



CertsMania

Free Questions for CAS-005

Shared by Harshita on Dec 2, 2025

For More Free Questions and Preparation Resources

Check the Links on Last Page



CertsMania

Questions # 1:

A vulnerability scan was performed on a website, and the following encryption suites were found:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256  
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256  
TLS_AES_128_GCM_SHA256  
TLS_CHACHA20_POLY1305_SHA256  
TLS_RSA_WITH_AES_128_CBC_SHA  
TLS_AES_128_GCM_SHA256  
TLS_AES_256_GCM_SHA384
```

CertsMania

Which of the following actions will remediate the vulnerability?

Options:

- A.
Removing any ciphers utilizing cipher block chaining
- B.
Rearranging the order of the ciphers from strongest to weakest
- C.
Deploying a WAF to monitor web traffic
- D.
Reissuing new SSL certificates for the website

Answer

A



CertsMania

Questions # 2:

Which of the following best describes the reason a network architect would enable forward secrecy on all VPN tunnels?

Options:

- A.

This process is a requirement to enable hardware-accelerated cryptography.

B.

This process reduces the success of attackers performing cryptanalysis.

C.

The business requirements state that confidentiality is a critical success factor.

D.

Modern cryptographic protocols list this process as a prerequisite for use.

Answer

B

Explanation

Forward secrecy (also known as perfect forward secrecy, PFS) ensures that session keys used in a VPN tunnel are ephemeral, meaning that even if an attacker compromises a long-term private key, past sessions cannot be decrypted. According to the CompTIA SecurityX CAS-005 study guide (Domain 3: Cybersecurity Technology, 3.1), enabling forward secrecy on VPN tunnels reduces the risk of cryptanalysis by ensuring that each session's encryption key is unique and not derived from a single compromised key. This directly mitigates the impact of attacks like key theft or future decryption attempts.

Option A: Forward secrecy is not required for hardware-accelerated cryptography, which depends on processor capabilities, not key management.

Option C: While confidentiality is important, this is too vague and does not specifically explain why forward secrecy is chosen.

Option D: Modern protocols (e.g., TLS 1.3, IPsec with ECDHE) support forward secrecy but do not mandate it as a prerequisite for use.

Option B: This is the most precise, as forward secrecy directly reduces the success of cryptanalysis by limiting the scope of key compromise.

[Reference:, CompTIA SecurityX CAS-005 Official Study Guide, Domain 3: Cybersecurity Technology, Section 3.1: "Explain cryptographic techniques, including perfect forward secrecy.", CAS-005 Exam Objectives, 3.1: "Evaluate the impact of cryptographic configurations on security.", , , ,]

Questions # 3:

A security engineer receives an alert from the threat intelligence platform with the following information:

Email	Source	Date	Data
jane@corporg.com	Third-party leakage	4 weeks ago	Email, name
john@corporg.com	Pastebin	3 weeks ago	Email, password, cell phone
alice@corporg.com	Deep web website	2 months ago	Name, address, cell phone
ann12@hotmail.com	Deep web forum	5 days ago	Email, password
joe@corporg.com	Initial access broker	1 week ago	Email, password

ania

Which of the following actions should the security engineer do first?

Options:

- A.
Reset John's and Joe's access.
- B.
Contact John, Ann, and Joe to inform them about the incident and schedule a password reset.
- C.
Reset John's, Ann's, and Joe's passwords and disconnect all users* active sessions
- D.
Reset John's and Joe's passwords and inform authorities about the leakage.

Answer

A

Explanation



CertsMania

The first action should be to reset access for John and Joe, who are corporate accounts belonging to the organization. Their credentials were exposed in recent leaks, including one from an initial access broker (Joe), which indicates an active exploitation risk. Immediate password resets and session invalidations prevent adversaries from using the compromised credentials to gain access.

Ann's account (@hotmail.com) is personal and not under corporate management, so while her exposure is concerning, it does not pose a direct risk to organizational systems. Contacting her can follow later steps but should not delay urgent remediation for John and

Joe.

Option B delays remediation. Option C overreaches by including Ann in corporate resets. Option D includes contacting authorities prematurely, which is important but secondary to immediate containment.

CAS-005 emphasizes rapid containment of credential leaks affecting corporate identities, making access resets for John and Joe the first step.

Questions # 4:

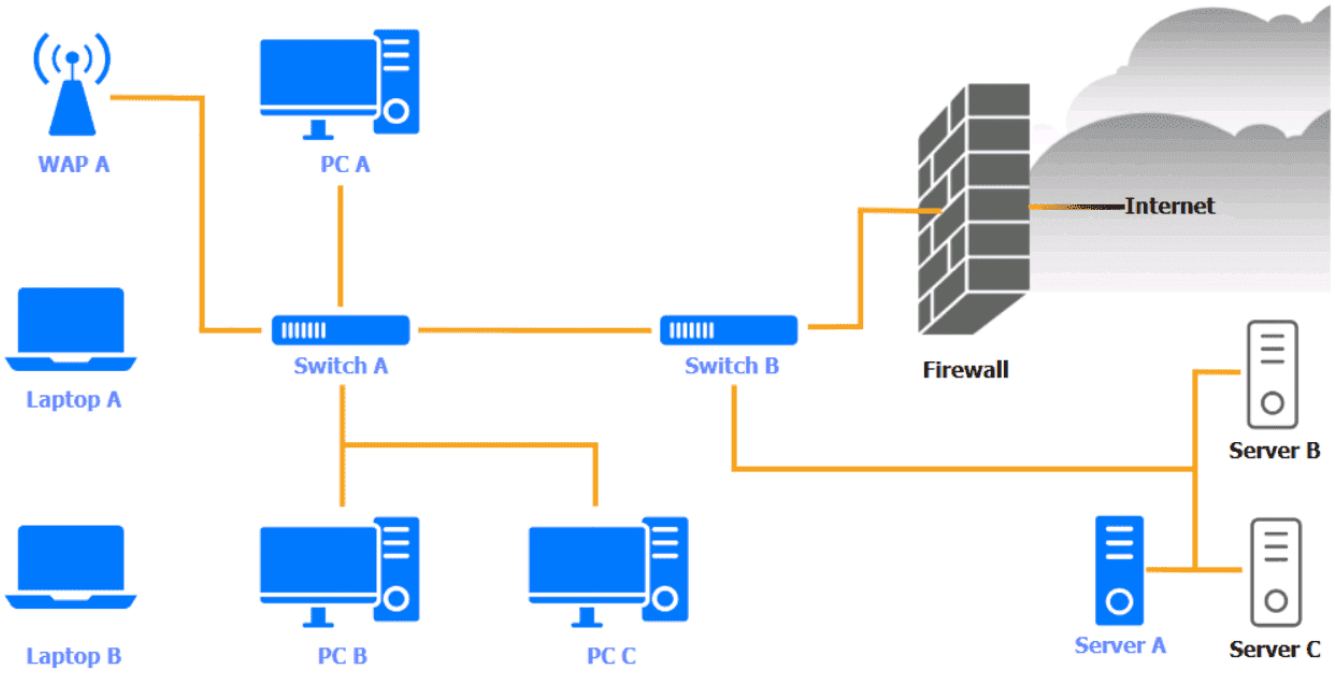
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

- The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
- The SSH daemon on the database server must be configured to listen to port 4022.
- The SSH daemon must only accept connections from a single workstation.
- All host-based firewalls must be disabled on all workstations.
- All devices must have the latest updates from within the past eight days.
- All HDDs must be configured to secure data at rest.
- Cleartext services are not allowed.
- All devices must be hardened when possible.

Instructions:

Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.

Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the PostgreSQL DATABASE VIA ssh



WAP A



CertsMania

WAP A



Finding	Status	Remediation
Firmware	Updated 5 days ago	<input checked="" type="checkbox"/> No issue
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management
SSID broadcast	Disabled	<input type="checkbox"/> Update endpoint protection
Default admin account	Default password has been changed	<input type="checkbox"/> Enabled disk encryption
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device
		<input type="checkbox"/> Enable password complexity
		<input type="checkbox"/> Enable host-based firewall to block all traffic
		<input type="checkbox"/> Antivirus scan
		<input type="checkbox"/> Change default administrative password
		<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

PC A



CertsMania

PC A ✕

OS updates	Updated 2 days ago, last checked 5:08 a.m.	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked 6:11 a.m.	<input type="checkbox"/> Patch management
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	Normal	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Laptop A



CertsMania

Laptop A ✕

OS updates	Updated 3 days ago, last checked 6:08 a.m.	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked in 6:13 a.m.	<input type="checkbox"/> Patch management
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	Medium	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password
Wireless	Enabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Switch A



CertsMania

Switch A
✕

Firmware	Updated 7 days ago	<input checked="" type="checkbox"/> No issue
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management
Interfaces disabled (out of 12)	4	<input type="checkbox"/> Update endpoint protection
Default admin account	Default password has not been changed	<input type="checkbox"/> Enabled disk encryption
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device
		<input type="checkbox"/> Enable password complexity
		<input type="checkbox"/> Enable host-based firewall to block all traffic
		<input type="checkbox"/> Antivirus scan
		<input type="checkbox"/> Change default administrative password
		<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Switch B:



CertsMania

Switch B ✕

Firmware	Updated 7 days ago	<input checked="" type="checkbox"/> No issue
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management
Interfaces disabled (out of 6)	1	<input type="checkbox"/> Update endpoint protection
Default admin account	Default password has been changed	<input type="checkbox"/> Enabled disk encryption
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device
		<input type="checkbox"/> Enable password complexity
		<input type="checkbox"/> Enable host-based firewall to block all traffic
		<input type="checkbox"/> Antivirus scan
		<input type="checkbox"/> Change default administrative password
		<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Laptop B



CertsMania

Laptop B ✕

OS updates	Updated 3 days ago, last checked 8:08 a.m.	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked in 8:11 a.m.	<input type="checkbox"/> Patch management
Browser version	81.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Disabled	<input type="checkbox"/> Enabled disk encryption
Password Complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	Normal	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 8080, 53	<input type="checkbox"/> Change default administrative password
Wireless	Enabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

PC B



CertsMania

PC B ✕

OS updates	Updated 2 days ago, last checked 5:10 a.m.	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked in 6:13 a.m.	<input type="checkbox"/> Patch management
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	Medium	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

PC C



CertsMania

PC C ✕		
OS updates	Updated 22 days ago	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked 6:19 a.m.	<input type="checkbox"/> Patch management
Browser version	91.2.5 (7/18/2022)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	High	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 23, 53	<input type="checkbox"/> Change default administrative password
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Server A



CertsMania

Nmap

IP Tables

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.4
80/tcp    closed http
443/tcp   closed ssl/http
1433/tcp  closed mssql
5432/tcp  closed postgresql
...
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
#iptables --list --verbose

Chain INPUT (policy DROP 5 packets, 341 bytes)

pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- any any anywhere anywhere tcp spts:login:65535 dpt:ssh state NEW,ESTABLISHED
1 28 DROP all -- any any anywhere anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

Options:

Answer

Answer:

See the Explanation below for the solution.

Explanation

WAP A: No issue found. The WAP A is configured correctly and meets the requirements.

PC A = Enable host-based firewall to block all traffic

This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.

Laptop A: Patch management

This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.

Switch A: No issue found. The Switch A is configured correctly and meets the requirements.

Switch B: No issue found. The Switch B is configured correctly and meets the

requirements.

Laptop B: Disable unneeded services

This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.

PC B: Enable disk encryption

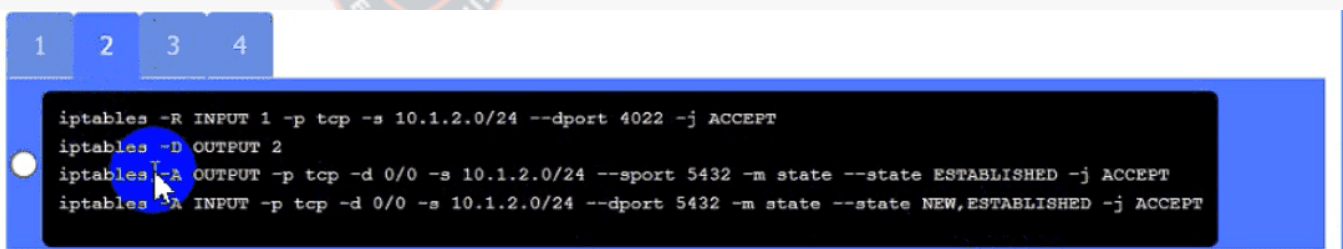
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.

PC C: Disable unneeded services

This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:

```
sudo nano /etc/ssh/sshd_config
```

Server A. Need to select the following:



```
1 2 3 4
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

A black and white screen with white text Description automatically generated

A security professional is investigating a trend in vulnerability findings for newly deployed cloud systems Given the following output:

Date	IP address	System name	Finding	Criticality rating
10/13/2023	10.123.34.98	System1	OpenSSL version 1.01	Medium
10/13/2023	10.3.114.72	System6	OpenSSL version 1.01	Medium
10/13/2023	10.12.134.45	System12	Java 11 runtime environment found	Medium
10/13/2023	10.68.65.11	System36	OpenSSL version 1.01	Medium
10/13/2023	10.23.74.9	System37	Java 11 runtime environment found	Medium
10/13/2023	10.13.124.3	System45	OpenSSL version 1.01	Medium

a

Which of the following actions would address the root cause of this issue?

Options:

A.

Automating the patching system to update base Images

B.

Recompiling the affected programs with the most current patches

C.

Disabling unused/unneeded ports on all servers

D.

Deploying a WAF with virtual patching upstream of the affected systems

Answer

A

Explanation



CertsMania

The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.

A. Automating the patching system to update base images: Automating the patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.

B. Recompiling the affected programs with the most current patches: While this can fix the immediate vulnerabilities, it does not address the root cause of the problem, which is the

lack of regular updates.

C. Disabling unused/unneeded ports on all servers: This improves security but does not address the specific issue of outdated software.

D. Deploying a WAF with virtual patching upstream of the affected systems: This can provide a temporary shield but does not resolve the underlying issue of outdated software.

Automating the patching system to update base images ensures that all deployed systems are using the latest, most secure versions of software, addressing the root cause of the vulnerability trend.

[References:, CompTIA Security+ Study Guide, NIST SP 800-40 Rev. 3, "Guide to Enterprise Patch Management Technologies", CIS Controls, "Control 7: Continuous Vulnerability Management", , , , , ,]

Questions # 6:

A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:

Date & Time	Public IP	Browser Info	Action
11 Dec 22:30:23	192.168.2.45	Mozilla/5.0 (Windows NT 5.1)	Access granted to admin
11 Dec 23:05:43	192.168.2.45	Mozilla/5.0 (Windows NT 5.1)	Access granted to admin
11 Dec 23:10:29	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Access granted to admin
11 Dec 23:12:18	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Logoff
12 Dec 00:05:43	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Access granted to admin

Which of the following actions should the analyst take to best mitigate the threat?

Options:

A.

Implement WAF protection for the web application.

B.

Upgrade the firmware on the camera.

C.

Only allow connections from approved IPs.

D.

Block IP 104.18.16.29 on the firewall.

Answer

C

Explanation



CertsMania

The logs indicate unauthorized access from 104.18.16.29, an external IP, to the building camera's administrative console during off-hours. Restricting access only to approved IP addresses ensures that only authorized personnel can remotely control the cameras, reducing the risk of unauthorized access and manipulation.

Implementing WAF protection (A) secures against web application attacks but does not restrict unauthorized administrative access.

Upgrading the firmware (B) is good security hygiene but does not immediately mitigate the active threat.

Blocking IP 104.18.16.29 (D) is a temporary measure, as an attacker can switch to another IP. A better long-term solution is whitelisting trusted IPs.

[Reference: CompTIA SecurityX (CAS-005) Exam Objectives- Domain 4.0 (Security Operations), Section on Access Control and Network Security, , , ,]

Questions # 7:

A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved to the repository. The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment. Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

Options:

A.

Software composition analysis

B.

Pre-commit code linting

C.

Repository branch protection

D.

Automated regression testing

E.

Code submit authorization workflow

F.

Pipeline compliance scanning



Answer

B, D

Explanation

B. Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.

D. Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.

Other options:

A. Software composition analysis: This helps identify vulnerabilities in third-party components but does not directly address code quality or deployment failures.

C. Repository branch protection: While this can help manage the code submission process, it does not directly prevent deployment failures caused by code issues or security check failures.

E. Code submit authorization workflow: This manages who can submit code but does not address the quality of the code being submitted.

F. Pipeline compliance scanning: This checks for compliance with security policies but does not address syntax or regression issues.

[References:, CompTIA Security+ Study Guide, "Continuous Integration and Continuous Delivery" by Jez Humble and David Farley, OWASP (Open Web Application Security Project) guidelines on secure coding practices, , , , ,]

Questions # 8:

After a penetration test on the internal network, the following report was generated:

Attack Target Result

Compromised host ADMIN01S.CORP.LOCAL Successful

Hash collected KRBTGT.CORP.LOCAL Successful

Hash collected SQLSV.CORP.LOCAL Successful

Pass the hash SQLSV.CORP.LOCAL Failed

Domain control CORP.LOCAL Successful

Which of the following should be recommended to remediate the attack?

Options:

A.

Deleting SQLSV

B.

Reimaging ADMIN01S

C.

Rotating KRBTGT password

D.

Resetting the local domain

Answer

C

Explanation

The attacker gained domain control by collecting the KRBTGT hash (used for Kerberos tickets). Let's evaluate:

A. Deleting SQLSV: Irrelevant since pass-the-hash failed there.

B. Reimaging ADMIN01S: Addresses the compromised host but not domain control.

C. Rotating KRBTGT password:Invalidates stolen Kerberos tickets, mitigating domain control per CAS-005's focus on identity security.

[Reference:CompTIA SecurityX (CAS-005) objectives, Domain 2: Security Operations, covering Kerberos security., , , , ,]

Questions # 9:

Emails that the marketing department is sending to customers are going to the customers' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated. Which of the following should the security team update in order to fix this issue? (Select three).

Options:

A.

DMARC

B.

SPF

C.

DKIM

D.

DNSSEC

E.

SASE

F.

SAN

G.

SOA

Answer

A, B, C

Questions # 10:

A company SIEM collects information about the log sources. Given the following report information:

Device	Type	Time	Status	Function
VM001	Server	10:23:241	UP	Critical
VM002	Server	10:22:323	UP	Normal
NET002	Router	10:23:391	UP	Normal
NET003	IPS	1:45:312	DOWN	Normal
VM003	Server	9:53:783	DOWN	Critical

Which of the following actions should a security engineer take to enhance the security monitoring posture?

Options:

A.

Calibrate the timing on the log sources to enhance event correlation.

B.

Implement a centralized use case library to get alerts based on the type of log sources.

C.

Perform a non-reporting device assessment to collect missing log sources.

D.

Create a resiliency plan to prevent losing event logs from log sources.

Answer

C

Explanation

The SIEM report shows that some devices, such as VM003 (Critical server) and NET003 (IPS), are DOWN and therefore not reporting logs. In security monitoring, the absence of log data from critical systems creates dangerous blind spots. If logs are missing, attacks can proceed undetected, or investigations may lack the data needed for incident response.

The most effective action is to perform a non-reporting device assessment (C). This means identifying and correcting issues where devices fail to send logs, whether due to outages,

misconfigurations, or integration gaps. Ensuring all critical devices, especially servers and intrusion prevention systems, consistently send logs to the SIEM strengthens overall visibility and monitoring posture.

Option A (time calibration) is important for correlation accuracy but does not address missing log feeds. Option B (centralized use case library) enhances detection but only works if the SIEM is receiving complete data. Option D (resiliency plan) helps protect log retention but is irrelevant if logs are never received in the first place.

Therefore, fixing non-reporting log sources is the highest priority to improve monitoring effectiveness.



CertsMania

To Get Premium Files for CAS-005 Visit

<https://www.certsmania.com/comptia/cas-005-practice>

For More Free Questions Visit

<https://www.certsmania.com/comptia/pdf/cas-005>



CertsMania