210-250.exam.25q

Number: 210-250
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Cisco 210-250

Understanding Cisco Cybersecurity Fundamentals (SECFND)

Exam A

QUESTION 1
A host is sending a ping packet to another host in the same subnet. For which IP address does the sending host perform an ARP broadcast to resolve?

A. its own IP address
B. the IP address of the router
C. the IP address of the DNS server
D. the IP address of the destination host

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: All communication within a subnet is based on MAC addresses. When the destination is in the same subnet, the source device performs an ARP broadcast to learn the MAC address of the destination host.

The Address Resolution Protocol (ARP) is used in TCP/IP to resolve media access control (MAC) addresses to IP addresses. Mac addresses are configured on each NIC on an Ethernet network so that the nodes can be identified on the network. ARP enables the MAC addressing that Ethernet requires to interoperate with the IP addressing that TCP/IP requires. You can use the arp utility to view and manage the ARP cache on a computer. To use the arp utility, you can issue the arp command with various switches at a command prompt. The source device will perform an ARP broadcast to learn the mac address of the router in cases were the destination is in another subnet. Then the router will take over from there.

The source device will never perform an ARP broadcast to learn its own MAC address.

The only time a source device will perform an ARP broadcast to learn the MAC address of the DNS server is when communication is being done by name and not IP address.

Objective: Network Concepts
Sub-Objective: Describe IP subnets and communication within an IP subnet and between IP subnets

Reference: https://www.dummies.com/programming/networking/cisco/network-basics-local-host-arp-requests/

QUESTION 2
At which layer does switching occur in the Cisco modified TCP/IP model?

A. Internet
B. Transport
C. Data Link
D. Physical

Correct Answer: C
Section: (none)
Explanation

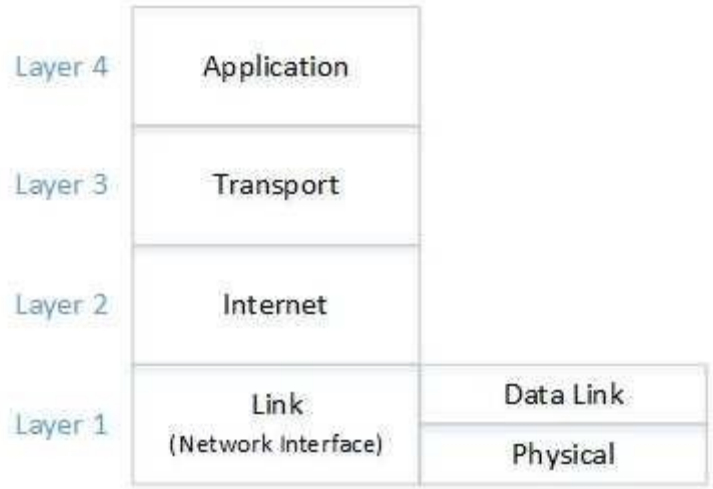
Explanation/Reference:
Explanation:

Switches make switching decisions based on MAC addresses. Because MAC address reside in the Data Link layer of the TCP/IP or DoD model, this is the layer where switching occurs. A switch is a high-speed networking device that receives incoming data packets from one of its ports and directs them to a destination port for local area network access. A switch will redirect traffic bound outside the local area to a router for forward through an appropriate WAN interface.

The modified TCP/IP model is a model by Cisco that departs from the DoD model by breaking the bottom layer, the Link layer, into two layers called the Data Link and the Physical layer.

Other versions of the model refer to the Link as the Network Interface layer.

The layers in ascending order are:



Switches do not operate on the Internet layer. Routers are an example of devices that operate on this layer, which is where IP addresses are located. A router is a device that examines the contents of data packets transmitted within or across networks. Routers determine if a source and destination are on the same network, or whether data mist be transferred from one network to another, either between locally available network segments, or across a wide-area link to access other, more distant networks.

Switches do not operate on the Transport layer. This is the layer where port numbers are added to the packet.

Switches do not operate on the Physical layer. This is the layer where the information is transmitted as ones and zeros using the underlying technology of the medium.

The Application layer of the TCP/IP model corresponds to the Application, Presentation, and Session layers of the OSI model.

The Transport layer of the TCP/IP model correspond to the Transport layer of the OSI model.

The Internet layer of the TCP/IP model correspond to the Network layer of the OSI model. Internet protocol (IP), address resolution protocol (ARP), and Internet control message protocol (ICMP) operate at the Internet layer.

The Link layer of the TCP/IP model corresponds to the Data Link and Physical layers of the OSI model.

Objective: Network Concepts
Sub-Objective: Describe the function of the network models

Reference: https://converse.org.ua/kak-otliit%27-original%27nye-konversy-ot-poddelki

QUESTION 3
Which of the following is used to prevent malicious software systems?

A. HIDS
B. HIPS
C. network AV
D. host AV

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To protect multiple devices from malware, network antivirus (AV) should be used. These tools can protect an entire network of devices.

A host antivirus (AV) can only protect the device on which it is installed.

A host intrusion prevention system (HIPS) can prevent multiple attack types, but it can only protect the device on which it is installed.

A host intrusion detection system (HIPS) can detect multiple attack types, but it can only detect attacks against the device on which it is installed.

Intrusion prevention systems (IPS) and intrusion detection systems (IDS) work together to complement each other. IPS systems can block activities on certain Web sites. Users may be allowed to access the sites but may be prevented from accessing certain features within the site. In other cases, the entire site may be blocked, depending on the security requirements for the organization.

Objective: Security Concepts
Sub-Objective: Compare and contrast these terms: Network and host antivirus, Agentless and agent-based protections, SIEM and log collection

References: https://www.techrepublic.com/article/pick-an-anti-virus-solution-that-will-grow-with-your-network/

QUESTION 4
What terms represents the leveraging of a security weakness present in a system?

A. breach
B. threat
C. vulnerability
D. exploit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When a security weakness or vulnerability exists in a system and threat actor takes advantage of it, the attack is considered an exploit.

A vulnerability is a susceptibility to a threat that exists in a system. An example of a vulnerability is keeping ports open for nonessential services.

A threat is an external danger to which a system may or may not be vulnerable. It is a potential danger that could take advantage of a system if it is vulnerable. A hacker is a threat actor. An attacker picking the lock of the back entrance to a facility is an example of a threat, not a vulnerability.

A breach is when an exploit is successful in providing unauthorized access to data.

Objective: Security Concepts
Sub-Objective: Compare and contrast these concepts: Risk, Threat, Vulnerability, Exploit

Reference: https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

QUESTION 5
Which of the following uses port 443?

A. DNS
B. SSH
C. SSL
D. Telnet
E. HTTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Secure Sockets Layer (SSL) is a security protocol that uses both encryption and authentication to protect data sent in network communications. SSL and HTTPS use port 443.

Port number 22 is reserved for Secure Shell (SSH) remote login.

Telnet uses port 23. Telnet is a terminal emulation protocol. You can use Telnet to establish a remote session with a server and to issue commands on a server.

Telnet client software provides you with a text-based interface and a command line from which you can issue commands on a server that supports the Telnet protocol. Telnet works at the Application layer of the OSI model.

HTTP uses port 80. HTTP is used to traverse web pages.

DNS uses port 53. Domain Name System (DNS) is the protocol that will manage the FQDN to IP address mappings.

There are a total of 65,535 ports in the TCP/IP protocol that are vulnerable to attacks. The following are the most commonly used ports and protocols:

- FTP – ports 20 and 21
- SSH, SCP, and SFTP – port 22
- Telnet – port 23
- SMTP – port 25
- TACACS – port 49
- DNS server – port 53
- DHCP – port 67 and 68
- TFTP – port 69
- HTTP – port 80
- Kerberos – port 88
- POP3 – port 110
- NetBIOS – ports 137-139
- IMAP4 – port 143
- SNMP – port 161
- LDAP – port 389
- SSL and HTTPS – port 443
- SMB – port 445
- LDAP with SSL – port 636
- FTPs – ports 989, 990
- Microsoft SQL Server – port 1433
- Point-to-Point Tunneling Protocol (PPTP) – port 1723
- RDP protocol and terminal Services – port 3389

Objective: Cryptography
Sub-Objective: Describe the security impact of these commonly used encryption algorithms and secure communications protocols: DES, 3DES, AES, AES256-CTR, RSA, DSA, SSH, SSL/TLS

Reference: http://info.ssl.com/article.aspx?id=10241

QUESTION 6
What is the process of scoring risks by their likelihood and their impact?

A. quantitative risk analysis

B. qualitative risk analysis C. business impact analysis
D. disaster recovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When scoring is used to rate risks by likelihood and impact, it is called qualitative risk analysis. Qualitative risk analysis does not assign monetary values. It is simply a subjective report that is compiled by the risk analysis team that describes the threats, countermeasures, and likelihood an event will occur.

Quantitative risk analysis attempts to attach dollar figures to potential risk outcomes. Quantitative risk analysis attempts to predict the likelihood a threat will occur and assigns a monetary value in the event a loss occurs. The likelihood of risk occurrence is usually based ob subject matter expert opinion and rankings from statistical data.

A business impact analysis (BIA) focuses on critical business systems and the impact if they are lost to an outage. A BIA is created to identify the company's vital functions and prioritize them based on need. It identifies vulnerabilities and threats and calculates the associated risks.

A disaster recovery plan is a short term plan that is implemented when a large disaster event occurs. The plan is created to ensure that your company can resume operations in a timely manner. It mainly focuses on alternative procedures for processing transactions in the short term. It is carried out when the emergency occurs and immediately following the emergency.

Objective: Security Concepts
Sub-Objective: Describe these security terms: Principle of least privilege, Risk scoring/risk weighting, Risk reduction, Risk assessment

Reference: https://www.pmi.org/learning/library/qualitative-risk-assessment-cheaper-faster-3188

QUESTION 7
Which of the following is not a hashing algorithm?

A. DES
B. MD5
C. SHA-1

D. SHA-3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Digital encryption standard (DES) is an encryption algorithm, not a hashing algorithm. DES is a private key encryption standard that is used in IPSec to ensure that data packets are confidentially transmitted.

MD5 is a one-way hashing algorithm. One-way hashing inserts a string of variable length into a hashing algorithm and produces a hash value of fixed length. This hash is appended to the end of the message being sent. The receiver recomputes the hash by using the same computational logic. If the recomputed hash value is the same as the generated hash value, the message was not altered during the course of transmission.

Secure Hashing Algorithm 1 (SHA 1) is the first and least secure version of SHA.
Secure Hashing Algorithm 3 (SHA 3) is the first and least secure version of SHA.

Objective: Cryptography
Sub-Objective: Describe the security impact of these commonly used hash algorithms: MD5, SHA-1, SHA-256, SHA-512

Reference: https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard

QUESTION 8
Which of the following is the most widely used public key cipher?

A. 3DES
B. El Gamal
C. RSA
D. AES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Rivest, Shamir, Adleman (RSA) is the most widely used public key or asymmetric cipher. RSA supports encryption and decryption and secures data with an algorithm that is based on the difficulty of factoring large numbers.

A public key encryption algorithm is sometimes referred to as an asymmetric encryption algorithm. With asymmetric encryption, the public key is shared and used to encrypt information, and the private key is secret and used to decrypt data that was encrypted with the matching public key. Using RSA, messages travelling between two points are encrypted and authenticated. RSA tokens are used to provide a rolling password for one-time use.

Triple DES or 3DES is a symmetric algorithm, which means the key used to encrypt is identical to the key used to decrypt. Triple DES is a later version of Data Encryption Standard (DES) that performs three rounds of encryption. The encryption and decryption process performed by 3ES takes longer due to the higher processing power required.

While El Gamal is a public key or asymmetric cipher, it is not the most widely used.

AES is a symmetric algorithm that is currently the best encryption algorithm available commercially.
Advanced Encryption Algorithm that is currently the best encryption algorithm available commercially. The Advanced Encryption Standard (AES) uses 128-bit, 192bit, and 256-bit encryption keys.

Objective: Cryptography
Sub-objective: Describe the security impact of these commonly used encryption algorithms and secure communications protocols: DES, 33DES, AES, AES256CTR, RSA, DSA, SSH, SSL/TLS.

Reference: https://www.techopedia.com/definition/21852/rsa-encryption

QUESTION 9
Which of the following provides the ability to allow scripting languages to manage Windows computers both locally and remotely?

A. STP
B. RMI
C. EMI
D. WMI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Windows Management Instrumentation (WMI) consists of a set of extension that allow access to settings and information through the command line, making the scripting of operations possible. The command-line interface to WMI called Windows Management Instrumentation Command-line (WMI).

Electromagnetic interference (EMI) is the inference with data traversing cables by strong electromagnetic energy generated by sources such as machinery. The transformers in fluorescent lighting systems are a common cause of network communications problems. If a network cable that is highly susceptible to EMI, such as unshielded-twisted pair (UTP) cable, is placed near lighting transformers, then the magnetic field produced by the transformers can cause network communications problems. You can replace UTP cable that runs near sources of EMI with shielded cable, such as shielded twisted-pair 9STP) cable or coaxial cable. Fiber-optic cable is immune to EMI.

Radio frequency interference (RFI) occurs near sources of high power radio transmissions. TV stations, radio stations, cellular telephones, and CB radios can be sources of RFI. RFI can cause network communications problems, and intermittent computer problems such as spontaneously rebooting computers and data errors.

Spanning tree protocol (STP) is a loop avoidance protocol used with switches. Switching loops occur when multiple Layer 2 paths to a network cause to flood broadcasts endlessly. This endless broadcast flood is called a “broadcast storm”, and it causes severe network congestion. STP can be used to prevent these problems on a switched or bridged network.

Objective: Host-Based Analysis
Sub-Objective: Define terms as they pertain to Microsoft Windows: Processes, Threads, Memory allocation, Windows Registry, WMI, Handles, Services

Reference: https://docs.microsoft.com/en-us/windows/win32/wmisdk/about-wmi

QUESTION 10
What is the function of ARP?

A. resolves IP addresses to MAC addresses
B. resolves host names to IP addresses
C. resolves MAC addresses to IP addresses
D. resolves port numbers to IP addresses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Address resolution Protocol (ARP) resolves IP addresses to MAC addresses. It uses a broadcast mechanism to learn the MAC address of a host known only by its address. The media access control (MAC) address uniquely identifies a node on a network segment. ARP tables show the relationship of IP addresses to MAC addresses and are located on most devices.

There is no mechanism for translating port numbers to IP addresses. The IP address and port number combination of a source or destination is called a socket.

Domain Name System (DNS) is the service that translates host names to IP addresses. DNS uses UDP when resolution queries are sent to a server by a client, but its uses TCP for zone transfers between DNS servers. According to RFC 1035, UDP is the recommended method for queries. A DNS server provides a centralized database of domain name-to –IP address resolutions on a server that other computers on a network can use for name resolution.

There is currently no service that resolves MAC addresses to IP addresses.

Objective: Network Concepts

Sub-Objective: Describe the operation of these network services: ARP, DNS, DHCP

Reference: https://www.lifewire.com/address-resolution-protocol-817941

QUESTION 11
Which hashing algorithm is the strongest?

A. SHA-1
B. MD5
C. SHA-256
D. SHA-512

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: SHA-512 is a more secure version of SHA-256 and differs only in the number of rounds of computation.

MD5 is the least secure of the listed hashing algorithms. MD5 is a one-way hashing algorithm. One-way hashing inserts a string of variable length into a hashing algorithm and produces a hash value of fixed length. This hash is appended to the end of the message being sent. The receiver recomputes the hash by using the same computational logic. If the recomputed hash value is the same as the generated hash value, the message was not altered during the course of transmission.

SHA-1 is the first version of SHA and is the least secure version of SHA hashing algorithm. The MD5 algorithm produces 128-bit checksums, and SHA produces 160-bit checksums.

The SHA-256 hashing algorithm is part of the SHA-2 family. SHA-256, also referred to as SHA-2, is a newer version of SHA and uses 256-bit checksum.

Objective: Cryptography
Sub-Objective: Describe the security impact of these commonly used hash algorithms: MD5, SHA-1, SHA-256, SHA-512

Reference: https://movable-type.co.uk/scripts/sha256.html

QUESTION 12
Which of the following is NOT an email protocol?

A. SMTP
B. IMAP
C. NTP
D. POP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Network Time Protocol (NTP) is used to synchronize the clock of computers on the network. Synchronization of time is important in areas such as event logs, billing services, e-commerce, banking and HIPAA Security Rules.

Simple Mail Transport Protocol (SMTP) is an application protocol, so it operates at the top layer of the OSI model. SMTP is the default protocol for sending e-mail in Microsoft operating systems. SMTP provides client and server functions and works with the Internet and UNIX. it is used to send and receive messages.

Post Office Protocol version 3 (POP3) and Internet Mail Access Protocol 4 (IMAP4) are client email programs. They are used to retrieve email from the server. POP3 and IMAP are the most popular protocols for receiving e-mail protocols.

The following is a list of the common ports in use:

- TCP Port 20 – FTP (File transfer Protocol) data
- TCP Port 21 – FTP
- TCP Port 22 – Secure Shell (ssh), Secure Copy (scp), or Secure FTP (SFTP)
- TCP Port 23 – Telnet
- TCP Port 25 – Simple Mail Transfer Protocol (SMTP)
- TCP/UDP Port 53 – Domain Name System (DNS)
- UDP Port 67 Dynamic Host Configuration Protocol (DHCP) Server
- UDP Port 68 Dynamic Host Configuration Protocol (DHCP) Client
- TCP Port 80 HyperText Transfer Protocol (HTTP)
- TCP Port 110 – Post Office Protocol version 3 (POP3)
- TCP Port 123 – Network Time Protocol (NTP)
- TCP Port 143 – Internet Mail Access Protocol

Objective: Security Monitoring
Sub-Objective: Describe the function of these protocols in the context of security monitoring: DNS, NTP, SMTP/POP/IMAP, HTTP/HTTPS

Reference: http://www.emailaddressmanager.com/tips/protocol.html

QUESTION 13
You are reading the output of a Syslog message. What type of information is contained in the facility section?

A. message type (UDP or TCP)
B. process that submitted the message
C. relationship to other messages
D. security level

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The facility section identifies the process or application that submitted the message.
The relationship to other messages is contained in the priority section.
The security level of the message is contained in the severity section.
The message type is contained in the transport section.

Syslog messages and SNMP traps trigger notification messages that can be sent via email and SMS. A syslog server receives and stores log messages sent from syslog clients. A syslog client sends logging information to a syslog server. A syslog server ensures that a network administrator can review device error information from a central location.

Objective: Host-Based Analysis
Sub-Objective: Interpret these operating system log data to identify an event: Windows security event logs, Unix-based syslog, Apache access logs, IIS access logs

Reference: http://www.solarwinds.com/documentation/kiwi/help/syslog/index.html?protocol_levels.htm

QUESTION 14
Which of the following is NOT an event category in the Windows Security Log?

A. Account management
B. Logoff events
C. Object access
D. Directory service access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

While there is a category called Logon events (which will also contain logoff vents), there is no Logoff events category. This category records all local logons and logoffs both successful and unsuccessful.

Object access records all attempts to access resources such as files and folders. Account management records all attempts to make changed to user accounts. Directory service access records all attempts to make changes to Active Directory.

Objective: Host-Based Analysis
Sub-Objective: Interpret these operating system log data to identify an event: Windows security event logs, Unix-based syslog, Apache access logs, IIS access logs

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/manage-auditing-and-security-log

QUESTION 15
Which of the following is most likely to be used in a reflected DoS attack?

A. NTP
B. STP

C. ARP
IGMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Network Time Protocol (NTP) servers are often used in a reflected attack, which if an attack bounced off a third to hit the target. This helps to hide the source of the attack. NTP is used to synchronize the clocks of computers on the network. Time synchronization is important in areas such as event logs, billing services, ecommerce, banking, and HIPAA security rules.

While spanning tree protocol can be used in network attacks on switches, it is not a DoS type attack. STP uses the Spanning Tree Algorithm (STA) to help a switch or bridge by allowing only one active path at a time. STP can prevent network congestion and broadcast storms.

There are two types of STP: spanning tree (802.1d) and rapid spanning tree (802.1w). 802.1d is an older standard that was designed when a minute or more of lost connectively was considered acceptable downtime.

Address resolution protocol (ARP) is also used in attacks, especially man in the middle, but it is not a DoS attack. ARP tables show the relationship of IP address to MAC address. But they cannot be used for DNS and DHCP integration.

Internet Group Messaging Protocol (IGMP) is not typically used in network attacks.

Objective: Attack Methods
Sub-Objective: Describe these network attacks: Denial of service, Distributed denial of service, Man-in-the-middle.

Reference: https://www.imperva.com/learn/application-security/ntp-amplification/?utm_campaign=Incapsula-moved

QUESTION 16
Which of the following represents a single set of sequential machine-code instructions that the processor executes?

A. forks
B. processes
C. threads
D. handles

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

A thread represents a single set of sequential machine-code instructions that the processor executes. A thread also may be thought of as a subset of a process, as a process may have multiple threads. Multithreading is when the processor can operate on more than one thread at a time.

A process is a single application as seen from the perspective of the processor. Multithreading is the operation of more than one process at a time.

Handles are logical associations with a shared resource like a file. When a thread opens a file, it establishes a “handle” to the file.

A fork is an operation whereby a process creates a copy of itself. The fork operation creates a separate address space for the child. The child process has an exact copy of all the memory segments of the parent process.

Objective: Host-Based Analysis
Sub-Objective: Define these terms as they pertain to Microsoft Windows: Processes, threads, memory allocation, Windows Registry, WMI, Handles, Services
Reference: https://whatis.techtarget.com/definition/thread

QUESTION 17
Which algorithm is a symmetric cipher?

A. ECC
B. El Gamai
C. 3DES
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Triple DES or 3DES is symmetric algorithm, which means they key used to encrypt is identical to the key used to decrypt. Triple DES is a later version of DES that performs three rounds of encryption. A 3DES takes longer due to the higher processing power required. Data Encryption Standard (DES) is also symmetric.

The other algorithms are all asymmetric. Asymmetric cryptography involves the use of different keys to encrypt and decrypt the data. These keys are referred to as private and public keys, respectively. The public encryption key is used to ensure only the intended recipient can decrypt the cipher text. These algorithms use two

keys that do not match, but are mathematically related such that if encryption is performed using one, the other is used for decryption. Asymmetric algorithms include Diffie-Hellman, RSA, EIGamal, Elliptic Curve Cryptosystem (ECC), CAST, and Knapsack.

EIGamal is an asymmetric public key encryption algorithm based on the Diffie-Hellman key agreement. It is used for digital signatures, encryption of data, and key exchange.

Rivest, Shamir, and Adleman (RSA) is used as the worldwide de facto standard for digital signatures. RSA is a public key algorithm that provides both encryption and authentication.

Elliptic Curve Cryptosystem (ECC) serves as an alternative to the RSA algorithm and provides similar functionalities, but ECC has a higher strength per bit than RSA.

Objective: Cryptography
Sub-Objective: Describe the security impact of these commonly used encryption algorithms and secure communications protocols: DES, 3DES, AES, AES256CTR, RSA, DSA, SSH, SSL/TLS

Reference: https://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explained

QUESTION 18
Which statement is FALSE with respect to access lists?

A. every rule is examined before a decision is made
B. the order of the rules is important
C. the rule in the list are examined from top to bottom
D. the first rule match is applied

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Every rule is NOT necessarily examined. An access list is a list of rules defined in a specific order. The rules are examined from the top of the list to the bottom. When one of the rules is encountered which matches the traffic type of the packet being examined, the action specified in that rule is taken and no more rules are examined.

The order of the rules is important. For example, examine this set of conceptual rules:

Allow traffic from subnet 192.168.5.0/24
Deny traffic from 192.168.5.5/24

The second rule would never be invoked because the first rule would always match the traffic of 192.168.5.5.

If all of the rules in a set are examined and none match the traffic type, the packet will be disallowed by an implied deny all at the end of each set. To counteract that, most of the time we configure an allow at the end of the set to counteract this implied rule.

Objective: Network Concepts
Sub-Objective: Describe the operation of ACLs applied filters on the interfaces of network devices

Reference: http://www.ciscopress.com/articles/article.asp?p=1697887

QUESTION 19
What type of data is displayed in the following output?

Date flow start Duration Proto Scr IP Addr:Port Dst IP Addr: Port Packets Bytes Flows

2010-09-01 00:00:00.459 0.000 UDP 127.0.0.1:24920 -> 192.168.0.1:22126 1 46 1
2010-09-01 00:00:00.363 0.000 UDP 192.168.0.1:22126 > 127.0.0.1:24920 1 80 1

A. firewall log
B. traffic from a tap
C. mirrored traffic
D. NetFlow traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The traffic displayed is from a NetFlow capture. NetFlow can collect IP traffic statistics on all interfaces where NetFlow is enabled, and later export those statistics as netFlow records toward at least one NetFlow collector. Each flow is a unidirectional set of communication processes that share the following.

- Ingress interface
- Source IP address
- Destination IP address
- IP protocol

- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP Type of Service

Traffic from a TAP or traffic mirrored to a SPAN port would not be organized in this way. Its output in a capture tool like Wireshark would provide the ability to open the packet and look at its parts.

A network test access points (TAP) is an external monitoring device that mirrors the traffic that passes between two network nodes. A tap (test access point) is a hardware device inserted at a specific point in the network to monitor data.

The SPAN feature, which is sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer.

A firewall log output would indicate whether traffic was allowed or denied according to the firewall rules, which is not indicated in the output provided.

Objective: Network Concepts
Sub-Objective: Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic.

Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

QUESTION 20
Which of the following provides the C in CIA?

A. redundancy
B. hashing
C. encryption
D. multiple components

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

CIA stands for Confidentiality, Integrity, and Availability. Confidentiality means preventing unauthorized access to data. One method of doing that is with encryption.

Integrity is a security service that ensures that digital files have not been changed. Digital signatures are an example of an integrity security method. A digital signature provides integrity and non-repudiation. Non-repudiation ensures that the data's origin is known. Availability is a security service that protects hardware and data from loss by ensuring that any needed data is available when necessary. Backups are an example of availability.

Redundancy or the use of multiple components increases availability, the A in CIA. Redundancy ensures that there are multiple components increases multiple ways to control the static environment. Redundancy occurs when you have systems in place ready to come online when a system fails.

Hashing algorithms generate hash values which can be compared to identify if data has changed. Protecting data from unauthorized change provides integrity. Hashing algorithms include MD2, MD4, MD5, HAVAL, and all of the Secure Hash Algorithm (SHA) variants.

Using multiple components is a synonym for redundancy.

Objective: Cryptography
Sub-Objective: Describe the uses of encryption algorithms

Reference: https://www.techopedia.com/definition/25830/cia-triad-of-information-security

QUESTION 21
You have been tasked with protecting user's medical records.

What type of information are you protecting?

A. PCI-DSS
B. PII
C. PHI
D. HIPAA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Medical records are considered Personal Health Information (PHI) and must be protected from unauthorized disclosure.

Personally identifiable (PII) is any piece of information that can be used to uniquely a person, such as full name, account name, phone number, license number, date of birth, social security number, or any other personal attribute.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the act governs the handling of PHI.

The Payment Card Industry Data Security Standard (PCI DSS) protects credit card information, not medical records.

Objective: Security Concepts
Sub-Objective: Describe these terms: Threat actor, Run Book Automation (RBA), Chain of custody (evidentiary), reverse engineering, Sliding windows anomaly detection, PII, PHI

Reference: https://www.getfilecloud.com/blog/2015/03/what-is-pii-and-phi-why-is-it-important/#.XSRUDf5S-Uk

QUESTION 22
What is DNS poisoning?

A. the practice of dispending IP addresses and host names with the goal of traffic diversion
B. the practice of many computers transmitting malformed packets to the DNS server to cause the server to crash
C. the practice of one computer transmitting malformed packets to the DNS server to cause the server to crash
D. the practice of continually sending a DNS server synchronization messages with spoofed packets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

DNS poisoning is the practice of dispensing IP addresses and host names with the goal of traffic diversion. Properly configured DNS security (DNSSES) on the server can provide message validation, which. in turn, would prevent DNS poisoning.

A SYN flood is the practice of continually sending a DNS server synchronization messages with spoofed packets. A SYN flood can transpire when a high number of half-open connections are established to a single computer.

A DNS denial-of-service (DoS) attack is the practice of one computer transmitting malformed packets to the DNS server to cause the server to crash. A DNS distributed DoS (DDoS) attack is the practice of many computers transmitting malformed packets to the DNS server to cause the server to crash.

Address resolution Protocol (ARP) poisoning is similar to DNS poisoning. In this attack, a malicious actor sends falsified ARP messages over a local area network.

In a domain hijacking attack, the registration of a domain name is changed without the permission of the original registrant.

Objective: Security Monitoring
Sub-Objective: Describe the function of these protocols in the context of security monitoring: DNS, NTP, SMTP/POP/IMAP, HTTP/HTTPS

Reference: https://adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf

QUESTION 23

Which of the following is defined by the NIST in the FIPS 180-4 standard?

A. SHA-1
B. MD5
C. SHA-256
D. SHA-512

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The SHA-256 hashing algorithm is defined in the FIPS 180-4 standard by the NIST. It is part of the SHA-2 family. The purpose of Secure Hash Algorithm (SHA) is to protect message integrity.

SHA-256, also referred to as SHA-2, is a newer version of SHA and uses 256-bit checksums. SHA-256 should be used with a disk image to protect the image's integrity so that image can be retained for forensic purposes.

MD5 is hashing algorithm but it is not defined in the FIPS 180-4 standard by the NIST. MD5 is the least secure of the listed hashing algorithms. MD5 is a one-way hashing algorithm. One-way hashing refers to inserting a string of variable length into a hashing algorithm and producing a hash value of fixed length. This hash is appended to the end of the message being sent. This hash value is recomputed at the receivers end in the same fashion in which it was created by using the same computational logic. If the recomputed hash value is the same as the generated hash value, the message was not altered during the course of transmission.

Secure hash algorithm (SHA)-1 is the first version of SHA, and is the least secure version of SHA hashing algorithm. SHA-1 is a hashing algorithm that creates a message digest, which can be used to determine whether a file has been changed since the message digest was created. An unchanged message should create the same message digest on multiple passes through a hashing algorithm. it is not defined in the FIPS 180-4 standard by the NIST.

SHA-512 is a more secure version of SHA-256 and differs only in the number of rounds of computation. It is not defined in the FIPS 180-4 standard by the NIST.

Objective: Cryptography
Sub-Objective: Describe the uses of a hash algorithm

Reference: https://movable-type.co.uk/scripts/sha256.html

QUESTION 24
You are examining NetFlow records. What is the state of the connection when you receive a packet with the RST flag set in response to a packet with the SYN flag set?

A. the port is open
B. the port is blocked by the firewall
C. the connection is set up
D. the port is closed

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Receiving a packet with the RST flag in response to a packet with the SYN flag means the port is closed. When a port is closed, the device answers back with a TCP packet with the RST flag set.

If the port were open, the response packet would have the SYN and ACK flags set.

Transmission Control Protocol (TCP) is a session-oriented or connection-based protocol. It uses a three-way handshake to ensure that every packet sent is successfully received and acknowledged by the destination. The handshake is performed at the start of each session by TCP, and contains a set of three segments (TCP "packets").

- The sender sends the first segment to the receiver with the Synchronization (SYN) flag enabled.
- Step two: The receiver sends the second segment back to the sender with both the Acknowledgement flag (ACK) and the Synchronization (SYN) flag enabled.
- Step three: The sender sends the third segment back to the receiver with just the Acknowledgement (ACK) flag enabled (in response to the server's Synchronization request).

Were the connection successfully set up, the response packet would have the ACK flag set.

If the port were blocked by the firewall, there would be no response. Firewalls do not send diagnostic or error messages when blocking a transmission.

Objective: Security Monitoring
Sub-Objective: Identify the types of data provided by these technologies: TCP Dump, NetFlow, Next-Gen firewall, Traditional stateful firewall, Application visibility and control, Web content filtering, Email content filtering.

Reference: https://www.lifewire.com/introduction-to-port-scanning-2486802

QUESTION 25
In which access control model does the owner of the resource decide who has access to the resource?

A. MAC

B. RBAC
C. DAC
D. NDAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Discretionary access control is used when the data owner configures the appropriate permission for each user.

In the mandatory access control model (MAC), a central assigns a sensitivity label to each document, such as secret, top secret, and so on. Users can access sensitivity levels to which they have been given access. The least privilege principle is most commonly associated with mandatory access control. Under MAC, only an administrator can change the category or classification of a subject or object.

In the non-discretionary access control (NDAC) model, a central body decides which users have access to which documents.

In role-based access control (RBAC), access is based on the job roles to which a user belongs.

Objective: Security Concepts
Sub-Objective: Compare and contrast these access control models: Discretionary access control, mandatory access control, Nondiscretionary access control

Reference: https://pdfs.semanticscholar.org/45a2/775770d870b8675fb1301919224c9bcb7361.pdf