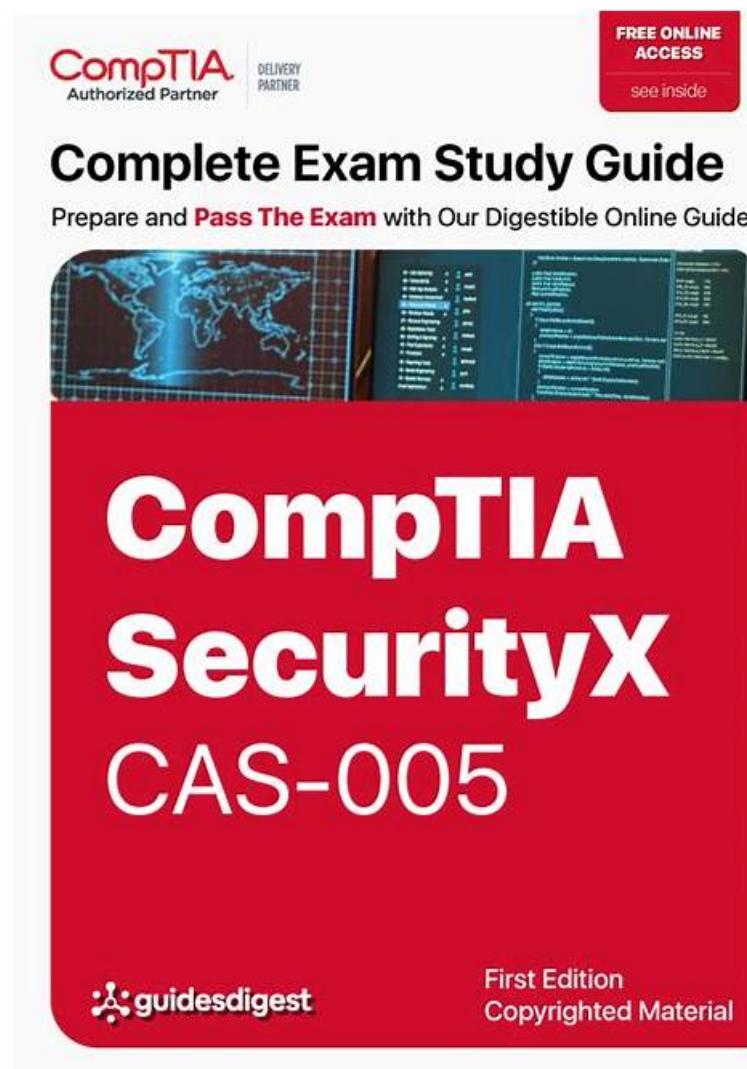


CAS-005 Testing Center - CAS-005 Latest Study Questions



What's more, part of that Exams4Collection CAS-005 dumps now are free: https://drive.google.com/open?id=1vPXi_fdx9Kt962BkSMSIB1J5V1zylrX1

With precious time passing away, many exam candidates are making progress with high speed and efficiency. You cannot lag behind and with our CAS-005 preparation materials, and your goals will be easier to fix. So stop idling away your precious time and begin your review with the help of our CAS-005 learning quiz as soon as possible. By using our CAS-005 exam questions, it will be your habitual act to learn something with efficiency.

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 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 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 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.

>> **CAS-005 Testing Center** <<

CAS-005 Latest Study Questions - New CAS-005 Exam Papers

If you are looking to advance in the fast-paced and technological world, Exams4Collection is here to help you achieve this aim. Exams4Collection provides you with the excellent CompTIA CAS-005 practice exam, which will make your dream come true of passing the CompTIA SecurityX Certification Exam certification exam on the first attempt.

CompTIA SecurityX Certification Exam Sample Questions (Q243-Q248):

NEW QUESTION # 243

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?

- A. Deleting SQLSV
- B. Resetting the local domain
- C. Rotating KRBTGT password**
- D. Reimaging ADMIN01S

Answer: C

Explanation:

Comprehensive and Detailed 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.

NEW QUESTION # 244

An application requires the storage of PII. A systems engineer needs to implement a solution that uses an external device for key management. Which of the following is the best solution?

- A. HSM
- B. TPM
- C. SBoM
- D. vTPM

Answer: A

NEW QUESTION # 245

A company detects suspicious activity associated with external connections. Security detection tools are unable to categorize this activity. Which of the following is the best solution to help the company overcome this challenge?

- A. Implement an Interactive honeypot
- B. Map network traffic to known IoCs.
- C. Monitor the dark web
- D. **implement UEBA**

Answer: D

Explanation:

User and Entity Behavior Analytics (UEBA) is the best solution to help the company overcome challenges associated with suspicious activity that cannot be categorized by traditional detection tools. UEBA uses advanced analytics to establish baselines of normal behavior for users and entities within the network. It then identifies deviations from these baselines, which may indicate malicious activity. This approach is particularly effective for detecting unknown threats and sophisticated attacks that do not match known indicators of compromise (IoCs).

Reference: CompTIA SecurityX Study Guide, Chapter on Advanced Threat Detection and Mitigation, Section on User and Entity Behavior Analytics (UEBA).

NEW QUESTION # 246

During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a comprised web server. Given the following portion of the code:

Which of the following best describes this incident?

- A. **Stored XSS**
- B. SQL injection
- C. XSRF attack
- D. Command injection

Answer: A

Explanation:

The provided code snippet shows a script that captures the user's cookies and sends them to a remote server.

This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.

* A. XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.

* B. Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.

* C. Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the page, the script executes and sends the user's cookies to the attacker's server.

* D. SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.

References:

* CompTIA Security+ Study Guide

* OWASP (Open Web Application Security Project) guidelines on XSS

* "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

NEW QUESTION # 247

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the

diagram.

Complete the configuration files to meet the following requirements:

- * The EAP method must use mutual certificate-based authentication (With issued client certificates).
- * The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
- * The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters, INSTRUCTIONS Click on the AAA server and VPN concentrator to complete the configuration.

Fill in the appropriate fields and make selections from the drop-down menus.

- VPN Concentrator:
- AAA Server:

Answer:

Explanation:

See the answer below in Explanation.

Explanation:

VPN Concentrator:

A screenshot of a computer Description automatically generated

AAA Server:

A screenshot of a computer Description automatically generated

NEW QUESTION # 248

.....

Our CAS-005 learning prep boosts many advantages and varied functions to make your learning relaxing and efficient. The client can have a free download and tryout of our CAS-005 exam torrent before they purchase our product and can download our CAS-005 study materials immediately after the client pay successfully. And if there is the update of our CAS-005 learning guide the system will send the update automatically to the client. Thus you can have an efficient learning and a good preparation of the exam. It is believed that our CAS-005 latest question is absolutely good choices for you.

CAS-005 Latest Study Questions: <https://www.exams4collection.com/CAS-005-latest-braindumps.html>

- CAS-005 Valid Exam Topics CAS-005 Test Torrent CAS-005 Test Lab Questions The page for free download of ⇒ CAS-005 ⇌ on ▶ www.prep4sures.top ▲ will open immediately CAS-005 Valid Test Duration
- CAS-005 actual test - CAS-005 test questions - CAS-005 actual exam Search for ➡ CAS-005 and download it for free immediately on ➡ www.pdfvce.com CAS-005 Valid Exam Topics
- CompTIA CAS-005 Testing Center: CompTIA SecurityX Certification Exam - www.pass4test.com Official Pass Certify Easily obtain [CAS-005] for free download through ▶ www.pass4test.com ▲ CAS-005 Reliable Test Cost
- CAS-005 Dumps Torrent Reliable CAS-005 Exam Practice CAS-005 Valid Test Duration Go to website [www.pdfvce.com] open and search for ➡ CAS-005 to download for free CAS-005 Actual Questions
- 100% Pass CompTIA - Newest CAS-005 Testing Center Easily obtain free download of « CAS-005 » by searching on “www.practicevce.com” CAS-005 Actual Questions
- CAS-005 Valid Exam Topics CAS-005 Test Torrent CAS-005 Valid Exam Topics Search for ➡ CAS-005 and obtain a free download on [www.pdfvce.com] CAS-005 Actual Questions
- CAS-005 Test Torrent CAS-005 Actual Questions Latest CAS-005 Exam Bootcamp Go to website www.troytecdumps.com open and search for { CAS-005 } to download for free CAS-005 Actual Questions
- CAS-005 Valid Exam Blueprint CAS-005 Valid Test Duration * CAS-005 Test Torrent Search for 「 CAS-005 」 and download exam materials for free through ➡ www.pdfvce.com Latest CAS-005 Exam Bootcamp
- Latest updated CAS-005 Testing Center - Excellent CAS-005 Latest Study Questions Ensure You a High Passing Rate Immediately open “www.pdfdumps.com” and search for 【 CAS-005 】 to obtain a free download Practice Test CAS-005 Pdf
- 100% Pass CompTIA - Newest CAS-005 Testing Center Immediately open ▷ www.pdfvce.com ▲ and search for ⇒ CAS-005 ⇌ to obtain a free download CAS-005 Reliable Dumps Files
- CAS-005 Valid Test Vce CAS-005 Top Dumps CAS-005 Actual Questions Search for “ CAS-005 ” and obtain a free download on « www.prepawayexam.com » CAS-005 Test Torrent
- 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, learn.anantlibrary.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, enroll.schoolpen.in,

www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of Exams4Collection CAS-005 dumps for free: https://drive.google.com/open?id=1vPXi_fdx9Kt962BkSMSIB1J5V1zylrX1