

CS0-001.exam.125q

Number: CS0-001  
Passing Score: 800  
Time Limit: 120 min



**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://vceplus.com/>

CS0-001

CompTIA CSA+ Certification Exam

Exam A

#### QUESTION 1

A vulnerability scan has returned the following information:

```
Detailed Results
10.10.10.214 (LOTUS-10-214)
```

```
Windows Shares
Category: Windows
CVE ID: -
Vendor Ref: -
Bugtraq ID: -
Service Modified - 4.16.2014
```

```
Enumeration Results:
print$      C:\windows\system32\spool\drivers
ofcscan     C:\Program Files\Trend Micro\OfficeScan\PCCSRV
Temp       C:\temp
```

Which of the following describes the meaning of these results?

- A. There is an unknown bug in a Lotus server with no Bugtraq ID.
- B. Connecting to the host using a null session allows enumeration of share names.
- C. Trend Micro has a known exploit that must be resolved or patched.
- D. No CVE is present, so it is a false positive caused by Lotus running on a Windows server.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

## QUESTION 2

A cybersecurity analyst is conducting a security test to ensure that information regarding the web server is protected from disclosure. The cybersecurity analyst requested an HTML file from the web server, and the response came back as follows:

```
HTTP/1.1 404 Object Not Found
Server: Microsoft-IIS/5.0
Date: Tues, 19 Apr 2016 06:32:24 GMT
Content-Type: text/html
Content-Length: 111
<html><head><title>Site Not Found</title></head>
<body>No web site is configured at this address. </body></html>
```

Which of the following actions should be taken to remediate this security issue?



<https://vceplus.com/>

- A. Set "Allowlatescanning" to 1 in the URLScan.ini configuration file.
- B. Set "Removeserverheader" to 1 in the URLScan.ini configuration file.
- C. Set "Enablelogging" to 0 in the URLScan.ini configuration file.
- D. Set "Perprocesslogging" to 1 in the URLScan.ini configuration file.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Reference: <http://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/>



### QUESTION 3

A cybersecurity professional typed in a URL and discovered the admin panel for the e-commerce application is accessible over the open web with the default password. Which of the following is the MOST secure solution to remediate this vulnerability?

- A. Rename the URL to a more obscure name, whitelist all corporate IP blocks, and require two-factor authentication.
- B. Change the default password, whitelist specific source IP addresses, and require two-factor authentication.
- C. Whitelist all corporate IP blocks, require an alphanumeric passphrase for the default password, and require two-factor authentication.
- D. Change the username and default password, whitelist specific source IP addresses, and require two-factor authentication.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 4

An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

[www.vceplus.com - PDF Online](#)

- A. Conduct a risk assessment.
- B. Develop a data retention policy.
- C. Execute vulnerability scanning.
- D. Identify assets.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 5

A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP?

- A. Sponsored guest passwords must be at least ten characters in length and contain a symbol.
- B. The corporate network should have a wireless infrastructure that uses open authentication standards.
- C. Guests using the wireless network should provide valid identification when registering their wireless devices.
- D. The network should authenticate all guest users using 802.1x backed by a RADIUS or LDAP server.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 6

After completing a vulnerability scan, the following output was noted:

```
CVE-2011-3389
QID 42366 - SSLv3.0 / TLSv1.0 Protocol weak CBC mode Server side vulnerability

Check with:

openssl s_client -connect qualys.jive.mobile.com:443 -tls1 -cipher "AES:CAMELLIA:SEED:3DES:DES"
```

Which of the following vulnerabilities has been identified?

- A. PKI transfer vulnerability.
- B. Active Directory encryption vulnerability.
- C. Web application cryptography vulnerability.

D. VPN tunnel vulnerability.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 7**

A security analyst is adding input to the incident response communication plan. A company officer has suggested that if a data breach occurs, only affected parties should be notified to keep an incident from becoming a media headline. Which of the following should the analyst recommend to the company officer?

- A. The first responder should contact law enforcement upon confirmation of a security incident in order for a forensics team to preserve chain of custody.
- B. Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance.
- C. An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a noncompromised recourse.
- D. The HR department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that might be viewed during an investigation.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 8**

A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website?

- A. VPN
- B. Honeypot
- C. Whitelisting
- D. DMZ
- E. MAC filtering

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 9**

A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response?

- A. Correct the audit. This finding is a well-known false positive; the services that typically run on 389 and 636 are identical.
- B. Change all devices and servers that support it to 636, as encrypted services run by default on 636.
- C. Change all devices and servers that support it to 636, as 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks.
- D. Correct the audit. This finding is accurate, but the correct remediation is to update encryption keys on each of the servers to match port 636.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 10**

A security analyst is reviewing IDS logs and notices the following entry:

```
(where email=john@john.com and password=' or 20==20')
```

Which of the following attacks is occurring?



<https://vceplus.com/>

- A. Cross-site scripting
- B. Header manipulation
- C. SQL injection
- D. XML injection

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 11

A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details?

- A. Acceptable use policy
- B. Service level agreement
- C. Rules of engagement
- D. Memorandum of understanding
- E. Master service agreement

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



#### QUESTION 12

A reverse engineer was analyzing malware found on a retailer's network and found code extracting track data in memory. Which of the following threats did the engineer MOST likely uncover?

- A. POS malware
- B. Rootkit
- C. Key logger
- D. Ransomware

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 13

Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team.

Which of the following frameworks would BEST support the program? (Select two)

- A. COBIT
- B. NIST
- C. ISO 27000 series
- D. ITIL
- E. OWASP

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 14

A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following is the MOST likely explanation for this?

- A. The administrator entered the wrong IP range for the assessment.
- B. The administrator did not wait long enough after applying the patch to run the assessment.
- C. The patch did not remediate the vulnerability.
- D. The vulnerability assessment returned false positives.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 15

An incident response report indicates a virus was introduced through a remote host that was connected to corporate resources. A cybersecurity analyst has been asked for a recommendation to solve this issue. Which of the following should be applied?

- A. MAC
- B. TAP
- C. NAC
- D. ACL

**Correct Answer:** C

**Section:** (none)

**Explanation**



**Explanation/Reference:**

Explanation:

**QUESTION 16**

An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server's BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed?

- A. Anti-malware application
- B. Host-based IDS
- C. TPM data sealing
- D. File integrity monitoring

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 17**

A security analyst is reviewing the following log after enabling key-based authentication.

```
Dec 21 11:00:57 comptia sshd[5657]: Failed password for root from
95.58.255.62 port 38980 ssh2
Dec 21 20:08:26 comptia sshd[5768]: Failed password for root from
91.205.189.15 port 38156 ssh2
Dec 21 20:08:30 comptia sshd[5770]: Failed password for nobody from
91.205.189.15 port 38556 ssh2
Dec 21 20:08:34 comptia sshd[5772]: Failed password for invalid user
asterisk from 91.205.189.15 port 38864 ssh2
Dec 21 20:08:38 comptia sshd[5774]: Failed password for invalid user
sjobeck from 91.205.189.15 port 39157 ssh2
Dec 21 20:08:42 comptia sshd[5776]: Failed password for root from
91.205.189.15 port 39467 ssh2
```

Given the above information, which of the following steps should be performed NEXT to secure the system?

- A. Disable anonymous SSH logins.
- B. Disable password authentication for SSH.
- C. Disable SSHv1.
- D. Disable remote root SSH logins.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 18**

A cybersecurity analyst has received a report that multiple systems are experiencing slowness as a result of a DDoS attack. Which of the following would be the BEST action for the cybersecurity analyst to perform?

- A. Continue monitoring critical systems.
- B. Shut down all server interfaces.
- C. Inform management of the incident.
- D. Inform users regarding the affected systems.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:



**QUESTION 19**

A security analyst has been asked to remediate a server vulnerability. Once the analyst has located a patch for the vulnerability, which of the following should happen NEXT?

- A. Start the change control process.
- B. Rescan to ensure the vulnerability still exists.
- C. Implement continuous monitoring.
- D. Begin the incident response process.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 20**

A software assurance lab is performing a dynamic assessment on an application by automatically generating and inputting different, random data sets to attempt to cause an error/failure condition. Which of the following software assessment capabilities is the lab performing AND during which phase of the SDLC should this occur? (Select two.)

- A. Fuzzing
- B. Behavior modeling
- C. Static code analysis
- D. Prototyping phase
- E. Requirements phase
- F. Planning phase

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://www.brighthub.com/computing/smb-security/articles/9956.aspx>

#### QUESTION 21

Law enforcement has contacted a corporation's legal counsel because correlated data from a breach shows the organization as the common denominator from all indicators of compromise. An employee overhears the conversation between legal counsel and law enforcement, and then posts a comment about it on social media. The media then starts contacting other employees about the breach. Which of the following steps should be taken to prevent further disclosure of information about the breach?



<https://vceplus.com/>

- A. Perform security awareness training about incident communication.
- B. Request all employees verbally commit to an NDA about the breach.
- C. Temporarily disable employee access to social media
- D. Have law enforcement meet with employees.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 22

A recent vulnerability scan found four vulnerabilities on an organization's public Internet-facing IP addresses. Prioritizing in order to reduce the risk of a breach to the organization, which of the following should be remediated FIRST? A. A cipher that is known to be cryptographically weak.

- B. A website using a self-signed SSL certificate.
- C. A buffer overflow that allows remote code execution.
- D. An HTTP response that reveals an internal IP address.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

## QUESTION 23

A security professional is analyzing the results of a network utilization report. The report includes the following information:

IP Address	Server Name	Server Uptime	Historical	Current
172.20.2.58	web.srvr.03	30D 12H 52M 09S	41.3GB	37.2GB
172.20.1.215	dev.web.srvr.01	30D 12H 52M 09S	1.81GB	2.2GB
172.20.1.22	hr.dbprod.01	30D 12H 17M 22S	2.24GB	29.97GB
172.20.1.26	mrktg.file.srvr.02	30D 12H 41M 09S	1.23GB	0.34GB
172.20.1.28	acctn.file.srvr.01	30D 12H 52M 09S	3.62GB	3.57GB
172.20.1.30	R&D.file.srvr.01	1D 4H 22M 01S	1.24GB	0.764GB

Which of the following servers needs further investigation?

- A. hr.dbprod.01
- B. R&D.file.srvr.01
- C. mrktg.file.srvr.02
- D. web.srvr.03

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

## QUESTION 24

An alert has been distributed throughout the information security community regarding a critical Apache vulnerability. Which of the following courses of action would ONLY identify the known vulnerability? [Exam Simulator - Download A+ VCE \(latest\) free Open VCE Exams - VCE to PDF Converter - PDF Online](#)

- A. Perform an unauthenticated vulnerability scan on all servers in the environment.
- B. Perform a scan for the specific vulnerability on all web servers.
- C. Perform a web vulnerability scan on all servers in the environment.
- D. Perform an authenticated scan on all web servers in the environment.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 25**

Which of the following commands would a security analyst use to make a copy of an image for forensics use?

- A. dd
- B. wget
- C. touch
- D. rm



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 26**

As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Select two.)

- A. Timing of the scan
- B. Contents of the executive summary report
- C. Excluded hosts
- D. Maintenance windows
- E. IPS configuration
- F. Incident response policies

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 27**

An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

- A. Reports show the scanner compliance plug-in is out-of-date.
- B. Any items labeled 'low' are considered informational only.
- C. The scan result version is different from the automated asset inventory.
- D. 'HTTPS' entries indicate the web page is encrypted securely.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 28**

Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports. Which of the following can be employed to allow this?

- A. ACL
- B. SIEM
- C. MAC
- D. NAC
- E. SAML

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 29**

After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company's computer.

[www.vceplus.com](http://www.vceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

```
16:26:42.943463 IP 192.168.1.10:25 > 10.38.219.20:3389 Flags  
[P.], seq 1768:1901, ack1, win 511, options [nop,nop,TS val  
271989777 ecr 475239494], length 133
```

Which of the following ACLs, if implemented, will prevent further access ONLY to the unauthorized service and will not impact other services?

- A. DENY TCP ANY HOST 10.38.219.20 EQ 3389
- B. DENY IP HOST 10.38.219.20 ANY EQ 25
- C. DENY IP HOST 192.168.1.10 HOST 10.38.219.20 EQ 3389
- D. DENY TCP ANY HOST 192.168.1.10 EQ 25

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 30

The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization?

- A. Recommend setup of IP filtering on both the internal and external interfaces of the gateway router.
- B. Recommend installation of an IDS on the internal interface and a firewall on the external interface of the gateway router.
- C. Recommend installation of a firewall on the internal interface and a NIDS on the external interface of the gateway router.
- D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 31

While a threat intelligence analyst was researching an indicator of compromise on a search engine, the web proxy generated an alert regarding the same indicator. The threat intelligence analyst states that related sites were not visited but were searched for in a search engine. Which of the following MOST likely happened in this situation?

- A. The analyst is not using the standard approved browser.
- B. The analyst accidentally clicked a link related to the indicator.

- C. The analyst has prefetch enabled on the browser in use.
- D. The alert is unrelated to the analyst's search.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 32

An analyst is observing unusual network traffic from a workstation. The workstation is communicating with a known malicious site over an encrypted tunnel. A full antivirus scan with an updated antivirus signature file does not show any sign of infection. Which of the following has occurred on the workstation?

- A. Zero-day attack
- B. Known malware attack
- C. Session hijack
- D. Cookie stealing

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 33

A university wants to increase the security posture of its network by implementing vulnerability scans of both centrally managed and student/employee laptops. The solution should be able to scale, provide minimum false positives and high accuracy of results, and be centrally managed through an enterprise console. Which of the following scanning topologies is BEST suited for this environment?

- A. A passive scanning engine located at the core of the network infrastructure
- B. A combination of cloud-based and server-based scanning engines
- C. A combination of server-based and agent-based scanning engines
- D. An active scanning engine installed on the enterprise console

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



**QUESTION 34**

A cybersecurity analyst is completing an organization's vulnerability report and wants it to reflect assets accurately. Which of the following items should be in the report?

- A. Processor utilization
- B. Virtual hosts
- C. Organizational governance
- D. Log disposition
- E. Asset isolation

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 35**

A threat intelligence feed has posted an alert stating there is a critical vulnerability in the kernel. Unfortunately, the company's asset inventory is not current. Which of the following techniques would a cybersecurity analyst perform to find all affected servers within an organization?

- A. A manual log review from data sent to syslog
- B. An OS fingerprinting scan across all hosts
- C. A packet capture of data traversing the server network
- D. A service discovery scan on the network

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 36**

A cybersecurity analyst traced the source of an attack to compromised user credentials. Log analysis revealed that the attacker successfully authenticated from an unauthorized foreign country. Management asked the security analyst to research and implement a solution to help mitigate attacks based on compromised passwords. Which of the following should the analyst implement?

- A. Self-service password reset
- B. Single sign-on
- C. Context-based authentication
- D. Password complexity

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 37

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website.

During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.

Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

- A. Transitive access
- B. Spoofing
- C. Man-in-the-middle
- D. Replay

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 38

A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors.

The company decides that it wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client.

Which of the following should the company implement?

- A. Port security
- B. WPA2
- C. Mandatory Access Control
- D. Network Intrusion Prevention

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 39**

Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw. Which of the following attacks has MOST likely occurred?

- A. Cookie stealing
- B. Zero-day
- C. Directory traversal
- D. XML injection

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 40**

Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter. The access records are used to identify which staff members accessed the data center in the event of equipment theft. Which of the following MUST be prevented in order for this policy to be effective?

- A. Password reuse
- B. Phishing
- C. Social engineering
- D. Tailgating

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 41**

A technician receives a report that a user's workstation is experiencing no network connectivity. The technician investigates and notices the patch cable running the back of the user's VoIP phone is routed directly under the rolling chair and has been smashed flat over time. Which of the following is the most likely cause of this issue?

- A. Cross-talk
- B. Electromagnetic interference
- C. Excessive collisions

D. Split pairs

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 42

A technician recently fixed a computer with several viruses and spyware programs on it and notices the Internet settings were set to redirect all traffic through an unknown proxy. This type of attack is known as which of the following?



<https://vceplus.com/>

A. Phishing

B. Social engineering

C. Man-in-the-middle

D. Shoulder surfing

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 43

An application development company released a new version of its software to the public. A few days after the release, the company is notified by end users that the application is notably slower, and older security bugs have reappeared in the new release. The development team has decided to include the security analyst during their next development cycle to help address the reported issues. Which of the following should the security analyst focus on to remedy the existing reported problems?

- A. The security analyst should perform security regression testing during each application development cycle.
- B. The security analyst should perform end user acceptance security testing during each application development cycle.
- C. The security analyst should perform secure coding practices during each application development cycle.
- D. The security analyst should perform application fuzzing to locate application vulnerabilities during each application development cycle.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 44

A security administrator determines several months after the first instance that a local privileged user has been routinely logging into a server interactively as “root” and browsing the Internet. The administrator determines this by performing an annual review of the security logs on that server. For which of the following security architecture areas should the administrator recommend review and modification? (Select TWO).

- A. Log aggregation and analysis
- B. Software assurance
- C. Encryption
- D. Acceptable use policies
- E. Password complexity
- F. Network isolation and separation



**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 45

Which of the following principles describes how a security analyst should communicate during an incident?

- A. The communication should be limited to trusted parties only.
- B. The communication should be limited to security staff only.
- C. The communication should come from law enforcement.
- D. The communication should be limited to management only.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 46**

A web application has a newly discovered vulnerability in the authentication method used to validate known company users. The user ID of Admin with a password of “password” grants elevated access to the application over the Internet. Which of the following is the BEST method to discover the vulnerability before a production deployment? A. Manual peer review

- B. User acceptance testing
- C. Input validation
- D. Stress test the application

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 47**

Which of the following represent the reasoning behind careful selection of the timelines and time-of-day boundaries for an authorized penetration test? (Select TWO).

- A. To schedule personnel resources required for test activities
- B. To determine frequency of team communication and reporting
- C. To mitigate unintended impacts to operations
- D. To avoid conflicts with real intrusions that may occur
- E. To ensure tests have measurable impact to operations

**Correct Answer: AC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 48**

Considering confidentiality and integrity, which of the following make servers more secure than desktops? (Select THREE).

- A. VLANs
- [www.vceplus.com](http://www.vceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

- B. OS
- C. Trained operators
- D. Physical access restriction
- E. Processing power
- F. Hard drive capacity

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 49

Given the following output from a Linux machine:

```
file2cable -i eth0 -f file.pcap
```

Which of the following BEST describes what a security analyst is trying to accomplish?

- A. The analyst is attempting to measure bandwidth utilization on interface `eth0`.
- B. The analyst is attempting to capture traffic on interface `eth0`.
- C. The analyst is attempting to replay captured data from a PCAP file.
- D. The analyst is attempting to capture traffic for a PCAP file.
- E. The analyst is attempting to use a protocol analyzer to monitor network traffic.

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 50

Various devices are connecting and authenticating to a single evil twin within the network. Which of the following are MOST likely being targeted?

- A. Mobile devices
- B. All endpoints
- C. VPNs
- D. Network infrastructure
- E. Wired SCADA devices

**Correct Answer:** A [www.vceplus.com](http://www.vceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <http://www.corecom.com/external/livesecurity/eviltwin1.htm>

**QUESTION 51**

As part of the SDLC, software developers are testing the security of a new web application by inputting large amounts of random data. Which of the following types of testing is being performed?

- A. Fuzzing
- B. Regression testing
- C. Stress testing
- D. Input validation

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 52**

An organization uses Common Vulnerability Scoring System (CVSS) scores to prioritize remediation of vulnerabilities.

Management wants to modify the priorities based on a difficulty factor so that vulnerabilities with lower CVSS scores may get a higher priority if they are easier to implement with less risk to system functionality. Management also wants to quantify the priority. Which of the following would achieve management's objective?

- A.  $(\text{CVSS Score}) * \text{Difficulty} = \text{Priority}$   
Where Difficulty is a range from 0.1 to 1.0 with 1.0 being easiest and lowest risk to implement
- B.  $(\text{CVSS Score}) * \text{Difficulty} = \text{Priority}$   
Where Difficulty is a range from 1 to 5 with 1 being easiest and lowest risk to implement
- C.  $(\text{CVSS Score}) / \text{Difficulty} = \text{Priority}$   
Where Difficulty is a range from 1 to 10 with 10 being easiest and lowest risk to implement
- D.  $((\text{CVSS Score}) * 2) / \text{Difficulty} = \text{Priority}$   
Where CVSS Score is weighted and Difficulty is a range from 1 to 5 with 5 being easiest and lowest risk to implement

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

[www.vceplus.com](http://www.vceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online



A cybersecurity consultant is reviewing the following output from a vulnerability scan against a newly installed MS SQL Server 2012 that is slated to go into production in one week:

**Summary**

The remote MS SQL server is vulnerable to the Hello overflow

**Solution**

Install Microsoft Patch Q316333 or disable the Microsoft SQL Server service or use a firewall to protect the MS SQL port

**References**

MSB: MS02-043, MS02-056, MS02-061

CVE: CVE-2002-1123

BID: 5411

Other: IAVA 2002-B-0007

Based on the above information, which of the following should the system administrator do? (Select TWO).

- A. Verify the vulnerability using penetration testing tools or proof-of-concept exploits.
- B. Review the references to determine if the vulnerability can be remotely exploited.
- C. Mark the result as a false positive so it will show in subsequent scans.
- D. Configure a network-based ACL at the perimeter firewall to protect the MS SQL port.
- E. Implement the proposed solution by installing Microsoft patch Q316333.

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 54**

Which of the following are essential components within the rules of engagement for a penetration test? (Select TWO).

- A. Schedule
- B. Authorization
- C. List of system administrators
- D. Payment terms
- E. Business justification

**Correct Answer:** AB

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 55**

A production web server is experiencing performance issues. Upon investigation, new unauthorized applications have been installed and suspicious traffic was sent through an unused port. Endpoint security is not detecting any malware or virus. Which of the following types of threats would this MOST likely be classified as?

- A. Advanced persistent threat
- B. Buffer overflow vulnerability
- C. Zero day
- D. Botnet

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 56**

Nmap scan results on a set of IP addresses returned one or more lines beginning with "cpe:/o:" followed by a company name, product name, and version. Which of the following would this string help an administrator to identify?

- A. Operating system
- B. Running services
- C. Installed software
- D. Installed hardware

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 57**

A company invested ten percent of its entire annual budget in security technologies. The Chief Information Officer (CIO) is convinced that, without this investment, the company will risk being the next victim of the same cyber attack its competitor experienced three months ago. However, despite this investment, users are sharing their usernames and passwords with their coworkers to get their jobs done. Which of the following will eliminate the risk introduced by this practice?

- A. Invest in and implement a solution to ensure non-repudiation
- B. Force a daily password change
- C. Send an email asking users not to share their credentials
- D. Run a report on all users sharing their credentials and alert their managers of further actions

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 58

A SIEM analyst noticed a spike in activities from the guest wireless network to several electronic health record (EHR) systems. After further analysis, the analyst discovered that a large volume of data has been uploaded to a cloud provider in the last six months. Which of the following actions should the analyst do FIRST?

- A. Contact the Office of Civil Rights (OCR) to report the breach
- B. Notify the Chief Privacy Officer (CPO)
- C. Activate the incident response plan
- D. Put an ACL on the gateway router



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 59

Given the following access log:

```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get  
/js/query-ui/js/?a.aspectRatio:this.originalSize.height%7c%7c1%3ba=e(HTTP/1.1" 403 22
```

```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.height | |  
1;a=e( HTTP/1.1" 303 333
```

```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /scripts/query-ui/js/J);F.optgroup=F .option;F .tbody=F  
.tfoot=F .colorgroup=F .caption=F .thead;F .th=F .td;if (!c.support.htmlSerialize)F._default=(1, HTTP/1.1 "  
403 338
```

Which of the following accurately describes what this log displays?

- A. A vulnerability in jQuery
- B. Application integration with an externally hosted database
- C. A vulnerability scan performed from the Internet
- D. A vulnerability in Javascript

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 60

An ATM in a building lobby has been compromised. A security technician has been advised that the ATM must be forensically analyzed by multiple technicians. Which of the following items in a forensic tool kit would likely be used FIRST? (Select TWO).

- A. Drive adapters
- B. Chain of custody form
- C. Write blockers
- D. Crime tape
- E. Hashing utilities
- F. Drive imager



**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 61

A business-critical application is unable to support the requirements in the current password policy because it does not allow the use of special characters. Management does not want to accept the risk of a possible security incident due to weak password standards. Which of the following is an appropriate means to limit the risks related to the application?



<https://vceplus.com/>

- A. A compensating control
- B. Altering the password policy
- C. Creating new account management procedures
- D. Encrypting authentication traffic

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 62

The Chief Information Security Officer (CISO) has asked the security staff to identify a framework on which to base the security program. The CISO would like to achieve a certification showing the security program meets all required best practices. Which of the following would be the BEST choice?

- A. OSSIM
- B. SDLC
- C. SANS
- D. ISO

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 63

A security analyst is concerned that employees may attempt to exfiltrate data prior to tendering their resignations. Unfortunately, the company cannot afford to purchase a data loss prevention (DLP) system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Select THREE).

- A. Prevent users from accessing personal email and file-sharing sites via web proxy
- B. Prevent flash drives from connecting to USB ports using Group Policy
- C. Prevent users from copying data from workstation to workstation
- D. Prevent users from using roaming profiles when changing workstations
- E. Prevent Internet access on laptops unless connected to the network in the office or via VPN
- F. Prevent users from being able to use the copy and paste functions

**Correct Answer:** ABE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 64

A cybersecurity analyst has identified a new mission-essential function that utilizes a public cloud-based system. The analyst needs to classify the information processed by the system with respect to CIA. Which of the following should provide the CIA classification for the information?

- A. The cloud provider
- B. The data owner
- C. The cybersecurity analyst
- D. The system administrator

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 65

A security analyst wants to scan the network for active hosts. Which of the following host characteristics help to differentiate between a virtual and physical host?

- A. Reserved MACs
- B. Host IPs
- C. DNS routing tables
- D. Gateway settings

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 66**

An executive tasked a security analyst to aggregate past logs, traffic, and alerts on a particular attack vector. The analyst was then tasked with analyzing the data and making predictions on future complications regarding this attack vector. Which of the following types of analysis is the security analyst MOST likely conducting?

- A. Trend analysis
- B. Behavior analysis
- C. Availability analysis
- D. Business analysis

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 67**

A malicious user is reviewing the following output:

```
root:~#ping 192.168.1.137
64 bytes from 192.168.2.1 icmp_seq=1 ttl=63 time=1.58 ms
64 bytes from 192.168.2.1 icmp_seq=2 ttl=63 time=1.45 ms
root: ~#
```

Based on the above output, which of the following is the device between the malicious user and the target?

- A. Proxy
- B. Access point
- C. Switch
- D. Hub

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

A software development company in the manufacturing sector has just completed the alpha version of its flagship application. The application has been under development for the past three years. The SOC has seen intrusion attempts made by indicators associated with a particular APT. The company has a hot site location for COOP. Which of the following threats would most likely incur the BIGGEST economic impact for the company?

- A. DDoS
- B. ICS destruction
- C. IP theft
- D. IPS evasion

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

A security analyst has noticed that a particular server has consumed over 1TB of bandwidth over the course of the month. It has port 3333 open; however, there have not been any alerts or notices regarding the server or its activities. Which of the following did the analyst discover?

- A. APT
- B. DDoS
- C. Zero day
- D. False positive

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 70**

A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and warnings. The analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is generating the same events. The analyst informs the manager of these findings, and the manager explains that these activities are already known and part of an ongoing events. Given this scenario, which of the following roles are the analyst, the employee, and the manager filling?

- A. The analyst is red team.  
The employee is blue team.  
The manager is white team.



- B. The analyst is white team.  
The employee is red team.  
The manager is blue team.
- C. The analyst is red team.  
The employee is white team.  
The manager is blue team.
- D. The analyst is blue team.  
The employee is red team.  
The manager is white team.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://danielmiessler.com/study/red-blue-purple-teams/>

#### QUESTION 71

A technician receives the following security alert from the firewall's automated system:

```
match_time: 10/10/16 16:20:43
serial: 002301028176
device_name: COMPSEC1
type: CORRELATION
scruser: domain\samjones
scr: 10.50.50.150
object_name: Beacon Detection
object_id: 6005
category: compromised-host
severity: medium
evidence: Host repeatedly visited a dynamic DNS domain (17 times).
```

After reviewing the alert, which of the following is the BEST analysis?

- A. This alert is a false positive because DNS is a normal network function.
- B. This alert indicates a user was attempting to bypass security measures using dynamic DNS.
- C. This alert was generated by the SIEM because the user attempted too many invalid login attempts.
- D. This alert indicates an endpoint may be infected and is potentially contacting a suspect host.

Seq	Direction	Source IP/Mask	Dest IP/Mask	Protocol	Src Port
1	In	10.1.1.0/255.255.255.0	172.21.50.5/255.255.255.255	17	0-65535
2	Out	172.21.50.5/255.255.255.255	10.1.1.0/255.255.255.0	17	53-53
3	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	17	3389-3389
4	Out	10.1.1.0/255.255.255.0	10.1.1.0/255.255.255.0	17	0-65535
5	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	3389-3389
6	Out	10.1.1.0/255.255.255.0	10.40.40.0/255.255.255.0	6	0-65535
7	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	0-65535
8	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535
9	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535
10	Any	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	1	0-65535

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



## QUESTION 72

During a review of security controls, an analyst was able to connect to an external, unsecured FTP server from a workstation. The analyst was troubleshooting and reviewed the ACLs of the segment firewall the workstation is connected to:

Based on the ACLs above, which of the following explains why the analyst was able to connect to the FTP server?

- A. FTP was explicitly allowed in Seq 8 of the ACL.
- B. FTP was allowed in Seq 10 of the ACL.
- C. FTP was allowed as being included in Seq 3 and Seq 4 of the ACL.
- D. FTP was allowed as being outbound from Seq 9 of the ACL.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 73

A cybersecurity analyst has several log files to review. Instead of using `grep` and `cat` commands, the analyst decides to find a better approach to analyze the logs. Given a list of tools, which of the following would provide a more efficient way for the analyst to conduct a timeline analysis, do keyword searches, and output a report?

- A. Kali
- B. Splunk
- C. Syslog
- D. OSSIM

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 74

The director of software development is concerned with recent web application security incidents, including the successful breach of a back-end database server. The director would like to work with the security team to implement a standardized way to design, build, and test web applications and the services that support them. Which of the following meets the criteria?

- A. OWASP
- B. SANS
- C. PHP
- D. Ajax



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.synopsys.com/software-integrity/resources/knowledge-database/owasp-top-10.html>

#### QUESTION 75

A company has several internal-only, web-based applications on the internal network. Remote employees are allowed to connect to the internal corporate network with a company-supplied VPN client. During a project to upgrade the internal application, contractors were hired to work on a database server and were given copies of the VPN client so they could work remotely. A week later, a security analyst discovered an internal web-server had been compromised by malware that originated from one of the contractor's laptops. Which of the following changes should be made to BEST counter the threat presented in this scenario?

- A. Create a restricted network segment for contractors, and set up a jump box for the contractors to use to access internal resources.
- B. Deploy a web application firewall in the DMZ to stop Internet-based attacks on the web server.
- C. Deploy an application layer firewall with network access control lists at the perimeter, and then create alerts for suspicious Layer 7 traffic.
- D. Require the contractors to bring their laptops on site when accessing the internal network instead of using the VPN from a remote location.
- E. Implement NAC to check for updated anti-malware signatures and location-based rules for PCs connecting to the internal network.

**Correct Answer:** E

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 76**

While preparing for a third-party audit, the vice president of risk management and the vice president of information technology have stipulated that the vendor may not use offensive software during the audit. This is an example of:

- A. organizational control.
- B. service-level agreement.
- C. rules of engagement.
- D. risk appetite

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 77**

Which of the following is a feature of virtualization that can potentially create a single point of failure?

- A. Server consolidation
- B. Load balancing hypervisors
- C. Faster server provisioning
- D. Running multiple OS instances

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 78**

An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.

Portions of the scan results are shown below:

Finding#5144322

First Time Detected 10 Nov 2015 09:00 GMT-0600

Last Time Detected 10 Nov 2015 09:00 GMT-0600

CVSS Base: 5

Access Path: <https://myOrg.com/maillingList.htm>

Request: <https://myOrg.com/maillingList.aspx?content=volunteer>

Reponse: C:\Documents\MarySmith\maillingList.pdf

Which of the following lines indicates information disclosure about the host that needs to be remediated?

- A. Response: C:\Documents\MarySmith\maillingList.pdf
- B. Finding#5144322
- C. First Time Detected 10 Nov 2015 09:00 GMT-0600
- D. Access Path: <http://myOrg.com/maillingList.htm>
- E. Request: GET <http://myOrg.com/maillingList.aspx?content=volunteer>



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 79

A cybersecurity analyst is hired to review the security posture of a company. The cybersecurity analyst notices a very high network bandwidth consumption due to SYN floods from a small number of IP addresses.

Which of the following would be the BEST action to take to support incident response?

- A. Increase the company's bandwidth.
- B. Apply ingress filters at the routers.
- C. Install a packet capturing tool.
- D. Block all SYN packets.

**Correct Answer:** B

**Section:** (none)

**Explanation**

[www.vceplus.com](http://www.vceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

**Explanation/Reference:****QUESTION 80**

There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis.

Which of the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

- A. Asset inventory of all critical devices
- B. Vulnerability scanning frequency that does not interrupt workflow
- C. Daily automated reports of exploited devices
- D. Scanning of all types of data regardless of sensitivity levels

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 81**

A cybersecurity analyst is conducting packet analysis on the following:

Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010281	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044812	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:43:b3:3f:23:e3
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:43:b3:3f:23:e3

Which of the following is occurring in the given packet capture?

- A. ARP spoofing
- B. Broadcast storm
- C. Smurf attack
- D. Network enumeration

E. Zero-day exploit

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 82

An investigation showed a worm was introduced from an engineer's laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to company policy and technical controls.

Which of the following would be the MOST secure control implement?



<https://vceplus.com/>

- A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.
- B. Implement role-based group policies on the management network for client access.
- C. Utilize a jump box that is only allowed to connect to clients from the management network.
- D. Deploy a company-wide approved engineering workstation for management access.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 83

HOTSPOT

A security analyst performs various types of vulnerability scans.

You must review the vulnerability scan results to determine the type of scan that was executed and determine if a false positive occurred for each device.

**Instructions:**

Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.  
The Linux Web Server, File-Print Server and Directory Server are draggable.

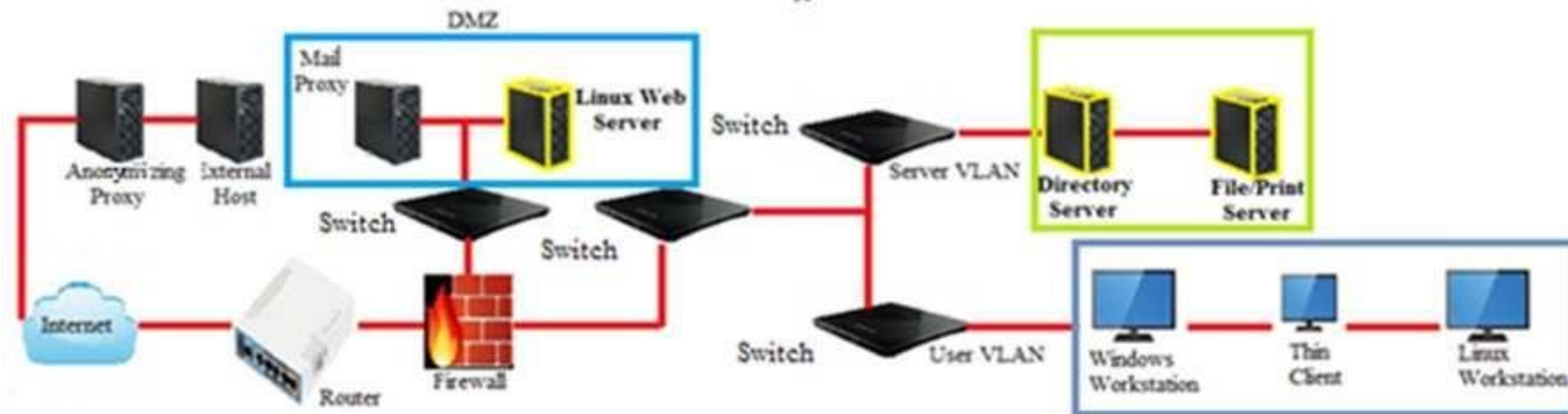
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

**Hot Area:**





Network Diagram



Results Generated	False Positive	Finding Listing1
	<input type="radio"/>	Critical (10.0) 12209 Security Update for Microsoft Windows(835732)
	<input type="radio"/>	Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
	<input type="radio"/>	Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
Credentialed	<input type="radio"/>	Critical (10.0) 58662 Samba 3.x <3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
Non-credentialed	<input type="radio"/>	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Compliance		

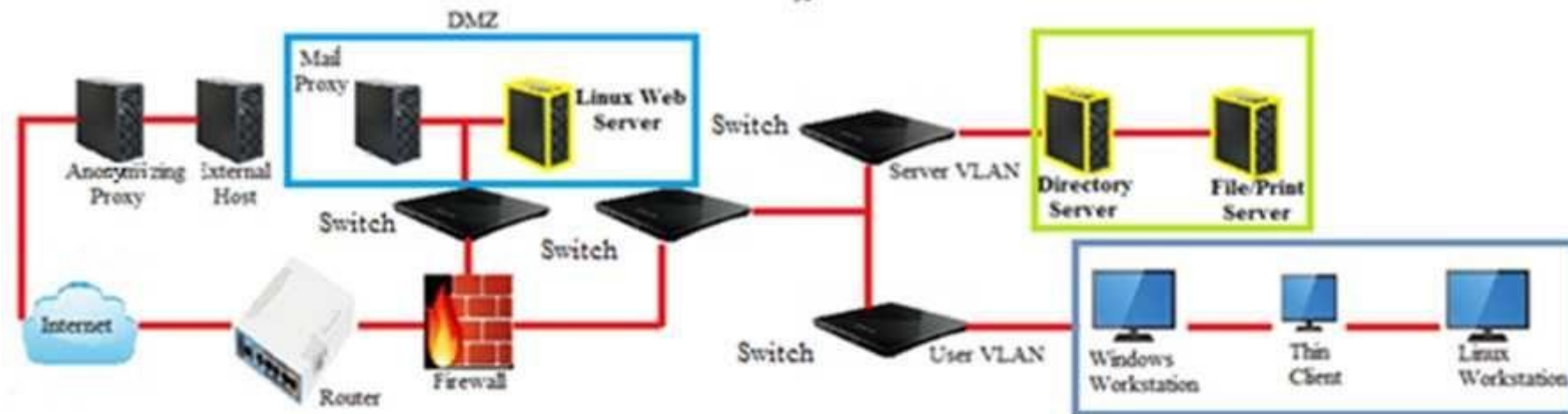
Results Generated	False Positive	Finding Listing1
	<input type="radio"/>	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (BI6423)
	<input type="radio"/>	Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS: Buffer Overrun in Messenger Service (CVE-2016-6035)
	<input type="radio"/>	Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS: php5 vulnerabilities (CVE-2016-362-1)
Credentialed	<input type="radio"/>	Critical (10.0) 27978 Ubuntu 5.04/5.10/6.06 LTS: group vulnerability (CVE-2016-1931)
Non-credentialed	<input type="radio"/>	Critical (10.0) 28017 Ubuntu 5.04/5.10/6.06 LTS: php5 regression CVE-2016-4242)
Compliance		

Results Generated	False Positive	Finding Listing1
	<input type="radio"/>	WARNING (1.0.1) 1.0.1 System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
	<input type="radio"/>	INFORM (1.2.4) 1.2.4 Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
	<input type="radio"/>	INFORM (1.3.4) 1.3.4 Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
Credentialed	<input type="radio"/>	INFORM (1.5.0) 1.5.0 Network access: Let Everyone permissions apply to anonymous users: Disabled
Non-credentialed	<input type="radio"/>	INFORM (1.6.5) 1.6.5 Network access: Sharing and security model for local account: Classic - local users authenticate as themselves
Compliance		

**Correct Answer:**



Network Diagram



Results Generated	False Positive	Finding Listing1
	<input checked="" type="radio"/>	Critical (10.0) 12209 Security Update for Microsoft Windows(835732)
	<input checked="" type="radio"/>	Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
	<input checked="" type="radio"/>	Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
Credentialed	<input checked="" type="radio"/>	Critical (10.0) 58662 Samba 3.x <3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
Non-credentialed	<input checked="" type="radio"/>	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Compliance		

Results Generated	False Positive	Finding Listing1
	<input checked="" type="radio"/>	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (BI6423)
	<input checked="" type="radio"/>	Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS: Buffer Overrun in Messenger Service (CVE-2016-6035)
Credentialed	<input checked="" type="radio"/>	Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS: php5 vulnerabilities (CVE-2016-362-1)
Non-credentialed	<input checked="" type="radio"/>	Critical (10.0) 27978 Ubuntu 5.04/5.10/6.06 LTS: group vulnerability (CVE-2016-1931)
Compliance	<input checked="" type="radio"/>	Critical (10.0) 28017 Ubuntu 5.04/5.10/6.06 LTS: php5 regression CVE-2016-4242)

Results Generated	False Positive	Finding Listing1
	<input checked="" type="radio"/>	WARNING (1.0.1) 1.0.1 System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
Credentialed	<input checked="" type="radio"/>	INFORM (1.2.4) 1.2.4 Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
Non-credentialed	<input checked="" type="radio"/>	INFORM (1.3.4) 1.3.4 Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
Compliance	<input checked="" type="radio"/>	INFORM (1.5.0) 1.5.0 Network access: Let Everyone permissions apply to anonymous users: Disabled
	<input checked="" type="radio"/>	INFORM (1.6.5) 1.6.5 Network access: Sharing and security model for local account: Classic - local users authenticate as themselves

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

1. non-credentialed scan - File Print Server: False positive is first bullet point.
2. credentialed scan – Linux Web Server: No False positives.
3. Compliance scan - Directory Server

**QUESTION 84**

A Chief Information Security Officer (CISO) wants to standardize the company's security program so it can be objectively assessed as part of an upcoming audit requested by management.

Which of the following would holistically assist in this effort?

- A. ITIL
- B. NIST
- C. Scrum
- D. AUP
- E. Nessus



**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

A cybersecurity analyst was hired to resolve a security issue within a company after it was reported that many employee account passwords had been compromised. Upon investigating the incident, the cybersecurity analyst found that a brute force attack was launched against the company.

Which of the following remediation actions should the cybersecurity analyst recommend to senior management to address these security issues?

- A. Prohibit password reuse using a GPO.
- B. Deploy multifactor authentication.
- C. Require security awareness training.
- D. Implement DLP solution.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 86**

Scan results identify critical Apache vulnerabilities on a company's web servers. A security analyst believes many of these results are false positives because the web environment mostly consists of Windows servers.

Which of the following is the BEST method of verifying the scan results?

- A. Run a service discovery scan on the identified servers.
- B. Refer to the identified servers in the asset inventory.
- C. Perform a top-ports scan against the identified servers.
- D. Review logs of each host in the SIEM.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 87**

A security analyst at a small regional bank has received an alert that nation states are attempting to infiltrate financial institutions via phishing campaigns. Which of the following techniques should the analyst recommend as a proactive measure to defend against this type of threat?

- A. Honeypot
- B. Location-based NAC
- C. System isolation
- D. Mandatory access control
- E. Bastion host

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 88**

A cybersecurity analyst is reviewing log data and sees the output below:

```
POST:// payload.php HTTP/1.1
HOST: localhost
Accept: */*
Referrer: http://localhost
*****
HTTP /1.1 403 Forbidden
connection : close
```

Which of the following technologies MOST likely generated this log?

- A. Stateful inspection firewall
- B. Network-based intrusion detection system
- C. Web application firewall
- D. Host-based intrusion detection system

**Correct Answer:** C

**Section:** (none)

**Explanation**



**Explanation/Reference:**

### QUESTION 89

A security analyst is reviewing a report from the networking department that describes an increase in network utilization, which is causing network performance issues on some systems. A top talkers report over a five-minute sample is included.

Source	Destination	Application	Packets	Volume (Kbps)
8.4.4.100	172.16.1.25	SMTP	4386	6141
96.23.114.14	172.16.1.1	IPSec	7734	10827
172.16.1.101	100.15.25.34	HTTP	3412	4776
96.23.114.18	172.16.1.1	IPSec	2723	3812
172.16.1.101	100.15.25.34	SSL	8697	12176
172.16.1.222	203.67.121.12	Quicktime	1302	1822
172.16.1.197	113.121.12.15	8180/tcp	6045	8463
172.16.1.131	172.16.1.67	DHCP	25	35
172.16.1.25	172.16.1.53	DNS	66	93

Given the above output of the sample, which of the following should the security analyst accomplish FIRST to help track down the performance issues?

- A. Perform reverse lookups on each of the IP addresses listed to help determine if the traffic is necessary.



- B. Recommend that networking block the unneeded protocols such as Quicktime to clear up some of the congestion.
- C. Put ACLs in place to restrict traffic destined for random or non-default application ports.
- D. Quarantine the top talker on the network and begin to investigate any potential threats caused by the excessive traffic.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 90

During the forensic phase of a security investigation, it was discovered that an attacker was able to find private keys on a poorly secured team shared drive. The attacker used those keys to intercept and decrypt sensitive traffic on a web server. Which of the following describes this type of exploit and the potential remediation?

- A. Session hijacking; network intrusion detection sensors
- B. Cross-site scripting; increased encryption key sizes
- C. Man-in-the-middle; well-controlled storage of private keys
- D. Rootkit; controlled storage of public keys



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 91

A penetration tester is preparing for an audit of critical systems that may impact the security of the environment. This includes the external perimeter and the internal perimeter of the environment. During which of the following processes is this type of information normally gathered?

- A. Timing
- B. Scoping
- C. Authorization
- D. Enumeration

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:** [www.vceplus.com](http://www.vceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

### QUESTION 92

A red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)

- A. A USB attack that tricks the computer into thinking the connected device is a keyboard, and then sends characters one at a time as a keyboard to launch the attack (a prerecorded series of keystrokes)
- B. A USB attack that turns the connected device into a rogue access point that spoofs the configured wireless SSIDs
- C. A Bluetooth attack that modifies the device registry (Windows PCs only) to allow the flash drive to mount, and then launches a Java applet attack
- D. A Bluetooth peering attack called "Snarfing" that allows Bluetooth connections on blocked device types if physically connected to a USB port
- E. A USB attack that tricks the system into thinking it is a network adapter, then runs a user password hash gathering utility for offline password cracking

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 93

Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting to locate the information on the drive. The PII in question includes the following:

comp@mail.com	564-23-4765
tia@mail.com	754-09-3276
puter@mail.com	143-32-2323
sam@mail.com	545-11-0192
jim@mail.com	093-45-3748

Which of the following would BEST accomplish the task assigned to the analyst?

- A. 3 [0-9]\d-2[0-9]\d-4[0-9]\d
- B. \d(3)-d(2)-\d(4)
- C. ?[3]-?[2]-?[3]
- D. \d[9] 'xxx-xx-xx'

**Correct Answer:** B

**Section:** (none)

**Explanation**



**Explanation/Reference:**

**QUESTION 94**

During which of the following NIST risk management framework steps would an information system security engineer identify inherited security controls and tailor those controls to the system?

- A. Categorize
- B. Select
- C. Implement
- D. Access

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

A security analyst begins to notice the CPU utilization from a sinkhole has begun to spike. Which of the following describes what may be occurring?

- A. Someone has logged on to the sinkhole and is using the device.
- B. The sinkhole has begun blocking suspect or malicious traffic.
- C. The sinkhole has begun rerouting unauthorized traffic.
- D. Something is controlling the sinkhole and causing CPU spikes due to malicious utilization.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 96**

After a recent security breach, it was discovered that a developer had promoted code that had been written to the production environment as a hotfix to resolve a user navigation issue that was causing issues for several customers. The code had inadvertently granted administrative privileges to all users, allowing inappropriate access to sensitive data and reports. Which of the following could have prevented this code from being released into the production environment?

- A. Cross training
- B. Succession planning
- C. Automated reporting

D. Separation of duties

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 97**

A security analyst is assisting with a computer crime investigation and has been asked to secure a PC and deliver it to the forensic lab. Which of the following items would be MOST helpful to secure the PC? (Choose three.)

- A. Tamper-proof seals
- B. Faraday cage
- C. Chain of custody form
- D. Drive eraser
- E. Write blockers
- F. Network tap
- G. Multimeter



**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 98**

A nuclear facility manager determined the need to monitor utilization of water within the facility. A startup company just announced a state-of-the-art solution to address the need for integrating the business and ICS network. The solution requires a very small agent to be installed on the ICS equipment. Which of the following is the MOST important security control for the manager to invest in to protect the facility?

- A. Run a penetration test on the installed agent.
- B. Require that the solution provider make the agent source code available for analysis.
- C. Require through guides for administrator and users.
- D. Install the agent for a week on a test system and monitor the activities.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:** [www.vceplus.com](http://www.vceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

**QUESTION 99**

A staff member reported that a laptop has degraded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization, and outbound network traffic are consuming the laptop resources. Which of the following is the BEST course of actions to resolve the problem? A. Identify and remove malicious processes.

- B. Disable scheduled tasks.
- C. Suspend virus scan.
- D. Increase laptop memory.
- E. Ensure the laptop OS is properly patched.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 100**

A security analyst has discovered that an outbound SFTP process is occurring at the same time of day for the past several days. At the time this was discovered, large amounts of business critical data were delivered. The authentication for this process occurred using a service account with proper credentials. The security analyst investigated the destination IP for this transfer and discovered that this new process is not documented in the change management log. Which of the following would be the BEST course of action for the analyst to take?

- A. Investigate a potential incident.
- B. Verify user permissions.
- C. Run a vulnerability scan.
- D. Verify SLA with cloud provider.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 101**

During an investigation, a computer is being seized. Which of the following is the FIRST step the analyst should take?

- A. Power off the computer and remove it from the network.
- B. Unplug the network cable and take screenshots of the desktop.
- C. Perform a physical hard disk image.

D. Initiate chain-of-custody documentation.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 102

A security analyst has determined the security team should take action based on the following log:

```
Host      192.168.2.7
[00:00:01] successful  login:015 192.168.2.7: local
[00:00:02] unsuccessful login:022 222.34.56.8: RDP 192.168.2.8
[00:00:04] unsuccessful login:010 222.34.56.8: RDP 192.168.2.8
[00:00:06] unsuccessful login:015 222.34.56.8: RDP 192.168.2.8
[00:00:09] unsuccessful login:012 222.34.56.8: RDP 192.168.2.8
```

Which of the following should be used to improve the security posture of the system?

- A. Enable login account auditing.
- B. Limit the number of unsuccessful login attempts.
- C. Upgrade the firewalls.
- D. Increase password complexity requirements.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 103

A medical organization recently started accepting payments over the phone. The manager is concerned about the impact of the storage of different types of data. Which of the following types of data incurs the highest regulatory constraints?

- A. PHI
- B. PCI
- C. PII
- D. IP

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 104**

An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

- A. Reports indicate that findings are informational.
- B. Any items labeled 'low' are considered informational only.
- C. The scan result version is different from the automated asset inventory.
- D. 'HTTPS' entries indicate the web page is encrypted securely.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 105**

A newly discovered malware has a known behavior of connecting outbound to an external destination on port 27500 for the purpose of exfiltrating data. The following are four snippets taken from running `netstat -an` on separate Windows workstations:

**Workstation A:**

Proto	Local Address	Foreign Address	State
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49323	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49324	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49325	EXTERNALIP:27500	ESTABLISHED

Workstation B:

Proto	Local Address	Foreign Address	State
TCP	:::135	:::0	Listening
TCP	:::445	:::0	Listening
TCP	:::27500	:::0	Listening

Workstation C:

Proto	Local Address	Foreign Address	State
TCP	:::135	:::0	Listening
TCP	:::445	:::0	Listening
TCP	:::27500	:::0	Listening

Workstation D:

Proto	Local Address	Foreign Address	State
TCP	10.1.2.5:27500	EXTERNALIP2:443	ESTABLISHED
TCP	10.1.2.5:27501	EXTERNALIP2:443	ESTABLISHED
TCP	10.1.2.5:27502	EXTERNALIP2:443	ESTABLISHED

Based on the above information, which of the following is MOST likely to be exposed to this malware?

- A. Workstation A
- B. Workstation B
- C. Workstation C
- D. Workstation D

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 106

A security analyst received several service tickets reporting that a company storefront website is not accessible by internal domain users. However, external users are accessing the website without issue. Which of the following is the MOST likely reason for this behavior?

- A. The FQDN is incorrect.

- B. The DNS server is corrupted.
- C. The time synchronization server is corrupted.
- D. The certificate is expired.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 107

A security analyst has just completed a vulnerability scan of servers that support a business critical application that is managed by an outside vendor. The results of the scan indicate the devices are missing critical patches. Which of the following factors can inhibit remediation of these vulnerabilities? (Choose two.)



<https://vceplus.com/>

- A. Inappropriate data classifications
- B. SLAs with the supporting vendor
- C. Business process interruption
- D. Required sandbox testing
- E. Incomplete asset inventory

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 108

A security analyst is reviewing packet captures for a specific server that is suspected of containing malware and discovers the following packets:



```
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [SYN] Seq=0 Win=4128 Len=0 MSS=1460
73.252.34.101 138.23.45.201 TCP dns (53) -> 56712 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0
138.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [ACK] Seq=1 Ack=1 Win=4128 Len=0
73.252.34.101 138.23.45.201 SSH Server: Protocol (SSH-2.0-Cisco-1.25)
138.23.45.201 73.252.34.101 SSH Client: Protocol (SSH-1.99-Cisco-1.25)
73.252.34.101 138.23.45.201 SSHv2 Server: Key Exchange Init
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [SYN] Seq=0 Win=65535 Len=0
73.252.34.101 103.34.243.12 TCP ftp (21) -> 62014 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [ACK] Seq=1 Ack=1 Win=65535 Len=0
73.252.34.101 103.34.243.12 FTP Response: 220 ProFTPD 1.3.0a Server
103.34.243.12 73.252.34.101 FTP Request: User FTP
73.252.34.101 103.34.243.12 FTP Response: 331 Anonymous login ok, send your complete email address
as your password.
103.34.243.12 73.252.34.101 FTP Request: Pass ftp
73.252.34.101 103.34.243.12 FTP Response: 230 Anonymous access granted, restrictions apply,
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=
835172936 TSecr=2216538 WS=64
73.252.34.101 202.53.245.78 TCP 8080 -> 57678[SYN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2216543
TSecr=835172936
202.53.245.78 73.252.34.101 HTTP GET /images/layout/logo.png HTTP/1.0
202.53.245.78 73.252.34.101 TCP 57678 -> 8080[ACK] Seq=135 Ack=2897 Win=11648 Len=0 TSval=2216543
TSecr=835172936
```

Which of the following traffic patterns or data would be MOST concerning to the security analyst?

- A. Port used for SMTP traffic from 73.252.34.101
- B. Unencrypted password sent from 103.34.243.12
- C. Anonymous access granted by 103.34.243.12
- D. Ports used for HTTP traffic from 202.53.245.78

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 109

A security analyst discovers a network intrusion and quickly solves the problem by closing an unused port. Which of the following should be completed?

- A. Vulnerability report
- B. Memorandum of agreement



- C. Reverse-engineering incident report
- D. Lessons learned report

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 110

An analyst reviews a recent report of vulnerabilities on a company's financial application server. Which of the following should the analyst rate as being of the HIGHEST importance to the company's environment?

- A. Banner grabbing
- B. Remote code execution
- C. SQL injection
- D. Use of old encryption algorithms
- E. Susceptibility to XSS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 111

A vulnerability analyst needs to identify all systems with unauthorized web servers on the 10.1.1.0/24 network. The analyst uses the following default Nmap scan:

```
nmap -sV -p 1-65535 10.1.1.0/24
```

Which of the following would be the result of running the above command?

- A. This scan checks all TCP ports.
- B. This scan probes all ports and returns open ones.
- C. This scan checks all TCP ports and returns versions.
- D. This scan identifies unauthorized servers.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 112**

Given the following log snippet:

```
Mar 20 10:08:47 superman sshd[1876]: fatal: Unable to negotiate with 192.168.1.166:  
no matching host key type found. Their offer: ssh-dss [preauth]  
  
Mar 20 10:08:47 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]  
  
Mar 20 10:08:47 superman sshd[1895]: Connection closed by 192.168.1.166 [preauth]  
  
Mar 20 10:08:48 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]  
  
Mar 20 10:08:48 superman sshd[1902]: fatal: Unable to negotiate with 192.168.1.166:  
no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
```

Which of the following describes the events that have occurred?

- A. An attempt to make an SSH connection from “superman” was done using a password.
- B. An attempt to make an SSH connection from 192.168.1.166 was done using PKI.
- C. An attempt to make an SSH connection from outside the network was done using PKI.
- D. An attempt to make an SSH connection from an unknown IP address was done using a password.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 113**

Several accounting department users are reporting unusual Internet traffic in the browsing history of their workstations after returning to work and logging in. The building security team informs the IT security team that the cleaning staff was caught using the systems after the accounting department users left for the day. Which of the following steps should the IT security team take to help prevent this from happening again? (Choose two.)

- A. Install a web monitor application to track Internet usage after hours.
- B. Configure a policy for workstation account timeout at three minutes.

- C. Configure NAC to set time-based restrictions on the accounting group to normal business hours.
- D. Configure mandatory access controls to allow only accounting department users to access the workstations.
- E. Set up a camera to monitor the workstations for unauthorized use.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 114**

Creating an isolated environment in order to test and observe the behavior of unknown software is also known as:

- A. sniffing
- B. hardening
- C. hashing
- D. sandboxing

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 115**

A security operations team was alerted to abnormal DNS activity coming from a user's machine. The team performed a forensic investigation and discovered a host had been compromised. Malicious code was using DNS as a tunnel to extract data from the client machine, which had been leaked and transferred to an unsecure public Internet site. Which of the following BEST describes the attack?

- A. Phishing
- B. Pharming
- C. Cache poisoning
- D. Data exfiltration

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

```
nmap -sX 192.168.1.55 -p22,80,445
```

```
45 33.105540 192.168.1.115 192.168.1.55 TCP 54 39007 -> 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
46 33.106599 192.168.1.115 192.168.1.55 TCP 54 39007 -> 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
47 33.107672 192.168.1.115 192.168.1.55 TCP 54 39007 -> 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
48 33.108730 192.168.1.55 192.168.1.115 TCP 54 445 -> 39007 [RST, ACK] Seq=1 Ack=2 Urg=0 Len=0
49 33.108972 192.168.1.55 192.168.1.115 TCP 54 22 -> 39007 [RST, ACK] Seq=1 Ack=2 Urg=0 Len=0
50 34.207377 192.168.1.115 192.168.1.55 TCP 54 39008 -> 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
```

#### QUESTION 116

Which of the following is the MOST secure method to perform dynamic analysis of malware that can sense when it is in a virtual environment?

- A. Place the malware on an isolated virtual server disconnected from the network.
- B. Place the malware in a virtual server that is running Windows and is connected to the network.
- C. Place the malware on a virtual server connected to a VLAN.
- D. Place the malware on a virtual server running SIFT and begin analysis.

**Correct Answer:** A

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### QUESTION 117

Given a packet capture of the following scan:

Which of the following should MOST likely be inferred on the scan's output?

- A. 192.168.1.115 is hosting a web server.
- B. 192.168.1.55 is hosting a web server.
- C. 192.168.1.55 is a Linux server.
- D. 192.168.1.55 is a file server.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 118

While reviewing web server logs, a security analyst notices the following code:

[www.ceplus.com](http://www.ceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

```
GET http://testphp.comptia.org/profiles.php?id=-1 UNION SELECT 1, 2, 3 HTTP/1.1
Host: testphp.comptia.org
```

Which of the following would prevent this code from performing malicious actions?

- A. Performing web application penetration testing
- B. Requiring the application to use input validation
- C. Disabling the use of HTTP and requiring the use of HTTPS
- D. Installing a network firewall in front of the application

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 119

The board of directors made the decision to adopt a cloud-first strategy. The current security infrastructure was designed for on-premise implementation. A critical application that is subject to the Federal Information Security Management Act (FISMA) of 2002 compliance has been identified as a candidate for a hybrid cloud deployment model. Which of the following should be conducted FIRST?

- A. Develop a request for proposal.
- B. Perform a risk assessment.
- C. Review current security controls.
- D. Review the SLA for FISMA compliance.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 120

NOTE: Question IP must be 192.168.192.123


During a network reconnaissance engagement, a penetration tester was given perimeter firewall ACLs to accelerate the scanning process. The penetration tester has decided to concentrate on trying to brute force log in to destination IP address 192.168.192.132 via secure shell.

```
access-list outside-acl permit tcp any host 192.168.192.123 eq https
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq www
access-list outside-acl permit tcp host 192.168.192.123 eq ssh
```

Given a source IP address of 10.10.10.30, which of the following ACLs will permit this access?

- A. 

```
access-list outside-acl permit tcp any host 192.168.192.123 eq https
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq www
```
- B. 

```
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
access-list outside-acl permit tcp host 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
```
- C. 
- D.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 121

An analyst is preparing for a technical security compliance check on all Apache servers. Which of the following will be the BEST to use?

- A. CIS benchmark
- B. Nagios
- C. OWASP
- D. Untidy
- E. Cain & Abel

**Correct Answer:** A

**Section:** (none)

**Explanation**

[www.vceplus.com](http://www.vceplus.com) - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

**Explanation/Reference:**

**QUESTION 122**

A security analyst is performing ongoing scanning and continuous monitoring of the corporate datacenter. Over time, these scans are repeatedly showing susceptibility to the same vulnerabilities and an increase in new vulnerabilities on a specific group of servers that are clustered to run the same application. Which of the following vulnerability management processes should be implemented?

- A. Frequent server scanning
- B. Automated report generation
- C. Group policy modification
- D. Regular patch application

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 123**

Which of the following describes why it is important to include scope within the rules of engagement of a penetration test?

- A. To ensure the network segment being tested has been properly secured
- B. To ensure servers are not impacted and service is not degraded
- C. To ensure all systems being scanned are owned by the company
- D. To ensure sensitive hosts are not scanned

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 124**

A cybersecurity analyst develops a regular expression to find data within traffic that will alarm on a hit.

```
^(?:4[0-9]{12}(?:[0-9]{3})?(?:5[1-5][0-9]{2}))$
```

The SIEM alarms on seeing this data in cleartext between the web server and the database server.

```
'4554-8795-1596-7948'
```

```
'3723-159786-57984'
```



Which of the following types of data would the analyst MOST likely to be concerned with, and to which type of data classification does it belong?

- A. Credit card numbers that are PCI
- B. Social security numbers that are PHI
- C. Credit card numbers that are PII
- D. Social security numbers that are PII

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 125

The development team recently moved a new application into production for the accounting department. After this occurred, the Chief Information Officer (CIO) was contacted by the head of accounting because the application is missing a key piece of functionality that is needed to complete the corporation's quarterly tax returns. Which of the following types of testing would help prevent this from reoccurring?

- A. Security regression testing
- B. User acceptance testing
- C. Input validation testing
- D. Static code testing

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



<https://vceplus.com/>