CAS-005 Q&As

CompTIA SecurityX

Pass CompTIA CAS-005 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A control systems analyst is reviewing the defensive posture of engineering workstations on the shop floor. Upon evaluation, the analyst makes the following observations:

1.

Unsupported, end-of-life operating systems were still prevalent on the shop floor.

2.

There are no security controls for systems with supported operating systems.

3.

There is little uniformity of installed software among the workstations.

Which of the following would have the greatest impact on the attack surface?

A. Deploy antivirus software to all of the workstations.

B. Increase the level of monitoring on the workstations.

C. Utilize network-based allow and block lists.

D. Harden all of the engineering workstations using a common strategy.

Correct Answer: D

QUESTION 2

Which of the following security features do email signatures provide?

A. Non-repudiation

B. Body encryption

C. Code signing

D. Sender authentication

E. Chain of custody

Correct Answer: AD

QUESTION 3

Which of the following industrial protocols is most likely to be found in public utility applications, such as water or electric?

A. CIP

B. Zigbee

C. Modbus

D. DNP3

Correct Answer: D

DNP3 (Distributed Network Protocol 3) is specifically designed for use in SCADA (Supervisory Control and Data Acquisition) systems, which are commonly employed in public utility sectors such as water and electric utilities. DNP3 is known for its robustness in handling communication over long distances and in noisy environments typical of utility operations. It supports features essential for reliable and secure communication, including time synchronization, data integrity checks, and error recovery mechanisms. These capabilities make DNP3 highly suitable for monitoring and controlling remote devices and systems critical to public utilities.

QUESTION 4

A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources The analyst reviews the following information:

User	Source IP	Source location	User assigned location	MFA satisfied?	Sign-in status
SALES1	8.11.4.16	Germany	France	Yes	Blocked
SALES1	8.11.4.16	Germany	France	Yes	Blocked
ACCT1	192.168.4.18	France	France	No	Allowed
SALES1	8.11.4.16	Germany	France	Yes	Blocked
ACCT1	8.11.4.16	Germany	France	Yes	Blocked
SALES2	8.11.4.20	France	France	Yes	Allowed

Which of the following is most likely the cause of the issue?

A. The local network access has been configured to bypass MFA requirements.

B. A network geolocation is being misidentified by the authentication server

C. Administrator access from an alternate location is blocked by company policy

D. Several users have not configured their mobile devices to receive OTP codes

Correct Answer: B

The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements. The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is

assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.

Why Network Geolocation Misidentification?

Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected

locations.

Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked. Consistent Pattern: The user

"SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation. Other options do not align with the pattern observed:

A. Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue. C. Administrator access policy: This is about user access, not specific administrator access.

D. OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.

References:

CompTIA SecurityX Study Guide

"Geolocation and Authentication," NIST Special Publication 800-63B "IP Geolocation Accuracy," Cisco Documentation

QUESTION 5

A security engineer is developing a solution to meet the following requirements?

1.

All endpoints should be able to establish telemetry with a SIEM.

2.

All endpoints should be able to be integrated into the XDR platform.

3.

SOC services should be able to monitor the XDR platform

Which of the following should the security engineer implement to meet the requirements?

A. CDR and central logging

B. HIDS and vTPM

C. WAF and syslog

D. HIPS and host-based firewall

Correct Answer: D

To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems

(HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host- based firewall ensures that only authorized traffic is

allowed, providing an additional layer of security.

References:

CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms. NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention

Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.

"Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

QUESTION 6

After an incident occurred, a team reported during the lessons-learned review that the team.

1.

Lost important Information for further analysis.

2.

Did not utilize the chain of communication

3.

Did not follow the right steps for a proper response

Which of the following solutions is the best way to address these findinds?

A. Requesting budget for better forensic tools to Improve technical capabilities for Incident response operations

B. Building playbooks for different scenarios and performing regular table-top exercises

C. Requiring professional incident response certifications tor each new team member D. Publishing the incident response policy and enforcing it as part of the security awareness program

Correct Answer: B

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here\\'s why: Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence. Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents. Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan. Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared. References: CompTIA Security+ Study Guide NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide" SANS Institute, "Incident Handler\\'s Handbook"

QUESTION 7

A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise.

Which of the following is the most secure way to achieve this goal?

A. Executing a script that deletes and overwrites all data on the SSD three times

B. Wiping the SSD through degaussing

C. Securely deleting the encryption keys used by the SSD

D. Writing non-zero, random data to all cells of the SSD

Correct Answer: C

The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively

unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.

References:

CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data. NIST Special Publication 800-88, "Guidelines for Media Sanitization":

Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

QUESTION 8

The identity and access management team is sending logs to the SIEM for continuous monitoring. The deployed log collector is forwarding logs to the SIEM. However, only false positive alerts are being generated.

Which of the following is the most likely reason for the inaccurate alerts?

A. The compute resources are insufficient to support the SIEM

B. The SIEM indexes are 100 large

C. The data is not being properly parsed

D. The retention policy is not property configured

Correct Answer: C

Proper parsing of data is crucial for the SIEM to accurately interpret and analyze the logs being forwarded by the log collector. If the data is not parsed correctly, the SIEM may misinterpret the logs, leading to false positives and inaccurate alerts. Ensuring that the log data is correctly parsed allows the SIEM to correlate and analyze the logs effectively, which is essential for accurate alerting and monitoring.

QUESTION 9

Two companies that recently merged would like to unify application access between the companies, without initially merging internal authentication stores. Which of the following technical strategies would best meet this objective?

A. Federation

B. RADIUS

C. TACACS+

D. MFA

E. ABAC

Correct Answer: A

Federation (option A) is the best technical strategy for allowing two recently merged companies to unify application access while keeping their internal authentication stores separate. It provides a secure, seamless, and standardized approach to authentication and authorization across organizational boundaries, ensuring efficient and controlled access to shared applications and resources.

QUESTION 10

A security analyst received a notification from a cloud service provider regarding an attack detected on a web server The cloud service provider shared the following information about the attack:

1.

The attack came from inside the network.

2.

The attacking source IP was from the internal vulnerability scanners.

3.

The scanner is not configured to target the cloud servers.

Which of the following actions should the security analyst take first?

A. Create an allow list for the vulnerability scanner IPs m order to avoid false positives

B. Configure the scan policy to avoid targeting an out-of-scope host

C. Set network behavior analysis rules

D. Quarantine the scanner sensor to perform a forensic analysis

Correct Answer: D

When a security analyst receives a notification about an attack that appears to originate from an internal vulnerability scanner, it suggests that the scanner itself might have been compromised. This situation is critical because a compromised scanner can potentially conduct unauthorized scans, leak sensitive information, or execute malicious actions within the network. The appropriate first action involves containing the threat to prevent further damage and allow for a thorough investigation. Here\\'s why quarantining the scanner sensor is the best immediate action: Containment and Isolation: Quarantining the scanner will immediately prevent it from continuing any malicious activity or

scans. This containment is crucial to protect the rest of the network from potential harm. Forensic Analysis: By isolating the scanner, a forensic analysis can be performed to understand how it was compromised, what actions it took, and what data or systems might have been affected. This analysis will provide valuable insights into the nature of the attack and help in taking appropriate remedial actions. Preventing Further Attacks: If the scanner is allowed to continue operating, it might execute more unauthorized actions, leading to greater damage. Quarantine ensures that the threat is neutralized promptly. Root Cause Identification: A forensic analysis can help identify vulnerabilities in the scanner\\'s configuration, software, or underlying system that allowed the compromise. This information is essential for preventing future incidents. Other options, while potentially useful in the long term, are not appropriate as immediate actions in this scenario:

A. Create an allow list for the vulnerability scanner IPs to avoid false positives:

This action addresses false positives but does not mitigate the immediate threat posed by the compromised scanner.

B. Configure the scan policy to avoid targeting an out-of-scope host: This step is preventive for future scans but does not deal with the current incident where the scanner is already compromised. C. Set network behavior analysis rules: While

useful for ongoing monitoring and detection, this does not address the immediate need to stop the compromised scanner\\'s activities. In conclusion, the first and most crucial action is to quarantine the scanner sensor to halt any malicious

activity and perform a forensic analysis to understand the scope and nature of the compromise. This step ensures that the threat is contained and provides a basis for further remediation efforts.

References:

CompTIA SecurityX Study Guide

NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

QUESTION 11

SIMULATION

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.

This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.

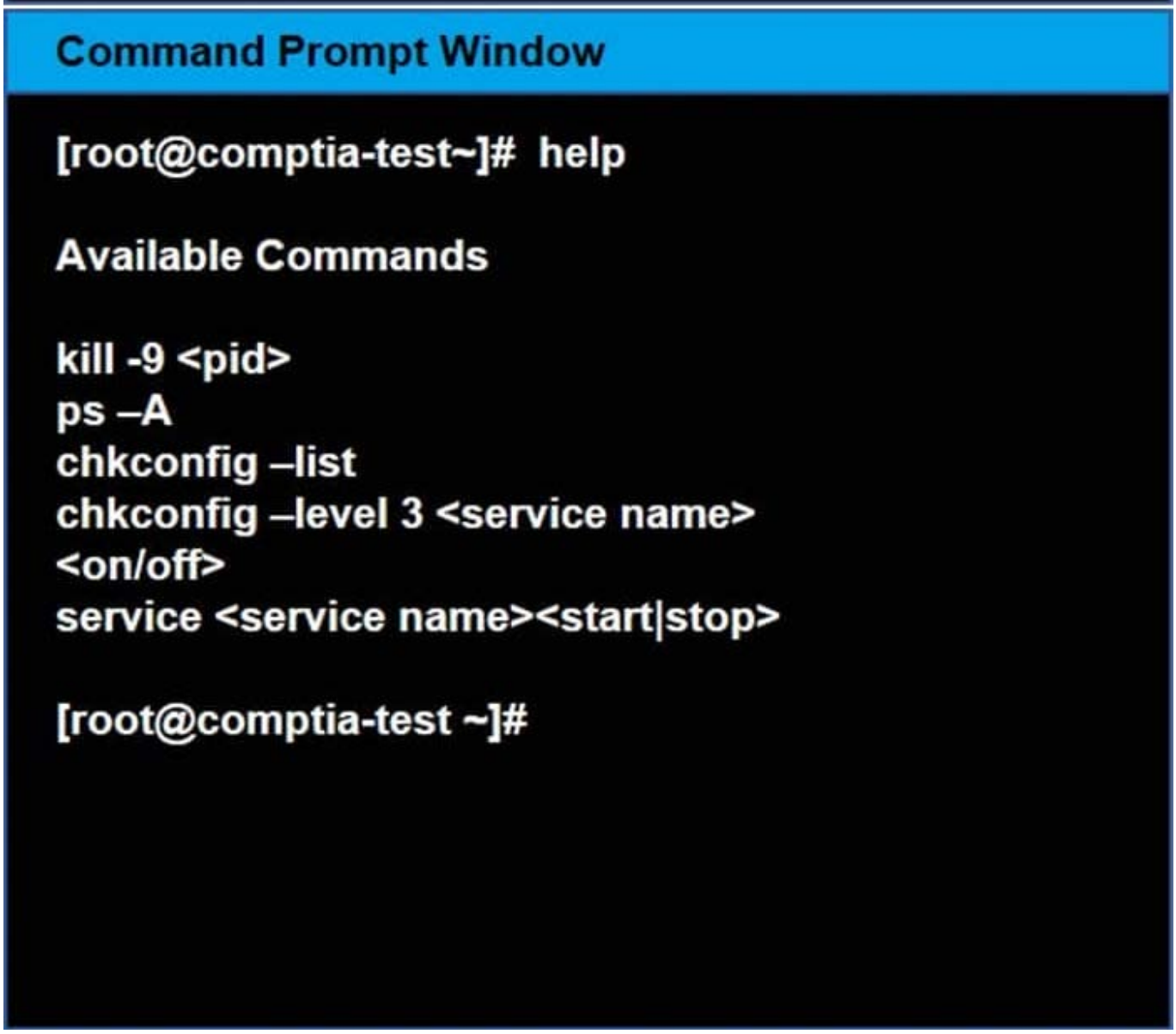
The command window will be provided along with root access. You are connected via a secure shell with root access.

You may query help for a list of commands.

Instructions:

You need to disable and turn off unrelated services and processes.

It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. See the complete solution below in Explanation.

B. PlaceHoder

C. PlaceHoder

D. PlaceHoder

Correct Answer: A

In Order to deactivate web services, database services and print service, we can do following things 1) deactivate its services /etc/init.d/apache2 stop /etc/init.d/mysqld stop 2) close ports for these services Web Server iptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables save Print Server iptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables save Database Server iptables -I INPUT -p tcp -m tcp --dport -j REJECTservice iptables save 3) Kill the process any running for the same ps -aef|grep mysql kill -9

QUESTION 12

A security officer received several complaints from users about excessive MPA push notifications at night The security team investigates and suspects malicious activities regarding user account authentication

Which of the following is the best way for the security officer to restrict MI~A notifications\\'\\'

A. Provisioning FID02 devices

B. Deploying a text message based on MFA

C. Enabling OTP via email

D. Configuring prompt-driven MFA

Correct Answer: D

Excessive MFA push notifications can be a sign of an attempted push notification attack, where attackers repeatedly send MFA prompts hoping the user will eventually approve one by mistake. To mitigate this:

A. Provisioning FIDO2 devices: While FIDO2 devices offer strong authentication, they may not be practical for all users and do not directly address the issue of excessive push notifications.

B. Deploying a text message-based MFA: SMS-based MFA can still be vulnerable to similar spamming attacks and phishing.

C. Enabling OTP via email: Email-based OTPs add another layer of security but do not directly solve the issue of excessive notifications. D. Configuring prompt-driven MFA: This option allows users to respond to prompts in a secure manner,

often including features like time-limited approval windows, additional verification steps, or requiring specific actions to approve. This can help prevent users from accidentally approving malicious attempts. Configuring prompt-driven MFA is

the best solution to restrict unnecessary MFA notifications and improve security.

References:

CompTIA Security+ Study Guide

NIST SP 800-63B, "Digital Identity Guidelines"

"Multi-Factor Authentication: Best Practices" by Microsoft

QUESTION 13

A security analyst is reviewing the following event timeline from an COR solution:

Time	File name	File action	Action verdict
4:08 p.m.	hr-reporting.docx	File save	Allowed
4:09 p.m.	hr-reporting.docx	Scan initiated	Pending
4:10 p.m.	hr-reporting.docx	File execute	Allowed
4:16 p.m.	paychecks.xlsx	File save	Allowed
4:16 p.m.	paychecks.xlsx	File shared	Allowed
4:17 p.m.	hr-reporting.docx	Script launched	Allowed
4:19 p.m.	hr-reporting.docx	Scan complete	Malware found
4:20 p.m.	paychecks.xlsx	File edit	Allowed

Which of the following most likely has occurred and needs to be fixed?

A. The Dl P has failed to block malicious exfiltration and data tagging is not being utilized property

B. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.

C. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor

D. A potential insider threat is being investigated and will be addressed by the senior management team.

Correct Answer: C

The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed.

This suggests a Time-Of- Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.

References:

CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated. NIST Special Publication 800-53, "Security and Privacy Controls for Federal

Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations. "The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers

logic flaws and timing vulnerabilities, including TOCTOU issues.

QUESTION 14

A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	190ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

which of the following should the company implement to best resolve the issue?

A. IDS

B. CDN

C. WAF

D. NAC

Correct Answer: B

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website\\'s performance. A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.

B. CDN (Content Delivery Network): A CDN stores copies of the website\\'s content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user

experience globally.

C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency. D. NAC (Network Access Control): NAC solutions control access

to network resources but are not designed to address web performance issues. Implementing a CDN is the best solution to resolve the performance issues observed in the log output.

References:

CompTIA Security+ Study Guide

"CDN: Content Delivery Networks Explained" by Akamai Technologies NIST SP 800-44, "Guidelines on Securing Public Web Servers"

QUESTION 15

After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation.

Which of the following would the company most likely do to decrease this type of risk?

A. Improve firewall rules to avoid access to those platforms.

B. Implement a cloud-access security broker

C. Create SIEM rules to raise alerts for access to those platforms

D. Deploy an internet proxy that filters certain domains

Correct Answer: B

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:

A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB. B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce

data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.

C. Create SIEM rules to raise alerts for access to those platforms: This helps in monitoring but does not prevent data leaks.

D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB. Implementing a CASB is the most comprehensive solution to decrease the risk of

data leaks by providing visibility, control, and enforcement of security policies for cloud services.

References:

CompTIA Security+ Study Guide

Gartner, "Magic Quadrant for Cloud Access Security Brokers" NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"