

CS0-001.exam.85q

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

Comptia CS0-001
CompTIA CSA+ Certification Exam

Exam A

QUESTION 1

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 2

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 3

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 4

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 5

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

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

Check with:

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

Which of the following vulnerabilities has been identified?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 6

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	acctn.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 7

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 8

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 9

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 10

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 11

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 12

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 13

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="password" 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 14

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 15

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 16

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 17

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 18

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 19

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 20

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 HOST 192.168.1.10 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 21

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 22

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 accidentally clicked a link related to the indicator.
- C. The analyst has prefetch enabled on the browser in use.
- D. The alert is unrelated to the analyst's search.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 23

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 24

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 25

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 26

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 27

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