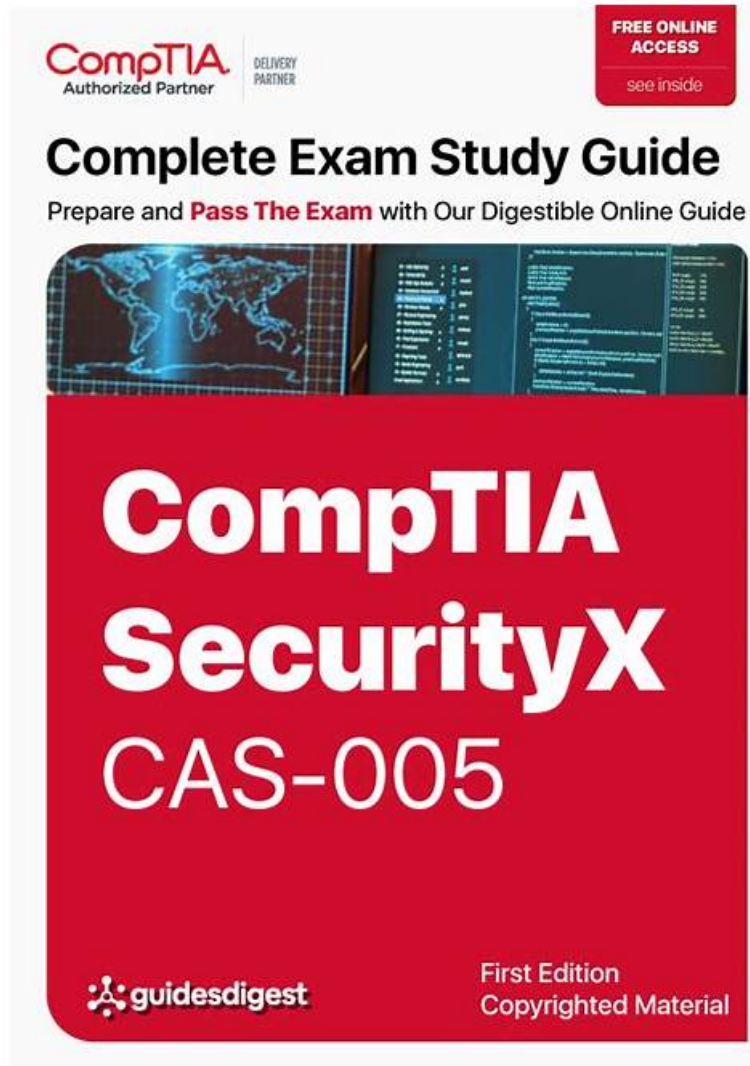


CAS-005 Real Exam Questions | CAS-005 Reliable Study Plan



What's more, part of that DumpsMaterials CAS-005 dumps now are free: https://drive.google.com/open?id=1yxxxXmQAdm7Oaoy_UTA9Ga-GuglgyGXC

We are committed to helping you pass the exam and get the certificate as soon as possible. CAS-005 exam bootcamp of us have the questions and answers, and it not only have quality but also contain certain quantity, it will be enough for you to deal with your exam. With the pass rate more than 98.65%, we can ensure you pass your exam. CAS-005 Exam Dumps also have most of knowledge points of the exam, and they may help you a lot. We offer you free update for 365 days after you purchase the CAS-005 exam bootcamp.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	<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 2	<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 3	<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.
Topic 4	<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.

>> CAS-005 Real Exam Questions <<

CAS-005 Reliable Study Plan & CAS-005 Study Dumps

It helps you to pass the CompTIA CAS-005 test with excellent results. CompTIA CAS-005 imitates the actual CAS-005 exam environment. You can take the CAS-005 practice exam many times to evaluate and enhance your CompTIA CAS-005 Exam Preparation level. Desktop CAS-005 practice test software is compatible with windows and the web-based software will work on these operating systems: Android, IOS, Windows, and Linux.

CompTIA SecurityX Certification Exam Sample Questions (Q220-Q225):

NEW QUESTION # 220

An organization found a significant vulnerability associated with a commonly used package in a variety of operating systems. The organization develops a registry of software dependencies to facilitate incident response activities. As part of the registry, the organization creates hashes of packages that have been formally vetted. Which of the following attack vectors does this registry address?

- A. Pass-the-hash attack
- **B. Supply chain attack**
- C. Cipher substitution attack
- D. On-path attack
- E. Side-channel analysis

Answer: B

Explanation:

A). Supply chain attack: This type of attack involves compromising the software supply chain by injecting malicious code into legitimate software packages.

B). Cipher substitution attack: This is a cryptographic attack focused on replacing ciphertext with a different ciphertext to deduce the key. It's not relevant to the scenario.

C). Side-channel analysis: This attack involves gathering information from the physical implementation of a system (e.g., timing, power consumption) rather than exploiting the algorithm itself. It's not applicable here.

D). On-path attack (formerly man-in-the-middle): This attack involves intercepting and potentially altering communication between two parties. While important, it's not the primary focus of the registry.

E). Pass-the-hash attack: This attack involves using a stolen hash of a user's password to authenticate without needing the actual password. It's unrelated to software package integrity.

Why A is the Correct answer:

A supply chain attack is exactly what the organization is trying to mitigate. By creating a registry of known-good software packages and their hashes, they can verify that the packages they are using are legitimate and haven't been altered.

If an attacker were to compromise a software package in the supply chain, the hash of the altered package would not match the hash in the organization's registry. This would immediately alert the organization to a potential compromise.

CASP+ Relevance: This aligns with the CASP+ exam objectives, which emphasize the importance of risk management, threat

intelligence, and implementing security controls to address various attack vectors, including supply chain risks.

How the Registry Works (Elaboration based on CASP+principles):

Hashing: When a package is vetted, a cryptographic hash function (like SHA-256) is used to generate a unique "fingerprint" (the hash) of the package's contents.

Verification: Before installing or using a package, its hash is calculated and compared to the hash stored in the registry. A match confirms the package's integrity. A mismatch indicates tampering.

Incident Response: If a vulnerability is discovered in a commonly used package, the registry helps the organization quickly identify which systems are affected based on the dependency list and the stored hashes.

In conclusion, maintaining a registry of software dependencies with hashes is a crucial security control that directly addresses the threat of supply chain attacks by ensuring the integrity and authenticity of software packages. The use of hash functions for verification is a common practice in security and is emphasized in the CASP+ material.

Explanation:

Step by Step

Understanding the Scenario: The question describes a proactive security measure where an organization maintains a registry of software dependencies and their corresponding hashes. This registry is used to verify the integrity of software packages.

Analyzing the Answer Choices:

NEW QUESTION # 221

A security engineer is reviewing the SIEM logs after a server crashed. The following list of events represents the timeline of actions collected from the SIEM:

Which of the following TTPs is most likely associated with this SIEM log?

- A. Credential dumping
- B. LOLBins use
- C. Data exfiltration
- D. Lateral movement

Answer: A

NEW QUESTION # 222

A security engineer is reviewing the following vulnerability scan report:

Which of the following should the engineer prioritize for remediation?

- A. OpenSSH
- B. Apache HTTP Server
- C. Migration to TLS 1.3
- D. Google Chrome

Answer: A

Explanation:

OpenSSH vulnerability is public facing and has a critical CVSS of 9.2.

Exploitable SSH services can lead to direct server compromise.

Although Apache has a higher score, it's internal.

From CAS-005, Domain 3: Vulnerability Management:

"Prioritize external vulnerabilities with high CVSS and exposed attack surfaces."

NEW QUESTION # 223

A company reduced its staff 60 days ago, and applications are now starting to fail. The security analyst is investigating to determine if there is malicious intent for the application failures. The security analyst reviews the following logs:

Mar 5 22:09:50 akj3 sshd

[21502]: Success login for userOl from 192.168.2.5

Mar 5 22:10:00 akj3 sshd

[21502]: Failed login for userID from 192.168.2.5

Which of the following is the most likely reason for the application failures?

- A. The root password has been changed.

- B. The user's home directory was deleted.
- C. The user does not have sudo access.
- D. The user's account was set as a service account.

Answer: B

Explanation:

Comprehensive and Detailed Step-by-Step

When an employee leaves a company, their home directory might be deleted along with their account, leading to application failures if the directory contained configuration files, dependencies, or system scripts.

NEW QUESTION # 224

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

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

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

Answer: A

Explanation:

Enabling dashboards for service status monitoring is the best action to support rapid incident response. Dashboards provide real-time visibility into the status of critical systems, enabling quicker identification of issues and a more informed, proactive response during an incident. By having a centralized view of service status, the security administrator can respond more quickly and efficiently to any disruptions.

NEW QUESTION # 225

.....

As the old saying goes people change with the times. People must constantly update their stocks of knowledge and improve their practical ability. Passing the test CAS-005 certification can help you achieve that and buying our CAS-005 study materials can help you pass the test smoothly. Our CAS-005 Study Materials are superior to other same kinds of study materials in many aspects. Our products' test bank covers the entire syllabus of the test and all the possible questions which may appear in the test. Each question and answer has been verified by the industry experts.

CAS-005 Reliable Study Plan: <https://www.dumpsmaterials.com/CAS-005-real-torrent.html>

- CAS-005 Reliable Dumps Ppt □ CAS-005 Test Assessment □ CAS-005 Test Collection □ Search for ➡ CAS-005 □□□ and easily obtain a free download on 《 www.dumpsquestion.com 》 □CAS-005 Test Collection
- CAS-005 Questions □ New CAS-005 Test Sims □ CAS-005 New Braindumps Free □ Open ➡ www.pdfvce.com □ and search for 《 CAS-005 》 to download exam materials for free □New CAS-005 Test Blueprint
- Latest CAS-005 Exam Experience ▶ CAS-005 Practice Exams □ CAS-005 Test Assessment □ { www.examcollectionpass.com } is best website to obtain ⇒ CAS-005 ⇐ for free download □Exam CAS-005 Simulator
- Pass CAS-005 Exam with High-quality CAS-005 Real Exam Questions by Pdfvce □ Search for “CAS-005 ” and obtain a free download on ➡ www.pdfvce.com □□□ □New CAS-005 Test Blueprint
- CAS-005 New Braindumps Free □ CAS-005 Questions □ New CAS-005 Test Blueprint □ Open website 《 www.prepawaypdf.com 》 and search for □ CAS-005 □ for free download □CAS-005 Test Collection
- CAS-005 Real Exam Questions | Ready to Pass The CompTIA SecurityX Certification Exam □ Download (CAS-005) for free by simply searching on □ www.pdfvce.com □ □CAS-005 Testking Learning Materials
- Pass Guaranteed 2026 CAS-005: CompTIA SecurityX Certification Exam High Hit-Rate Real Exam Questions □ Download ▷ CAS-005 ◁ for free by simply entering ➡ www.prepawaypdf.com □ website □CAS-005 New Braindumps Free
- CAS-005 Real Exam Questions | Efficient CAS-005 Reliable Study Plan: CompTIA SecurityX Certification Exam 100% Pass □ Open ➡ www.pdfvce.com □ and search for 《 CAS-005 》 to download exam materials for free □Dumps CAS-005 Questions
- Verified CAS-005 Real Exam Questions - Leader in Qualification Exams - 100% Pass-Rate CAS-005 Reliable Study Plan □ Search on “ www.torrentvce.com ” for □ CAS-005 □ to obtain exam materials for free download □Relevant CAS-

005 Exam Dumps

- CAS-005 Testking Learning Materials □ Reliable CAS-005 Braindumps Pdf □ Reliable CAS-005 Braindumps Pdf □ Download ➔ CAS-005 □□□ for free by simply searching on 「 www.pdfvce.com 」 □ CAS-005 Reliable Dumps Ppt
- Relevant CAS-005 Exam Dumps □ CAS-005 Practice Exams □ New CAS-005 Test Blueprint □ Immediately open 【 www.easy4engine.com 】 and search for □ CAS-005 □ to obtain a free download □ CAS-005 Training Online
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.ganjingworld.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.gtcn.info, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New CAS-005 dumps are available on Google Drive shared by DumpsMaterials: https://drive.google.com/open?id=1yxxxXmQAdm7Oaoy_UTA9Ga-GuglgyGXC