

Latest CAS-005 Guide Files & Pdf CAS-005 Braindumps



BTW, DOWNLOAD part of RealVCE CAS-005 dumps from Cloud Storage: <https://drive.google.com/open?id=1OLzPdCYGH7fQbI6HaDprMuQ2luNngY00>

If you are looking to advance in the fast-paced and technological world, RealVCE is here to help you achieve this aim. RealVCE provides you with the excellent CompTIA SecurityX Certification Exam (CAS-005) practice exam, which will make your dream come true of passing the CompTIA SecurityX Certification Exam (CAS-005) certification exam on the first attempt.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security.
Topic 2	<ul style="list-style-type: none">Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.
Topic 3	<ul style="list-style-type: none">Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering.
Topic 4	<ul style="list-style-type: none">Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems.

>> Latest CAS-005 Guide Files <<

2026 Realistic Latest CAS-005 Guide Files - Pdf CompTIA SecurityX Certification Exam Braindumps Pass Guaranteed Quiz

After you practice our CAS-005 study materials, you can master the examination point from the CAS-005 exam torrent. Then, you will have enough confidence to pass your CAS-005 exam. We can succeed so long as we make efforts for one thing. As for the safe environment and effective product, why don't you have a try for our CAS-005 Test Question, never let you down! Before your purchase, there is a free demo of our CAS-005 training material for you. You can know the quality of our CAS-005 guide question earlier before your purchase.

CompTIA SecurityX Certification Exam Sample Questions (Q174-Q179):

NEW QUESTION # 174

□

Answer:

Explanation:

□ An organization is planning for disaster recovery and continuity of operations.

INSTRUCTIONS

Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

NEW QUESTION # 175

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

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

- A. Recompiling the affected programs with the most current patches
- **B. Automating the patching system to update base Images**
- C. Disabling unused/unneeded ports on all servers
- D. Deploying a WAF with virtual patching upstream of the affected systems

Answer: B

Explanation:

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.

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.

NEW QUESTION # 176

A security analyst received a report that an internal web page is down after a company-wide update to the web browser. Given the following error message:

□ Which of the following is the best way to fix this issue?

- A. Rewriting any legacy web functions
- **B. Discontinuing the use of self-signed certificates**
- C. Blocking all non-essential ports
- D. Disabling all deprecated ciphers

Answer: B

Explanation:

The error message "NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM" indicates that the web browser is rejecting the certificate because it uses a weak signature algorithm. This commonly happens with self-signed certificates, which often use outdated or insecure algorithms.

Why Discontinue Self-Signed Certificates?

Security Compliance: Modern browsers enforce strict security standards and may reject certificates that do not comply with these standards.

Trusted Certificates: Using certificates from a trusted Certificate Authority (CA) ensures compliance with security standards and is less likely to be flagged as insecure.

Weak Signature Algorithm: Self-signed certificates might use weak algorithms like MD5 or SHA-1, which are considered insecure.

Other options do not address the specific cause of the certificate error:

A: Rewriting legacy web functions: Does not address the certificate issue.

B: Disabling deprecated ciphers: Useful for improving security but not related to the certificate error.

C: Blocking non-essential ports: This is unrelated to the issue of certificate validation.

References:

CompTIA SecurityX Study Guide

"Managing SSL/TLS Certificates," OWASP

"Best Practices for Certificate Management," NIST Special Publication 800-57

NEW QUESTION # 177

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

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

- A. Only allow connections from approved IPs.
- B. Block IP 104.18.16.29 on the firewall.
- C. Upgrade the firmware on the camera.
- D. Implement WAF protection for the web application.

Answer: A

Explanation:

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 IPs 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.

NEW QUESTION # 178

After an incident response exercise, a security administrator reviews the following table:

Which of the following should the administrator do to beat support rapid incident response in the future?

- A. Configure automated Isolation of human resources systems
- B. Automate alerting to IT support for phone system outages.
- C. Enable dashboards for service status monitoring
- D. Send emails for failed log-in attempts on the public website

Answer: C

Explanation:

Enabling dashboards for service status monitoring is the best action to support rapid incident response. The table shows various services with different risk, criticality, and alert severity ratings. To ensure timely and effective incident response, real-time visibility into the status of these services is crucial.

Why Dashboards for Service Status Monitoring?

Real-time Visibility: Dashboards provide an at-a-glance view of the current status of all critical services, enabling rapid detection of issues.

Centralized Monitoring: A single platform to monitor the status of multiple services helps streamline incident response efforts.

Proactive Alerting: Dashboards can be configured to show alerts and anomalies immediately, ensuring that incidents are addressed as soon as they arise.

Improved Decision Making: Real-time data helps incident response teams make informed decisions quickly, reducing downtime and mitigating impact.

Other options, while useful, do not offer the same level of comprehensive, real-time visibility and proactive alerting:

A: Automate alerting to IT support for phone system outages: This addresses one service but does not provide a holistic view.

C: Send emails for failed log-in attempts on the public website: This is a specific alert for one type of issue and does not cover all services.

D: Configure automated isolation of human resources systems: This is a reactive measure for a specific service and does not provide real-time status monitoring.

• • • • •

Pdf CAS-005 Braindumps: https://www.realvce.com/CAS-005_free-dumps.html

- DOWNLOAD the newest RealVCE CAS-005 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1OLzPdCYGH7fObI6HaDprMuO2luNngY00>