CompTIA - Newest CAS-005 - CompTIA SecurityX Certification Exam Test Voucher

P.S. Free 2025 CompTIA CAS-005 dumps are available on Google Drive shared by CertkingdomPDF: https://drive.google.com/open?id=172_m20eGKMh42gNR8-z5us8ntqVZ8wFo

We have a large number of regular customers exceedingly trust our CAS-005 training materials for their precise content about the exam. You may previously have thought preparing for the CAS-005 preparation materials will be full of agony, actually, you can abandon the time-consuming thought from now on. Our CAS-005 Exam Questions are famous for its high-efficiency and high pass rate as 98% to 100%. Buy our CAS-005 study guide, and you will pass the exam easily.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.
Topic 3	• 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.
Topic 4	• 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.

>> CAS-005 Test Voucher <<

2025 Authoritative CAS-005 – 100% Free Test Voucher | CAS-005 Exam Dumps Pdf

Two CompTIA CAS-005 practice tests of CertkingdomPDF (desktop and web-based) create an actual test scenario and give you a CAS-005 real exam feeling. These CAS-005 Practice Tests also help you gauge your CompTIA Certification Exams preparation and identify areas where improvements are necessary.

CompTIA SecurityX Certification Exam Sample Questions (Q204-Q209):

NEW QUESTION # 204
A security analyst is reviewing the following vulnerability assessment report:
192.168.1.5, Host = Server1, CVSS 7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVSS 6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVSS 5.5, Email Server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVSS 9.8, Domain Controller, Remotely Executable = Yes, Exploit = Yes Which of the following should be patched first to minimize attacks against internet-facing hosts?

- A. Server2
- B. Server1
- C. Server3
- D. Server4

Answer: A

Explanation:
The question focuses oninternet-facing hosts, implying external exposure. CVSS scores, remote executability, and exploitavailability guide prioritization. Server2 (205.1.3.5, CVSS 6.5, Bind Server) has a public IP, suggesting it's internet-facing, unlike Server1 and Server4 (192.168.x.x, private IPs). Server3 (207.1.5.7, CVSS 5.5) is also public but has a lower score and risk compared to Server2's proof-of-concept (POC) exploit. Server2's Bind Server (DNS) role is critical and commonly targeted, making it the priority.
* Option A:Server1 (CVSS 7.5) is private, not internet-facing.
* Option B:Server2 (CVSS 6.5) is internet-facing with an exploit POC, warranting immediate patching.
* Option C:Server3 (CVSS 5.5) is internet-facing but less severe.
* Option D:Server4 (CVSS 9.8) is critical but private, not internet-facing.
Reference:CompTIA SecurityX CAS-005 Domain 1: Risk Management - Vulnerability Prioritization.

NEW QUESTION # 205
A company migrating to aremote work model requires that company-owned devices connect to a VPN before logging in to the device itself. The VPN gateway requires that a specific key extension is deployed to the machine certificates in the internal PKI. Which of the following best explains this requirement?

- A. The VPN client selected the certificate with the correct key usage without user interaction.
- B. The certificate is an additional factor to meet regulatory MFA requirements for VPN access.
- C. The server connection uses SSL VPN, which uses certificates for secure communication.
- D. The internal PKI certificate deployment allows for Wi-Fi connectivity before logging in to other systems.

Answer: A

Explanation:

Comprehensive and Detailed Explanation:
This scenario describes anenterprise VPN setup that requires machine authenticationbefore a user logs in. The best explanation for this requirement is that theVPN client selects the appropriate certificate automaticallybased on the key extension in the machine certificate.
* Understanding the Key Extension Requirement:
* PKI (Public Key Infrastructure)issues machine certificates that include specific key usages such asClient AuthenticationorIPSec IKE Intermediate.
* Key usage extensionsdefine how a certificate can be used, ensuring that onlyvalid certificates are selected by the VPN client.
* Why Option B is Correct:
* The VPNautomaticallyselects the correct machine certificate with the appropriate key extension.
* The process occurswithout user intervention, ensuring seamless VPN authentication before login.
* Why Other Options Are Incorrect:
* A (MFA requirement):Certificates used in this scenario are for machine authentication, not user MFA. MFA typically involves user credentials plus a second factor (like OTPs or biometrics), which isnot applicable here.
* C (Wi-Fi connectivity before login):This refers topre-logon networking, which is a separate concept where devices authenticate to a Wi-Fi network before login, usually via 802.1X EAP- TLS. However, this question specifically mentions VPN authentication, not Wi-Fi authentication.
* D (SSL VPN with certificates):While SSL VPNs do use certificates,this scenario involves machine certificates issued by an internal PKI, which are commonly used inIPSec VPNs, not SSL VPNs.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide: Section onMachine Certificate Authentication in VPNs NIST SP 800-53: Guidelines on authentication mechanisms RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile

NEW QUESTION # 206
A security engineer wants to reduce the attack surface of a public-facing containerized application Which of the following will best reduce the application's privilege escalation attack surface?

- A. Designing a muiticontainer solution, with one set of containers that runs the mam application, and another set oi containers that perform automatic remediation by replacing compromised containers or disabling compromised accounts
- B. Running the container in an isolated network and placing a load balancer in a public-facing network. Adding the following ACL to the load balancer:PZRKZI HTTES from 0-0.0.0.0/0 pert 443
- C. Implementing the following commands in the Dockerfile:RUN echo user:x:1000:1000iuser:/home/user:/dew/null > /ete/passwd
- D. Installing an EDR on the container's host with reporting configured to log to a centralized SIFM and Implementing the followingalerting rules TF PBOCESS_USEB=rooC ALERT_TYPE=critical

Answer: C

Explanation:
Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of privilege escalation attacks because even if anattacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.
A . Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges.
B . Installing an EDR on the container's host: While useful for detecting threats, this does not reduce the privilege escalation attack surface within the containerized application.
C .Designing a multi-container solution: While beneficial for modularity and remediation, it does not specifically address privilege escalation.
D . Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface.
Reference:
CompTIA Security+ Study Guide
Docker documentation on security best practices
NIST SP 800-190, "Application Container Security Guide"

NEW QUESTION # 207
A vulnerability can on a web server identified the following:

Which of the following actions would most likely eliminate on path decryption attacks? (Select two).

- A. Adding TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256
- B. Implementing HIPS rules to identify and block BEAST attack attempts
- C. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA
- D. Disallowing cipher suites that use ephemeral modes of operation for key agreement
- E. Removing support for CBC-based key exchange and signing algorithms
- F. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA

Answer: A,E

Explanation:
On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:
Removing support for CBC-based key exchange and signing algorithms: CBC mode is vulnerable to certain attacks like BEAST. By removing support for CBC-based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.
Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC.
SHA-256 is a strong hash function that ensures data integrity.

NEW QUESTION # 208
A user reports application access issues to the help desk. The help desk reviews the logs for the user:

Time	Internal IP	Public IP	IP geolocation	Application	Action
8:47 p.m.	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Human resources system	Allow
8:49 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 p.m.	192.168.1.5	104.18.16.29	Toronto	Human resources system	Deny

Which of the following is most likely the reason for the issue?

- A. A threat actor has compromised the user's account and attempted to lop, m
- B. The user is not allowed to access the human resources system outside of business hours
- C. The user inadvertently tripped the impossible travel security rule in the SSO system.
- D. The user did not attempt to connect from an approved subnet

Answer: C

Explanation:
Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.
Analysis of Logs:
At 8:47 p.m., the user accessed a VPN from Toronto.
At 8:48 p.m., the user accessed email from Los Angeles.
At 8:48 p.m., the user accessed the human resources system from Los Angeles.
At 8:49 p.m., the user accessed email again from Los Angeles.
At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.
These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial.

NEW QUESTION # 209
.....

In this Desktop-based CompTIA CAS-005 practice exam software, you will enjoy the opportunity to self-exam your preparation. The chance to customize the CompTIA SecurityX Certification Exam (CAS-005) practice exams according to the time and types of CompTIA SecurityX Certification Exam (CAS-005) practice test questions will contribute to your ease. This format operates only on Windows-based devices. But what is helpful is that it functions without an active internet connection. It copies the exact pattern and style of the real CompTIA CAS-005 Exam to make your preparation productive and relevant.

CAS-005 Exam Dumps Pdf: https://www.certkingdompdf.com/CAS-005-latest-certkingdom-dumps.html

- Latest CAS-005 Test Voucher - Useful CAS-005 Exam Dumps Pdf - Accurate Exam CAS-005 Fee □ ➠ www.prep4away.com □ is best website to obtain ▹ CAS-005 ◃ for free download □Valid Dumps CAS-005 Pdf
- Save Time And Study Anywhere With CompTIA CAS-005 PDF Dumps Format □ Open website ✔ www.pdfvce.com □✔□ and search for 《 CAS-005 》 for free download □Test CAS-005 Voucher
- Pass Guaranteed CompTIA - CAS-005 - CompTIA SecurityX Certification Exam Accurate Test Voucher □ Simply search for □ CAS-005 □ for free download on ▹ www.testsimulate.com ◃ □Latest CAS-005 Test Cost
- Free PDF 2025 High-quality CompTIA CAS-005: CompTIA SecurityX Certification Exam Test Voucher □ Search for { CAS-005 } and download exam materials for free through " www.pdfvce.com " □CAS-005 Reliable Test Pattern
- CompTIA SecurityX Certification Exam Study Training Dumps Grasp the Core Knowledge of CAS-005 Exam - www.free4dump.com □ Search for " CAS-005 " and download exam materials for free through ➠ www.free4dump.com □ □Test CAS-005 Voucher
- CompTIA SecurityX Certification Exam Study Training Dumps Grasp the Core Knowledge of CAS-005 Exam - Pdfvce □ Immediately open 【 www.pdfvce.com 】 and search for ✔ CAS-005 □✔□ to obtain a free download □Valid Dumps CAS-005 Pdf
- www.actual4labs.com offers Real and Verified CompTIA CAS-005 Exam Practice Test Questions □ Copy URL " www.actual4labs.com " open and search for ⇛ CAS-005 ⇚ to download for free □CAS-005 Valid Exam Simulator
- Dumps CAS-005 Reviews □ Valid Dumps CAS-005 Pdf □ Test CAS-005 Voucher □ Search on ➤ www.pdfvce.com □ for ▸ CAS-005 ◂ to obtain exam materials for free download □Dumps CAS-005 Reviews
- Pass Guaranteed CompTIA - CAS-005 - CompTIA SecurityX Certification Exam Accurate Test Voucher □ Search for ☀ CAS-005 □☀□ and easily obtain a free download on ▸ www.dumps4pdf.com ◂ □CAS-005 Valid Exam Simulator
- Test CAS-005 Voucher □ Latest CAS-005 Test Cost □ Dumps CAS-005 Reviews □ Copy URL 《 www.pdfvce.com 》 open and search for ➡ CAS-005 □□□ to download for free □CAS-005 Reliable Test Pattern
- CAS-005 Free Practice Exams □ CAS-005 Interactive Course □ CAS-005 Latest Exam Review □ Easily obtain ➥ CAS-005 □ for free download through ➥ www.prep4pass.com □ □CAS-005 Latest Exam Review
- lms.ait.edu.za, wheelwell.efundisha.co.za, lms.ait.edu.za, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, zeritenetwork.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, creativesindigenous.nativemax.com, bbs.yongrenqianyou.com, ncon.edu.sa, learn.psmsurat.com, Disposable vapes

2025 Latest CertkingdomPDF CAS-005 PDF Dumps and CAS-005 Exam Engine Free Share: https://drive.google.com/open?id=172_m20eGKMh42gNR8-z5us8ntqVZ8wFo