is, therefore, more secure than a normal password.
D: Token devices generate a One-time password, which is more secure than a normal password.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 192, 196, 197, 199

QUESTION 461
When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?

A. Type I error
B. Type II error
C. Type III error
D. Crossover error

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.

Incorrect Answers:
A: A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.
C: A Type III error does not exist in biometrics.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=93

QUESTION 462
Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access?

A. Smart cards
B. Single Sign-On (SSO)
C. Symmetric Ciphers
D. Public Key Infrastructure (PKI)

Correct Answer: B
Section: Identity and Access Management
Explanation
Explanation/Reference:
Explanation:
Single Sign-On (SSO) allows a user to enter credentials once to gain access to all resources in primary and secondary network domains. Thereby, minimizing the amount of time users spend authenticating to resources and enabling the administrator to streamline user accounts and better control access rights. Furthermore, security is improved by reducing the likelihood that users will record passwords and also lessens the administrator's time spent on adding and removing user accounts and modifying access permissions. Because SSO requires a user to remember only one password, a but one of the goals is that if a user only has to remember one password, a more complicated and secure password policy can be enforced.

Incorrect Answers:
A: Smart cards are used for authentication purposes in access control. Although it can provide extra protection in an SSO environment, it does not provide the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access.
C: Symmetric Ciphers are used for encryption and decryption. It does not provide the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access.
D: Public Key Infrastructure allows for people who are widely dispersed to communicate securely and predictably.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 200, 207, 208, 833 https://en.wikipedia.org/wiki/Symmetric-key_algorithm#Cryptographic_primitives_based_on_symmetric_ciphers

QUESTION 463
Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?

A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
B. The initial logon process is cumbersome to discourage potential intruders.
C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems

Correct Answer: A

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A security issue to consider in an SSO environment is that If an attacker uncovers a credential set, the attacker would have access to every resource within the environment that the compromised account has access to.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 207, 2078

QUESTION 464
Which of the following is implemented through scripts or smart agents that replay the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?

A. Single Sign-On
B. Dynamic Sign-On
C. Smart cards
D. Kerberos

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Single Sign-On (SSO) addresses the cumbersome situation of logging on multiple times to access different resources. In SSO, a user provides one ID and password per work session and is automatically logged-on to all the required applications. SSO can be implemented by using scripts that replay the users' multiple log-ins, or by using authentication servers to verify a user's identity and encrypted authentication tickets to permit access to system services.

Incorrect Answers:
B: Dynamic Sign-On is not the correct term to describe an authentication system that can be implemented through scripts or smart agents that replay the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services.
C: Smart cards provide static or dynamic passwords or certificates to authenticate a user. The authentication happens every time the smart card is presented and the login. This is not what is described in the question.
D: Kerberos can be used to implement Single-Sign on. However, "single sign-on" is the term described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 40

QUESTION 465
Which of the following protects a password from eavesdroppers and supports the encryption of communication?

A. Challenge Handshake Authentication Protocol (CHAP)
B. Challenge Handshake Identification Protocol (CHIP) C. Challenge Handshake Encryption Protocol (CHEP)
D. Challenge Handshake Substitution Protocol (CHSP)

Correct Answer: A
Section: Identity and Access Management
Explanation
Explanation/Reference:
Explanation:
One approach to remote access security is the Challenge Handshake Authentication Protocol (CHAP). CHAP protects the password from eavesdroppers and supports the encryption of communication.
Challenge Handshake Authentication Protocol (CHAP) addresses some of the vulnerabilities found in PAP. It uses a challenge/response mechanism to authenticate the user instead of sending a password. When a user wants to establish a PPP connection and both ends have agreed that CHAP will be used for authentication purposes, the user's computer sends the authentication server a logon request. The server sends the user a challenge (nonce), which is a random value. This challenge is encrypted with the use of a predefined password as an encryption key, and the encrypted challenge value is returned to the server. The authentication server also uses the predefined password as an encryption key and decrypts the challenge value, comparing it to the original value sent. If the two results are the same, the authentication server deduces that the user must have entered the correct password, and authentication is granted.

Incorrect Answers:
B: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Identification Protocol (CHIP).
C: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Encryption Protocol (CHEP).
D: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Substitution Protocol (CHSP).

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 66
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 710

QUESTION 466
The act of requiring two of the three factors to be used in the authentication process refers to:

A. Two-Factor Authentication
B. One-Factor Authentication
C. Bi-Factor Authentication
D. Double Authentication

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Two-Factor Authentication, also known as strong authentication, must include two out of the three authentication types.

Incorrect Answers:
B: One-Factor Authentication would only include a single authentication type.
C: Bi-Factor Authentication is not a valid authentication term.
D: Double Authentication is not a valid authentication term.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 163

QUESTION 467
Which of the following would be true about Static password tokens?

A. The owner identity is authenticated by the token B.
The owner will never be authenticated by the token.
C. The owner will authenticate himself to the system.
D. The token does not authenticates the token owner but the system.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Static password token is a device that contains a password which is physically hidden, but which is transmitted for each authentication. The token authenticates the identity of the owner to the information system.

Incorrect Answers:
B: Static password tokens will authenticate the identity of the owner to the information system.
C: Static password tokens do not allow the owner to authenticate himself to the system. It authenticates the identity of the owner to the information system.
D: Static password tokens authenticate the identity of the owner to the information system, not the system.

References:

https://en.wikipedia.org/wiki/Security_token
http://www.informit.com/guides/content.aspx?g=security&seqNum=146

QUESTION 468
In Synchronous dynamic password tokens:

A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
C. The unique password is not entered into a system or workstation along with an owner's PIN.
D. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Synchronous dynamic password tokens generate new passwords at specific time intervals that are synched with the main system. Passwords are only valid for a specific time period.

Incorrect Answers:
B: With synchronous dynamic password tokens, a timer is used to rotate through various combinations produced by a cryptographic algorithm. Therefore the password will be unique.
C: With synchronous dynamic password tokens, the user enters the generated value and a user ID (this could be a PIN) into the computer, which then passes them to the server running the authentication service.
D: This is incorrect as the time value on the token device and a secret key is used to create the one-time password, which the authentication service decrypts and compares to the value it expected.

References:
http://www.informit.com/guides/content.aspx?g=security&seqNum=146
https://en.wikipedia.org/wiki/Security_token
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 196

QUESTION 469
In biometrics, "one-to-many" search against database of stored biometric images is done in:

A. Authentication
B. Identification
C. Identities
D. Identity-based access control

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A biometric system executes a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown user in identification mode. If the comparison of the biometric sample to a template in the database falls within a threshold previously set, identifying the individual will succeed.

Incorrect Answers:
A: In authentication mode, the biometric system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to confirm the individual is the person they claim to be.
C: Identities refer to who users are, not a mode used in biometrics.
D: An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.

References:
https://en.wikipedia.org/wiki/Biometrics
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 220

QUESTION 470
Which of the following is true of biometrics?

A. It is used for identification in physical controls and it is not used in logical controls.
B. It is used for authentication in physical controls and for identification in logical controls.
C. It is used for identification in physical controls and for authentication in logical controls.

D. Biometrics has no role in logical controls.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Biometrics is used for identification in physical controls and for authentication in logical controls. Physical controls are items put into place to protect facility, personnel, and resources. As a physical control, biometrics provides protection by identifying a person to see if that person is authorized to access a facility. When a user is identified and granted physical access to a facility, biometrics can be used for authentication in logical controls to provide access to resources. Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Biometrics is used in logical controls.
B: Biometrics is used for identification in physical controls and for authentication in logical controls, not the other way round. Biometrics is used first as a physical control to identify a person to grant access to a facility, and then as a logical control to authenticate the user to provide access to resources. D: Biometrics does have a role in logical controls.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 58

QUESTION 471
What is the percentage of valid subjects that are falsely rejected by a Biometric Authentication system called?

A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Rejection Rate (TRR) or Type III Error

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.

Incorrect Answers:
B: A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.
C: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.
D: The true reject rate refers to the percentage of times a system correctly rejects a false claim of identity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=93

QUESTION 472
What is the percentage of invalid subjects that are falsely accepted by a Biometric authentication system called?

A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Acceptance Rate (TAR) or Type III Error

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.

Incorrect Answers:
A: A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.
C: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.
D: The true accept rate is the percentage of times a system correctly verifies a true claim of identity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=92

QUESTION 473

What is the percentage at which the False Rejection Rate equals the False Acceptance Rate called?

A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. Failure to enroll rate (FTE or FER)

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.

Incorrect Answers:
A: A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.
B: A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.
D: The Failure to enroll rate is the rate at which attempts to create a template from an input is unsuccessful.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 188
https://en.wikipedia.org/wiki/Biometrics

QUESTION 474
What is a password called that is the same for each log-on session?

A. one-time password
B. two-time password
C. static password
D. dynamic password

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:

Static passwords are passwords that can be reused, but may or may not expire. They can, therefore, be used for each log-on session if password expiration has not been configured.

Incorrect Answers:
A: A one-time password is no longer valid and, if obtained by a hacker, cannot be reused after it has been used.
B: A two-time password is not a valid password type.
D: A dynamic password is no longer valid and, if obtained by a hacker, cannot be reused after it has been used.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 195, 196
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 30

QUESTION 475
What is a sequence of characters that is usually longer than the allotted number for a password called?

A. passphrase
B. cognitive phrase
C. anticipated phrase
D. Real phrase

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A passphrase is a sequence of characters that is longer than a password and, in some cases, takes the place of a password during an authentication process. Passphrases are long static passwords, which is made up of words in a phrase or sentence.

Incorrect Answers:
B: A sequence of characters that is usually longer than the allotted number for a password is called a passphrase, not a cognitive phrase.
C: A sequence of characters that is usually longer than the allotted number for a password is called a passphrase, not an anticipated phrase.
D: A sequence of characters that is usually longer than the allotted number for a password is called a passphrase, not a real phrase.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 199
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 30

QUESTION 476

Which BEST describes a tool (i.e. keyfob, calculator, memory card or smart card) used to supply dynamic passwords?

A. Tickets
B. Tokens
C. Token passing networks
D. Coupons

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A security token (or sometimes a hardware token, authentication token, USB token, cryptographic token, software token, virtual token, or key fob) may be a physical device that an authorized user is given to ease authentication.
Security tokens are used to prove one's identity electronically (as in the case of a customer trying to access their bank account). The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something.
Some may store cryptographic keys, such as a digital signature, or biometric data, such as fingerprint minutiae. Some designs feature tamper resistant packaging, while others may include small keypads to allow entry of a PIN or a simple button to start a generating routine with some display capability to show a generated key number.
All tokens contain some secret information that is used to prove identity. There are different ways in which this information can be used.

Examples include:
- Synchronous dynamic password token: A timer is used to rotate through various combinations produced by a cryptographic algorithm. The token and the authentication server must have synchronized clocks.
- Asynchronous password token: A one-time password is generated without the use of a clock, either from a one-time pad or cryptographic algorithm.

Incorrect Answers:
A: A tool such as a keyfob, calculator, memory card or smart card used to supply dynamic passwords is not known as a ticket.
C: Token passing networks are computer networks such as Token Ring or FDDI networks. They do not supply dynamic passwords.
D: A tool such as a keyfob, calculator, memory card or smart card used to supply dynamic passwords is not known as a coupon.

References:
https://en.wikipedia.org/wiki/Security_token

QUESTION 477
Which one of the following factors is NOT one on which Authentication is based?

A. Type 1 Something you know, such as a PIN or password

B. Type 2 Something you have, such as an ATM card or smart card
C. Type 3 Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan
D. Type 4 Something you are, such as a system administrator or security administrator

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Something you are, or authentication by characteristic, is based on a unique physical attribute, not what role you fulfill.

Incorrect Answers:
A: Something you know, or authentication by knowledge, can be a password, PIN, mother's maiden name, or the combination to a lock.
B: Something you have, or authentication by ownership, can be a key, swipe card, access card, or badge.
C: Something you are, or authentication by characteristic, is based on a unique physical attribute, referred to as biometrics.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 163

QUESTION 478
What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources?

A. Micrometrics
B. Macrometrics
C. Biometrics
D. MicroBiometrics

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Some biometric systems base authentication decisions on physical attributes such as iris, retina, or fingerprints.

Incorrect Answers:
A: Micrometrics is a business term used for measures that support the improvement and management of a particular project, program or initiative.
B: Macrometrics is a business term used for the overall organization or cross-functional metrics used to drive strategy.

D: MicroBiometrics is not a technology that uses fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 187
http://www.humanresourcesiq.com/hr-technology/columns/macro-vs-micro-metrics/

QUESTION 479
What is the access protection system that limits connections by calling back the number of a previously authorized location called?

A. Sendback systems
B. Callback forward systems
C. Callback systems
D. Sendback forward systems

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Callback is when the host system disconnects the caller and then dials the authorized telephone number of the remote terminal in order to reestablish the connection.

Incorrect Answers:
A: A sendback system is not a valid system type with regards to CISSP.
B: A callback forward system is not a valid system type with regards to CISSP.
D: A sendback forward system is not a valid system type with regards to CISSP.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. G-3

QUESTION 480
Which of the following is the most reliable authentication method for remote access?

A. Variable callback system
B. Synchronous token
C. Fixed callback system
D. Combination of callback and caller ID

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
A Synchronous token generates a one-time password that is only valid for a short period of time. Once the password is used it is no longer valid, and it expires if not entered in the acceptable time frame.

Incorrect Answers:
A: Although variable callback systems are more flexible than fixed callback systems, the system assumes the identity of the individual unless two-factor authentication is also implemented.
C: Callback systems authenticate a person, but anyone can pretend to be that person. They are tied to a specific place and phone number, which can be spoofed by implementing call-forwarding.
D: The caller ID and callback functionality provides greater confidence and auditability of the caller's identity. However, unless combined with strong authentication, any individual at the location could obtain access.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 196, 696
https://technet.microsoft.com/en-us/library/cc778189(v=ws.10).aspx

QUESTION 481
Which of the following is NOT a security characteristic we need to consider while choosing a biometric identification system?

A. data acquisition process
B. cost
C. enrollment process
D. speed and user interface

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
The cost of the biometric identification system is a financial consideration, not a security consideration.

The data acquisition process refers to how a user's biometric data will be acquired. Will you use a fingerprint scan, a retina scan, a palm scan etc. This is an obvious security characteristic to be considered while choosing a biometric identification system.
The enrollment process refers to how the user's biometric data will be initially acquired and the data stored as a template for comparison for future identifications.

This is also a security characteristic to be considered while choosing a biometric identification system.
The speed and user interface are security characteristics to be considered while choosing a biometric identification system. You need a biometric identification system that does not keep the user waiting before being identified and authenticated. The user interface for a biometric identification system should include instructional and feedback aspects that would enable users to use the system effectively without assistance.

Incorrect Answers:
A: The data acquisition process refers to how a user's biometric data will be acquired. This is a security characteristic to be considered while choosing a biometric identification system.
C: The enrollment process is a security characteristic to be considered while choosing a biometric identification system.
D: The speed and user interface are security characteristics to be considered while choosing a biometric identification system.

QUESTION 482
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessity of answering two questions:

A. What was the sex of a person and his age?
B. What part of body to be used and how to accomplish identification that is viable?
C. What was the age of a person and his income level?
D. What was the tone of the voice of a person and his habits?

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
When it became apparent that truly positive identification could only be based on physical attributes of a person, two questions had to be answered. First, what part of body could be used? Second, how could identification be accomplished with sufficient accuracy, reliability and speed so as to be viable?
Because most identity authentication requirements take place when people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are the hands, face and eyes.

Incorrect Answers:
A: The sex of a person and his age are not considered in biometric identification systems.
C: The age of a person and his income level are not considered in biometric identification systems.
D: The tone of the voice of a person and his habits are not considered in biometric identification systems.
References:
Tipton, Harold F. and Micki Krause, *Information Security Management Handbook*, 5th Edition, Auerbach Publications, Boca Raton, 2006, p. 62

QUESTION 483

What is the primary role of smartcards in a PKI?

A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data
D. Tamper resistant, mobile storage and application of private keys of the users

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A smart card, which includes the ability to process data stored on it, is also able to deliver a two-factor authentication method as the user may have to enter a PIN to unlock the smart card. The authentication can be completed by using an OTP, by utilizing a challenge/response value, or by presenting the user's private key if it is used within a PKI environment. The fact that the memory of a smart card is not readable until the correct PIN is entered, as well as the complexity of the smart token makes these cards resistant to reverse-engineering and tampering methods.

Incorrect Answers:
A: Transparent renewal of user keys is not the primary role of smartcards in a PKI.
B: Easy distribution of the certificates between the users is not the primary role of smartcards in a PKI.
C: Fast hardware encryption of the raw data is not the primary role of smartcards in a PKI.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 200, 201
http://en.wikipedia.org/wiki/Tamper_resistance

QUESTION 484
In biometric identification systems, the parts of the body conveniently available for identification are:

A. neck and mouth
B. hands, face, and eyes
C. feet and hair
D. voice and neck
Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Most identity authentication takes place when people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes.

Incorrect Answers:
A: The neck is not convenient as it can be covered.
C: The feet normally have shoes on, and therefore not convenient.
D: The neck is not convenient as it can be covered.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 187-192

QUESTION 485
Which of the following is TRUE of two-factor authentication?

A. It uses the RSA public-key signature based on integers with large prime factors.
B. It requires two measurements of hand geometry.
C. It does not use single sign-on technology.
D. It relies on two independent proofs of identity.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three general factors that are used for authentication:
- Something a person knows.
- Something a person has.
- Something a person is.

Two-factor authentication requires two of the three factors to be part of authentication process.

Incorrect Answers:
A: RSA encryption uses integers with exactly two prime factors, but the term "two-factor authentication" is not used in that context.
B: Measuring hand geometry twice only provides one factor.
C: Single sign-on (SSO) technology allows a user to enter their credentials once to gain access to multiple systems. Two-factor authentication could be used for SSO, not the other way around.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 162, 163, 207, 815

QUESTION 486
What kind of certificate is used to validate a user identity?

A. Public key certificate
B. Attribute certificate
C. Root certificate
D. Code signing certificate

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

Incorrect Answers:
B: In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use.
C: A root certificate is an unsigned or a self-signed public key certificate that identifies the Root Certificate Authority (CA).
D: Code signing digitally signs executables and scripts to verify the software author and guarantee that the code has not been changed or tainted since it was signed by use of a cryptographic hash.

References:
http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate
https://en.wikipedia.org/wiki/Root_certificate
https://en.wikipedia.org/wiki/Code_signing

QUESTION 487
Single Sign-on (SSO) is characterized by which of the following advantages?

A. Convenience
B. Convenience and centralized administration C. Convenience and centralized data administration

D. Convenience and centralized network administration

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Single sign-on allows users to type their passwords only once when they first log in to access all the network resources. This makes SSO convenient.
Single Sign-on allows a single administrator to add and delete accounts across the entire network from one user interface, providing centralized administration.

Incorrect Answers:
A: Single Sign-on does offer convenience, but it also offers centralized administration, making option B a more suitable answer.
C: Centralized data administration is not an advantage of Single Sign-on.
D: Centralized network administration is not an advantage of Single Sign-on.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 42

QUESTION 488
What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?

A. Authentication
B. Identification
C. Authorization
D. Confidentiality

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identification involves a user supplying identification information using a username, user ID, or account number.

Incorrect Answers:
A: Authentication involves verifying a user's identification information using a passphrase, PIN value, biometric, one-time password, or password.
C: Authorization is when a system establishes whether the user is authorized to access the particular resource and what actions he is permitted to perform on that resource.

D: Confidentiality is used to make sure that the required level of secrecy is imposed at every junction of data processing and prevents unauthorized disclosure.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 24, 166, 203

QUESTION 489
What is the verification that the user's claimed identity is valid called and is usually implemented through a user password at log-on time?

A. Authentication
B. Identification
C. Integrity
D. Confidentiality

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Authentication involves verifying a user's identification information using a passphrase, PIN value, biometric, one-time password, or password.

Incorrect Answers:
B: Identification involves a user supplying identification information using a username, user ID, or account number.
C: Integrity is a security principle that ensures information and systems are not maliciously or accidentally modified.
D: Confidentiality is used to make sure that the required level of secrecy is imposed at every junction of data processing and prevents unauthorized disclosure.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 23, 24, 166

QUESTION 490
Which of the following is TRUE about Kerberos?

A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.

Correct Answer: C
Section: Identity and Access Management

Explanation

Explanation/Reference:
Explanation:
Kerberos makes use of symmetric key cryptography and offers end-to-end security. The majority Kerberos implementations works with shared secret keys.

Incorrect Answers:
A: Kerberos makes use of symmetric key cryptography, which does not include the use of public keys.
B: Kerberos was specifically designed to remove the need to transmit passwords over the network.
D: Kerberos is a trusted third-party service.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 782
https://en.wikipedia.org/wiki/Kerberos_(protocol)

QUESTION 491
A confidential number used as an authentication factor to verify a user's identity is called a:

A. PIN
B. User ID
C. Password
D. Challenge

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Personal Identification Number (PIN) is a numeric password shared between a user and a system, which can be used to authenticate the user to the system.

Incorrect Answers:
B: User ID is used for identification, not authentication.
C: A password is a word or string of characters used for user authentication.
D: Challenge-response authentication involves one party presenting a question ("challenge") and another party providing a valid answer ("response") to be authenticated. It does not specifically be a number sequence.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 162
https://en.wikipedia.org/wiki/Personal_identification_number
https://en.wikipedia.org/wiki/Password https://en.wikipedia.org/wiki/Challenge-response_authentication#Cryptographic_techniques

QUESTION 492
Which type of password provides maximum security because a new password is required for each new log-on?

A. One-time or dynamic password
B. Cognitive password
C. Static password
D. Passphrase

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A one-time or dynamic password is no longer valid and, if obtained by a hacker, cannot be reused after it has been used. A one-time or dynamic password is used in environments where a higher level of security than static passwords is required.

Incorrect Answers:
B: After a user is enrolled by answering several questions based on her life experiences, the user can answer the questions asked of her to be authenticated instead of having to remember a password. The questions do not change from log-on to log-on.
C: Static passwords are passwords that can be reused, but may or may not expire.
D: Passphrases are long static passwords, which is made up of words in a phrase or sentence.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 195, 196
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 30

QUESTION 493
The primary service provided by Kerberos is which of the following?

A. non-repudiation
B. confidentiality

C.

authentication

D. authorization

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a third-party authentication service that can be used to support SSO.

Incorrect Answers:
A: Non-repudiation provides assurance that a specific user performed a specific transaction that did not change. It is not, however, the primary service provided by Kerberos.
B: Confidentiality strives to prevent unauthorized read access to data. It is not, however, the primary service provided by Kerberos.
D: Authorization refers to the actions you are allowed to carry out on a system after identification and authentication has taken place. It is not, however, the primary service provided by Kerberos.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 12, 14, 15, 43

QUESTION 494
Which of the following is NOT true of the Kerberos protocol?

A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos uses shared secret keys and tickets for the initial authentication, not a public key algorithm.

Incorrect Answers:

A: Kerberos is an example of a single sign-on system for distributed environments, and therefore only requires a single login per session.
C: the foundation of Kerberos security is trust that clients and services have in the integrity of the KDC.
D: Kerberos provides mutual authentication in that both the user and the server verify each other's identity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213
https://en.wikipedia.org/wiki/Kerberos_(protocol)

QUESTION 495
The authenticator within Kerberos provides a requested service to the client after validating which of the following?

A. timestamp
B. client public key
C. client private key
D. server public key

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
In Kerberos implementations where the use of an authenticator is configured, the user sends their identification information and a timestamp and sequence number encrypted with the shared session key to the requested service, which then decrypts this information and compares it with the identification data the KDC sent to it about this requesting user. If the data matches, the user is allowed access to the requested service.

Incorrect Answers:
B: A requested service is provided to the client after validating a user's identification information and a timestamp and encrypted sequence number, not a client public key.
C: A requested service is provided to the client after validating a user's identification information and a timestamp and encrypted sequence number, not a client private key.
D: A requested service is provided to the client after validating a user's identification information and a timestamp and encrypted sequence number, not a server public key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213

QUESTION 496
Which of the following is addressed by Kerberos?

C.

A. Confidentiality and Integrity
B. Authentication and Availability
Validation and Integrity
D. Auditability and Integrity

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT. In Greek mythology, Kerberos is a three-headed dog that guards the entrance to the Underworld. Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network of which a client requires services.
Kerberos addresses the confidentiality and integrity of information. It does not directly address availability and attacks such as frequency analysis.

Incorrect Answers:
B: Kerberos an authentication protocol. However, it does not address availability.
C: Kerberos does address integrity but it does not address validation.
D: Kerberos does address integrity but it does not address auditability.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 78

QUESTION 497
Kerberos is vulnerable to replay in which of the following circumstances?

A. When a private key is compromised within an allotted time window.
B. When a public key is compromised within an allotted time window.
C. When a ticket is compromised within an allotted time window.
D. When the KSD is compromised within an allotted time window.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:

Kerberos addresses the confidentiality and integrity of information. It does not directly address availability and attacks such as frequency analysis. Furthermore, because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code. Replay can be accomplished on Kerberos if the compromised tickets are used within an allotted time window. Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Incorrect Answers:
A: Kerberos does not use a private key like an asymmetric key cryptography system does. It uses symmetric key cryptography (shared key).
B: Kerberos does not use a public key like an asymmetric key cryptography system does. It uses symmetric key cryptography (shared key).
D: KSD being compromised is not a vulnerability of Kerberos.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 78

QUESTION 498
Like the Kerberos protocol, SESAME is also subject to which of the following?

A. timeslot replay
B. password guessing
C. symmetric key guessing
D. asymmetric key guessing

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Just like Kerberos, SESAME depends on the initial user authentication. For that reason, SESAME has the same weakness to attacks on the user's password as Kerberos does.

Incorrect Answers:
A: SESAME is not susceptible to timeslot replay attacks.
C: Symmetric key guessing is not a weakness of Kerberos.
D: Asymmetric key guessing is not a weakness of Kerberos.

References:
Miller, David R, *CISSP Training Kit*, O'Reilly Media, 2013, Sebastopol, p. 101
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 46

QUESTION 499

C.

RADIUS incorporates which of the following services?

A. Authentication server and PIN codes.
B. Authentication of clients and static passwords generation.
Authentication of clients and dynamic passwords generation.
D. Authentication server as well as support for Static and Dynamic passwords.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A central authentication service for dial-up users is the standard Remote Authentication and Dial-In User Service (RADIUS). RADIUS incorporates an authentication server and dynamic passwords. The RADIUS protocol is an open lightweight, UDP-based protocol that can be modified to work with a variety of security systems. It provides authentication, authorization and accounting services to routers, modem servers, and wireless applications. RADIUS is described in RFC 2865.

Incorrect Answers:
A: RADIUS does not incorporate PIN codes.
B: Authentication of clients is provided by the authentication server which is incorporated into RADIUS. RADIUS does not incorporate static passwords 'generation'.
C: Authentication of clients is provided by the authentication server which is incorporated into RADIUS. RADIUS does not incorporate dynamic passwords 'generation'.

References:
Cole, Eric, *Network Security Bible*, Wiley Publishing, Indianapolis, 2009, p. 124

QUESTION 500
Which of the following would constitute the BEST example of a password to use for access to a system by a network administrator?

A. holiday
B. Christmas12
C. JennyD. GyN19Za!

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A generally accepted minimum standard for password complexity is a minimum of eight characters, one uppercase alpha character, one lowercase alpha character, one number character, and one symbol character. Therefore, "**GyN19Za!**" is the best example.
Incorrect Answers:
A: This option does not satisfy the minimum complexity as it only has lowercase characters.
B: This option does not satisfy minimum complexity as there are no alpha or symbol characters.
C: This option does not satisfy the minimum complexity as it is less than eight characters, and has no alpha, number, or symbol characters.

References:
Miller, David R, *CISSP Training Kit*, O'Reilly Media, 2013, California, p. 77

QUESTION 501
What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?

A. Accountability controls
B. Mandatory access controls
C. Assurance procedures
D. Administrative controls

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

Incorrect Answers:
A: Controls are administrative, logical/technical or physical. Accountability controls are not a defined control type and do not ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
B: Mandatory access controls are an access control type. They do not ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
D: Administrative controls are a group of controls that include policies and procedures. However, assurance procedures are the specific name for the set of procedures that ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

References:

C.

Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 47

QUESTION 502
Smart cards are an example of which type of control?

A. Detective control

B. Administrative control
C. Technical control
D. Physical control

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Smart cards are an example of a Preventive/Technical control.

Incorrect Answers:
A: Detective controls include Motion detectors, Closed-circuit TVs, Monitoring and Supervising, Job rotation, Investigations, Audit logs, and IDS.
B: Administrative controls include Security policy, Monitoring and Supervising, Separation of duties, Job rotation, Information Classification, Personnel Procedures, Testing, and Security-awareness training.
D: Physical controls include Fences, Locks, Badge system, Security guard, Biometric system, Mantrap doors, Lighting, Motion detectors, and Closed-circuit TVs.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 32, 33

QUESTION 503
Which of the following is NOT a two-factor authentication mechanism?

A. Something you have and something you know.
B. Something you do and a password.
C. A smartcard and something you are.
D. Something you know and a password.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Two-factor authentication includes two of the following three factors:
- Something you know - Password
- Something you have - Token

- Something you are - Biometrics

A password is something you know, and cannot be used together for two-factor authentication.

Incorrect Answers:
A, B, C: This answer satisfies the requirements for two-factor authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 163

QUESTION 504
Which of following is NOT a service provided by AAA servers (Radius, TACACS and DIAMETER)?

A. Authentication
B. Administration
C. Accounting
D. Authorization

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
The AAA term refers to authentication, authorization, and accounting/audit. Administration is not one of the options, therefore, the correct answer.

Incorrect Answers:
A, C, D: Authentication, Accounting, and Authorization are what the AAA term refers to.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 236

QUESTION 505
Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

A. TCP
B. SSL
C. UDP
D. SSH

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
TACACS has been through three generations: TACACS, Extended TACACS (XTACACS), and TACACS+. TACACS combines its authentication and authorization processes; XTACACS separates authentication, authorization, and auditing processes; and TACACS+ is XTACACS with extended two-factor user authentication. TACACS uses fixed passwords for authentication, while TACACS+ allows users to employ dynamic (one-time) passwords, which provides more protection. The original TACACS was developed during the days of ARPANET which is the basis for the Internet. TACACS uses UDP as its communication protocol. TACACS + uses TCP as its communication protocol.

Incorrect Answers:
A: TACACS uses UDP as its communication protocol, not TCP.
B: TACACS uses UDP as its communication protocol, not SSL.
D: TACACS uses UDP as its communication protocol, not SSH.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 234
Jacobs, Josh, et al., *SSCP Systems Security Certified Practitioner Study Guide and DVD Training System*, Syngress, Rockland, 2003, p. 450
http://en.wikipedia.org/wiki/TACACS

QUESTION 506
What is Kerberos?

A. A three-headed dog from the Egyptian mythology.
B. A trusted third-party authentication protocol.
C. A security model.
D. A remote authentication dial-in user server.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a third-party authentication service that can be used to support SSO.
Kerberos (or Cerberus) was the name of the three-headed dog that guarded the entrance to Hades in Greek mythology.

Incorrect Answers:
A: Kerberos (or Cerberus) was the name of the three-headed dog that guarded the entrance to Hades in Greek mythology. We are, however, dealing with information systems, not mythology.
C: Kerberos is an authentication protocol, not just a security model.
D: A remote authentication dial in user server refers to RADIUS, not Kerberos.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 22, 43

QUESTION 507
Which of the following can BEST eliminate dial-up access through a Remote Access Server as a hacking vector?

A. Using a TACACS+ server.
B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall. C. Setting modem ring count to at least 5
D. Only attaching modems to non-networked hosts.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
As client computers used to have built-in modems to allow for Internet connectivity, organizations commonly had a pool of modems to allow for remote access into and out of their networks. In some cases the modems were installed on individual servers here and there throughout the network or they were centrally located and managed. Most companies did not properly enforce access control through these modem connections, and they served as easy entry points for attackers. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall can best eliminate dial-up access through a Remote Access Server as a hacking vector. This solution would mean that even if an attacker gained access to the Remote Access Server, the firewall would provide another layer of protection.

Incorrect Answers:
A: Using a TACACS+ server does provide a good remote access authentication and authorization solution. However, to best eliminate dial-up access through a Remote Access Server as a hacking vector, you should place the remote access server outside the firewall.
C: Setting modem ring count to at least 5 may deter wardialers but it does not eliminate dial-up access through a Remote Access Server as a hacking vector.
D: Only attaching modems to non-networked hosts do not eliminate dial-up access through a Remote Access Server as a hacking vector. Besides being impractical, the non-network hosts would be vulnerable to attack.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 695

QUESTION 508
Which authentication technique BEST protects against hijacking?

A. Static authentication
B. Continuous authentication
C. Robust authentication
D. Strong authentication

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three major types of authentication available: static, robust, and continuous. Static authentication includes passwords and other techniques that can be compromised through replay attacks. They are often called reusable passwords. Robust authentication involves the use of cryptography or other techniques to create one-time passwords that are used to create sessions. These can be compromised by session hijacking. Continuous authentication prevents session hijacking.
Continuous Authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect.

Incorrect Answers:
A: Static authentication only provides protection against attacks in which an imposter cannot see, insert or alter the information passed between the claimant and the verifier during an authentication exchange and subsequent session. Static authentication does not protect against hijacking.
C: Robust Authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and verifier. Robust or dynamic authentication does not protect against hijacking.
D: Strong authentication is not a specific authentication type; it is another term for multi-factor authentication.

References:
http://www.windowsecurity.com/whitepapers/policy_and_standards/Internet_Security_Policy/Internet_Security_Policy__Sample_Policy_Areas.html

QUESTION 509
Which of the following is NOT a security goal for remote access?

A. Reliable authentication of users and systems
B. Protection of confidential data

C. Easy to manage access control to systems and network resources
D. Automated login for remote users

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Protection of confidential data is one of the most important security aspects of any business.
Providing remote access to a network and its computer systems brings new risks. Is the person logging in remotely who he claims to be? Is someone physically or electronically looking over his shoulder, or tapping the communication line? Is the client device from which he is performing the remote access in a secure configuration, or has it been compromised by spyware, Trojan horses, and other malicious code?
When providing remote access to your network, you need reliable authentication of users and systems. You also need to be able to control access to the systems and network resources.
Automated login for remote users is not a security goal for remote access. Logins should not be automated for remote users. Automated logins do not improve the security of the network or systems.

Incorrect Answers:
A: Reliable authentication of users and systems is a security goal for remote access.
B: Protection of confidential data is a security goal for remote access.
C: Easy to manage access control to systems and network resources is a security goal for remote access.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1250

QUESTION 510
During an IS audit, one of your auditors has observed that some of the critical servers in your organization can be accessed ONLY by using a shared/common user name and password. What should be the auditor's PRIMARY concern be with this approach?

A. Password sharing
B. Accountability
C. Shared account management
D. Difficulty in auditing shared account

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identification and authentication are the keystones of most access control systems. Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system. Identification establishes user accountability for the actions on the system. Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.
Audit trails list the actions performed by the user account used to perform the actions. However, if all the users are using the same user account, you have no way of knowing which person performed which action. Therefore, you have no "accountability".
Incorrect Answers:
A: Password sharing is not the primary concern in this case. The only password shared is the password for the shared account.
C: Shared account management is not a concern. The fact that the account is shared is the concern.
D: Difficulty in auditing shared account is not the primary concern. Auditing a single account is not a problem. The problem is that you do not know which person is using the account at any given time.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 57

QUESTION 511
During an IS audit, auditor has observed that authentication and authorization steps are split into two functions and there is a possibility to force the authorization step to be completed before the authentication step. Which of the following technique an attacker could user to force authorization step before authentication?

A. Eavesdropping
B. Traffic analysis
C. Masquerading
D. Race Condition

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A race condition happens when two different processes need to carry out their tasks on the same resource.

Incorrect Answers:
A: Sniffing or eavesdropping involves the capturing and recording of all frames traveling across the network media. B: Traffic analysis is used for discovering information by watching traffic patterns on a network. C: Masquerading occurs by impersonating another user to gain unauthorized access to a system

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 410, 411, 1060, 1294
Miller, David R, CISSP Training Kit, O'Reilly Media, 2013, Sebastopol, p. 508

QUESTION 512
Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of its internals?

A. Black-box testing

B. Parallel Test
C. Regression Testing
D. Pilot Testing

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Black box testing examines the functionality of an application without peering into its internal structures or workings. Black box testing provides the tester with no internal details; the software is treated as a black box that receives inputs.

Incorrect Answers:
B: Parallel Testing is the process of entering the same inputs in two different versions of the application and reporting the anomalies.
C: Regression Testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors.
D: Pilot Testing is a preliminary test that focuses on specific and predefined aspect of a system.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 194
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1105 https://en.wikipedia.org/wiki/Black-box_testing
http://www.tutorialspoint.com/software_testing_dictionary/parallel_testing.htm http://soft-engineering.blogspot.co.za/2010/12/what-is-difference-between-pilot-and.html

QUESTION 513
Which of the following is NOT a technique used to perform a penetration test?

A. traffic padding
B. scanning and probing

C. war dialing
D. sniffing

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Traffic padding is a countermeasure to traffic analysis.
Even if perfect cryptographic routines are used, the attacker can gain knowledge of the amount of traffic that was generated. The attacker might not know what Alice and Bob were talking about, but can know that they were talking and how much they talked. In certain circumstances this can be very bad. Consider for example when a military is organizing a secret attack against another nation: it may suffice to alert the other nation for them to know merely that there is a lot of secret activity going on.
Padding messages is a way to make it harder to do traffic analysis. Normally, a number of random bits are appended to the end of the message with an indication at the end how much this random data is. The randomness should have a minimum value of 0, a maximum number of N and an even distribution between the two extremes. Note, that increasing 0 does not help, only increasing N helps, though that also means that a lower percentage of the channel will be used to transmit real data. Also note, that since the cryptographic routine is assumed to be uncrackable (otherwise the padding length itself is crackable), it does not help to put the padding anywhere else, e.g. at the beginning, in the middle, or in a sporadic manner.

Incorrect Answers:
B: Scanning and probing is a technique used in Penetration Testing. Various scanners, like a port scanner, can reveal information about a network's infrastructure and enable an intruder to access the network's unsecured ports.
C: War dialing is a technique used in Penetration Testing. War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers to hack in to.
D: Sniffing (packet sniffing) is a technique used in Penetration Testing. Packet sniffing is the process of intercepting data as it is transmitted over a network.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, pp. 233, 238. https://secure.wikimedia.org/wikipedia/en/wiki/Padding_%28cryptography%29#Traffic_analysis

QUESTION 514
Which of the following is NOT a valid reason to use external penetration service firms rather than corporate resources?

A. They are more cost-effective
B. They offer a lack of corporate bias
C. They use highly talented ex-hackers
D. They ensure a more complete reporting

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Two points are important to consider when it comes to ethical hacking: integrity and independence.

By not using an ethical hacking firm that hires or subcontracts to ex-hackers of others who have criminal records, an entire subset of risks can be avoided by an organization. Also, it is not cost-effective for a single firm to fund the effort of the ongoing research and development, systems development, and maintenance that is needed to operate state-of-the-art proprietary and open source testing tools and techniques.
External penetration firms are more effective than internal penetration testers because they are not influenced by any previous system security decisions, knowledge of the current system environment, or future system security plans. Moreover, an employee performing penetration testing might be reluctant to fully report security gaps.

Incorrect Answers:
A: External penetration service firms are more cost-effective than using corporate resources for penetration testing. This is a valid reason to use external penetration service firms.
B: External penetration service firms do offer a lack of corporate bias compared to corporate resources. This is a valid reason to use external penetration service firms.
D: External penetration service firms do tend to ensure more complete reporting than corporate resources. This is a valid reason to use external penetration service firms.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 517

QUESTION 515
Which of the following statements pertaining to ethical hacking is NOT true?

A. An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services.
B. Testing should be done remotely to simulate external threats.
C. Ethical hacking should not involve writing to or modifying the target systems negatively.
D. Ethical hackers never use tools that have the potential of affecting servers or services.

Correct Answer: D
Section: Security Assessment and Testing
Explanation

Explanation/Reference:

Explanation:
Ethical hackers should use tools that have the potential of affecting servers or services to provide a valid security test. These are the tools that a malicious hacker would use.
The first step before sending even one single packet to the target would be to have a signed agreement with clear rules of engagement and a signed contract. The signed contract explains to the client the associated risks and the client must agree to them before you even send one packet to the target range. This way the client understands that some of the tests could lead to interruption of service or even crash a server. The client signs that he is aware of such risks and willing to accept them.

Incorrect Answers:
A: An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services. An ethical hacking firm's independence can be questioned if they sell security solutions at the same time as doing testing for the same client.
B: Testing should be done remotely to simulate external threats. Testing simulating a cracker from the Internet is often one of the first tests being done. This is to validate perimeter security. By performing tests remotely, the ethical hacking firm emulates the hacker's approach more realistically.
C: Ethical hacking should not involve writing to or modifying the target systems negatively. Proving the ability to write to or modify the target systems (without causing harm) is enough to demonstrate the existence of a vulnerability.

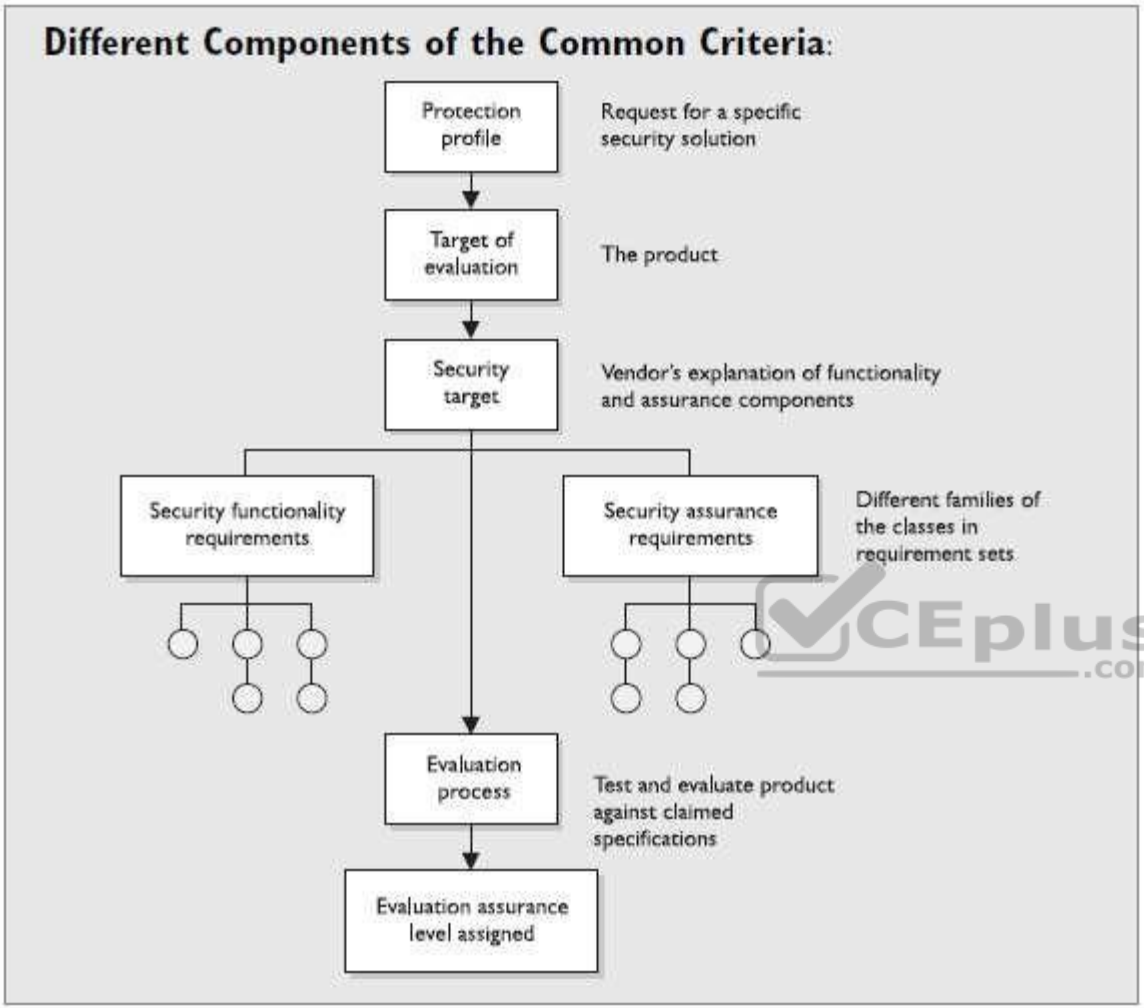
References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 520

QUESTION 516
Common Criteria 15408 generally outlines assurance and functional requirements through a security evaluation process concept of _____, _____, _____ for Evaluated Assurance Levels (EALs) to certify a product or system.

A. EAL, Security Target, Target of Evaluation
B. SFR, Protection Profile, Security Target
C. Protection Profile, Target of Evaluation, Security Target
D. SFR, Security Target, Target of Evaluation

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Under the Common Criteria model, an evaluation is carried out on a product and it is assigned an Evaluation Assurance Level (EAL). The thorough and stringent testing increases in detailed-oriented tasks as the assurance levels increase. The Common Criteria has seven assurance levels. The range is from EAL1, where functionality testing takes place, to EAL7, where thorough testing is performed and the system design is verified. The different components are shown in the exhibit below:



Incorrect Answers:
A: Evaluated Assurance Levels (EALs) determine the levels of evaluation required. EAL is not a common criteria security evaluation process concept. B: Security functional requirements (SFRs) are individual security functions which must be provided by a product. An SFR is not a common criteria security evaluation process concept.
D: Security functional requirements (SFRs) are individual security functions which must be provided by a product. An SFR is not a common criteria security evaluation process concept.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 403-405

QUESTION 517
You are a security consultant who is required to perform penetration testing on a client's network. During penetration testing, you are required to use a compromised system to attack other systems on the network to avoid network restrictions like firewalls.

Which method would you use in this scenario:

A. Black box Method
B. Pivoting methodC. White Box Method.
D. Grey Box Method

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Pivoting is a method that makes use of the compromised system to attack other systems on the same network to avoid restrictions that might prohibit direct access to all machines.

Incorrect Answers:
A: Black box testing examines the functionality of an application without peering into its internal structures or workings.
C: With white box testing, the testers are provided with complete knowledge of the infrastructure being tested.
D: With gray-box pen testing, the tester is provided with partial knowledge of the infrastructure being tested.

References:
https://en.wikipedia.org/wiki/Exploit_(computer_security)#Pivoting https://en.wikipedia.org/wiki/Black-box_testing http://www.redsphereglobal.com/content/penetration-testing

QUESTION 518
Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?

A. Test environment using test data.
B. Test environment using sanitized live workloads data.
C. Production environment using test data.
D. Production environment using sanitized live workloads data.

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
You should perform stress tests in a test environment. It is best to use live workload data as the stress test would be more realistic.
Stress testing (sometimes called torture testing) is a form of deliberately intense or thorough testing used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

Incorrect Answers:
A: It would be better to use live workload data.
C: You should not perform stress tests in the product environment.
D: You should not perform stress tests in the product environment.

References:
https://en.wikipedia.org/wiki/Stress_testing

QUESTION 519
Which of the following are required for Life-Cycle Assurance?

A. System Architecture and Design specification
B. Security Testing and Covert Channel Analysis
C. Security Testing and Trusted distribution
D. Configuration Management and Trusted Facility Management

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.
The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces the requirements. By extension, assurance must include a guarantee that the trusted portion of the system works only as intended. To accomplish these objectives, two types of assurance are needed with their respective elements:
Operational Assurance: System Architecture, System Integrity, Covert Channel Analysis, Trusted Facility Management and Trusted Recovery

Life-cycle Assurance: Security Testing, Design Specification and Verification, Configuration Management and Trusted System Distribution

Incorrect Answers:
A: System Architecture is not required for Life-Cycle Assurance. System Architecture is part of Operational Assurance.
B: Covert Channel Analysis is not required for Life-Cycle Assurance. Covert Channel Analysis is part of Operational Assurance.
D: Trusted Facility Management is not required for Life-Cycle Assurance. Trusted Facility Management is part of Operational Assurance.

References:
https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria

QUESTION 520
What is the most effective means of determining that controls are functioning properly within an operating system?

A. Interview with computer operator
B. Review of software control features and/or parameters
C. Review of operating system manual
D. Interview with product vendor

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Various operating system software products provide parameters and options for the tailoring of the system and activation of features such as activity logging. Parameters are important in determining how a system runs because they allow a standard piece of software to be customized to diverse environments. The reviewing of software control features and/or parameters is the most effective means of determining how controls are functioning within an operating system and of assessing and operating system's integrity.
The review of software control features and/or parameters would be part of your security audit. A security audit is typically performed by an independent third party to the management of the system. The audit determines the degree with which the required controls are implemented.

A security review is conducted by the system maintenance or security personnel to discover vulnerabilities within the system. A vulnerability occurs when policies are not followed, misconfigurations are present, or flaws exist in the hardware or software of the system. System reviews are sometimes referred to as a vulnerability assessment.

Incorrect Answers:
A: An interview with the computer operator is not an effective means of determining that controls are functioning properly within an operating system because the computer operator will not necessarily be aware of the detailed settings of the parameters.

C: The operating system manual should provide information as to what settings can be used but will not give any hint as to how parameters are actually set.
D: An interview with the product vendor is not an effective means of determining that controls are functioning properly within an operating system because the product vendor will not be aware of the detailed settings of the parameters.

QUESTION 521

Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:

Explanation:
You should always separate test and development environments.
When testing a system, you need to isolate the system to ensure the test system is controlled and stable. This will ensure the system is tested in a realistic environment that mirrors the live environment as closely as possible.
Access control methods can be used to easily separate the test and development environments.

Incorrect Answers:
A: Restricting access to systems under test is not the best reason for separating the test and development environments. Preventing instability in a development environment from affecting the test environment is a better answer.
C: Segregate user and development staff is not the best reason for separating the test and development environments.
D: Securing access to systems under development is not the best reason for separating the test and development environments. Securing access to systems under development would not be achieved by separating the test and development environments.

QUESTION 522

Which of the following is the act of performing tests and evaluations to test a system's security level to see if it complies with the design specifications and security requirements?

A. Validation
B. Verification
C. Assessment
D. Accuracy

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Verification is the process of determining whether the product accurately represents and meets the design specifications given to the developers.

Incorrect Answers:
A: Validation is the process of determining whether the product provides the necessary solution for the real-world problem that is was created to solve.
C: Assessments are performed to determine the potential risks to a system. It does not test a system's compliance with design specifications and security requirements.
D: Accuracy is related to the integrity of information and systems. The integrity of information and systems requires that the information and systems remain accurate and reliable. This is ensured by preventing any unauthorized modification to the information or systems.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 23-24, 74-74, 1106
https://en.wikipedia.org/wiki/Verification_and_validation

QUESTION 523
Which of the following is a not a preventative control?

A. Deny programmer access to production data.

B. Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.
C. Run a source comparison program between control and current source periodically.
D. Establish procedures for emergency changes.

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
To run a source comparison does not prevent any specific action from occurring.

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

To help review or design security controls, they can be classified by several criteria, for example according to the time that they act, relative to a security incident:
- Before the event, preventive controls are intended to prevent an incident from occurring e.g. by locking out unauthorized intruders;
- During the event, detective controls are intended to identify and characterize an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police;
- After the event, corrective controls are intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible.

Incorrect Answers:
A: Denying a programmer access to production data is an example of preventive control as it prevents the programmer from accessing the data.
B: To make a change request to include extra information would prevent unauthorized changes from being made.
D: By establishing procedure for emergency changes unauthorized changes could be prevented.

References:
https://en.wikipedia.org/wiki/Security_controls

QUESTION 524
A network-based vulnerability assessment is a type of test also referred to as:

A. An active vulnerability assessment.
B. A routing vulnerability assessment.
C. A host-based vulnerability assessment.
D. A passive vulnerability assessment.

Correct Answer: A

Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
An Intrusion Detection System (IDS) typically follows a two-step process. First procedures include inspection of the configuration files of a system to detect inadvisable settings; inspection of the password files to detect inadvisable passwords; and inspection of other system areas to detect policy violations.
In a second step, procedures are network-based and considered an active component; mechanisms are set in place to reenact known methods of attack and to record system responses.

Incorrect Answers:
B: A network-based vulnerability assessment is referred to as an active vulnerability assessment, not a routing vulnerability assessment.
C: A network-based vulnerability assessment is referred to as an active vulnerability assessment, not a host-based vulnerability assessment.
D: A network-based vulnerability assessment is referred to as an active vulnerability assessment, not a passive vulnerability assessment.

QUESTION 525
Which of the following answers best describes the type of penetration testing where the analyst has full knowledge of the network on which he is going to perform his test?
A. White-Box Penetration Testing
B. Black-Box Pen Testing
C. Penetration Testing
D. Gray-Box Pen Testing

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
In general there are three ways a pen tester can test a target system.
▪ White-Box: The tester has full access and is testing from inside the system.
▪ Gray-Box: The tester has some knowledge of the system he's testing. ▪ Black-Box: The tester has no knowledge of the system.

Each of these forms of testing has different benefits and can test different aspects of the system from different approaches.

Incorrect Answers:
B: Black-Box Pen Testing: This is where no prior knowledge is given about the target network. Only a domain name or business name may be given to the analyst. This is not what is described in the question.

C: The term “Penetration Testing” does not specify what type of penetration testing is being performed.
D: With Gray-Box testing, the tester has some knowledge of the system he's testing. This is not what is described in the question.

QUESTION 526
Which one of the following is NOT one of the outcomes of a vulnerability assessment?

A. Quantative loss assessment
B. Qualitative loss assessment
C. Formal approval of BCP scope and initiation document
D. Defining critical support areas

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Formal approval of BCP scope is not part of the vulnerability assessment. A vulnerability assessment identifies a wide range of vulnerabilities in the environment. Vulnerability assessments just find the vulnerabilities (the holes). A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Incorrect Answers:
A: Quantifying losses is part of the vulnerability assessment.
B: Prioritizing (qualifying) losses is part of the vulnerability assessment.
D: Identifying critical vulnerabilities is part of the vulnerability assessment.

References:
https://en.wikipedia.org/wiki/Vulnerability_assessment

QUESTION 527
Which of the following testing method examines internal structure or working of an application?

A. White-box testing
B. Parallel Test
C. Regression Testing
D. Pilot Testing

Correct Answer: A

Section: Security Assessment and Testing
Explanation

Explanation/Reference:
White-box testing is a method of testing software that tests internal structures or workings of an application, versus its functionality. White-box testing allows access to program source code, data structures, variables, etc.

Incorrect Answers:
B: Parallel Testing is the process of entering the same inputs in two different versions of the application and reporting the anomalies.
C: Regression Testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors.
D: Pilot Testing is a preliminary test that focuses on specific and predefined aspect of a system.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 194
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1105 https://en.wikipedia.org/wiki/White-box_testing
http://www.tutorialspoint.com/software_testing_dictionary/parallel_testing.htm http://soft-engineering.blogspot.co.za/2010/12/what-is-difference-between-pilot-and.html

QUESTION 528
What setup should an administrator use for regularly testing the strength of user passwords?
A. A networked workstation so that the live password database can easily be accessed by the cracking program.
B. A networked workstation so the password database can easily be copied locally and processed by the cracking program.
C. A standalone workstation on which the password database is copied and processed by the cracking program.
D. A password-cracking program is unethical; therefore it should not be used.

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Poor password selection is frequently a major security problem for any system's security. Administrators should obtain and use password-guessing programs frequently to identify those users having easily guessed passwords.

Because password-cracking programs are very CPU intensive and can slow the system on which it is running, it is a good idea to transfer the encrypted passwords to a standalone (not networked) workstation. Also, by doing the work on a non-networked machine, any results found will not be accessible by anyone unless they have physical access to that system.

Out of the four choice presented above this is the best choice.
However, in real life you would have strong password policies that enforce complexity requirements and does not let the user choose a simple or short password that can be easily cracked or guessed. That would be the best choice if it was one of the choices presented.

Another issue with password cracking is one of privacy. Many password cracking tools can avoid this by only showing the password was cracked and not showing what the password actually is. It is masking the password being used from the person doing the cracking.

Incorrect Answers:
A: The password cracking program should not be on a networked computer. This is a security risk as someone could access the computer over the network. Furthermore, you should not run the password cracking program on the live password database.
B: The password cracking program should not be on a networked computer. This is a security risk as someone could access the computer over the network. D: Whether or not a password-cracking program is unethical depends on why you are cracking the passwords. Cracking passwords as a test of password strength is a valid security test.

QUESTION 529
Which of the following would best describe the difference between white-box testing and black-box testing?

A. White-box testing is performed by an independent programmer team.
B. Black-box testing uses the bottom-up approach.
C. White-box testing examines the program internal logical structure.
D. Black-box testing involves the business units

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
White box software testing gives the tester access to program source code, data structures, variables, etc.
White box testing gives the tester access to the internal logical structure of the program, while black box testing gives the tester no internal details: The software is treated as a black box that receives inputs.

Incorrect Answers:
A: White-box testing can be performed by any programmer who has access the source code.
B: Black-box testing just hides the internal details of the program. Black-box testing does not use either a bottom-up, or top down approach.
D: Black-box testing is blind to business units, as it has not access to any internal details of the program.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 194

QUESTION 530
Who should measure the effectiveness of Information System security related controls in an organization?

A. The local security specialist
B. The business manager
C. The systems auditor
D. The central security manager

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations. Organizations can have internal auditors and/or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met.
CobiT is a model that most information security auditors follow when evaluating a security program. The Control Objectives for Information and related Technology (CobiT) is a framework and set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs.
Incorrect Answers:
A: A local security specialist could be hired to measure the effectiveness of Information System security related controls in an organization. However, in doing so, the local security specialist would be performing the role of systems auditor.
B: The business manager does not measure the effectiveness of Information System security related controls in an organization.
D: The central security manager could measure the effectiveness of Information System security related controls in an organization. However, in doing so, central security manager would be performing the role of systems auditor.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 55, 125

QUESTION 531
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

A. IS security specialists
B. Senior Management
C. Senior security analysts
D. systems Auditors

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Computers and the information processed on them usually have a direct relationship with a company's critical missions and objectives. Because of this level of importance, senior management should make protecting these items a high priority and provide the necessary support, funds, time, and resources to ensure that systems, networks, and information are protected in the most logical and cost-effective manner possible.
For a company's security plan to be successful, it must start at the top level and be useful and functional at every single level within the organization. Senior management needs to define the scope of security and identify and decide what must be protected and to what extent.

Incorrect Answers:
A: IS security specialists may be the ones who implement the security measures; however, they do not bear the primary responsibility for determining the level of protection needed for information systems resources.
C: Senior security analysts may be the ones who determine how to implement the security measures; however, they do not bear the primary responsibility for determining the level of protection needed for information systems resources.
D: Systems Auditors ensure the appropriate security controls are in place. However, they do not bear the primary responsibility for determining the level of protection needed for information systems resources.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 101

QUESTION 532
Common Criteria has assurance level from EAL 1 to EAL 7 regarding the depth of design and testing. Which of following assure the Target of Evaluation (or TOE) is methodically designed, tested and reviewed?

A. EAL 3
B. EAL 4
C. EAL 5
D. EAL 6

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Under the Common Criteria model, an evaluation is carried out on a product and it is assigned an *Evaluation Assurance Level (EAL).* The thorough and stringent testing increases in detailed-oriented tasks as the assurance levels increase. The Common Criteria has seven assurance levels. The range is from EAL1, where

functionality testing takes place, to EAL7, where thorough testing is performed and the system design is verified. The different EAL packages are listed next: ▪ EAL1 Functionally tested
▪ EAL2 Structurally tested
▪ EAL3 Methodically tested and checked
▪ EAL4 Methodically designed, tested, and reviewed
▪ EAL5 Semi-formally designed and tested
▪ EAL6 Semi-formally verified design and tested ▪ EAL7 Formally verified design and tested

Incorrect Answers:
A: EAL3 is 'methodically tested and checked', not 'methodically designed, tested, and reviewed'.
C: EAL5 is 'semi-formally designed and tested, not 'methodically designed, tested, and reviewed'.
D: EAL6 is 'semi-formally verified design and tested, not 'methodically designed, tested, and reviewed'.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 402

QUESTION 533
Which Orange Book evaluation level is described as "Verified Design"?

A. A1. B. B3.
C. B2.
D. B1.

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Level A1 is "Verified Design".
A1: Verified Design: The architecture and protection features are not much different from systems that achieve a B3 rating, but the assurance of an A1 system is higher than a B3 system because of the formality in the way the A1 system was designed, the way the specifications were developed, and the level of detail in the verification techniques. Formal techniques are used to prove the equivalence between the TCB specifications and the security policy model. A more stringent change configuration is put in place with the development of an A1 system, and the overall design can be verified. In many cases, even the way in which the system is delivered to the customer is under scrutiny to ensure there is no way of compromising the system before it reaches its destination.
The type of environment that would require A1 systems is the most secure of secured environments. This type of environment deals with top-secret information and cannot adequately trust anyone using the systems without strict authentication, restrictions, and auditing.

Incorrect Answers:
B: Level B3 is “Security Domains”, not “Verified Design”.
C: Level B2 is “Structured Protection”, not “Verified Design”.
D: Level B1 is “Labeled Security”, not “Verified Design”.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 395-397

QUESTION 534
Which Orange Book evaluation level is described as "Structured Protection"?

A. A1
B. B3
C. B2
D. B1

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Level B2 is described as “Structured Protection”.
B2: Structured Protection The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers. Subjects and devices require labels, and the system must not allow covert channels. A trusted path for logon and authentication processes must be in place, which means the subject communicates directly with the application or operating system, and no trapdoors exist. There is no way to circumvent or compromise this communication channel. Operator and administration functions are separated within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolate processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system. The type of environment that would require B2 systems is one that processes sensitive data that require a higher degree of security. This type of environment would require systems that are relatively resistant to penetration and compromise.

Incorrect Answers:
A: Level A1 is “Verified Design”, not “Structured Protection”.
B: Level B3 is “Security Domains”, not “Structured Protection”.
D: Level B1 is “Labeled Security”, not “Structured Protection”.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 395-397

QUESTION 535
What can be BEST defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?

A. Risk management
B. Risk analysis
C. Threat analysis
D. Due diligence

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Threat analysis is defined as the examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

Incorrect Answers:
A: Risk management is defined the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.
B: Risk analysis is defined as a method of identifying risks and assessing the possible damage that could be caused in order to justify security safeguards.
D: Due diligence is the act of gathering the necessary information so the best decision-making activities can take place.

QUESTION 536
Operations Security seeks to PRIMARILY protect against which of the following?

A. object reuse
B. facility disaster
C. compromising emanations
D. asset threats

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

Operations Security refers to the act of understanding the threats to and vulnerabilities of computer operations in order to routinely support operational activities that enable computer systems to function correctly. It also refers to the implementation of security controls for normal transaction processing, system administration tasks, and critical external support operations. These controls can include resolving software or hardware problems along with the proper maintenance of auditing and monitoring processes.
Like the other domains, the Operations Security domain is concerned with triples — threats, vulnerabilities, and assets.

- A threat in the Operations Security domain can be defined as an event that could cause harm by violating the security. An example of an operations threat would be an operator's abuse of privileges, thereby violating confidentiality.
- A vulnerability is defined as a weakness in a system that enables security to be violated. An example of an operations vulnerability would be a weak implementation of the separation of duties.
- An asset is considered anything that is a computing resource or ability, such as hardware, software, data, and personnel.

Incorrect Answers:
A: Object Reuse is the concept of reusing data storage media after its initial use. Object reuse is one type of risk. Preventing object reuse alone is not the primary purpose of Operations Security.
B: Operations Security seeks to primarily protect against all types of asset threats. It does not seek to primarily protect against a single threat such as a facility disaster.
C: Operations Security does not seek to protect against a single threat such as compromising emanations. It protects all assets against all threats.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 302

QUESTION 537
The viewing of recorded events after the fact using a closed-circuit TV camera is considered a

A. Preventative control.

B. Detective control
C. Compensating control
D. Corrective control

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The question states that you are looking at recorded events on closed-circuit TV camera. This is a detective control. The purpose of a detective control is to identify an incident's activities after it took place. Examples or detective controls are cameras, logs, investigations and IDS.

Incorrect Answers:
A: Preventative controls are intended to avoid an incident from occurring. In this question, the event has occurred. Therefore, this answer is incorrect. C: Compensating control are controls that provide an alternative measure of control. This is not what is described in the question. Therefore, this answer is incorrect.
D: Corrective controls fix components or systems after an incident has occurred. Watching camera footage does not fix anything. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 30

QUESTION 538
How would nonrepudiation be BEST classified as?

A. A preventive control
B. A logical control
C. A corrective control
D. A compensating control

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
For example, if a user sends a message and then later claims he did not send it, this is an act of repudiation. When a cryptography mechanism provides nonrepudiation, the sender cannot later deny he sent the message (well, he can try to deny it, but the cryptosystem proves otherwise). It's a way of keeping the sender honest.
Nonrepudiation is a preventive control – it prevents someone having the ability to deny something.

Incorrect Answers:
B: Logical controls (also called technical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. Nonrepudiation is not a logical control.
C: Corrective controls are used to restore systems after an attack or other harmful occurrence. Nonrepudiation is not a corrective control.
D: Compensating controls are used to provide an alternative measure of control. Nonrepudiation is not a compensating control.

References:
http://searchsecurity.techtarget.com/definition/nonrepudiation

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 770

QUESTION 539
Which of the following is NOT a preventive login control?

A. Last login message
B. Password aging
C. Minimum password length
D. Account expiration

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Password management and account management are preventive login controls.
Password aging determines how long a password can be used for before the password must be changed. For example a maximum password age of 30 days would force users to change their passwords every 30 days.
Minimum password length determines the minimum number of characters a password should have. A minimum of eight characters is generally regarded as a requirement for a good password.
Account expiration determines when a user account will expire. This is especially useful for temporary workers and helps to ensure that unused accounts are not left active.

A last login message is not a preventive login control. A last login message is informational only and does nothing to improve the security of the system.

Incorrect Answers:
B: Password aging is an example of a preventive login control.
C: Minimum password length is an example of a preventive login control.
D: Account expiration is an example of a preventive login control.

QUESTION 540
Which type of control is concerned with avoiding occurrences of risks?

A. Deterrent controls
B. Detective controls
C. Preventive controls
D. Compensating controls

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Preventive controls are concerned with avoiding occurrences of risks.
The different functionalities of security controls are preventive, detective, corrective, deterrent, recovery, and compensating. The six different control functionalities are as follows: ▪ Deterrent: Intended to discourage a potential attacker
▪ Preventive: Intended to avoid an incident from occurring
▪ Corrective: Fixes components or systems after an incident has occurred
▪ Recovery: Intended to bring the environment back to regular operations
▪ Detective: Helps identify an incident's activities and potentially an intruder
▪ Compensating: Controls that provide an alternative measure of control

Incorrect Answers:
A: Deterrent controls are intended to discourage a potential attacker. A potential hacker is a risk; however, it is just one type of risk. Preventive controls are concerned with avoiding all risks.
B: Detective controls are used to discover harmful occurrences; not avoid them.
D: Compensating controls provide an alternative measure of control. They are not the primary control type concerned with avoiding occurrences of risks.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 30

QUESTION 541
Password management falls into which control category?

A. Compensating
B. Detective
C. Preventive
D. Technical

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

Preventive controls are put in place to inhibit harmful occurrences. Access control is an example of a preventive control. Passwords are used in access control; therefore, password control is a preventive control.
Preventive controls can be administrative, physical or
technical. Preventive Technical controls include: ▪ Passwords,
biometrics, smart cards
▪ Encryption, secure protocols, call-back systems, database views, constrained user interfaces ▪
Antimalware software, access control lists, firewalls, intrusion prevention system

Incorrect Answers:
A: Compensating controls are controls that provide an alternative measure of control. Password management does not fall into the Compensating control category.
B: Detective controls are established to discover harmful occurrences. Password management does not fall into the Detective control category.
D: Technical is a control type, not a control category. Password management is a technical control but it falls into the Preventive control category.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 31

QUESTION 542
What is the primary goal of setting up a honey pot?

A. To lure hackers into attacking unused systems
B. To entrap and track down possible hackersC. To set up a sacrificial lamb on the network
D. To know when certain types of attacks are in progress and to learn about attack techniques so the network can be fortified.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A honeypot system is a computer that usually sits in the screened subnet, or DMZ, and attempts to lure attackers to it instead of to actual production computers. To make a honeypot system lure attackers, administrators may enable services and ports that are popular to exploit. Some honeypot systems have services emulated, meaning the actual service is not running but software that acts like those services is available. Honeypot systems can get an attacker's attention by advertising themselves as easy targets to compromise. They are configured to look like regular company systems so that attackers will be drawn to them like bears are to honey.
Honeypots can work as early detection mechanisms, meaning that the network staff can be alerted that an intruder is attacking a honeypot system, and they can quickly go into action to make sure no production systems are vulnerable to that specific attack type.
Organizations use these systems to identify, quantify, and qualify specific traffic types to help determine their danger levels. The systems can gather network traffic statistics and return them to a centralized location for better analysis. So as the systems are being attacked, they gather intelligence information that can help the network staff better understand what is taking place within their environment.

Incorrect Answers:
A: A honeypot does act as a decoy system in that it can lure hackers into attacking the honeypot system instead of live production servers. However, this is not the primary goal of a honeypot. The primary goal is to learn about attack techniques so the network can be fortified.
B: Entrapping and tracking down attackers is not the goal of a honeypot. Learning about possible attack techniques is more valuable to a company.
C: It is not the goal of a honeypot to set up a sacrificial lamb on the network.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 655

QUESTION 543
Ensuring that printed reports reach proper users and that receipts are signed before releasing sensitive documents are examples of:

A. Deterrent controls
B. Output controls
C. Information flow controls
D. Asset controls

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Output controls are used for two things — for protecting the confidentiality of an output, and for verifying the integrity of an output by comparing the input transaction with the output data. Elements of proper output controls would involve ensuring the output reaches the proper users, restricting access to the printed output storage areas, printing heading and trailing banners, requiring signed receipts before releasing sensitive output, and printing “no output” banners when a report is empty

Incorrect Answers:
A: Deterrent controls are used to encourage compliance with external controls, such as regulatory compliance. These controls are meant to complement other controls, such as preventative and detective controls. This is not what is described in the question.
C: Ensuring that printed reports reach proper users and that receipts are signed before releasing sensitive documents are not examples of information flow controls.
D: Ensuring that printed reports reach proper users and that receipts are signed before releasing sensitive documents are not examples of asset controls.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 218

QUESTION 544

Which of the following security control is intended to avoid an incident from occurring?

A. Deterrent
B. Preventive
C. Corrective
D. Recovery

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Preventive controls stop actions from taking place. It applies restrictions to what a possible user can do, whether the user is authorized or unauthorized.

Incorrect Answers:
A: Deterrent controls discourage users from performing actions on a system.
C: Corrective controls deals with correcting a damaged system or process.
D: Recovery controls may be required to restore functionality of the system and organization subsequent to a security incident taking place.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 27, 28

QUESTION 545
Which of the following are the three classifications of RAID identified by the RAID Advisory Board?

A. Failure Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems.
B. Foreign Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems.
C. Failure Resistant Disk Systems (FRDSs), File Transfer Disk Systems, and Disaster Tolerant Disk Systems.
D. Federal Resistant Disk Systems (FRDSs), Fault Tolerant Disk Systems, and Disaster Tolerant Disk Systems.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

The RAID Advisory Board has defined three classifications of RAID: Failure Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems. As of this writing only the first one, FRDS, is an existing standard, and the others are still pending. We will now discuss the various implementation levels of an FRDS.
Failure Resistant Disk System: The basic function of an FRDS is to protect file servers from data loss and a loss of availability due to disk failure. It provides the ability to reconstruct the contents of a failed disk onto a replacement disk and provides the added protection against data loss due to the failure of many hardware parts of the server. One feature of an FRDS is that it enables the continuous monitoring of these parts and the alerting of their failure.
Failure Resistant Disk System Plus: An update to the FRDS standard is called FRDS+. This update adds the ability to automatically hot swap (swapping while the server is still running) failed disks. It also adds protection against environmental hazards (such as temperature, out-of-range conditions, and external power failure) and includes a series of alarms and warnings of these failures.

Incorrect Answers:
B: Foreign Resistant Disk Systems is not one of the three classifications of RAID identified by the RAID Advisory Board.
C: File Transfer Disk Systems is not one of the three classifications of RAID identified by the RAID Advisory Board.
D: Federal Resistant Disk Systems is not one of the three classifications of RAID identified by the RAID Advisory Board.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

QUESTION 546
RAID Level 1 is commonly called which of the following?

A. mirroring
B. striping
C. clustering
D. hamming

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 1 is commonly called mirroring. It mirrors the data from one disk or set of disks by duplicating the data onto another disk or set of disks. This is often implemented by a one-for-one disk to disk ratio: Each drive is mirrored to an equal drive partner that is continually being updated with current data. If one drive fails, the system automatically gets the data from the other drive. The main issue with this level of RAID is that the one-for-one ratio is very expensive — resulting in the highest cost per megabyte of data capacity. This level effectively doubles the amount of hard drives you need, therefore it is usually best for smaller capacity systems.

Incorrect Answers:
B: Striping is used in other RAID levels, but not in RAID level 1.
C: Clustering is not a RAID level.
D: RAID Level 1 is not called hamming. Hamming is code used to create parity data in RAID level 2.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

QUESTION 547
Which of the following is often implemented by a one-for-one disk to disk ratio?

A. RAID Level 1 B.
RAID Level 0 C.
RAID Level 2
D. RAID Level 5

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 1 is commonly called mirroring. It mirrors the data from one disk or set of disks by duplicating the data onto another disk or set of disks. This is often implemented by a one-for-one disk to disk ratio: Each drive is mirrored to an equal drive partner that is continually being updated with current data. If one drive fails, the system automatically gets the data from the other drive. The main issue with this level of RAID is that the one-for-one ratio is very expensive — resulting in the highest cost per megabyte of data capacity. This level effectively doubles the amount of hard drives you need, therefore it is usually best for smaller capacity systems.

Incorrect Answers:
B: RAID level 0 is not implemented by a one-for-one disk to disk ratio.
C: RAID level 2 is not implemented by a one-for-one disk to disk ratio.
D: RAID level 5 is not implemented by a one-for-one disk to disk ratio.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

QUESTION 548
The MAIN issue with Level 1 of RAID is which of the following?

A. It is very expensive.
B. It is difficult to recover.
C. It causes poor performance.
D. It is relatively unreliable.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 1 is commonly called mirroring. It mirrors the data from one disk or set of disks by duplicating the data onto another disk or set of disks. This is often implemented by a one-for-one disk to disk ratio: Each drive is mirrored to an equal drive partner that is continually being updated with current data. If one drive fails, the system automatically gets the data from the other drive. The main issue with this level of RAID is that the one-for-one ratio is very expensive — resulting in the highest cost per megabyte of data capacity. This level effectively doubles the amount of hard drives you need, therefore it is usually best for smaller capacity systems.

Incorrect Answers:
B: RAID level 1 is not difficult to recover. If one drive fails, the system automatically gets the data from the other drive.
C: RAID level 1 does not cause poor performance. The performance is quite good because no parity data needs to be calculated.
D: RAID level 1 is not relatively unreliable; duplicating data onto another disk is a reliable system.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

QUESTION 549
Which of the following effectively doubles the amount of hard drives needed but also provides redundancy?

A. RAID Level 0 B.
RAID Level 1 C.
RAID Level 2
D. RAID Level 5

Correct Answer: B
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:

RAID Level 1 is commonly called mirroring. It mirrors the data from one disk or set of disks by duplicating the data onto another disk or set of disks. This is often implemented by a one-for-one disk to disk ratio: Each drive is mirrored to an equal drive partner that is continually being updated with current data. If one drive fails, the system automatically gets the data from the other drive. The main issue with this level of RAID is that the one-for-one ratio is very expensive — resulting in the highest cost per megabyte of data capacity. This level effectively doubles the amount of hard drives you need, therefore it is usually best for smaller capacity systems.

Incorrect Answers:
A: RAID Level 0 requires a minimum of two disks so in that sense, it does double the minimum disk requirement. However, if the minimum amount of disks you require to store your data is more than two, then RAID level 0 does not double the disk requirement. For example, if you needed 4 disks to store all your data, you could just create a 4-disk RAID. RAID level 0 also provides no redundancy.
C: RAID Level 2 defines a 39-disk system. This doesn't double the amount of hard drives needed because it is a fixed disk requirement.
D: RAID Level 5 does not double the amount of hard drives needed. RAID level 5 requires the equivalent of one extra drive for parity data. For example, if 4 disks were needed for the amount of data to be stored, the RAID would need 5 disks. If 10 disks were required for the amount of data to be stored, the RAID would need 11 disks in total.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

QUESTION 550
Which of the following is used to create parity information?

A. a hamming code
B. a clustering code
C. a mirroring code
D. a striping code

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 2 consists of bit-interleaved data on multiple disks. The parity information is created using a hamming code that detects errors and establishes which part of which drive is in error. It defines a disk drive system with 39 disks: 32 disks of user storage 66 and seven disks of error recovery coding. This level is not used in practice and was quickly superseded by the more flexible levels of RAID such as RAID 3 and RAID 5.

Incorrect Answers:
B: Clustering code is not used to create parity information.

C: A mirroring code is not used to create parity information. Mirroring is used to describe the method used in RAID level 1.
D: A striping code is not used to create parity information. Striping is the method used to write data across multiple disks in RAID systems.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

QUESTION 551
The only difference between RAID 3 and RAID 4 is that level 3 is implemented at the byte level while level 4 is usually implemented at which of the following?

A. Block level.
B. Bridge level.
C. Channel level.
D. Buffer level.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Levels 3 and 4 function in a similar way. The only difference is that level 3 is implemented at the byte level and level 4 is usually implemented at the block level. In this scenario, data is striped across several drives and the parity check bit is written to a dedicated parity drive. This is similar to RAID 0. They both have a large data volume, but the addition of a dedicated parity drive provides redundancy. If a hard disk fails, the data can be reconstructed by using the bit information on the parity drive. The main issue with this level of RAID is that the constant writes to the parity drive can create a performance hit. In this implementation, spare drives can be used to replace crashed drives.

Incorrect Answers:
B: RAID level 4 is not implemented at bridge level.
C: RAID level 4 is not implemented at channel level.
D: RAID level 4 is not implemented at buffer level.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 145

QUESTION 552
The spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on the server in which of the following scenarios?

A. system is up and running
B. system is quiesced but operational
C. system is idle but operational
D. system is up and in single-user-mode

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 5 stripes the data and the parity information at the block level across all the drives in the set. It is similar to RAID 3 and 4 except that the parity information is written to the next available drive rather than to a dedicated drive by using an interleave parity. This enables more flexibility in the implementation and increases fault tolerance as the parity drive is not a single point of failure, as it is in RAID 3 or 4. The disk reads and writes are also performed concurrently, thereby increasing performance over levels 3 and 4. The spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on the server while the system is up and running. This is probably the most popular implementation of RAID today.

Incorrect Answers:
B: Hot swappable means that the disk drives can be replaced on the server while the server is system is up and running. The server does not need to be quiesced. C: Hot swappable means that the disk drives can be replaced on the server while the server is system is up and running. The server does not need to be idle. D: Hot swappable means that the disk drives can be replaced on the server while the server is system is up and running. The server does not need to be in singleuser-mode.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 145

QUESTION 553
RAID level 10 is created by combining which of the following?

A. level 0 (striping) with level 1 (mirroring).
B. level 0 (striping) with level 2 (hamming).
C. level 0 (striping) with level 1 (clustering).
D. level 0 (striping) with level 1 (hamming).

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID 10, also known as RAID 1+0, combines disk mirroring and disk striping to protect data.
A RAID 10 configuration requires a minimum of four disks, and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved. If two disks in the same mirrored pair fail, all data will be lost because there is no parity in the striped sets.
RAID 10 provides redundancy and performance, and is the best option for I/O-intensive applications. One disadvantage is that only 50% of the total raw capacity of the drives is usable due to mirroring.

Incorrect Answers:
B: Level 0 (striping) is combined with level 1 (mirroring), not level 2 (hamming).
C: Level 1 is mirroring, not clustering.
D: Level 1 is mirroring, not hamming.

References:
http://searchstorage.techtarget.com/definition/RAID-10-redundant-array-of-independent-disks

QUESTION 554
A hardware RAID implementation is usually:

A. platform-independent.
B. platform-dependent.
C. operating system dependent.
D. software dependent.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
RAID can be implemented in either hardware or software. Each type has its own issues and benefits. A hardware RAID implementation is usually platformindependent. It runs below the operating system (OS) of the server and usually does not care if the OS is Novell, NT, or Unix. The hardware implementation uses its own Central Processing Unit (CPU) for calculations on an intelligent controller card. There can be more than one of these cards installed to provide hardware redundancy in the server. RAID levels 3 and 5 run faster on hardware. A software implementation of RAID means it runs as part of the operating system on the file server.

Incorrect Answers:
B: A hardware RAID implementation is not platform-dependent.
C: A hardware RAID implementation is not operating system dependent.
D: A hardware RAID implementation is not software dependent.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 145

QUESTION 555
RAID levels 3 and 5 run:

A. faster on hardware.
B. slower on hardware.
C. faster on software.
D. at the same speed on software and hardware.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID can be implemented in either hardware or software. Each type has its own issues and benefits. A hardware RAID implementation is usually platformindependent. It runs below the operating system (OS) of the server and usually does not care if the OS is Novell, NT, or Unix. The hardware implementation uses its own Central Processing Unit (CPU) for calculations on an intelligent controller card. There can be more than one of these cards installed to provide hardware redundancy in the server. RAID levels 3 and 5 run faster on hardware. A software implementation of RAID means it runs as part of the operating system on the file server.

Incorrect Answers:
B: RAID levels 3 and 5 run faster, not slower on hardware.
C: RAID levels 3 and 5 run faster on hardware, not software.

D: RAID levels 3 and 5 run faster hardware than they do on software.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 145

QUESTION 556
When RAID runs as part of the operating system on the file server, it is an example of a:

A. software implementation.

B. hardware implementation.
C. network implementation.
D. server implementation.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID can be implemented in either hardware or software. Each type has its own issues and benefits.
A software implementation of RAID means it runs as part of the operating system on the file server. Often RAID levels 0, 1, and 10 run faster on software RAID because of the need for the server's software resources. Simple striping or mirroring can run faster in the operating system because neither use the hardware-level parity drives.

Incorrect Answers:
B: RAID running as part of the operating system on the file server is an example of a software implementation, not a hardware implementation.
C: RAID running as part of the operating system on the file server is an example of a software implementation, not a network implementation.
D: RAID running as part of the operating system on the file server is an example of a software implementation, not a server implementation.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 145

QUESTION 557
A server cluster looks like a:

A. single server from the user's point of view.

B. dual server from the user's point of view.
C. triple server from the user's point of view.
D. quadruple server from the user's point of view.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A server cluster is a group of independent servers, which are managed as a single system that provides higher availability, easier manageability, and greater scalability.
The cluster looks like a single server from the user's point of view. If any server in the cluster crashes, processing continues transparently.

Incorrect Answers:
B: A server cluster looks like a single server, not a dual server from the user's point of view.
C: A server cluster looks like a single server, not a triple server from the user's point of view.
D: A server cluster looks like a single server, not a quadruple server from the user's point of view.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 145

QUESTION 558
Which of the following backup methods makes a complete backup of every file on the server every time it is run?

A. The full backup method.
B. The incremental backup method.
C. The differential backup method.
D. The tape backup method.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The Full Backup Method makes a complete backup of every file on the server every time it is run. The method is primarily run when time and tape space permits, and is used for system archive or baselined tape sets.

Incorrect Answers:
B: The incremental backup method backs up only the files that have changed since the previous full or incremental backup. This backup method does not back up all files every time it is run.
C: The differential backup method backs up only the files that have changed since the previous full backup. This backup method does not back up all files every time it is run.
D: The tape backup method is not a method that determines what files are backed up; it just specifies that the files are backed up to tape.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 148

QUESTION 559
Which backup method usually resets the archive bit on the files after they have been backed up?
A. Incremental backup method.
B. Differential backup method.
C. Partial backup method.
D. Tape backup method.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The incremental backup method backs up all the files that have changed since the last full or incremental backup and resets the archive bit to 0. This is known as “clearing the archive bit”. A full backup backs up all files regardless of whether the archive bit is 1 or 0 and sets the archive bit to 0.
The archive bit is used by the backup process to determine whether a file has been changed. When you modify a file or create a new file, the archive bit is set to 1. This tells the backups process that the file has changed (or is a new file) and needs to be backed up. When an incremental backup backs up the file, it sets the archive bit to 0. When the next incremental backup runs and sees that the archive bit is 0, the incremental backup knows that the file has not changed since the last backup and so will not back up the file again.

Incorrect Answers:
B: The differential backup method backs up only the files that have changed since the previous full backup. This backup method does not reset the archive bit.
C: The partial backup method is not a method that determines whether the archive bit is reset or not; it just specifies that a subset of data is backed up.
D: The tape backup method is not a method that determines whether the archive bit is reset or not; it just specifies that the files are backed up to tape.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 69

QUESTION 560
Which backup method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup?

A. The differential backup method.
B. The full backup method.
C. The incremental backup method.
D. The tape backup method.

Correct Answer: A
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
The Differential Backup Method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup.
Archive bits let the backup software know what needs to be backed up. The differential and incremental backup types rely on the archive bit to direct them.

Incorrect Answers:
B: Full backups back up all files. Full backups are not additive.
C: Incremental backups are not additive because they reset the archive bit so the file is not backed up again next day (unless the file was changed again).
D: The tape backup method is not a method that determines whether the archive bit is reset or not; it just specifies that the files are backed up to tape.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 69
http://www.brighthub.com/computing/windows-platform/articles/24531.aspx

QUESTION 561
Which of the following backup method must be made regardless of whether Differential or Incremental methods are used?

A. Full Backup Method.
B. Incremental backup method.
C. Supplemental backup method.
D. Tape backup method.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A Full Backup must be made regardless of whether Differential or Incremental methods are used.
The Full Backup Method makes a complete backup of every file on the server every time it is run. The full backup will reset the archive bits on all the files that were backed up. The archive bits are used by incremental and differential backups to determine which files have been changed since the full backup and therefore, which files need to be backed up.

Incorrect Answers:
B: Incremental backups back up all files that were changed since the last full or incremental backup. You do not have to use incremental backups.
C: "Supplemental" is not the backup type that must be made regardless of whether Differential or Incremental methods are used. A supplemental backup is an 'extra' or 'additional' backup; it is not part of the regular backup schedule.
D: The tape backup method is not one of the defined backup types; it just specifies that the files are backed up to tape.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 69

QUESTION 562
Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?

A. Digital Video Tape (DVT).
B. Digital Analog Tape (DAT).
C. Digital Voice Tape (DVT).
D. Digital Audio Tape (DAT).

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Digital Audio Tape (DAT) can be used to backup data systems in addition to its original intended audio uses.

Incorrect Answers:
A: Digital Video Tape (DVT) is not used to backup data systems.
B: Digital Analog Tape (DAT) is not a defined type of tape; DAT stands for Digital Audio Tape.
C: Digital Voice Tape (DVT) is not a defined type of tape; DVT stands for Digital Video Tape.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 70

QUESTION 563
This type of backup management provides a continuous on-line backup by using optical or tape "jukeboxes," similar to WORMs (Write Once, Read Many):

A. Hierarchical Storage Management (HSM).
B. Hierarchical Resource Management (HRM).
C. Hierarchical Access Management (HAM).
D. Hierarchical Instance Management (HIM).

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Hierarchical Storage Management (HSM) provides a continuous on-line backup by using optical or tape "jukeboxes," similar to WORMs. It appears as an infinite disk to the system, and can be configured to provide the closest version of an available real-time backup. This is commonly employed in very large data retrieval systems.

Incorrect Answers:
B: Hierarchical Resource Management (HRM) is not a defined backup media technology.
C: Hierarchical Access Management (HAM) is not a defined backup media technology.
D: Hierarchical Instance Management (HIM) is not a defined backup media technology.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 71

QUESTION 564
Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:

A. Operations Security Domain.
B. Operations Security Domain Analysis.
C. Telecommunications and Network Security Domain.
D. Business Continuity Planning and Disaster Recovery Planning.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Physically securing the tapes from unauthorized access is obviously a security concern and is considered a function of the Operations Security Domain. Operations Security can be described as the controls over the hardware in a computing facility, the data media used in a facility, and the operators using these resources in a facility.
Operations Security refers to the act of understanding the threats to and vulnerabilities of computer operations in order to routinely support operational activities that enable computer systems to function correctly. It also refers to the implementation of security controls for normal transaction processing, system administration tasks, and critical external support operations. These controls can include resolving software or hardware problems along with the proper maintenance of auditing and monitoring processes.

Incorrect Answers:
B: Physically securing backup tapes from unauthorized access is not considered a function of the Operations Security Domain Analysis.
C: Physically securing backup tapes from unauthorized access is not considered a function of the Telecommunications and Network Security Domain.
D: Physically securing backup tapes from unauthorized access is not considered a function of the Business Continuity Planning and Disaster Recovery Planning.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 71 Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 301

QUESTION 565
The main issue with RAID Level 1 is that the one-for-one ratio is:

A. very expensive, resulting in the highest cost per megabyte of data capacity.
B. very inexpensive, resulting in the lowest cost per megabyte of data capacity.
C. very unreliable resulting in a greater risk of losing data.
D. very reliable resulting in a lower risk of losing data.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 1 is commonly called mirroring. It mirrors the data from one disk or set of disks by duplicating the data onto another disk or set of disks. This is often implemented by a one-for-one disk to disk ratio: Each drive is mirrored to an equal drive partner that is continually being updated with current data. If one drive fails, the system automatically gets the data from the other drive. The main issue with this level of RAID is that the one-for-one ratio is very expensive — resulting in the highest cost per megabyte of data capacity. This level effectively doubles the amount of hard drives you need, therefore it is usually best for smaller capacity systems.

Incorrect Answers:
B: RAID Level 1 is not inexpensive, resulting in the lowest cost per megabyte of data capacity; it is the opposite.
C: RAID Level 1 is not unreliable resulting in a greater risk of losing data; it is the opposite.
D: RAID Level 1 is very reliable resulting in a lower risk of losing data. However, this is not an 'issue', it's a good thing.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 90

QUESTION 566
Which of the following RAID levels is not used in practice and was quickly superseded by the more flexible levels?

A. RAID Level 0 B.
RAID Level 1 C.
RAID Level 2
D. RAID Level 7
Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 2 consists of bit-interleaved data on multiple disks. The parity information is created using a hamming code that detects errors and establishes which part of which drive is in error. It defines a disk drive system with 39 disks: 32 disks of user storage 66 and seven disks of error recovery coding. This level is not used in practice and was quickly superseded by the more flexible levels.

Incorrect Answers:
A: RAID Level 0 "Writes files in stripes across multiple disks without the use of parity information. This technique allows for fast reading and writing to disk. However, without the parity information, it is not possible to recover from a hard drive failure. This technique does not provide redundancy and should not be used for systems with high availability requirements. RAID Level 0 is widely used today where performance is required but not redundancy.
B: RAID Level 1 "This level duplicates all disk writes from one disk to another to create two identical drives. This technique is also known as data mirroring. RAID Level 1 is widely used today.
D: RAID Level 7 is a variation of RAID 5 wherein the array functions as a single virtual disk in the hardware. This is sometimes simulated by software running over a RAID level 5 hardware implementation. This enables the drive array to continue to operate if any disk or any path to any disk fails. RAID Level 7 was not superseded by the more flexible levels.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2003, p. 90

QUESTION 567
Which RAID implementation is commonly called mirroring?

A. RAID level 2 B.
RAID level 3 C.
RAID level 5
D. RAID level 1

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 1 is commonly called mirroring. It mirrors the data from one disk or set of disks by duplicating the data onto another disk or set of disks. This is often implemented by a one-for-one disk to disk ratio: Each drive is mirrored to an equal drive partner that is continually being updated with current data. If one drive fails, the system automatically gets the data from the other drive. The main issue with this level of RAID is that the one-for-one ratio is very expensive — resulting in the highest cost per megabyte of data capacity. This level effectively doubles the amount of hard drives you need, therefore it is usually best for smaller capacity systems.

Incorrect Answers:
A: RAID level 2 uses hamming code parity. It is not called mirroring.
B: RAID level 3 uses byte level parity. It is not called mirroring.
C: RAID level 5 uses interleave parity. It is not called mirroring.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

QUESTION 568
Ding Ltd. is a firm specialized in intellectual property business. A new video streaming application needs to be installed for the purpose of conducting the annual awareness program as per the firm security program. The application will stream internally copyrighted computer based training videos. The requirements for the application installation are to use a single server, low cost technologies, high performance and no high availability capacities.

In regards to storage technology, what is the most suitable configuration for the server hard drives?

A. Single hard disk (no RAID)
B. RAID 0
C. RAID 1

D. RAID 10

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The questions states that the requirements are low cost technologies, high performance and no high availability capacities.
RAID Level 0 creates one large disk by using several disks. This process is called striping. It stripes data across all disks (but provides no redundancy) by using all of the available drive space to create the maximum usable data volume size and to increase the read/write performance.

Incorrect Answers:
A: Single hard disk does meet the low cost requirement and no high availability but it does not provide high performance.
C: RAID 1 (mirroring) does not provide high performance; it does provide high cost and high availability. This does not meet the requirements.
D: RAID 10 does provide high performance but it is an expensive solution with high availability capacities. This does not meet the requirements.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 65 **QUESTION 569**
Which of the following answers is directly related to providing High Availability to your users?

A. Backup data circuits
B. Good hiring practices
C. Updated Antivirus Software
D. Senior Executive Support

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When planning for high availability, any critical component of your data network should have some sort of redundancy or backup plan in case it does fail.
One of the ways to provide uninterrupted access to information assets is through redundancy and fault tolerance. Redundancy refers to providing multiple instances of either a physical or logical component such that a second component is available if the first fails. Fault tolerance is a broader concept that includes redundancy but refers to any process that allows a system to continue making information assets available in the case of a failure.

This can include items like these:

- RAID array disks on servers so that if any single drive fails the server remains available.
- Backup network connections. Many internet services providers provide these for a fee.
- Backup power for all systems and circuits.
- Fire suppression and evacuation plans.
- A data backup practice to backup and restore data while storing backups offsite in a safe, remote location.

Incorrect Answers:
B: Good hiring practices can ensure that good staff are hired. However, this does not ensure high availability.
C: Updated Antivirus Software does not ensure high availability, although it's a critical part of defense in depth.
D: Senior Executive Support, while this is important for funding equipment for high availability, it isn't directly related to providing the high availability.

QUESTION 570
When backing up an applications system's data, which of the following is a key question to be answered first?

A. When to make backups.
B. Where to keep backups.
C. What records to backup.
D. How to store backups.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
It is critical that a determination be made of WHAT data is important and should be retained and protected. Without determining the data to be backed up, the potential for error increases. A record or file could be vital and yet not included in a backup routine. Alternatively, temporary or insignificant files could be included in a backup routine unnecessarily.

Incorrect Answers:
A: Although it is important to consider schedules for backups, this is done after it has been determined what data should be included in the backup routine.
B: The location of the backup copies of data should be decided after determining what data should be included in the backup routine.
C: How to store backups is a question that needs to be answered. However, what to backup is the first question to be answered.

QUESTION 571
Which of the following security controls is intended to bring an environment back to regular operation?

A. Deterrent
B. Preventive

C. Corrective
D. Recovery

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The different functionalities of security controls are preventive, detective, corrective, deterrent, recovery, and compensating. The six different control functionalities are as follows: ▪ Deterrent Intended to discourage a potential attacker
▪ Preventive Intended to avoid an incident from occurring
▪ Corrective Fixes components or systems after an incident has occurred
▪ Recovery Intended to bring the environment back to regular operations
▪ Detective Helps identify an incident's activities and potentially an intruder
▪ Compensating Controls that provide an alternative measure of control

Incorrect Answers:
A: The Deterrent security control is intended to discourage a potential attacker. This is not what is described in the question.
B: The Preventative security control is intended to avoid an incident from occurring. This is not what is described in the question.
C: The Corrective security control fixes components or systems after an incident has occurred. This is not what is described in the question.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 30

QUESTION 572
Which of the following activities would not be included in the contingency planning process phase?

A. Prioritization of applications
B. Development of test procedures
C. Assessment of threat impact on the organization
D. Development of recovery scenarios

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
When an incident strikes, more is required than simply knowing how to restore data from backups. Also necessary are the detailed procedures that outline the activities to keep the critical systems available and ensure that operations and processing are not interrupted. Contingency management defines what should take place during and after an incident. Actions that are required to take place for emergency response, continuity of operations, and dealing with major outages must be documented and readily available to the operations staff.
Development of test procedures is not part of contingency planning. This has nothing to do with recovering from an incident.

Incorrect Answers:
A: Prioritization of applications is used to determine which applications are most important to the company and should be recovered first. This should be part of your contingency planning.
C: Assessment of threat impact on the organization should be part of the contingency plan to determine what affect an incident would have. This should be part of your contingency planning.
D: Development of recovery scenarios are the most obvious part of a contingency plan. You need to plan how to recover from an incident. This should be part of your contingency planning.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1276

QUESTION 573
Which RAID Level often implements a one-for-one disk to disk ratio?

A. RAID Level 1
B. RAID Level 0
C. RAID Level 2
D. RAID Level 5

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID Level 1, disk mirroring, uses a one-for-one setup, where data are written to two drives at once. If one drive fails, the other drive has the exact same data available.

Incorrect Answers:
B: RAID Level 0 uses data striped over several drives, not just two drives. There is not one-to-one disk ratio.
C: RAID Level 2 uses data striped over several drives, not just two drives. There is not one-to-one disk ratio.
D: RAID Level 5 does not use a one-to-one disk ratio.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 574
What is the PRIMARY purpose of using redundant array of inexpensive disks (RAID) level zero?

A. To improve system performance.
B. To maximize usage of hard disk space.
C. To provide fault tolerance and protection against file server hard disk crashes.
D. To implement integrity.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID level 0 offers no fault tolerance, just performance improvements.

Incorrect Answers:
B: RAID level 0 provides no increase in hard disk usage compared to non-raid disks.
C: RAID level 0 offers no fault tolerance.
D: RAID does provide integrity.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 142

QUESTION 575
Which RAID implementation stripes data and parity at block level across all the drives?

A. RAID level 1 B.
RAID level 2 C.
RAID level 4
D. RAID level 5

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
With RAID level 5 data are written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure.

Incorrect Answers:
A: RAID Level 1 does not use a parity bit. It uses mirroring of drives.
B: RAID Level 2 does not use block level parity. It uses hamming code parity.
C: RAID level 4 uses byte-level parity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 576
Which RAID level concept is considered more expensive and is applied to servers to create what is commonly known as server fault tolerance?

A. RAID level 0 B.
RAID level 1 C.
RAID level 2
D. RAID level 5

Correct Answer: B
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
RAID level 1 is mirroring of drives. Data are written to two drives at once. 50% of the disks are used for fault tolerance.

Incorrect Answers:
A: RAID level 0, data striping, provides no fault tolerance.
C: RAID Level 2 uses parity for fault tolerance, but is not used in production today.
D: RAID level 5 uses one parity bit for fault tolerance. With three drives, the minimum amount, 33% of the disks are for fault tolerance.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 577
Which backup method only copies files that have been recently added or changed and also leaves the archive bit unchanged?

A. Full backup method
B. Incremental backup method

C. Fast backup method
D. Differential backup method

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The Differential backup method backs up the files that have been modified since the last full backup. The differential process does not change the archive bit value.

Incorrect Answers:
A: During a full backup all data are backed up and saved to some type of storage media, and the archive bit is cleared.
B: The Incremental backup method backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0.
C: There is no backup method named fast backup method.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 936

QUESTION 578
Which of the following items is NOT primarily used to ensure integrity?

A. Cyclic Redundancy Check (CRC)
B. Redundant Array of Inexpensive Disks (RAID) system
C. Hashing Algorithms
D. The Biba Security model

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID can be used for fault tolerance, but it does not provide integrity.

Incorrect Answers:
A: Cyclic redundancy checks (CRCs) act as an integrity tool.
C: Hash totals act as an integrity tool.

D: The Biba integrity security model focuses on integrity.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 171

QUESTION 579
Which backup method does not reset the archive bit on files that are backed up?

A. Full backup method
B. Incremental backup method
C. Differential backup method
D. Additive backup method

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The Differential backup method backs up the files that have been modified since the last full backup. The differential process does not change the archive bit value.

Incorrect Answers:
A: During a full backup all data are backed up and saved to some type of storage media, and the archive bit is cleared.
B: The Incremental backup method backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0.
D: There is no backup method named the Additive backup method.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 936

QUESTION 580
Which of the following defines when RAID separates the data into multiple units and stores it on multiple disks?

A. striping
B. scanning
C. screening
D. shadowing

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When data are written across all drives, the technique of striping is used. This activity divides and writes the data over several drives.

Incorrect Answers:
B: Scanning is not a concept used in relation to RAID.
C: Screening is not a concept used in relation to RAID.
D: Shadowing is not a concept used in relation to RAID.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1268

QUESTION 581
What is the process that RAID Level 0 uses as it creates one large disk by using several disks?

A. striping
B. mirroring
C. integrating
D. clustering

Correct Answer: A
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
With RAID Level 0 data is striped over several drives creating one single logical disk.

Incorrect Answers:
B: Mirroring is RAID Level 1 and uses only two disks.
C: There is not RAID Level named integrating.
D: There is not RAID Level named clustering.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 582
RAID Level 1 mirrors the data from one disk or set of disks using which of the following techniques?

A. Duplicating the data onto another disk or set of disks.
B. Moving the data onto another disk or set of disks.
C. Establishing dual connectivity to another disk or set of disks.
D. Establishing dual addressing to another disk or set of disks.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
With RAID Level 1 data are written to two drives at once. If one drive fails, the other drive has the exact same data available.

Incorrect Answers:
B: RAID Level 1 does not move data, it make two copies of it and stores it on two separate disks.
C: Dual connectivity is not used by any RAID level.
D: Dual addressing is not used by any RAID level.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 583
Which of the following stripes the data and the parity information at the block level across all the drives in the set?

A. RAID Level 5
B. RAID Level 0 C. RAID Level 2
D. RAID Level 1

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
With RAID level 5 data are written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure.

Incorrect Answers:
B: RAID Level 0 does not use a parity bit. It just stripes data over several drives.
C: RAID Level 2 does not use block level parity. It uses hamming code parity.
D: RAID Level 1 does not use a parity bit. It uses mirroring of drives.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 584
A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:

A. server cluster.
B. client cluster.
C. guest cluster.
D. host cluster.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system. Clustering provides for availability and scalability. It groups physically different systems and combines them logically, which provides immunity to faults and improves performance.

Incorrect Answers:
B: A cluster contains servers, not clients.
C: A guest cluster is referring to something more specific compared to a server cluster. For example, for Windows Server 2012, a failover cluster that is made up of two or more virtual machines is typically referred to as a guest cluster.
D: A host cluster is a more specific notion compared to server cluster, specifically, it is a type of web hosting.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1272

QUESTION 585
If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a:

A. server farm
B. client farm
C. cluster farm
D. host farm

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Clusters may also be referred to as server farms. If one of the systems within the cluster fails, processing continues because the rest pick up the load, although degradation in performance could occur.

Incorrect Answers:
B: A cluster contains servers, not clients.
C: A cluster and a cluster farm is not the same thing. A cluster is server farm.
D: A cluster and a host farm is not the same thing. A cluster is server farm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1272

QUESTION 586
Which of the following backup methods is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets?
A. full backup method.
B. incremental backup method.
C. differential backup method.

D. tape backup method.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In a full backup all data are backed up and saved to some type of storage media. From this baseline differential and incremental backups can later be made.

Incorrect Answers:
B: An incremental process backs up all the files that have changed since the last full or incremental backup.
C: A differential backup backs up the files that have been modified since the last full backup. When the data need to be restored, the full backup is laid down first, and then the most recent differential backup is put down on top of it.
D: A tape backup is any type of backup which backs up data to the tape medium. It can be a full backup, an incremental backup, or a differential backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 936

QUESTION 587
Which backup method is used if backup time is critical and tape space is at an extreme premium?

A. Incremental backup method.
B. Differential backup method.
C. Full backup method.
D. Tape backup method.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
An incremental process backs up only the files that have changed since the last full or incremental backup. Compared to a differential or a full back, an incremental backup copies less files.
Incorrect Answers:
B: A differential backup backs up the files that have been modified since the last full backup. More files are copies compared to an incremental backup.
C: In a full backup all data are backed up and saved to some type of storage media.
D: A tape backup is any type of backup which backs up data to the tape medium. It can be a full backup, an incremental backup, or a differential backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 936

QUESTION 588
Hierarchical Storage Management (HSM) is commonly employed in:

A. very large data retrieval systems.
B. very small data retrieval systems.
C. shorter data retrieval systems.
D. most data retrieval systems.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
HSM (Hierarchical Storage Management) provides continuous online backup functionality. It combines hard disk technology with the cheaper and slower optical or tape jukeboxes. HSM is typically used in very large data retrieval systems.

Incorrect Answers:
B: HSM is typically not used in small data retrieval systems.
C: HSM is not used in small data retrieval systems.
D: Due to the added complexity of HSM, it is used only in very large data retrieval systems.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1274

QUESTION 589
Which of the following best describes what would be expected at a "hot site"?

A. Computers, climate control, cables and peripherals
B. Computers and peripherals
C. Computers and dedicated climate control systems.
D. Dedicated climate control systems
Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A hot site is a facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The hot site would include computers, cables and peripherals. A climate control system might be required as well as most electronic equipment must operate in a climate-controlled atmosphere.

Incorrect Answers:
B: Computer cables would be required as well.
C: Peripherals and cables would be required as well.
D: A hot site would require computers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 920

QUESTION 590
Which of the following computer recovery sites is only partially equipped with processing equipment?

A. hot site.
B. rolling hot site.
C. warm site.
D. cold site.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A warm site is a leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers.

Incorrect Answers:
A: A hot site is a facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data.
B: A rolling hot site is a mobile facility, typically the back of an 18-wheel truck. It has all of the capabilities of a hot site and is very versatile, but expensive. Hot sites are fully equipped.
D: A cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 591
Which of the following computer recovery sites is the least expensive and the most difficult to test?

A. non-mobile hot site.
B. mobile hot site.
C. warm site.
D. cold site.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A cold site is less expensive compared to a warm site or a hot site. A cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. A cold site is essentially an empty data center.

Incorrect Answers:
A: A hot site is fully equipped and is therefore more expensive than a cold site.
B: A mobile (rolling) hot site is a mobile facility, typically the back of an 18-wheel truck. It has all of the capabilities of a hot site and is very versatile, but expensive.
C: A warm site is more expensive than a cold site, since it is a leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 592
Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?

A. It is unlikely to be affected by the same disaster.
B. It is close enough to become operational quickly.
C. It is close enough to serve its users.
D. It is convenient to airports and hotels.
Correct Answer: A

Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When choosing a backup facility, it should be far enough away from the original site so that one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about, for example, tornado damage, because the backup site could also be affected or destroyed.

Incorrect Answers:
B: The alternate site should be too close so that one disaster does not take out both locations.
C: The alternate site should be too close so that one disaster does not take out both locations.
D: That the alternate city is convenient to airports and hotels is A major factor when considering an alternate site.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 924

QUESTION 593
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?

A. hot site.
B. warm site.
C. cold site.
D. reciprocal agreement.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Reciprocal agreements are Enforceable. This means that although company A said company B could use its facility when needed, when the need arises, company A legally does not have to fulfill this promise.

Incorrect Answers:
A: A hot site contract is enforceable, while a reciprocal agreement could be hard to enforce.
B: A warm site contract is enforceable, while a reciprocal agreement could be hard to enforce.
C: A cold site contract is enforceable, while a reciprocal agreement could be hard to enforce.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 924

QUESTION 594
A Differential backup process will:

A. Backs up data labeled with archive bit 1 and leaves the data labeled as archive bit 1
B. Backs up data labeled with archive bit 1 and changes the data label to archive bit 0
C. Backs up data labeled with archive bit 0 and leaves the data labeled as archive bit 0
D. Backs up data labeled with archive bit 0 and changes the data label to archive bit 1

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When a file is modified or created, the file system sets the archive bit to 1. A differential backup process backs up the files that have been modified since the last full backup, but does not change the archive bit value.

Incorrect Answers:
B: A differential backup process does not change the archive bit value.
C: Because a differential backup process backs up the files that have been modified since the last full backup, the archive bit at the start of the process would be set to 1.
D: Because a differential backup process backs up the files that have been modified since the last full backup, the archive bit at the start of the process would be set to 1.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 935-936

QUESTION 595
Who should direct short-term recovery actions immediately following a disaster?

A. Chief Information Officer.
B. Chief Operating Officer.
C. Disaster Recovery Manager.
D. Chief Executive Officer.

Correct Answer: C

Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
The disaster recovery manager should direct short-term recovery actions immediately following a disaster.

Incorrect Answers:
A: The Chief Information Officer (CIO) does not handle disaster recovery.
As a CIO must make executive decisions regarding things such as the purchase of IT equipment from suppliers or the creation of new systems, they are therefore responsible to lead and direct the workforce of their specific organization. In addition, the CIO is 'required to have strong organizational skills'. This is particularly relevant for a Chief Information Officer of an organization, who must balance roles in order to gain a competitive advantage and keep the best interests of the organization's employees. CIOs also have the responsibility of recruiting, so it is important that they take on the best employees to complete the jobs the company needs fulfilling.
B: The Chief Operating Officer does Direct recovery actions following a disaster. The Chief Operating Officer is responsible for the daily operation of the company, and routinely reports to the highest ranking executive.
D: The Chief Executive Officer (CEO) does not handle disaster recovery. The CEO has responsibilities as a director, decision maker, leader, manager and executor.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 657

QUESTION 596
Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?

A. Composition
B. Priorities
C. Dependencies
D. Service levels

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Data points obtained as part of the BIA information gathering process will be used later during analysis. It is important that the team members ask about how different tasks—whether processes, transactions, or services, along with any relevant dependencies—get accomplished within the organization.

Incorrect Answers:
A: To determine the dependencies, not the composition, between the business processes is an import step of the BIA process.
B: To determine the dependencies, not the priorities, between the business processes is an import step of the BIA process.
D: To determine the service levels, not the priorities, between the business processes is an import step of the BIA process.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 905

QUESTION 597
Which of the following recovery plan test results would be most useful to management?

A. elapsed time to perform various activities.
B. list of successful and unsuccessful activities.
C. amount of work completed.
D. description of each activity.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
The team of testers must agree upon what activities are getting tested and how to properly determine success or failure.

Incorrect Answers:
A: The key when testing the recovery plan is to know fail or success of the activities, not the elapsed time of them.
C: The recovery plan test refers to activities not to work completed.
D: The key when testing the recovery plan is to know fail or success of the activities, not the description time of time.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 954

QUESTION 598
Which of the following answers BEST indicates the most important part of a data backup plan?

A. Testing the backups with restore operations
B. An effective backup plan
C. A reliable network infrastructure
D. Expensive backup hardware

Correct Answer: A
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
If you can't restore lost files from your backup system then your backup plan is useless. You could have the best backup system and plan available but if you are unable to restore files then the system cannot assure data availability.

Develop an effective disaster recovery plan and include in that plan a good backup strategy that meets the needs of your organization. Be sure to include periodic recovery practice operations to prove the effectiveness of the system.

Incorrect Answers:
B: This question is asking for the BEST answer for the most important part of a data backup plan. An effective backup plan is what you want; however the MOST IMPORTANT part of the backup plan is the ability to restore the data.
C: A reliable network infrastructure makes it easier to backup and restore your data. However, network reliability is not the MOST IMPORTANT part of a backup plan. The ability to restore the data is more important.
D: Expensive backup hardware is not the BEST answer. If your expensive backup hardware cannot restore your data, it is no good to you.

QUESTION 599
Fault tolerance countermeasures are designed to combat threats to which of the following?

A. an uninterruptible power supply.
B. backup and retention capability.
C. design reliability.
D. data integrity.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
One of the ways to provide uninterrupted access to information assets is through redundancy and fault tolerance. Redundancy refers to providing multiple instances of either a physical or logical component such that a second component is available if the first fails. Fault tolerance is a broader concept that includes redundancy but refers to any process that allows a system to continue making information assets available in the case of a failure.
Fault tolerance countermeasures are designed to combat threats to design reliability. Although fault tolerance can include redundancy, it also refers to systems such as RAID where if a disk fails, the data can be made available from the remaining disks.

Incorrect Answers:

A: Fault tolerance countermeasures ensure that data assets remain available in the event of a failure of any component, not just an uninterruptible power supply.
B: Fault tolerance countermeasures ensure that data assets remain available in the event of a failure of any component, not just the backup and retention capability.
D: Fault tolerance countermeasures do not protect data integrity.

QUESTION 600

An incremental backup process

A. Backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0.
B. Backs up the files that been modified since the last full backup. It does not change the archive bit value.
C. Backs up all the data and changes the archive bit to 0.
D. Backs up all the data and changes the archive bit to 1.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The incremental backup method backs up all the files that have changed since the last full or incremental backup and resets the archive bit to 0. This is known as "clearing the archive bit". A full backup backs up all files regardless of whether the archive bit is 1 or 0 and sets the archive bit to 0.
The archive bit is used by the backup process to determine whether a file has been changed. When you modify a file or create a new file, the archive bit is set to 1. This tells the backups process that the file has changed (or is a new file) and needs to be backed up. When an incremental backup backs up the file, it sets the archive bit to 0. When the next incremental backup runs and sees that the archive bit is 0, the incremental backup knows that the file has not changed since the last backup and so will not back up the file again.

Incorrect Answers:
B: This answer describes the differential backup process. The differential backup does not change the archive bit value; an incremental backup does change the archive bit value to 0.
C: This answer describes the full backup process. An incremental backup does not back up ALL files; it only backs up changed files.
D: An incremental backup does not back up ALL files; it only backs up changed files. Furthermore, it changes the archive bit value to 0, not 1.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 801-802

QUESTION 601

A Differential backup process:

A. Backs up data labeled with archive bit 1 and leaves the data labeled as archive bit 1
B. Backs up data labeled with archive bit 1 and changes the data label to archive bit 0

C. Backs up data labeled with archive bit 0 and leaves the data labeled as archive bit 0
D. Backs up data labeled with archive bit 0 and changes the data label to archive bit 1

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Archive bit 1 = On (the archive bit is set).
Archive bit 0 = Off (the archive bit is NOT set).

A full backup backs up all files regardless of whether the archive bit is 1 or 0 and sets the archive bit to 0.
When the archive bit is set to ON, it indicates a file that has changed and needs to be backed up. Differential backups back up all files that have changed since the last full backup - all files that have their archive bit value set to 1. Differential backups do not change the archive bit value when they backup a file; they leave the archive bit value set to 1.
Incorrect Answers:
B: Backs up data labeled with archive bit 1 and changes the data label to archive bit 0. - This is the behavior of an incremental backup, not a differential backup.
C: Backs up data labeled with archive bit 0 and leaves the data labeled as archive bit 0. - If the archive bit is set to 0 (Off), it will only be backed up with a Full backup. Differential and incremental backups will not back up the file.
D: Backs up data labeled with archive bit 0 and changes the data label to archive bit 1. - If the archive bit is set to 0 (Off), it will only be backed up with a Full backup. Differential and incremental backups will not back up the file.

References:
https://en.wikipedia.org/wiki/Archive_bit

QUESTION 602
Prior to a live disaster test also called a Full Interruption test, which of the following is most important?

A. Restore all files in preparation for the test.
B. Document expected findings.
C. Arrange physical security for the test site.
D. Conduct of a successful Parallel Test

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
A Full Interruption Test is the most intrusive to regular operations and business productivity. The original site is actually shut down, and processing takes place at the alternate site. A parallel test is one in which some systems are actually run at the alternate site.

Incorrect Answers:
A: Restoration of files is not the most important when conducting a Full Interruption. The most important is to set up a secondary site and conduct a parallel test on that site.
B: To document expected findings is not the most important when conducting a Full Interruption. The most important is to set up a secondary site and conduct a parallel test on that site.
C: To arrange physical security for the test site is not the most important when conducting a Full Interruption. The most important is to conduct a parallel test on the test site.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 956

QUESTION 603
Organizations should not view disaster recovery as which of the following?

A. Committed expense.
B. Discretionary expense.
C. Enforcement of legal statutes.
D. Compliance with regulations.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A discretionary expense is a cost which is Essential for the operation of a business. The disaster recovery is concerned with business functions and costs that are essential for the business, and does Address discretionary expense.

Incorrect Answers:
A: A committed expense is an unavoidable expensive. Disaster recovery must take unavoidable expenses into account.
C: The disaster recovery procedures must be in compliance with the law. D:
The disaster recovery procedures must be in compliance with regulations

References:
http://www.investopedia.com/terms/d/discretionary-expense.asp

QUESTION 604
Which of the following is BEST defined as a physical control?

A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Physical controls are controls that pertain to controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility, monitoring for intrusion, and checking environmental controls.
Fencing (protecting the perimeter of the facility) is an example of a physical control.

Incorrect Answers:
A: Monitoring of system activity is an example of a technical control.
C: Identification and authentication methods are an example of a technical control.
D: Logical access control mechanisms are an example of a technical control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 28

QUESTION 605
Which of the following is a NOT a guideline necessary to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations?

A. Restrict access to main air intake points to persons who have a work-related reason to be there
B. Maintain access rosters of maintenance personnel who are not authorized to work on the system
C. Escort all contractors with access to the system while on site
D. Ensure that all air intake points are adequately secured with locking devices

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
Over the past several years, there has been an increasing awareness dealing with anthrax and airborne attacks. Harmful agents introduced into the HVAC system can rapidly spread throughout the structure and infect all persons exposed to the circulated air.
The following is a list of guidelines necessary to enhance security in this critical aspect of facility operations:
- Restrict access to main air intake points to persons who have a work-related reason to be there.
- Escort all contractors with access to the system while on site.
- Ensure that all air intake points are adequately secured with locking devices.

Maintaining access rosters of maintenance personnel who are not authorized to work on the system is a recommended guideline; however, it is not a 'necessary' guideline to ensure safety.

Incorrect Answers:
A: Restricting access to main air intake points to persons who have a work-related reason to be there is a necessary guideline to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations. Therefore, this answer is incorrect.
C: Escorting all contractors with access to the system while on site is a necessary guideline to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations. Therefore, this answer is incorrect.
D: Ensuring that all air intake points are adequately secured with locking devices is a necessary guideline to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations. Therefore, this answer is incorrect.

QUESTION 606
Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

A. Accountability of biometrics systems
B. Acceptability of biometrics systems
C. Availability of biometrics systems
D. Adaptability of biometrics systems

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye.
Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

Incorrect Answers:

A: Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are not elements of accountability of biometrics systems.
C: Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are not elements of availability of biometrics systems.
D: Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are not elements of adaptability of biometrics systems.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 60

QUESTION 607
The Orange Book requires auditing mechanisms for any systems evaluated at which of the following levels?

A. C1 and above.

B. C2 and above.
C. B1 and above.
D. B2 and above.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The Orange Book provides a classification system that is divided into hierarchical divisions of assurance levels:
A. Verified protection
B. Mandatory protection
C. Discretionary protection
D. Minimal security

Classification A represents the highest level of assurance, and D represents the lowest level of assurance. Each division can have one or more numbered classes with a corresponding set of requirements that must be met for a system to achieve that particular rating. The classes with higher numbers offer a greater degree of trust and assurance. So B2 would offer more assurance than B1, and C2 would offer more assurance than C1. Each division and class incorporates the requirements of the ones below it. This means that C2 must meet its criteria requirements and all of C1's requirements, and B3 has its requirements to fulfill along with those of C1, C2, B1, and B2.
C2: Controlled Access Protection Users need to be identified individually to provide more precise access control and auditing functionality. Logical access control mechanisms are used to enforce authentication and the uniqueness of each individual's identification. Security-relevant events are audited, and these records must be protected from unauthorized modification.

Incorrect Answers:

A: Auditing mechanisms are not required for systems at C1 level.
C: Auditing mechanisms are at C2 level which is lower than B1.
D: Auditing mechanisms are at C2 level which is lower than B2.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-395

QUESTION 608
The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:

A. Security Testing.
B. Design Verification.
C. System Integrity.
D. System Architecture Specification.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Orange Book Pages 15 states:
2.1.3.1.2 System Integrity:
Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Incorrect Answers:
A: The requirement for security testing: The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. This is not what is described in the question.
B: There are five requirements defined for design verification. The statement in the question is not one of those five requirements.
D: The statement in the question is not one of the requirements for System Architecture Specification.

References:
http://csrc.nist.gov/publications/history/dod85.pdf, pp. 15, 101

QUESTION 609
Covert Channel Analysis is FIRST introduced at what level of the TCSEC rating?

A. C2 and above.
B. B1 and above.C. B2 and above.
D. B3 and above.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In the Orange Book, covert channels in operating systems are not addressed until security level B2 and above because these are the systems that would be holding data sensitive enough for others to go through all the necessary trouble to access data in this fashion.

B2: Structured Protection: The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers. Subjects and devices require labels, and the system **must not allow covert channels**. A trusted path for logon and authentication processes must be in place, which means the subject communicates directly with the application or operating system, and no trapdoors exist. There is no way to circumvent or compromise this communication channel. Operator and administration functions are separated within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolate processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system. The type of environment that would require B2 systems is one that processes sensitive data that require a higher degree of security. This type of environment would require systems that are relatively resistant to penetration and compromise.

Incorrect Answers:
A: Covert Channel Analysis is not used at layer C2.
B: Covert Channel Analysis is not used at layer B1.
D: B3 is not the lowest level that uses Covert Channel Analysis. Level B2 uses Covert Channel Analysis.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 380, 396

QUESTION 610
Which of the following is most concerned with personnel security?

A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls

Correct Answer: B

Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
On the CISSP exam you can see control categories broken down into administrative, technical, and physical categories and the categories outlined by NIST, which are management, technical, and operational. You need to be familiar with both ways of categorizing control types.

According to the NIST control categories, Personnel Security is an Operational control.

Incorrect Answers:
A: Personnel security is not a management control.
C: Personnel security is not a technical control.
D: Human resources controls are not a defined control category although there are human resource controls listed in the administrative control category.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 58

QUESTION 611
Which of the following backup sites is the most effective for disaster recovery?

A. Time brokers
B. Hot sites
C. Cold sites
D. Reciprocal Agreement

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Hot sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible. The only missing resources from a hot site are usually the data. A hot site is a facility that is leased or rented and is fully configured and ready to operate within a few hours.

Incorrect Answers:
A: A time brokers backup solution would be less effective compared to hot or cold sites.
C: A cold site is less effective than a hot site since the cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. A cold site is essentially an empty data center.

D: Reciprocal agreements are less effective compared to hot or cold sites, since reciprocal agreements are Enforceable. This means that although company A said company B could use its facility when needed, when the need arises, company A legally does not have to fulfill this promise.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 612
Which of the following is a transaction redundancy implementation?

A. On-site mirroring
B. Electronic Vaulting
C. Remote Journaling
D. Database Shadowing

Correct Answer: A
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
On-site mirroring is a transaction redundancy solution.

Incorrect Answers:
B: Electronic vaulting is one type of transaction redundancy solution. Electronic vaulting makes copies of files as they are modified and periodically transmits them to an offsite backup site.
C: Remote journaling is one type of transaction redundancy solution. Remote journaling is a method of transmitting data offsite. It usually only includes moving the journal or transaction logs to the offsite facility, not the actual files. These logs contain the deltas (changes) that have taken place to the individual files. If and when data are corrupted and need to be restored, the bank can retrieve these logs, which are used to rebuild the lost data.
D: Database Shadowing is one type of transaction redundancy solution. It is a mirroring technology used in databases, in which information is written to at least two hard drives for the purpose of redundancy.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 938-939

QUESTION 613
A site that is owned by the company and mirrors the original production site is referred to as a _____?

A. Hot site.
B. Warm Site.
C. Reciprocal site.

D. Redundant Site.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A redundant site is owned by the company and is a mirror of the original production environment.

Incorrect Answers:
A: A hot site is not owned by the company. A hot site is leased or rented.
B: A warm site is a leased or rented facility. It is not owned by the company.
C: A reciprocal site is owned by another company, and is set up through a reciprocal agreement. A reciprocal agreement is one in which a company promises another company it can move in and share space if it experiences a disaster, and vice versa.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 925

QUESTION 614
Which of the following is the most critical item from a disaster recovery point of view?

A. Data
B. Hardware/Software
C. Communication LinksD. Software Applications

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Data loss has the most negative impact on business functions. Data loss often lead to business failure.

Incorrect Answers:
B: Software can be reinstalled and hardware can replaced, and are therefore less critical compared to loss of data.
C: Communication links can quite easily put back again, compared to loss of data.
D: Loss of applications is Critical as they can be reinstalled.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 957

QUESTION 615
Which of the following is defined as the most recent point in time to which data must be synchronized without adversely affecting the organization (financial or operational impacts)?

A. Recovery Point Objective
B. Recovery Time Objective
C. Point of Time Objective
D. Critical Time Objective

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A Recovery Point Objective (RPO) is the maximum period of time in which data might be lost if a disaster strikes. It is the most recent point in time to which data must be synchronized to avoid major negative impact on the organization.

Incorrect Answers:
B: The Recovery Time Objective is the amount of time in which you think you can feasibly recover the function in the event of a disruption.
C: There is no Point of Time Objective within the CISSP framework.
D: There is no Critical Time Objective within the CISSP framework.

QUESTION 616
Which of the following items is NOT a benefit of cold sites?

A. No resource contention with other organization
B. Quick Recovery

C. A secondary location is available to reconstruct the environment
D. Low Cost

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. A cold site cannot provide a quick recovery. A warm site is needed for a quick recovery.

Incorrect Answers:
A: A cold site is a separate site and would Be a resource contention with another company.
C: A cold site is located at another location where the original site can be reconstructed.
D: Compared to a hot site, or a warm site, a cold site has a lower cost.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 617
When you update records in multiple locations or you make a copy of the whole database at a remote location as a way to achieve the proper level of faulttolerance and redundancy, it is known as?

A. Shadowing
B. Data mirroring
C. Backup
D. Archiving

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Database Shadowing is one type of transaction redundancy solution whereby a full copy of the user's database is maintained at an alternate information processing facility.

Incorrect Answers:

B: Data mirroring does not necessarily use a remote location. Data mirroring mirrors data to another server, or to another hard drive on the same server, on the local network.
C: A backup solution would not handle database records. It handles data at the file level.
D: An archiving solution would not handle database records. It handles data at the file level.

References:
http://www.bcmpedia.org/wiki/Database_Shadowing

QUESTION 618
Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?

A. External Hot site
B. Warm Site
C. Internal Hot Site
D. Dual Data Center

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
An internal hot site is standby ready with all the technology and equipment necessary to run the applications to be recovered there.

Incorrect Answers:
A: An external hot site has equipment on the floor waiting for recovery, but the environment must be rebuilt for the recovery. An external hot site is not standby ready.
B: A warm site is not standby ready. A warm site is a leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers.
D: A dual data center is employed for application that canAccept any downtime without unacceptably impacting the business. A dual data center would be more than standby ready, but it would be more expensive.

QUESTION 619
What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?

A. The most critical operations are moved from alternate site to primary site before others

B. Operation may be carried by a completely different team than disaster recovery team
C. The least critical functions should be moved back first
D. You move items back in the same order as the categories document in your plan or exactly in the same order as you did on your way to the alternate site

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The salvage team must ensure the reliability of primary site. This is done by returning the least-mission-critical processes to the restored original site to stress – test the rebuilt network. As the restored site shows resiliency, more important processes are transferred.

Incorrect Answers:
A: The most critical operations should be to the primary site after, Before, the other less critical operations have been moved.
B: As many operations that the salvage team handles are the same as the operations carried out by the disaster recovery team, there can be very well be an overlap between the team members. A person can be a member of both teams.
D: The order in which the operations are restored should Be exactly the same order in which the operations where moved to the alternative site. You should transfer the least critical operations first.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 669

QUESTION 620
Which of the following is a large hardware/software backup system that uses the RAID technology?

A. Tape Array.
B. Scale Array.
C. Crimson Array
D. Table Array.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

Cheyenne Software (now owned by Computer Associates) was the first to offer RAID 5 for tape devices. Because by nature tape devices employ a sequential access method, RAID 5 is an ideal solution for a tape array.

Incorrect Answers:
B: A scale array is A RAID backup system.
C: A crimson array is A RAID backup system.
D: A table array is A RAID backup system.

QUESTION 621
What is the MOST critical piece to disaster recovery and continuity planning?

A. Security policy
B. Management support
C. Availability of backup information processing facilities
D. Staff training

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The most critical part of establishing and maintaining a current continuity plan is management support. Management must be convinced of the necessity of such a plan. Therefore, a business case must be made to obtain this support.

Incorrect Answers:
A: Compared to get management support for the plan, security policy is less important.
C: Compared to get management support for the plan, availability of backup facilities is less important.
D: Compared to get management support for the plan, staff training is less important.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 897

QUESTION 622
During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?

A. Measurement of accuracy
B. Elapsed time for completion of critical tasks

C. Quantitatively measuring the results of the test
D. Evaluation of the observed test results

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Once you develop a list of threats, you must individually evaluate each threat and its related risk. There are two risk assessment methodologies: quantitative and qualitative. Quantitative risk analysis assigns real dollar figures to the loss of an asset.

Incorrect Answers:
A: Accuracy is not measured. It is the list of threats that are quantitative measured.
B: Elapsed time for completion of critical tasks is Critical. It is critical to evaluate the risks.
D: the observed test results are Evaluated. The business function either passes or fails the test.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 243

QUESTION 623
Which of the following statements regarding an off-site information processing facility is TRUE?

A. It should have the same amount of physical access restrictions as the primary processing site.
B. It should be located in proximity to the originating site so that it can quickly be made operational.
C. It should be easily identified from the outside so in the event of an emergency it can be easily found.
D. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The physical access restrictions at the off-site facility does Be at same level as at the original site.

Incorrect Answers:

B: An off-site location which is close would be ill-advised as the same disaster can strike both the main site and the alternate site. C: The off-site facility must be readily accessed and should be easily identified from the outside. D: The same operational environment should be possible at the alternate location.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 444

QUESTION 624
Business Continuity and Disaster Recovery Planning (Primarily) addresses the:

A. Availability of the CIA triad
B. Confidentiality of the CIA triad
C. Integrity of the CIA triad
D. Availability, Confidentiality and Integrity of the CIA triad

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Availability is one of the main themes behind business continuity planning, in that it ensures that the resources required to keep the business going will continue to be available to the people and systems that rely upon them.
Note: The CIA Triad, primary goals and objectives of security, is the three essential security principles of confidentiality, integrity, and availability. Vulnerabilities and risks are also evaluated based on the threat they pose against one or more of the CIA Triad principles.

Incorrect Answers:
B: Business Continuity and Disaster Recovery Planning primarily addresses availability, Confidentiality.
C: Business Continuity and Disaster Recovery Planning primarily addresses availability, not integrity.
D: Business Continuity and Disaster Recovery Planning primarily addresses availability, , Confidentiality or integrity.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 888

QUESTION 625
Which of the following best defines a Computer Security Incident Response Team (CSIRT)?

A. An organization that provides a secure channel for receiving reports about suspected security incidents.
B. An organization that ensures that security incidents are reported to the authorities.
C. An organization that coordinates and supports the response to security incidents.

D. An organization that disseminates incident-related information to its constituency and other involved parties.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Many organizations now have a dedicated team responsible for investigating any computer security incidents that take place. These teams are commonly known as computer incident response teams (CIRTs) or computer security incident response teams (CSIRTs).
Note: When an incident occurs, the response team has four primary responsibilities:
- Determine the amount and scope of damage caused by the incident.
- Determine whether any confidential information was compromised during the incident.
- Implement any necessary recovery procedures to restore security and recover from incident - related damages.
- Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

Incorrect Answers:
A: The CSIRT is not set up to receive reports on security incidents. The CSIRT handles the security incidents when they occur.
B: The CSIRT is not set up to alert authorities of security incidents. The CSIRT handles the security incidents when they occur.
D: The CSIRT is not set up to inform on security incidents. The CSIRT handles the security incidents when they occur.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 726

QUESTION 626
If an employee's computer has been used by a fraudulent employee to commit a crime, the hard disk may be seized as evidence and once the investigation is complete it would follow the normal steps of the Evidence Life Cycle. In such case, the Evidence life cycle would not include which of the following steps listed below?

A. Acquisition collection and identification
B. Analysis
C. Storage, preservation, and transportation
D. Destruction

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The evidence lifecycle does not include destruction. The evidence need to be preserved.

Incorrect Answers:
A: The evidence lifecycle include collection and identification of evidence.
B: Analysis of evidence is included in the evidence lifecycle.
C: The evidence lifecycle include storage, preservation, and transportation of evidence.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1054

QUESTION 627
If an organization were to monitor their employees' e-mail, it should not:

A. Monitor only a limited number of employees.
B. Inform all employees that e-mail is being monitored.
C. Explain who can read the e-mail and how long it is backed up.
D. Explain what is considered an acceptable use of the e-mail system.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
All the employees should be monitored, not only a few.

Incorrect Answers:
B: If a company feels it may be necessary to monitor e-mail messages and usage, this must be explained to the employees.
C: The company should outline who can and cannot read employee messages, describe the circumstances under which e-mail monitoring may be acceptable, and specify where the e-mail can be accessed.
D: The company should state which e-mail activity is acceptable.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1020

QUESTION 628

A server farm consisting of multiple similar servers seen as a single IP address from users interacting with the group of servers is an example of which of the following?

A. Server clustering
B. Redundant servers
C. Multiple servers
D. Server fault tolerance

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system through a single IP address.

Incorrect Answers:
B: Redundant servers are not grouped together and can be managed through a single IP address.
C: In general, a group of multiple servers can be grouped together and managed through a single IP address.
D: Server fault tolerance is not related to managing a group of servers through a single IP address.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1272

QUESTION 629
Which of the following is NOT a common backup method?

A. Full backup method
B. Daily backup method
C. Incremental backup method
D. Differential backup method

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

You can have daily backup schedule, but there is no specific backup method called daily backup.

Incorrect Answers:
A: The full backup method copies all the data from the system to the backup medium.
C: The incremental backup method copies only the files that have been modified since the previous backup.
D: The differential backup method is a type of data backup that preserves data, saving only the difference in the data since the last full backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1410

QUESTION 630
Which common backup method is the fastest on a daily basis?

A. Full backup method
B. Incremental backup method
C. Fast backup method
D. Differential backup method

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
An incremental backup is fast because it copies only the files that have been modified since the previous backup.

Incorrect Answers:
A: A full backup is not fast as it copies all the data from the system to the backup medium.
C: There is no backup method called the fast backup method.
D: A differential backup is slower than an incremental backup since it copies more data. A differential backup copies only the difference in the data since the last full backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1410

QUESTION 631
Which of the following backup methods is most appropriate for off-site archiving?
A. Incremental backup method
B. Off-site backup method

C. Full backup method
D. Differential backup method

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
All data should be archived. A full backup copies all the data from the system to the backup medium. After the full backup has finished, the backup media is physically transported to another off-site location.

Incorrect Answers:
A: Archiving should copy all the data, but an incremental backup copies only the files that have been modified since the previous backup.
B: There is no special off-site backup method. Instead use a standard full backup and transport the backup media to the other site.
D: Archiving should copy all the data, but a differential backup copies only the difference in the data since the last full backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1410

QUESTION 632
Which of the following specifically addresses cyber-attacks against an organization's IT systems?

A. Continuity of support plan
B. Business continuity plan
C. Incident response plan
D. Continuity of operations plan

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A Cyber incident response plan focuses on malware, hackers, intrusions, attacks, and other security issues. It outlines procedures for incident response. There are no other types of Incident response plans.
Incorrect Answers:
A: There is no continuity of support plan which addresses cyber-attacks. The Incident response plan addresses cyber-attacks.

B: A business continuity plan (BCP) does address cyber-attacks. A BCP contains strategy documents that provide detailed procedures that ensure critical business functions are maintained.
D: There is no continuity of operations plan which addresses cyber-attacks. The Incident response plan addresses cyber-attacks.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 953

QUESTION 633
During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?

A. Damage mitigation
B. Install LAN communications network and servers
C. Assess damage to LAN and servers
D. Recover equipment

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The damage assessment team should be responsible determining the disaster's cause and the amount of damage that has occurred to organizational assets. The assessment of the damage should include the status of the equipment at the site such as servers and network devices.

Incorrect Answers:
A: Damage mitigation is a preventive method which is applied prior to a disaster, while salvage are done after a disaster.
B: Before installing new equipment the damage must be assessed and the equipment must be salvaged.
D: Before the salvage team starts to recover the equipment, the damage assessment team should assess the damage on the site.

QUESTION 634
Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?

A. Simulation test
B. Checklist test
C. Parallel test
D. Structured walk-through test

Correct Answer: D

Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In a Structured walk-through test representatives from each department or functional area come together and go over the plan to ensure its accuracy. The group reviews the objectives of the plan; discusses the scope and assumptions of the plan; reviews the organization and reporting structure; and evaluates the testing, maintenance, and training requirements described.

Incorrect Answers:
A: In a Simulation test the plan is not reviewed in detail. In a Simulation test all employees who participate in operational and support functions, or their representatives, come together to practice executing the disaster recovery plan based on a specific scenario.
B: A Checklist test, like a Structured walk-through test, has the aim to review the plan, but in a Checklist test the functional representatives do not meet. Instead copies of the BCP are distributed to the different departments and functional areas for review.
C: The purpose of a Parallel test is not to review the plan in detail. A parallel test is done to ensure that the specific systems can actually perform adequately at the alternate offsite facility.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 955

QUESTION 635
When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?

A. Executive management staff
B. Senior business unit management
C. BCP committee
D. Functional business units

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Senior management is ultimately responsible for all phases of the plan, and who should be most concerned about the protection of its assets. They must sign off on all policy issues, and they will be held liable for overall success or failure of a security solution.

Incorrect Answers:

A: If possible the BCP plan should by endorsed by the Executive management staff, but the Executive management staff is not responsible for identifying and prioritizing time-critical systems.
C: The BCP committee does not identify and prioritize systems. The BCP committee oversees, initiates, plans, approves, tests and audits the BCP. It also implements the BCP, coordinates activities, approve the BIA survey. The BCP committee also oversees the creation of continuity plans and reviews the results of quality assurance activities
D: Functional business units are a part of the BCP committee. Functional business units are not responsible for identifying and prioritizing time-critical system.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 55

QUESTION 636
In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?

A. Human Resources
B. Industrial Security
C. Public Relations
D. External Audit Group

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
If the incident response team determines that a crime has been carried out, senior management should be informed immediately. If the suspect is an employee, a human resources representative must be called right away.

Incorrect Answers:
B: Industrial Security does not need to be involved when an employee is suspected of a crime.
C: Public Relations does not need to be involved when an employee is suspected of a crime.
D: The External Audit Group does not need to be involved when an employee is suspected of a crime.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1035

QUESTION 637
To be admissible in court, computer evidence must be which of the following?

A. Relevant
B. Decrypted
C. Edited
D. Incriminating

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
For evidence to be admissible in court, it needs to be relevant, sufficient, and reliable.

Incorrect Answers:
B: The evidence should not be changed. If it is encrypted it should be kept encrypted.
C: Evidence should not be changed or edited.
D: Evidence does not need to be incriminating. It can very well be used in favor of the suspect, such as an alibi.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1068

QUESTION 638
Once evidence is seized, a law enforcement officer should emphasize which of the following?

A. Chain of command
B. Chain of custody
C. Chain of control
D. Chain of communications

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When evidence is seized, it is important to make sure a proper chain of custody is maintained to ensure any data collected can later be properly and accurately represented in case it needs to be used for later events such as criminal proceedings or a successful prosecution.

Incorrect Answers:

A: Chain of command is not related to the collection of evidence. In a military context, the chain of command is the line of authority and responsibility along which orders are passed within a military unit and between different units.
C: Chain of control is not related to collection of evidence. Chain of custody relates to how evidence is collected.
D: Chain of communication is not related to collection of evidence. Chain of custody relates to how evidence is collected.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 248

QUESTION 639
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?

A. System development activity
B. Help-desk function
C. System Imaging
D. Risk management process

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The computer system should not be changed, while the incident handling is ongoing. System development should not occur during incident handling.

Incorrect Answers:
B: As part of the ongoing incident handling employees, vendors, customers, partner, devices or sensors report the event to Help Desk. C: System imaging would not affect the ongoing incident handling and should take place to D: The Risk management process would not affect the ongoing incident handling.

References:
https://en.wikipedia.org/wiki/Computer_security_incident_management

QUESTION 640
In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?

A. Using a write blocker
B. Made a full-disk image
C. Created a message digest for log files

D. Displayed the contents of a folder

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The original media should have two copies created: a primary image (a control copy that is stored in a library) and a working image (used for analysis and evidence collection). These should be timestamped to show when the evidence was collected. Displaying the contents of a folder would affect the original media, and would compromise the evidence collection process.

Incorrect Answers:
A: A write blocker would be a step to secure the integrity of the media.
B: Making a full-disk image would be a part of the investigation process.
C: To create a message digest for log files would be part of the documentation.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1049

QUESTION 641
What is the PRIMARY goal of incident handling?

A. Successfully retrieve all evidence that can be used to prosecute
B. Improve the company's ability to be prepared for threats and disasters
C. Improve the company's disaster recovery planD. Contain and repair any damage caused by an event.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The primary goal of incident handling is to contain, eradicate, and recovery from the incident. See step 3 below.
Note: The Incident Handling lifecycle can be divided into the following four steps:
1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-incident Activity

Incorrect Answers:
A: Retrieving evidence to prosecute is not part of Incident Handling.
B: Preparation is part of incident handling lifecycle, but it is not the most important goal.
C: Improving the disaster recovery plan is not a goal of incident handling.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 331

QUESTION 642
Which of the following would be LESS likely to prevent an employee from reporting an incident?

A. They are afraid of being pulled into something they don't want to be involved with.
B. The process of reporting incidents is centralized.
C. They are afraid of being accused of something they didn't do.
D. They are unaware of the company's security policies and procedures.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A centralized incident reporting would increase, not decrease, the likelihood that an employee would report an incident.

Incorrect Answers:
A: An employee could be afraid to get involved and refrain from reporting an incident.
C: Employees that are afraid of being accused of something they didn't do would be less likely to report an incident.
D: Employees that are unaware of the company's security policies and procedures would be less likely to report an incident.

References:
https://en.wikipedia.org/wiki/Computer_security_incident_management

QUESTION 643
What is the PRIMARY reason to maintain the chain of custody on evidence that has been collected?

A. To ensure that no evidence is lost.
B. To ensure that all possible evidence is gathered.
C. To ensure that it will be admissible in court
D. To ensure that incidents were handled with due care and due diligence.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Real evidence, like any type of evidence, must meet the relevancy, materiality, and competency requirements before being admitted into court. In many cases, it is not possible for a witness to uniquely identify an object in court. In those cases, a chain of evidence (also known as a chain of custody) must be established.

Incorrect Answers:
A: Chain of custody is not used to avoid loss of evidence. It is used to ensure that evidence can be admitted.
B: Chain of custody is not used to ensure that all possible evidence is collected. It is used to ensure that evidence can be admitted.
D: Chain of custody concern evidence, it does not concern incidents.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 704

QUESTION 644
What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?

A. Evidence Circumstance Doctrine
B. Exigent Circumstance Doctrine
C. Evidence of Admissibility Doctrine
D. Exigent Probable Doctrine

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances.

Incorrect Answers:
A: The exception to the search warrant is called exigent Circumstance, not Evidence Circumstance.

C: Admissible evidence is not related to any search warrant.
The general rule in evidence is that all relevant evidence is admissible and all irrelevant evidence is inadmissible.
D: A search without a warrant can only be executed under exigent circumstances, not under exigent probabilities.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1057

QUESTION 645
A copy of evidence or oral description of its contents; which is not as reliable as best evidence is what type of evidence?

A. Direct evidence
B. Circumstantial evidence
C. Hearsay evidence
D. Secondary evidence

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Oral evidence, such as a witness's testimony, and copies of original documents are placed in the secondary evidence category.
Secondary evidence is not viewed as reliable and strong in proving innocence or guilt (or liability in civil cases) when compared to best evidence.

Incorrect Answers:
A: Direct evidence can prove a fact all by itself and does not need backup information to refer to.
B: Circumstantial evidence can prove an intermediate fact that can then be used to deduce or assume the existence of another fact.
C: Hearsay evidence pertains to oral or written evidence presented in court that is secondhand and has no firsthand proof of accuracy or reliability. Hearsay is even less reliable compared to secondary evidence.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1055

QUESTION 646
Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

A. Direct evidence.
B. Circumstantial evidence.
C. Conclusive evidence.
D. Corroborative evidence.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Direct evidence can prove a fact all by itself and does not need backup information to refer to. Direct evidence often is based on information gathered from a witness's five senses.

Incorrect Answers:
B: Circumstantial evidence can prove an intermediate fact, but not a direct fact by itself. The intermediate fact can then be used to deduce or assume the existence of another fact.
C: Conclusive evidence is not collected from the five senses of a witness. Conclusive evidence is irrefutable and cannot be contradicted. Conclusive evidence is very strong all by itself and does not require corroboration.
D: Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand its own, so it cannot disprove a specific act.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1055

QUESTION 647
This type of supporting evidence is used to help prove an idea or a point, however it cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?

A. Circumstantial evidence
B. Corroborative evidence
C. Opinion evidence
D. Secondary evidence

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand its own.

Incorrect Answers:
A: Circumstantial evidence can prove an intermediate fact, but not a direct fact by itself. The intermediate fact can then be used to deduce or assume the existence of another fact. This type of fact is used so the judge or jury will logically assume the existence of a primary fact.
C: Opinion evidence would be the opinion of a witness, but the opinion rule dictates that the witness must testify to only the facts of the issue and not her opinion of the facts.
D: Secondary evidence is not viewed as reliable and strong in proving innocence or guilt (or liability in civil cases) when compared to best evidence. Oral evidence, such as a witness's testimony, and copies of original documents are placed in the secondary evidence category.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1055

QUESTION 648
Which of the following would be MOST important to guarantee that the computer evidence will be admissible in court?

A. It must prove a fact that is immaterial to the case.
B. Its reliability must be proven.
C. The process for producing it must be documented and repeatable.
D. The chain of custody of the evidence must show who collected, secured, controlled, handled, transported the evidence, and that it was not tampered with.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

Incorrect Answers:
A: The immateriality of the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.

B: The reliability of the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.
C: The process of producing the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1050

QUESTION 649
Why would a memory dump be admissible as evidence in court?

A. Because it is used to demonstrate the truth of the contents.
B. Because it is used to identify the state of the system.
C. Because the state of the memory cannot be used as evidence.
D. Because of the exclusionary rule.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A memory dump identifies the state of the system.
Computer-generated evidence that is in the form of routine operational business data or reports and binary disk or memory dumps now constitute exceptions to the rule that computer-generated evidence is hearsay, and is therefore admissible in court.

Incorrect Answers:
A: A memory dump does not identify the truth, it is identification of the state of the system.
C: The state of the memory, the system state, can be admissible as evidence in court.
D: The exclusionary rule refers to evidence that is inadmissible. The exclusionary rule is a legal principle in the United States, under constitutional law, which holds that evidence collected or analyzed in violation of the defendant's constitutional rights is sometimes inadmissible for a criminal prosecution in a court of law.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 504

QUESTION 650
When a possible intrusion into your organization's information system has been detected, which of the following actions should be performed first?

A. Eliminate all means of intruder access.

B. Contain the intrusion.
C. Determine to what extent systems and data are compromised.
D. Communicate with relevant parties.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
If the event is determined to be a real incident, it is identified and classified. Once we understand the severity of the incident taking place, we move on to the next stage, which is investigation. Investigation involves the proper collection of relevant data, which will be used in the analysis and following stages. The goals of these stages are to reduce the impact of the incident, identify the cause of the incident, resume operations as soon as possible, and apply what was learned to prevent the incident from recurring.

Incorrect Answers:
A: Before we can eliminate intruder access we would have to determine the extent of the intrusion.
B: Before containing the intrusion we need to determine the extent of the intrusion.
D: Before we can communicate with the relevant parties we need to determine the extent of the intrusion.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1038

QUESTION 651
When first analyzing an intrusion that has just been detected and confirming that it is a true positive, which of the following actions should be done as a first step if you wish to prosecute the attacker in court?

A. Back up the compromised systems.
B. Identify the attacks used to gain access.
C. Capture and record system information.
D. Isolate the compromised systems.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

For a crime to be successfully prosecuted, solid evidence is required. Computer forensics is the art of retrieving this evidence and preserving it in the proper ways to make it admissible in court. Related system information must be captures and recorded.

Incorrect Answers:
A: To backup up a compromised system is a good idea, but it is not required for prosecution.
B: Identifying the attacks would be a useful further step, but first the evidence must be safeguarded.
D: To isolate a compromised system is a good idea, but it is not required for prosecution.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1052

QUESTION 652
In order to be able to successfully prosecute an intruder:

A. A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B. A proper chain of custody of evidence has to be preserved.
C. Collection of evidence has to be done following predefined procedures.
D. Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When evidence is seized, it is important to make sure a proper chain of custody is maintained to ensure any data collected can later be properly and accurately represented in case it needs to be used for later events such as criminal proceedings and a successful prosecution.

Incorrect Answers:
A: To successfully prosecute an intruder you do not need a designed point of contact. You need proper chain of custody of evidence.
C: To successfully prosecute an intruder you do not to follow predefined procedures. You need proper chain of custody of evidence.
D: It is import to make a replica of digital evidence to avoid tamping with evidence, though it is not strictly required to make a successfully prosecution.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 248

QUESTION 653
What does "System Integrity" mean?

A. The software of the system has been implemented as designed.
B. Users can't tamper with processes they do not own.
C. Hardware and firmware have undergone periodic testing to verify that they are functioning properly.
D. Design specifications have been verified against the formal top-level specification.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
System Integrity means that all components of the system cannot be tampered with by unauthorized personnel and can be verified that they work properly.

Incorrect Answers:
A: System Integrity concerns how software runs, and is not related to implementation of software.
C: System Integrity does not mean hardware and firmware verification. System Integrity relates to how running software behaves.
D: System Integrity is not part of the specification verification. System Integrity concerns how software runs.

References:
http://www.cerberussystems.com/INFOSEC/stds/d520028.htm
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 12

QUESTION 654
In computing what is the name of a non-self-replicating type of malware program containing malicious code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it, when executed, carries out actions that are unknown to the person installing it, typically causing loss or theft of data, and possible system harm.

A. virus
B. worm
C. Trojan horse
D. trapdoor

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:

A trojan horse is any code that appears to have some useful purpose but contains code that has a malicious or harmful purpose imbedded in it. It is non-selfreplicating malware that often includes a trapdoor as a means to gain access to a computer system bypassing security controls.

Incorrect Answers:
A: A Virus is a malicious program that can replicate itself and spread from one system to another. It does not appear to be harmless; its sole purpose is malicious intent often doing damage to a system.
B: A Worm is similar to a Virus but does not require user intervention to execute. Rather than doing damage to the system, worms tend to self-propagate and devour the resources of a system.
D A trapdoor is a means to bypass security by hiding an entry point into a system. Trojan Horses often have a trapdoor imbedded in them.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1213, 1214 http://en.wikipedia.org/wiki/Trojan_horse_(computing)
http://en.wikipedia.org/wiki/Computer_virus http://en.wikipedia.org/wiki/Computer_worm
http://en.wikipedia.org/wiki/Backdoor_(computing)

QUESTION 655
The security of a computer application is MOST effective and economical in which of the following cases?

A. The system is optimized prior to the addition of security.

B. The system is procured off-the-shelf.
C. The system is customized to meet the specific security threat.
D. The system is originally designed to provide the necessary security.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The earlier in the process that security is planned for and implement the cheaper it is. It is also much more efficient if security is addressed in each phase of the development cycle rather than an add-on because it gets more complicated to add at the end. If security plan is developed at the beginning it ensures that security won't be overlooked.

Incorrect Answers:
A: If you wait to implement security after a system is completed the cost of adding security increases dramatically and can become much more complex.
B: It is often difficult to add security to a system that has been procured off-the shelf.
C: This implies only a single threat.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 298, 357

QUESTION 656
Which of the following virus types changes some of its characteristics as it spreads?

A. Boot Sector
B. Parasitic
C. Stealth
D. Polymorphic

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A Polymorphic virus produces varied but operational copies of itself in an attempt to evade anti-virus software.

Incorrect Answers:
A: A boot sector virus attacks the boot sector of a drive. It describes the type of attack of the virus and not the characteristics of its composition.
B: A parasitic virus attaches itself to other files but does not change its characteristics.
C: A stealth virus attempts to hide changes of the affected files but not itself.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1199, 1200, 1201

QUESTION 657
Which of the following is commonly used for retrofitting multilevel security to a database management system?

A. trusted front-end
B. trusted back-end
C. controller
D. kernel

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
In a multilevel security (MLS) database system, a trusted front-end is configured. Users connect to the trusted front-end and the trusted front-end connects to the database system.
The trusted front end is responsible for directing queries to the correct database processor, for ensuring that there is no illegal flow of information between the database processors, for maintaining data consistency between replicated database fragments, and for properly labeling query responses and sending them back to the appropriate user. In addition, the trusted front end is responsible for user identification and authentication, maintenance of the trusted path to the user, and auditing.

Incorrect Answers:
B: A trusted back-end is not configured. The back-end would be the database system. Users connect to a trusted-front end which in turn connects to the back-end database system.
C: A 'controller' is not the correct term for a system that is configured for a multilevel security database system.
D: A kernel is the heart of an operating system. This is not what is configured for a multilevel security database system.

References:
http://www.acsac.org/secshelf/book001/19.pdf

QUESTION 658
Which of the following is an advantage of using a high-level programming language?

A. It decreases execution times for programs
B. It allows programmers to define syntax
C. It requires programmer-controlled storage management
D. It enforces coding standards

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
High-level languages enforce coding standards as a specific order to statements is required as well as a syntax that must be used.

Incorrect Answers:
A: High-level language makes a program easier to code but does not affect the execution times for a program.
B: High-level languages have a set syntax that the programmer needs to follow. It does not allow the programmer to define their own syntax.
C: High-level languages abstract the actual operation of the computer system such as memory usage, and storage.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1125-1128

QUESTION 659
In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?

A. The transactions should be dropped from processing.
B. The transactions should be processed after the program makes adjustments.
C. The transactions should be written to a report and reviewed.
D. The transactions should be corrected and reprocessed.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An online transaction processing system is used in conjunction with a database to commit transactions to a database in real time. The database must maintain its integrity, meaning the data in the database must be accurate at all times. Therefore, transactions must occur correctly or not at all to ensure that that only accurate data are entered into the database. If any of the steps in a transaction fails to complete to due invalid data, all the steps of the transaction are rolled back (dropped).

Incorrect Answers:
B: Invalid transactions should not be processed as it would affect the accuracy of the data and the integrity of the database. Instead, the transaction should be dropped.
C: Writing the transaction to a report for later review would help identify potential problems and/or threats. However, the database must maintain its integrity, meaning the data in the database must be accurate at all times. This means that the invalid transactions should not be allowed as it would compromise the database integrity. Therefore, the transaction should be dropped.
D: Generally, an online transaction processing system does not have mechanisms to correct invalid transactions. These transactions are made by information entered into a web form or other front-end interface. The user needs to correct their error and resubmit the information.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1180-1182, 1187-1188
http://en.wikipedia.org/wiki/Online_transaction_processing
http://databases.about.com/od/administration/g/concurrency.htm

QUESTION 660
When considering all the reasons that buffer overflow vulnerabilities exist what is the real reason?

A. Human error
B. The Windows Operating system
C. Insecure programming languages
D. Insecure Transport Protocols

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The human error in this answer is poor programming by the software developer.
A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed.
When a programmer writes a piece of software that will accept data, this data and its associated instructions will be stored in the buffers that make up a stack. The buffers need to be the right size to accept the inputted data. So if the input is supposed to be one character, the buffer should be one byte in size. If a programmer does not ensure that only one byte of data is being inserted into the software, then someone can input several characters at once and thus overflow that specific buffer.

Incorrect Answers:
B: The Windows Operating system does not cause buffer overflow vulnerabilities.
C: Insecure programming languages do not cause buffer overflow vulnerabilities.
D: Insecure Transport Protocols do not cause buffer overflow vulnerabilities.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 332

QUESTION 661
A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?

A. project initiation and planning phase
B. system design specification phase
C. development & documentation phase
D. acceptance phase

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Certification and accreditation (C&A) processes are performed before a system can be formally installed in the production environment. Certification is the technical testing and evaluation of a system while accreditation is the formal authorization given by management to allow a system to operate in a specific environment. The accreditation decision is based upon the results of the certification process. This occurs during the acceptance phase.

Incorrect Answers:
A: The project initiation and planning phase is the initial phase that establishes the need for a system. Nothing has been developed yet to be evaluated, tested, accredited, etc.
B: System requirement specifications are gathered in the system design and specifications phase. This phase determines how the system will accomplish design goals and could cover required functionality, compatibility, fault tolerance, extensibility, security, usability, and maintainability.
C: During the development & documentation phase programmers are assigned tasks to meet the specifications laid out in the design phase. This is where the system is developed.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 300, 406-407, 1092, 1095

QUESTION 662
Which of the following is often the GREATEST challenge of distributed computing solutions?

A. scalability
B. security
C. heterogeneity
D. usability

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A distributed computing environment is dependent on a network to ensure interoperability. This increases the footprint of the system and increases the potential for attack.

Incorrect Answers:
A: A distributed computing environment is almost infinitely scalable as additional systems can just be added to the environment.
C: The distributed computing environment has evolved to support heterogeneous systems early in its emergence. It is thus possible to have systems from different vendors in a distributed computing environment.
D: The support for heterogeneous systems in a distributed computing environment reduces the problem of usability.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 70, 1142-1143

QUESTION 663
What is the appropriate role of the security analyst in the application system development or acquisition project?

A. policeman
B. control evaluator & consultant
C. data owner
D. application user

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The security analyst contributes to the development of policies, standards, guidelines, and baselines. They help define the security controls and ensure the security controls are being implemented and maintained. This role is fulfilled through consultation and evaluation.

Incorrect Answers:
A: During system development or acquisition, there should be no need of anyone filling the role of policeman.
C: The data owner is responsible for the protection of the data used by the application and can decide what security controls would be required to protect the Databased on the sensitivity and criticality of the data.
D: The application user is an individual who uses the application for work-related tasks. The user must have the necessary level of access to the data to perform the duties within their position. The application user is not responsible for implementing or evaluating security measures.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 114, 121-122, 123, 125

QUESTION 664
The information security staff's participation in which of the following system development life cycle phases provides maximum benefit to the organization?

A. project initiation and planning phase
B. system design specifications phase
C. development and documentation phase
D. in parallel with every phase throughout the project

Correct Answer: D

Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A system has a developmental life cycle, which is made up of the following phases: initiation, acquisition/development, implementation, operation/maintenance, and disposal. Collectively these are referred to as a system development life cycle (SDLC). Security is critical in each phase of the life cycle.
In the initiation phase the company establishes the need for a specific system. The company has figured out that there is a problem that can be solved or a function that can be carried out through some type of technology. A preliminary risk assessment should be carried out to develop an initial description of the confidentiality, integrity, and availability requirements of the system.
The Acquisition/Development phase should include security analysis such as Security functional requirements analysis and Security assurance requirements analysis
In the Implementation phase, it may be necessary to carry out certification and accreditation (C&A) processes before a system can be formally installed within the production environment. Certification is the technical testing of a system.
In the Operation and Maintenance phase, continuous monitoring needs to take place to ensure that security baselines are always met. Vulnerability assessments and penetration testing should also take place in this phase. These types of periodic testing allow for new vulnerabilities to be identified and remediated.
Disposal phase: When a system no longer provides a needed function, plans for how the system and its data will make a transition should be developed. Data may need to be moved to a different system, archived, discarded, or destroyed. If proper steps are not taken during the disposal phase, unauthorized access to sensitive assets can take place.

Incorrect Answers:
A: Security staff should participate in all phases of the system development life cycle, not just the project initiation and planning phases.
B: Security staff should participate in all phases of the system development life cycle, not just the development phase. Documentation is not one of the phases in the system development life cycle.
C: System design specifications would happen in the development phase. 'System design specifications' is not a recognized phase in itself. Security staff should participate in all phases of the system development life cycle, not just the development phase.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1087-1093

QUESTION 665
Which answer BEST describes a computer software attack that takes advantage of a previously unpublished vulnerability?

A. Zero-Day Attack
B. Exploit Attack
C. Vulnerability Attack
D. Software Crack

Correct Answer: A

Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A zero-day is an undisclosed computer application vulnerability that could be misused to harmfully affect the computer programs, data, additional computers or a network.

Incorrect Answers:
B: An exploit refers to a piece of software or data, or a sequence of commands that takes advantage of a bug or vulnerability with the aim of causing unplanned or unexpected behavior to take place on computerized hardware, or its software.
C: A vulnerability is a weakness which allows an attacker to reduce a system's information assurance.
D: Software cracking is the modification of software to get rid of or deactivate features that are considered undesirable by the person cracking the software.

References:
https://en.wikipedia.org/wiki/Zero_day_attack
https://en.wikipedia.org/wiki/Exploit_%28computer_security%29
https://en.wikipedia.org/wiki/Vulnerability_(computing)
https://en.wikipedia.org/wiki/Software_cracking

QUESTION 666
A 'Pseudo flaw' is which of the following?

A. An apparent loophole deliberately implanted in an operating system program as a trap for intruders.
B. An omission when generating Pseudo-code.
C. Used for testing for bounds violations in application programming.
D. A normally generated page fault causing the system to halt.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A Pseudo flaw is appearing as a vulnerability in an operating system program but is in actual fact a trap for intruders who may attempt to exploit the vulnerability.

Incorrect Answers:
B: Pseudocode is an informal high-level description of the operating principle of a software program. It uses some of the syntax and conventions of a programming language, but is intended for human reading rather than machine reading.

C: Bounds checking is used to test for violations in application programming. Essentially, it tests the application's response to inputted data and ensures the inputted data are of an acceptable length.
D: A page fault is caused when the operating kernel attempts to access a page that is in virtual memory rather than in RAM. This often causes the system to halt.

References:
http://itlaw.wikia.com/wiki/Pseudo-flaw
https://en.wikipedia.org/wiki/Pseudocode
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 334
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 267

QUESTION 667
Which of the following is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes?

A. The Software Capability Maturity Model (CMM)
B. The Spiral Model
C. The Waterfall Model
D. Expert Systems Model

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The Software Capability Maturity Model (CMM) is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes. It introduces five maturity levels that serve as a foundation for conducting continuous process improvement and as an ordinal scale for measuring the maturity of the organization involved in the software processes.

CMM has Five Maturity Levels of Software Processes:
- The initial level: processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable as processes would not be sufficiently defined and documented to allow them to be replicated.
- The repeatable or managed level: basic project management techniques are established, and successes could be repeated as the requisite processes would have been made established, defined, and documented.
- The defined level: an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.
- The quantatively managed level: an organization monitors and controls its own processes through data collection and analysis.
- The optimized level: processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

Incorrect Answers:
B: The Spiral model uses an iterative approach to software development with an emphasis on risk analysis. The iterative approach allows new requirements to be addressed as they are uncovered. Testing takes place early in the development project, and feedback based upon these tests is integrated into the following iteration of steps. The risk analysis ensures that all issues are actively reviewed and analyzed. The evaluation phase allows the customer to evaluate the product in its current state and provide feedback, which is an input value for the following iteration of steps. This is a good model for complex projects that have fluid requirements.
C: The Waterfall model uses a linear-sequential life-cycle approach with each phase having to be completed in its entirety before the next phase can begin. At the end of each phase, a review takes place to make sure the project is on the correct path. In this model all requirements are gathered in the initial phase and it is difficult to integrate changes as more information becomes available or requirements change.
D: Expert systems is not a model for the development of software products. It is the use artificial intelligence (AI) to solve problems and is also called knowledgebased systems.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 62, 1112, 1115-1116, 1120-1122, 1192
http://en.wikipedia.org/wiki/Capability_Maturity_Model

QUESTION 668
Which of the following determines that the product developed meets the projects goals?

A. verification
B. validation
C. concurrence
D. accuracy

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Validation is the process of determining whether the product provides the necessary solution for the real-world problem that is was created to solve.
Incorrect Answers:
A: Verification is the process of determining whether the product accurately represents and meets the design specifications given to the developers.
C: Concurrence occurs when there is a piece of software that will be accessed at the same time by different users and/or applications. It is not an issue of product development.
D: Accuracy is related to the integrity of information and systems. The integrity of information and systems requires that the information and systems remain accurate and reliable. This is ensured by preventing any unauthorized modification to the information or systems.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 23-24, 1106, 1124, 1180-1181
http://iase.disa.mil/ditscap/DITSCAP.html

QUESTION 669
What is RAD?

A. A development methodology
B. A project management technique
C. A measure of system complexity
D. Risk-assessment diagramming

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The Rapid Application Development (RAD) model is a software development model or methodology that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.

Incorrect Answers:
B: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not a project management technique.
C: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not a measure of system complexity
D: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not Risk-assessment diagramming.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1116-1118

QUESTION 670
Which of the following best describes the purpose of debugging programs?
A. To generate random data that can be used to test programs before implementing them.
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.
D. To compare source code versions before transferring to the test environment

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production. Logical errors and coding mistakes are referred to as bugs in the code.

Incorrect Answers:
A: The process of generating random data that can be sent to a target program in order to trigger failures is called fuzzing.
C: Debugging does not protect the program from changes.
D: Debugging is not used to compare code versions.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1102-1103, 1105
https://en.wikipedia.org/wiki/Debugging

QUESTION 671
Which of the following is one of the oldest and most common problem in software development that is still very prevalent today?

A. Buffer Overflow
B. Social Engineering
C. Code injection for machine languageD. Unassembled reversible DOS instructions.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Buffer overflows are in the source code of various applications and operating systems. They have been around since programmers started developing software. This means it is very difficult for a user to identify and fix them. When a buffer overflow is identified, the vendor usually sends out a patch, so keeping systems current on updates, hotfixes, and patches is usually the best countermeasure.

A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed. So, the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory

segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task. This task could be to open a command shell with administrative privilege or execute malicious code.

Incorrect Answers:
B: Social engineering is when one person tricks another person into sharing confidential information, for example, by posing as someone authorized to have access to that information. This is a user issue; it is not a problem in software development.
C: Code injection is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. This is not one of the most common problems in software development today.
D: DOS applications are rare nowadays so unassembled reversible DOS instructions is not a prevalent problem today.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 332, 337

QUESTION 672
Which of the following is NOT true concerning Application Control?

A. It limits end users use of applications in such a way that only particular screens are visible.
B. Only specific records can be requested through the application controls
C. Particular usage of the application can be recorded for audit purposes
D. It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:

Application control limits what users can see or do within the application. For example, if a user does not have the necessary access privilege to perform some functions, the functions can be hidden from the screen or the screen itself can be hidden so the user cannot select it within the application. In a similar way, only the records a user has access to can be displayed.
Application control is transparent to the user; the user does not know that a particular screen, function or data records have been hidden.
Application control can be implemented to record the activities a user performs within the application for auditing purposes.

Incorrect Answers:
A: It is true that application control limits end users use of applications in such a way that only particular screens are visible.
B: It is true that only specific records can be requested through the application controls.
C: It is true that particular usage of the application can be recorded for audit purposes by Application Control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1084-1085

QUESTION 673
The object-relational and object-oriented models are better suited to managing complex data such as required for which of the following?

A. computer-aided development and imaging
B. computer-aided duplexing and imaging
C. computer-aided processing and imaging
D. computer-aided design and imaging

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An object-oriented database has classes to define the attributes and procedures of its objects, which can be a variety of data types such as images, audio, documents, and video. This complex data is required for computer-aided design and imaging.

Incorrect Answers:
A, B, C: Computer-aided development, computer-aided duplexing, and computer-aided processing are not valid computing terms. The correct term is computeraided design.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1173-1174

QUESTION 674

Which of the following is not an element of a relational database model?

A. Relations, tuples, attributes and domains
B. Data Manipulation Language (DML) on how the data will be accessed and manipulated
C. Constraints to determine valid ranges and values
D. Security structures called referential validation within tables

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A relational database model uses attributes (columns) and tuples (rows) to contain and organize information. The relational database model is the most widely used model today. It presents information in the form of tables. A relational database is composed of two-dimensional tables, and each table contains unique rows, columns, and cells (the intersection of a row and a column). Each cell contains only one data value that represents a specific attribute value within a given tuple. These data entities are linked by relationships. The relationships between the data entities provide the framework for organizing data. A primary key is a field that links all the data within a record to a unique value.
Data manipulation language (DML) contains all the commands that enable a user to view, manipulate, and use the database (view, add, modify, sort, and delete commands).
A constraint is usually associated with a table and is created with a CREATE CONSTRAINT or CREATE ASSERTION SQL statement. They define certain properties that data in a database must comply with. They can apply to a column, a whole table, more than one table or an entire schema.

Security structures called referential validation within tables are not an element of a relational database model. Referential integrity is used to ensure all foreign keys reference primary keys. Referential validation is not a security structure within a table.

Incorrect Answers:
A: Relations, tuples, attributes and domains are elements of a relational database model.
B: Data Manipulation Language (DML) is an element of a relational database model.
C: Constraints to determine valid ranges and values are an element of a relational database model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1171-1177

QUESTION 675
A persistent collection of interrelated data items can be defined as which of the following?

A. database
B. database management system

C. database security
D. database shadowing

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A database can be defined as a persistent collection of interrelated data items.
Persistency is obtained through the preservation of integrity and through the use of nonvolatile storage media. The description of a database is a schema and a Data Description Language (DDL) defines the schema.

Incorrect Answers:
B: A database management system is the software that maintains and provides access to the database. This is not what is described in the question.
C: Database security restricts access to the database to authorized users and applications. This is not what is described in the question.
D: Database shadowing creates a replica of the database on another database server for redundancy purposes. This is not what is described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 67

QUESTION 676
The description of the database is called a schema. The schema is defined by which of the following?

A. Data Control Language (DCL).
B. Data Manipulation Language (DML).
C. Data Definition Language (DDL).
D. Search Query Language (SQL).

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The description of the database is called a schema, and the schema is defined by a Data Definition Language (DDL). DDL is similar to a computer programming language and is used for defining data structures, such as database schemas.

Incorrect Answers:
A: The Data Control Language (DCL) is a subset of the Structured Query Language (SQL) that allows database administrators to configure security access to relational databases.
B: The Data Manipulation Language (DML) is used to retrieve, insert and modify database information. These commands will be used by all database users during the routine operation of the database.
D: SQL is the abbreviation for structured query language and not search query language. SQL is a standardized query language for requesting information from a database.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1177, 1178
https://secure.wikimedia.org/wikipedia/en/wiki/Data_Definition_Language
http://databases.about.com/od/Advanced-SQL-Topics/a/Data-Control-Language-Dcl.htm
http://www.webopedia.com/TERM/S/SQL.html http://www.w3schools.in/mysql/ddl-dml-dcl/
http://www.orafaq.com/faq/what_are_the_difference_between_ddl_dml_and_dcl_commands

QUESTION 677
Which of the following defines the software that maintains and provides access to the database?

A. database management system (DBMS)
B. relational database management system (RDBMS)
C. database identification system (DBIS)
D. Interface Definition Language system (IDLS)

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The database management system (DBMS) is a software suite that is used to manage access to the database and provides data integrity and redundancy. It is usually controlled by a database administrator.

Incorrect Answers:
B: A relational database management system (RDBMS) provides access to a relational database.
C: There is no database identification system.
D: An Interface Definition Language (IDL) is a language that is used to define the interface between a client and server process in a distributed system. It is not used to provide access to a database.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1170
http://csis.pace.edu/~marchese/CS865/Papers/interface-definition-language.pdf

QUESTION 678
Which of the following represents a relation, which is the basis of a relational database?

A. One-dimensional table
B. Two-dimensional table
C. Three-dimensional table
D. Four-dimensional table

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The relational database model is based on a series of interrelated two-dimensional tables that have columns representing the variables and rows that contain specific instances of data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1171

QUESTION 679
Which of the following represents the rows of the table in a relational database?

A. attributes
B. records or tuples
C. record retention
D. relation

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The rows of the table represent records or tuples.

Incorrect Answers:
A: The columns of the table represent the attributes.
C: Record retention refers to the usually legal requirement to retain data that are no longer of value to the business for a period of time. This ensures compliance with legal requirements.
D: The relation represents the link between data entities, usually from different tables in the database.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1171, 1174
Miller, David R., *CISSP Training Kit*, O'Reilly Media, Sebastopol, 2013, pp. 687-688

QUESTION 680
Which of the following can be defined as the set of allowable values that an attribute can take?

A. domain of a relation
B. domain name service of a relationC. domain analysis of a relation
D. domains, in database of a relation

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The domain of a relation is the set of allowable values that an attribute can take. In other words, it is the values that can be entered in a column (attribute) of a table (relation).

References:
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, p. 272

QUESTION 681
Which of the following can be defined as a unique identifier in the table that unambiguously points to an individual tuple or record in the table?

A. primary key
B. candidate key
C. secondary key
D. foreign key

Correct Answer: A

Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The primary key is the attribute that is used to make each row or tuple in a table unique.

Incorrect Answers:
B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
C: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.
D: A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 682
Which of the following can be defined as THE unique attribute used as a unique identifier within a given table to identify a tuple?

A. primary key
B. candidate key
C. foreign key
D. secondary key

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The primary key is the attribute that is used to make each row or tuple in a table unique.

Incorrect Answers:
B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
C: A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.

D: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 683
Which of the following can be defined as an attribute in one relation that has values matching the primary key in another relation?

A. foreign key
B. candidate key
C. primary key
D. secondary key

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.

Incorrect Answers:
B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
C: The primary key is the attribute that is used to make each row or tuple in a table unique.
D: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 684
Referential Integrity requires that for any foreign key attribute, the referenced relation must have a tuple with the same value for which of the following?

A. primary key
B. secondary key
C. foreign key
D. candidate key

Correct Answer: A
Section: Software Development Security
Explanation
Explanation/Reference:
Explanation:
A foreign key is an attribute in one table that references or matches the primary key of another table. The primary key is the attribute that is used to ensure that each row or tuple in a table unique. Together, the foreign key and the primary key ensure referential integrity.

Incorrect Answers:
B: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.
C: A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.
D: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180, 1181
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 685
Matches between which of the following are important because they represent references from one relation to another and establish the connections among these relations?

A. foreign key to primary key
B. foreign key to candidate key
C. candidate key to primary key
D. primary key to secondary key

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A foreign key is an attribute in one table that references or matches the primary key of another table. The primary key is the attribute that is used to ensure that each row or tuple in a table unique. Together, the foreign key and the primary key ensure referential integrity.

Incorrect Answers:
B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table. There are usually more than one candidate key attributes in a table.
C: A foreign key is an attribute in one table that references or matches the primary key of another table. Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
D: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180, 1181
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 686
A database view is the results of which of the following operations?

A. Join and Select.
B. Join, Insert, and Project.
C. Join, Project, and Create.
D. Join, Project, and Select.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
SQL offers three classes of operators for creating views: select, project, and join.

- The select operator serves to shrink the table vertically by eliminating unwanted rows (tuples).
- The project operator serves to shrink the table horizontally by removing unwanted columns (attributes). Most commercial implementations of SQL do not support a project operation, instead projections are achieved by specifying the columns desired in the output.
- The join operator allows the dynamic linking of two tables that share a common column value.

Incorrect Answers:
A: SQL offers three classes of operators for creating views: select, project, and join. However, modern implementations of SQL do not support a project operation, instead projections are achieved by specifying the columns desired in the output. Nevertheless, project is a SQL operator.
B: Insert is a SQL command used to insert data into a table. It is not used to output a view.
C: Create is a SQL command used to create a new database, table, view, or index. However, the data or output of the view requires a select statement to shrink the table vertically by not showing unwanted rows, a project operation that shrinks the table horizontally by not showing unwanted columns, and a join statement when data from more than one table is required.

References:
http://db.grussell.org/section010.html
http://databasemanagement.wikia.com/wiki/Relational_Database_Model

QUESTION 687
In regards to the query function of relational database operations, which of the following represent implementation procedures that correspond to each of the lowlevel operations in the query?

A. query plan
B. relational plan
C. database plan
D. structuring plan

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A query plan (or query execution plan) is an ordered set of steps used to access data in a SQL relational database management system. This is a specific case of the relational model concept of access plans.
Since SQL is declarative, there are typically a large number of alternative ways to execute a given query, with widely varying performance. When a query is submitted to the database, the query optimizer evaluates some of the different, correct possible plans for executing the query and returns what it considers the best option.

Incorrect Answers:

B: Relational plan is not the correct term to describe implementation procedures that correspond to each of the low-level operations in the query.
C: Database plan is not the correct term to describe implementation procedures that correspond to each of the low-level operations in the query.
D: Structural plan is not the correct term to describe implementation procedures that correspond to each of the low-level operations in the query.

References:
https://en.wikipedia.org/wiki/Query_plan

QUESTION 688
In regards to relational database operations using the Structure Query Language (SQL), which of the following is a value that can be bound to a placeholder declared within an SQL statement?

A. A bind value
B. An assimilation value
C. A reduction value
D. A resolution value

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Bind parameters—also called dynamic parameters or bind variables—are an alternative way to pass data to the database. Instead of putting the values directly into the SQL statement, you just use a placeholder like ?, :name or @name and provide the actual values using a separate API call.
When using bind parameters you do not write the actual values but instead insert placeholders into the SQL statement. That way the statements do not change when executing them with different values.

Incorrect Answers:
B: An assimilation value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.
C: A reduction value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.
D: A resolution value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.

References:
http://use-the-index-luke.com/sql/where-clause/bind-parameters

QUESTION 689
Which of the following are placeholders for literal values in a Structured Query Language (SQL) query being sent to the database on a server?

A. Bind variables

B. Assimilation variables
C. Reduction variables
D. Resolution variables

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Bind variables placeholders for literal values in a Structured Query Language (SQL) query being sent to the database on a server. The SQL statement is sent to the server for parsing and the later values are bound to the placeholders and sent separately to the server. This separate step is the origin of the term 'bind variable'.

Incorrect Answers:
B: An assimilation value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.
C: A reduction value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.
D: A resolution value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 84

QUESTION 690
Which of the following is an important part of database design that ensures that attributes in a table depend only on the primary key?

A. Normalization
B. AssimilationC. Reduction
D. Compaction

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The first normal form (1NF) requires that we create separate tables for each group of related data and identify each row with a unique column identified as the primary key. The second normal form (2NF) requires that we move data that is only partially dependent on the primary key to another table. The third normal form (3NF) requires that we remove data that do not depend only on the primary key. The process of conforming with the normal form us called normalization.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 199-200

QUESTION 691
Normalizing data within a database could include all or some of the following except which one?

A. Eliminate duplicative columns from the same table.
B. Eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key
C. Eliminates Functional dependencies on non-key fields by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.
D. Eliminating duplicate key fields by putting them into separate tables.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Normalizing data within a database does not eliminate duplicate key fields by putting them into separate tables.

An entity is in First Normal Form (1NF) when all tables are two-dimensional with no repeating groups.
A row is in first normal form (1NF) if all underlying domains contain atomic values only. 1NF eliminates repeating groups by putting each into a separate table and connecting them with a one-to-many relationship. Make a separate table for each set of related attributes and uniquely identify each record with a primary key.
- Eliminate duplicative columns from the same table.
- Create separate tables for each group of related data and identify each row with a unique column or set of columns (the primary key).

An entity is in Second Normal Form (2NF) when it meets the requirement of being in First Normal Form (1NF) and additionally:
- Does not have a composite primary key. Meaning that the primary key cannot be subdivided into separate logical entities.
- All the non-key columns are functionally dependent on the entire primary key.
- A row is in second normal form if, and only if, it is in first normal form and every non-key attribute is fully dependent on the key.
- 2NF eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key. An example is resolving many:many relationships using an intersecting entity

An entity is in Third Normal Form (3NF) when it meets the requirement of being in Second Normal Form (2NF) and additionally:
- Functional dependencies on non-key fields are eliminated by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.
- A row is in third normal form if and only if it is in second normal form and if attributes that do not contribute to a description of the primary key are move into a separate table. An example is creating look-up tables.

Incorrect Answers:
A: Normalizing data within a database does eliminate duplicative columns from the same table.

B: Normalizing data within a database does eliminate functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key.
C: Normalizing data within a database does eliminate Functional dependencies on non-key fields by putting them in a separate table.

References:
http://psoug.org/reference/normalization.html
http://searchsqlserver.techtarget.com/definition/normalization?vgnextfmt=print

QUESTION 692
Which of the following is used to create and modify the structure of your tables and other objects in the database?

A. SQL Data Definition Language (DDL)
B. SQL Data Manipulation Language (DML)
C. SQL Data Relational Language (DRL)
D. SQL Data Identification Language (DIL)

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The Data Definition Language (DDL) is similar to a computer programming language and is used for defining data structures, such as database schemas, database tables, and other database objects.

Incorrect Answers:
B: The Data Manipulation Language (DML) is used to retrieve, insert and modify database data. These commands will be used by all database users during the routine operation of the database.
C: The SQL language consists of three components: the Data Definition Language (DDL), the Data Manipulation Language (DML), and the Data Control Language (DCL). It does not contain a data relational language.
D: The SQL language consists of three components: the Data Definition Language (DDL), the Data Manipulation Language (DML), and the Data Control Language (DCL). It does not contain a data identification language.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1177

QUESTION 693
SQL commands do not include which of the following?

A. Select, Update
B. Grant, Revoke
C. Delete, Insert
D. Add, Relist

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
There is no Add command within the Structure Query Language (SQL). Instead the Insert command is used to add new data to the database.

There is also no Relist command within SQL.

Incorrect Answers:
A: Select and Update are Data Manipulation Language (DML) commands. The Select statement is used to select data from a database while the Update statement is used to update existing records in a table.
B: Grant and Revoke are Data Control Language (DCL) commands are used to enforce database security. The Grant statement is used to provide access or privileges on the database objects while the Revoke statement is used to remove those privileges.
C: Delete and Insert are Data Manipulation Language (DML) commands. The Delete statement is used to remove data from a database while the Insert statement is used to add data to a table.

References:
https://technet.microsoft.com/en-us/library/ff848799.aspx https://technet.microsoft.com/en-us/library/ff848766.aspx http://www.cs.utexas.edu/~mitra/csFall2012/cs329/lectures/sql.html http://www.w3schools.com/SQl/sql_select.asp http://www.w3schools.com/SQl/sql_update.asp http://beginner-sql-tutorial.com/sql-grant-revoke-privileges-roles.htm

QUESTION 694
Complex applications involving multimedia, computer aided design, video, graphics, and expert systems are more suited to which of the following database type?

A. Object-Oriented Databases (OODB)
B. Object-Relational Databases
C. Relational Databases
D. Database management systems (DBMS)

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An object-oriented database (OODB) has classes to define the attributes and procedures of its objects, which can be a variety of data types such as images, audio, documents, and video. This complex data is required for computer-aided design and imaging.

Incorrect Answers:
B: An object-relational database (ORD) is a relational database with a software front end that is written in an object-oriented programming language and is used with Object-Oriented Databases (OODB). It does not store data.
C: A relational database organizes data into two-dimensional tables consisting of attributes (columns) and tuples (rows). It is not suited to storing complex data types such as video, graphics, etc.
D: The database management system (DBMS) is a software suite that is used to manage access to the database and provides data integrity and redundancy. It is usually controlled by a database administrator.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1170, 1171, 1173-1174, 1175

QUESTION 695
With regard to databases, which of the following has characteristics of ease of reusing code and analysis and reduced maintenance?

A. Object-Oriented Databases (OODB)
B. Object-Relational Databases (ORDB)
C. Relational Databases
D. Database management systems (DBMS)

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An object-oriented database (OODB) is more dynamic than a relational database as it stores data as objects. It allows object-oriented programming (OOP) code, including classes, to manipulate the objects. This also makes the reusing of code possible.

Incorrect Answers:

B: An object-relational database (ORD) is a relational database with a software front end that is written in an object-oriented programming language. This allows programmers to develop a front-end that incorporates the business logic procedures to be used by requesting applications and the data within the database. C: A relational database stores data in a two-dimensional table and uses query language, such as Structured Query Language (SQL), to access and manipulate that data.
D: The database management system (DBMS) is a software suite that is used to manage access to the database and provides data integrity and redundancy. It is usually controlled by a database administrator.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1173-1174, 1175
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 202

QUESTION 696
Which of the following is the marriage of object-oriented and relational technologies combining the attributes of both?

A. object-relational database
B. object-oriented database
C. object-linking database
D. object-management database

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An object-relational database is described as is the marriage of object-oriented and relational technologies combining the attributes of both.
An object-relational database (ORD) or object-relational database management system (ORDBMS) is a relational database with a software front end that is written in an object-oriented programming language. A relational database just holds data in static two-dimensional tables. When the data are accessed, some type of processing needs to be carried out on it—otherwise, there is really no reason to obtain the data. If we have a front end that provides the procedures (methods) that can be carried out on the data, then each and every application that accesses this database does not need to have the necessary procedures. This means that each and every application does not need to contain the procedures necessary to gain what it really wants from this database.

Incorrect Answers:
B: An object-oriented database is a database designed to handle a variety of data types (images, audio, documents, video). This is not what is described in the question.
C: An object-linking database is not a valid database type.
D: An object-management database is not a valid database type.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1175

QUESTION 697
What is used to hide data from unauthorized users by allowing a relation in a database to contain multiple tuples with the same primary keys with each instance distinguished by a security level?

A. Data mining
B. Polyinstantiation
C. Cell suppression
D. Noise and perturbation

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Polyinstantiation enables a table, which is also known as a relation, to contain multiple tuples with the same primary keys, with each instance distinguished by a security level. At a lower security level the tuple will not contain sensitive data and it will effectively be hidden from users who do not have the appropriate access permissions.

Incorrect Answers:
A: Data mining is the process of analyzing large amounts of data to determine patterns that would not previously be apparent.
C: Cell suppression is a technique used to hide specific cells in a database that contain information that could be used in inference attacks.
D: Noise and perturbation is a technique of inserting fake information in a database in an attempt to misdirect an attacker or create sufficient confuse that the actual attack will not be fruitful.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1185, 1186, 1188

QUESTION 698
Which of the following translates source code one command at a time for execution on a computer?

A. A translator
B. An interpreter
C. A compiler
D. An assembler

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Interpreters translate one command at a time during run-time or execution time.

Incorrect Answers:
A: A translator converts source code to another format, which could be another high-level language, an intermediate language, or machine language.
C: A compiler converts high-level language source code to the necessary a target language for specific processors to understand.
D: An assembler converts assembly language source code into machine code that the computer understands.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1128-1130

QUESTION 699
Which of the following is a Microsoft technology for communication among software components distributed across networked computers?

A. DDE
B. OLE
C. ODBC
D. DCOM

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Component Object Model (COM) is a model that allows for interprocess communication within one application or between applications on the same computer system. The model was created by Microsoft and outlines standardized APIs, component naming schemes, and communication standards. So if I am a developer and I want my application to be able to interact with the Windows operating system and the different applications developed for this platform, I will follow the COM outlined standards.
Distributed Component Object Model (DCOM) supports the same model for component interaction, and also supports distributed interprocess communication (IPC). COM enables applications to use components on the same systems, while DCOM enables applications to access objects that reside in different parts of a network. So this is how the client/server-based activities are carried out by COM-based operating systems and/or applications.

Incorrect Answers:
A: Dynamic Data Exchange (DDE) allows information to be shared or communicated between programs on one computer, not across networked computers. B: Object linking and embedding (OLE) provides a way for objects to be shared on a local personal computer and to use COM as their foundation. OLE enables objects—such as graphics, clipart, and spreadsheets—to be embedded into documents. This is not what is described in the question.

C: Open Database Connectivity (ODBC) is an API that allows an application to communicate with a database, either locally or remotely. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1146, 1176

QUESTION 700
Which of the following statements relating to Distributed Computing Environment (DCE) is FALSE?

A. It is a layer of software that sits on the top of the network layer and provides services to the applications above it.
B. It uses a Universal Unique Identifier (UUID) to uniquely identify users, resources and components.
C. It provides the same functionality as DCOM, but it is more proprietary than DCOM.
D. It is a set of management services with a communication layer based on RPC.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Distributed Computing Environment (DCE) does provide the same functionality as DCOM, but it is NOT more proprietary than DCOM.
Distributed Computing Environment (DCE) is a standard developed by the Open Software Foundation (OSF), also called Open Group. It is a client/server framework that is available to many vendors to use within their products. This framework illustrates how various capabilities can be integrated and shared between heterogeneous systems. DCE provides a Remote Procedure Call (RPC) service, security service, directory service, time service, and distributed file support. It was one of the first attempts at distributed computing in the industry.
DCE is a set of management services with a communications layer based on RPC. It is a layer of software that sits on the top of the network layer and provides services to the applications above it. DCE and Distributed Component Object Model (DCOM) offer much of the same functionality. DCOM, however, was developed by Microsoft and is more proprietary in nature.

Incorrect Answers:
A: It is true that DCE is a layer of software that sits on the top of the network layer and provides services to the applications above it.
B: It is true that DCE uses a Universal Unique Identifier (UUID) to uniquely identify users, resources and components.
D: It is true that DCE is a set of management services with a communication layer based on RPC.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1146, 1142

QUESTION 701
Which virus category has the capability of changing its own code, making it harder to detect by anti-virus software?

A. Stealth viruses
B. Polymorphic viruses
C. Trojan horses
D. Logic bombs

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A Polymorphic virus produces varied but operational copies of itself in an attempt to evade anti-virus software.

Incorrect Answers:
A: A stealth virus attempts to hide changes of the affected files but not itself.
C: A Trojan horse is code that is disguised as a useful application but contains code that has a malicious or harmful purpose imbedded in it.
D: A logic bomb executes a set of instructions when specific conditions are met.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1199, 1200, 1201, 1206

QUESTION 702
Why would a database be denormalized?

A. To ensure data integrity
B. To increase processing efficiency
C. To prevent duplication of data
D. To save storage space

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The purpose of denormalization is to improve the read performance and processing efficiency of a database by adding redundant data or by grouping data.

Incorrect Answers:

A: The duplication of data creates a problem for data integrity as the data needs to be updated in numerous places. Normalization, which eliminates the duplication of data, improves data integrity.
C: The purpose of normalization is to eliminate duplication of the data. All duplicated data items should be deleted and replaced by a pointer. Denormalization could reverse this process. It attempts to improve the read performance and processing efficiency of a database by adding redundant data or by grouping data.
D: The purpose of denormalization is to improve the read performance and processing efficiency of a database by adding redundant data or by grouping data. This increases storage space consumption.

References:
https://en.wikipedia.org/wiki/Denormalization
https://en.wikipedia.org/wiki/Database_normalization
Miller, David R., *CISSP Training Kit*, O'Reilly Media, Sebastopol, 2013, pp. 620, 622

QUESTION 703
Which of the following BEST explains why computerized information systems frequently fail to meet the needs of users?

A. Inadequate quality assurance (QA) tools.
B. Constantly changing user needs.
C. Inadequate user participation in defining the system's requirements.
D. Inadequate project management.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The most important stages of developing computerized information systems (or any other system or software) are the early requirement gathering and design phases. If the needs of the users are not correctly determined, the system will not meet those needs. As end users will be the people using the system, they are

will have the most valuable input into the system requirements definition. Inadequate user participation in defining the system's requirements can lead to a system design that does not meet the requirements of the users.

Incorrect Answers:
A: This question is asking for the BEST answer. Inadequate quality assurance (QA) tools may result in poor QA tests so floors in the system aren't recognized. However, defining the system's requirements is the most important stage of the project. If this is not done correctly, then QA testing will have no effect on the suitability of the new system.
B: Constantly changing user needs can be a hazard in a development project. However, this only has an effect if the users are involved in the design of the system. D: Inadequate project management generally leads to late or over-budget projects. Incorrectly determining the system requirements could be due to inadequate project management. However, Answer C is more specific to the cause of the problem.

QUESTION 704
Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?

A. Interface errors are detected earlier.
B. Errors in critical modules are detected earlier.
C. Confidence in the system is achieved earlier.
D. Major functions and processing are tested earlier.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Bottom Up Testing is an approach to integrated testing where the lowest level components are tested first, then used to facilitate the testing of higher level components. The process is repeated until the component at the top of the hierarchy is tested.
With Bottom Up Testing critical modules can be tested first and the main advantage of this approach is that bugs are more easily found.

All the bottom or low-level modules, procedures or functions are integrated and then tested. After the integration testing of lower level integrated modules, the next level of modules will be formed and can be used for integration testing. This approach is helpful only when all or most of the modules of the same development level are ready. This method also helps to determine the levels of software developed and makes it easier to report testing progress in the form of a percentage.

Incorrect Answers:
A: Interface modules are located at higher levels of the software design, not at the bottom levels.
C: The major advantage of the top-down approach is that bugs are found earlier, not that confidence is achieved earlier.
D: The major functions are not located at the bottom, and would not be tested earlier.

References:

https://en.wikipedia.org/wiki/Integration_testing#Top-down_and_Bottom-up

QUESTION 705
Which of the following is an advantage of prototyping?

A. Prototype systems can provide significant time and cost savings.
B. Change control is often less complicated with prototype systems.
C. It ensures that functions or extras are not added to the intended system.
D. Strong internal controls are easier to implement.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
A sample of software code or a model (prototype) can be developed to explore a specific approach to a problem before investing expensive time and resources. A team can identify the usability and design problems while working with a prototype and adjust their approach as necessary. Within the software development industry three main prototype models have been invented and used. These are the rapid prototype, evolutionary prototype, and operational prototype.

Incorrect Answers:
B: Change control is not less complicated with prototype systems.
C: Prototyping does nothing to ensure that functions or extras are not added to the intended system.
D: Strong internal controls are not easier to implement with prototyping. Being a new/prototype system, strong internal controls are likely to be more difficult to implement than a non-prototype system.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1114

QUESTION 706
Why do buffer overflows happen? What is the main cause?

A. Because buffers can only hold so much data
B. Because of improper parameter checking within the application
C. Because they are an easy weakness to exploit
D. Because of insufficient system memory

Correct Answer: B

Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
In computer security and programming buffer overflow is a type of application error. The application's lack of proper checking of parameters causes the buffer overflow.
A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety.

Incorrect Answers:
A: It is true that there is a limit of data that can be handled by a buffer, but this limit is not the cause of the overflow.
B: Buffer overflows can be exploited, but the cause is a flaw in the program. The exploitation does not cause the overflow.
D: Insufficient memory does not cause overflows. The overflow is caused by a flow in the application.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 71

QUESTION 707
What is called the number of columns in a table?

A. Schema
B. Relation
C. Degree
D. Cardinality

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The number of columns in a database table (relation) is referred to as the degree.
Incorrect Answers:
A: Schema describes that structure of the database
B: A database table is also referred to as a relation.
D: Cardinality is the number of rows (tuples) in a database table (relation).

References:

Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 275, 277

QUESTION 708
Which of the following would not correspond to the number of primary keys values found in a table in a relational database?
A. Degree
B. Number of tuples
C. Cardinality
D. Number of rows

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The degree of a table represents the number of columns in a database table. This does not correspond to the number of primary key values in a table as each row must have a unique primary key.

Incorrect Answers:
B, D: A row in a database table is referred to as a tuple. Each row or tuple must have a unique primary key. Therefore, the number of rows or tuples will correspond to the number of primary keys values found in a table.
D: Cardinality is the number of rows, also known as tuples, in a table. Each row or tuple must have a unique primary key. Therefore, the cardinality of a table will correspond to the number of primary keys values found in a table.

References:
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 275, 277
http://databases.about.com/od/specificproducts/a/keys.htm

QUESTION 709
Which of the following represents the best programming?

A. Low cohesion, low coupling
B. Low cohesion, high coupling
C. High cohesion, low coupling
D. High cohesion, high coupling

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Cohesion reflects how many different types of tasks a module can carry out. If a module carries out only one task (i.e., subtraction) or several tasks that are very similar (i.e., subtract, add, multiply), it is described as having high cohesion, which is a good thing. The higher the cohesion, the easier it is to update or modify and not affect other modules that interact with it. This also means the module is easier to reuse and maintain because it is more straightforward when compared to a module with low cohesion.

Coupling is a measurement that indicates how much interaction one module requires to carry out its tasks. If a module has low (loose) coupling, this means the module does not need to communicate with many other modules to carry out its job. High (tight) coupling means a module depends upon many other modules to carry out its tasks. Low coupling is more desirable because the modules are easier to understand, easier to reuse, and changes can take place and not affect many modules around it. Low coupling indicates that the programmer created a well-structured module.

Incorrect Answers:
A: With low cohesion it is harder to update a module of the program.
B: With low cohesion it is harder to update a module of the program. High coupling would make the modules of the program harder to understand and harder to reuse.
D: High coupling would make the modules of the program harder to understand and harder to reuse.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 1138-1139

QUESTION 710
Java is not:

A. Object-oriented.
B. Distributed.
C. Architecture Specific.
D. Multithreaded.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
JAVA was developed so that the same program could be executed on multiple hardware and operating system platforms, it is not Architecture Specific.

Incorrect Answers:
A: JAVA is object-oriented as it works with classes and objects.
B: JAVA was developed to be used in a distributed computing environment.
D: JAVA is multi-threaded that is calls to subroutines as is the case with object-oriented programming.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1148

QUESTION 711
What are user interfaces that limit the functions that can be selected by a user called?

A. Constrained user interfaces
B. Limited user interfaces
C. Mini user interfaces
D. Unlimited user interfaces

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Constrained user interfaces limit users' access abilities by not allowing them to request certain functions or information, or to have access to specific system resources.

Incorrect Answers:
B: Limited user interfaces is not a valid term with regards to CISSP.
C: Mini user interfaces are designed for hand-held devices like smartphones.
D: Unlimited user interfaces are not a valid term with regards to CISSP.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 228
http://www.reinteract.org/design/mini.html

QUESTION 712
Buffer overflow and boundary condition errors are subsets of which of the following?

A. Race condition errors.
B. Access validation errors.
C. Exceptional condition handling errors.

D. Input validation errors.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The buffer overflow is probably the most notorious of input validation mistakes. A buffer overflow is an example of boundary condition error where data is allowed to be written outside the allocated buffer.

Incorrect Answers:
A: Buffer overflow and boundary conditions errors are not race conditions errors. Race conditions exist when the design of a program puts it in a vulnerable condition before ensuring that those vulnerable conditions are mitigated. Examples include opening temporary files without first ensuring the files cannot be read, or written to, by unauthorized users or processes, and running in privileged mode or instantiating dynamic load library functions without first verifying that the dynamic load library path is secure. Either of these may allow an attacker to cause the program (with its elevated privileges) to read or write unexpected data or to perform unauthorized commands.
B: Buffer overflow and boundary conditions errors are not access validation errors. An example of an access validation error would be when a process is denied access to an object.
C: An example of exceptions handling error would be a division by zero. Buffer overflows and boundary conditions are not examples of exceptional conditions errors.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 1162, 1304

QUESTION 713
Which of the following does not address Database Management Systems (DBMS) Security?

A. Perturbation
B. Cell suppression
C. Padded cells
D. Partitioning

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:

A padded cell system is used in Intrusion Detection Systems (IDSs) and is similar to a honeypot. When an IDS detects an intruder, that intruder is automatically transferred to a padded cell. The padded cell has the look and layout of the actual network, but within the padded cell the intruder can neither perform malicious activities nor access any confidential data.

Incorrect Answers:
A: Noise and perturbation is a database security technique of inserting fake information in the database to misdirect an attacker or cause confusion on the part of the attacker that the actual attack will not be fruitful.
B: Cell suppression is a database security technique used to hide specific cells in a database that contain information that could be used in inference attacks. D: Partitioning is a database security technique that involves dividing the database into different parts, which makes it much harder for an unauthorized individual to find connecting pieces of data that can be brought together and other information that can be deduced or uncovered.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1185
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, p. 58

QUESTION 714
Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?

A. Implementation
B. System feasibility
C. Product design
D. Software plans and requirements

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Information security best practice is a consensus of the best way to protect the confidentiality, integrity, and availability of assets. Following best practices is a way to demonstrate due care and due diligence.
Due Care and Due Diligence should therefore be a part of the Software plans and requirements phase.
Note: Due care is doing what a reasonable person would do. It is sometimes called the “prudent man” rule. The term derives from “duty of care. Due diligence is the management of due care. Expecting your staff to keep their systems patched means you expect them to exercise due care. Verifying that your staff has patched their systems is an example of due diligence.

Incorrect Answers:
A: Due Care and Due Diligence would be a part of the requirements of a project, and not a part of the implementation phase.

B: Due Care and Due Diligence would be a part of the requirements of a project, and not a part of the System feasibility phase.
C: Due Care and Due Diligence would be a part of the requirements of a project, and not a part of the design phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 161

QUESTION 715
Which of the following phases of a software development life cycle normally incorporates the security specifications, determines access controls, and evaluates encryption options? A. Detailed design

B. Implementation
C. Product design
D. Software plans and requirements

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The design stage takes as its initial input the requirements identified in the approved requirements document, this would include security specifications. For each requirement, a set of one or more design elements will be produced as a result of interviews, workshops, and/or prototype efforts.

Incorrect Answers:
A: In the Systems Development Life Cycle (SDLC) model there is not Detailed Design just a Product Design or simply a Design phase.
B: The security specifications are implemented in the implementation phase, but they are incorporated earlier in the product design phase.
D: The security specifications are made in the Software plans and requirements phase, but incorporated in the product design phase.

References:
https://en.wikipedia.org/wiki/Systems_development_life_cycle

QUESTION 716
In a database management system (DBMS), what is the "cardinality"?

A. The number of rows in a relation.
B. The number of columns in a relation.
C. The set of allowable values that an attribute can take.
D. The number of relations in a database.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
In database design, the cardinality or fundamental principle of one data table with respect to another is a critical aspect. The relationship of one to the other must be precise and exact between each other in order to explain how each table links together.
In the relational model, tables can be related as any of "one-to-many" or "many-to-many." This is said to be the cardinality of a given table in relation to another.

Incorrect Answers:
B: The number of columns in a relation would be the size of the key. It is not the cardinality of the relation.
C: Cardinality concerns the relation between two tables, not allowable attributes.
D: Cardinality concerns one specific relation between two tables, not the number of relations in a database.

References:
https://en.wikipedia.org/wiki/Cardinality_(data_modeling)

QUESTION 717
Which of the following statements pertaining to software testing is incorrect?

A. Unit testing should be addressed and considered when the modules are being designed.
B. Test data should be part of the specifications.
C. Testing should be performed with live data to cover all possible situations.
D. Test data generators can be used to systematically generate random test data that can be used to test programs.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Live data would cover less of the possible input data range compared to generated data.

Incorrect Answers:
A: Unit testing can start very early in development. After a programmer develops a component, or unit of code, it is tested with several different input values and in many different situations. The goal of this type of testing is to isolate each part of the software and show that the individual parts are correct.
B: An important problem in testing is that of generating quality test data and is seen as an important step in reducing the cost of software testing. Test data should therefore be part of the specification.

D: An important problem in testing is that of generating quality test data and is seen as an important step in reducing the cost of software testing. Hence, test data generation is an important part of software testing.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1104

QUESTION 718
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?

A. Estimating the cost of the changes requested
B. Recreating and analyzing the problem
C. Determining the interface that is presented to the user
D. Establishing the priorities of requests

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
To determine the user interface would not be part of the change control phase. This would be done in an earlier phase.
The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerability, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity.

Incorrect Answers:
A: Calculation the cost of the change should be a part of analyzing a change request.
B: Testing is a part of change control. If a problem occurs during testing change control should recreate and analyze the problem.
D: If there are multiple change requests then they must be prioritized in the change control phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1122

QUESTION 719
Sensitivity labels are an example of what application control type?

A. Preventive security controls
B. Detective security controls
C. Compensating administrative controls

D. Preventive accuracy controls

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Sensitivity (Security) labels are attached to all objects; thus, every file, directory, and device has its own security label with its classification information. A user may have a security clearance of secret, and the data he requests may have a security label with the classification of top secret. In this case, the user will be denied (prevented) because his clearance is not equivalent or does not dominate (is not equal or higher than) the classification of the object.

The terms “security labels” and “sensitivity labels” can be used interchangeably.
Incorrect Answers:
B: Sensitivity labels are preventive, not detective, as the label may prevent the user or process from accessing the resource.
C: A compensating control is a data security measure that is designed to satisfy the requirement for some other security measure that is deemed too difficult or impractical to implement. Sensitive controls are preventive, not compensating.
D: Sensitivity labels have nothing to do with accuracy. They are preventive.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 222

QUESTION 720
What is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?

A. Polyinstantiation
B. Inference
C. Aggregation
D. Data mining

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Aggregation is the act of combining information from separate sources. The combination of the data forms new information, which the subject does not have the necessary rights to access. The combined information has a sensitivity that is greater than that of the individual parts.

Incorrect Answers:
A: Polyinstantiation enables a table, which is also known as a relation, to contain multiple tuples with the same primary keys, with each instance distinguished by a security level. At a lower security level the tuple will not contain sensitive data and it will effectively be hidden from users who do not have the appropriate access permissions.
B: Inference is the intended result of aggregation. The inference problem happens when a subject deduces the full story from the pieces he learned of through aggregation. This is seen when data at a lower security level indirectly portrays data at a higher level.
D: Data mining is about finding new information in a lot of data. Sensitivity or security is not related to data mining.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1183
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1186, 1188

QUESTION 721
Which expert system operating mode allows determining if a given hypothesis is valid?
A. Blackboard
B. Lateral chaining
C. Forward chaining
D. Backward chaining

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Backward chaining (or backward reasoning) is an inference method that can be described as working backward from the goal/hypothesis. It is used in automated theorem provers, inference engines, proof assistants and other artificial intelligence applications.

Incorrect Answers:
A: A blackboard system is an artificial intelligence application based on the blackboard architectural model, where a common knowledge base, the "blackboard", is iteratively updated by a diverse group of specialist knowledge sources, starting with a problem specification and ending with a solution.
B: Lateral chaining is not one of the expert system operating modes.
C: Forward chaining is the opposite of backward chaining. Forward chaining starts with the available data and uses inference rules to extract more data until a goal (hypothesis) is reached.

References:
https://en.wikipedia.org/wiki/Backward_chaining

QUESTION 722

Why does compiled code pose more of a security risk than interpreted code?

A. Because malicious code can be embedded in compiled code and be difficult to detect.
B. If the executed compiled code fails, there is a chance it will fail insecurely.
C. Because compilers are not reliable.
D. There is no risk difference between interpreted code and compiled code.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Compiled code poses more of a security risk than interpreted code because of malicious code can be embedded in the compiled code and be difficult to detect.
Incorrect Answers:
B: Compiled code that fails would be an example of an application runtime error, which in itself is no security risk.
C: Compilers are to be trusted.
D: Compiled code is more of a security risk.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 425

QUESTION 723
Which of the following is not a defined maturity level within the Software Capability Maturity Model?

A. Repeatable
B. Defined
C. Managed
D. Oriented

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:

The Software Capability Maturity Model (CMM) is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes. It introduces five maturity levels that serve as a foundation for conducting continuous process improvement and as an ordinal scale for measuring the maturity of the organization involved in the software processes.

CMM has Five Maturity Levels of Software Processes:

- The initial level: processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable as processes would not be sufficiently defined and documented to allow them to be replicated.
- The repeatable or managed level: basic project management techniques are established, and successes could be repeated as the requisite processes would have been made established, defined, and documented.
- The defined level: an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.
- The quantatively managed level: an organization monitors and controls its own processes through data collection and analysis.
- The optimized level: processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

There is thus no Oriented level.

Incorrect Answers:
A: The repeatable level is the second maturity level. At this level basic project management techniques are established, and successes could be repeated as the requisite processes would have been made established, defined, and documented.
B: The defined level is the third maturity level. At this level an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.
C: The (quantatively) managed level is the fourth maturity level. At this level an organization monitors and controls its own processes through data collection and analysis.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 62, 1120-1122
http://en.wikipedia.org/wiki/Capability_Maturity_Model

QUESTION 724
Which software development model is actually a meta-model that incorporates a number of the software development models?

A. The Waterfall model
B. The modified Waterfall model
C. The Spiral model
D. The Critical Path Model (CPM)

Correct Answer: C

Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The spiral model is a risk-driven process model generator for software projects. Thus, the incremental, waterfall, prototyping, and other process models are special cases of the spiral model that fit the risk patterns of certain projects.

Incorrect Answers:
A: The Waterfall model is a special case of the Spiral model, not the opposite way around.
B: The modified Waterfall model is a special case of the Spiral model, not the opposite way around.
D: A critical path model is not a meta-model. The critical path model requires you to establish the time frame for a project and schedule start and end times for each task in the project.

References:
https://en.wikipedia.org/wiki/Spiral_model
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1112, 1115-1116