CAS-005 Pruefungssimulationen, CAS-005 Prüfungsfrage

P.S. Kostenlose und neue CAS-005 Prüfungsfragen sind auf Google Drive freigegeben von ZertPruefung verfügbar: https://drive.google.com/open?id=1LErwjflYW2ybzXk0GVHFfG2BlKg_wxrH

Die Qualifikation ist nicht gleich wie die Fähigkeit eines Menschen. Die Qualifikation bedeutet nur, dass Sie dieses Lernerlebnis hat. Und die reale Fähigkeit sind in der Ppraxis entstanden. Sie hat keine direkte Verbindung mit der Qualifikation. Sie sollen niemals das Gefühl haben, dass Sie nicht exzellent ist. Sie sollen auch nie an Ihrer Fähigkeit zweifeln. Wenn Sie die Dumps zurCompTIA CAS-005 Zertifizierungsprüfung wählen, sollen Sie sich bemühen, die Prüfung zu bestehen. Wenn Sie sich fürchten, CAS-005 Prüfung nicht bestehen zu können, wählen Sie doch die Sulungsunterlagen zur CompTIA CAS-005 Prüfung von ZertPruefung. Egal ob welche Qualifikation haben, können Sie ganz einfach die Inhalte der Fragenkataloge verstehen und die CAS-005 Prüfung erfolgreich abschließen.

Fühlen Sie sich schmerzvoll, wenn Sie so viele IT-Zertifizierungen und Zertifizierungsunterlagen sehen? Was sollen Sie machen? Welche Prüfung und welche Prüfungsunterlage sollen Sie wählen? Wir ZertPruefung können die geeignete Prüfungen für Sie wählen, wenn Sie wissen nicht, wie sich zu entscheiden. Sie können jetzt sehr populäre CompTIA CAS-005 Zertifizierungsprüfung wählen. Diese Zertifizierung hat viele Vorteile. Außerdem, wenn Sie sehr effektiv die Prüfung vorbereiten, können Sie sich für CompTIA CAS-005 Dumps von ZertPruefung entscheiden. Es ist die beste Methode für dich, diese CompTIA CAS-005 Prüfung einfach zu bestehen.

>> CAS-005 Pruefungssimulationen <<

CompTIA CAS-005 Prüfungsfrage, CAS-005 Prüfungs-Guide

Die Schulungsunterlagen zur CompTIA CAS-005 Zertifizierungsprüfung von ZertPruefung werden Ihnen nicht nur Energie und Ressourcen, sondern auch viel Zeit ersparen. Denn normalerweise müssen Sie einige Monate verwenden, um sich auf die Prüfung vorzubereiten. So, was Sie tun sollen, ist die Schulungsunterlagen zur CompTIA CAS-005 Zertifizierungsprüfung von ZertPruefung zu kaufen und somit das Zertifikat erhalten. Unser ZertPruefung wird Ihnen helfen, die relevanten Kenntnisse und Erfahrungen zu bekommen. Wir bieten Ihnen auch ein ausführliches Prüfungsziel. Mit ZertPruefung können Sie die CompTIA CAS-005 Zertifizierungsprüfung einfach bestehen.

CompTIA CAS-005 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.
Thema 2	• 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.
Thema 3	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.
Thema 4	• 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.

CompTIA SecurityX Certification Exam CAS-005 Prüfungsfragen mit Lösungen (Q226-Q231):

226. Frage
A software company deployed a new application based on its internal code repository. Several customers are reporting anti-malware alerts on workstations used to test the application. Which of the following is the most likely cause of the alerts?

- A. Misconfigured code commit
- B. Data leakage
- C. Unsecure bundled libraries
- D. Invalid code signing certificate

Antwort: C

Begründung:
The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third- party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.
Why Unsecure Bundled Libraries?
Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.
Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.
Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.

227. Frage
A global company's Chief Financial Officer (CFO) receives a phone call from someone claiming to be the Chief Executive Officer

(CEO). The caller claims to be stranded and in desperate need of money. The CFO is suspicious, but the caller's voice sounds similar to the CEO's. Which of the following best describes this type of attack?

- A. Spear phishing
- B. Automated exploit generation
- C. Smishing
- D. Deepfake

Antwort: D

Begründung:
This scenario describes an attack where the attacker mimics the CEO's voice to deceive the CFO, likely using AI-generated audio. According to the CompTIA SecurityX CAS-005 study guide (Domain 1: Security Strategy and Risk Management, 1.2), a deepfake attack involves using artificial intelligence to create realistic but fake audio, video, or other media to impersonate someone. In this case, the voice similarity suggests a deepfake audio attack, which is a targeted social engineering tactic.
Option A: Smishing involves SMS-based phishing, not voice calls.
Option C: Automated exploit generation refers to creating software exploits, not impersonation.
Option D: Spear phishing targets specific individuals but typically via email, not voice-based impersonation.
Option B: Deepfake is the most accurate, as it describes AI-driven impersonation of the CEO's voice.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide, Domain 1: Security Strategy and Risk Management, Section 1.2: "Identify advanced social engineering attacks, including deepfakes." CAS-005 Exam Objectives, 1.2: "Analyze the impact of AI-based attacks on security."

228. Frage
Which of the following key management practices ensures that an encryption key is maintained within the organization?

- A. Encrypting using encryption and key storage systems provided by the cloud provider
- B. Encrypting using a key stored in an on-premises hardware security module
- C. Encrypting using server-side encryption capabilities provided by the cloud provider
- D. Encrypting using a key escrow process for storage of the encryption key

Antwort: B

Begründung:
Comprehensive and Detailed Step by Step
Understanding the Scenario: The question is about ensuring that an organization retains control over its encryption keys. It focuses on different key storage and management methods.
Analyzing the Answer Choices:
A . Encrypting using a key stored in an on-premises hardware security module (HSM): This is the best option for maintaining complete control over encryption keys. An HSM is a dedicated, tamper-resistant hardware device specifically designed for secure key storage and cryptographic operations. Storing keys on-premises within an HSM ensures the organization has exclusive access.
Reference:
B . Encrypting using server-side encryption capabilities provided by the cloud provider: With server-side encryption, the cloud provider typically manages the encryption keys. This means the organization is relinquishing some control over the keys.
C . Encrypting using encryption and key storage systems provided by the cloud provider: Similar to option B, using cloud-provider-managed key storage systems means the organization doesn't have full, exclusive control over the keys.
D . Encrypting using a key escrow process for storage of the encryption key: Key escrow involves entrusting a third party with a copy of the encryption key. This introduces a potential security risk, as the organization no longer has sole control over the key. Also, the key is not maintained within the organization.
Why A is the Correct answer:
Control: On-premises HSMs provide the highest level of control over encryption keys. The organization has physical and logical control over the HSM and the keys stored within it.
Security: HSMs are designed to be tamper-resistant and protect keys from unauthorized access, even if the surrounding systems are compromised.
Compliance: In some industries, regulatory requirements may mandate that organizations maintain direct control over their encryption keys. On-premises HSMs can help meet these requirements.
CASP+ Relevance: HSMs, key management, and data encryption are fundamental topics in CASP+. The exam emphasizes understanding the security implications of different key management approaches.
Elaboration on Key Management Principles:

Key Lifecycle Management: Proper key management involves managing the entire lifecycle of a key, from generation and storage to rotation and destruction.
Separation of Duties: It's generally a good practice to separate the roles of key management and data encryption to enhance security.
Access Control: Strict access controls should be in place to limit who can access and use encryption keys.
In conclusion, using an on-premises HSM for key storage is the best way to ensure that an organization maintains control over its encryption keys. It provides the highest level of security and control, aligning with best practices in cryptography and key management as emphasized in the CASP+ exam objectives.

229. Frage
An administrator brings the company's fleet of mobile devices into its PKI in order to align device WLAN NAC configurations with existing workstations and laptops. Thousands of devices need to be reconfigured in a cost-effective, time-efficient, and secure manner. Which of the following actions best achieve this goal? (Select two)

- A. Submitting a CSR to the CA to obtain a single certificate that can be used across all devices
- B. Deploying netAuth extended key usage certificate templates
- C. Deploying serverAuth extended key usage certificate templates
- D. Configuring SCEP on the CA with an OTP for bulk device enrollment
- E. Deploying clientAuth extended key usage certificate templates
- F. Using the existing MDM solution to integrate with directory services for authentication and enrollment

Antwort: D,F

Begründung:
For bulk PKI enrollment:
MDM integration with directory services streamlines certificate request and deployment per device, leveraging existing authentication methods.
Simple Certificate Enrollment Protocol (SCEP) with one-time passwords allows automated, secure, large-scale certificate issuance without manual CSR handling.
clientAuth templates are used for device authentication, but selecting it alone is insufficient without automated enrollment mechanisms.
A single certificate for all devices violates PKI security principles and compromises individual device accountability.

230. Frage
A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes The following email headers are being reviewed
Which of thefollowing is the best action for the security analyst to take?

- A. Block vendor com for repeated attempts to send suspicious messages
- B. Reroute all messages with unusual security warning notices to the IT administrator
- C. Block messages from hr-saas.com because it is not a recognized domain.
- D. Quarantine all messages with sales-mail.com in the email header

Antwort: A

Begründung:
In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here's the analysis of the options provided:
A . Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.
B . Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.
C . Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.
D . Block vendor com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.
Reference:
CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated

suspicious activity.
NIST Special Publication 800-45 Version 2, "Guidelines on Electronic Mail Security": Provides guidelines on email security, including the management of suspicious email domains.
"Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.
By blocking the domain that has consistently attempted to send suspicious messages, the security analyst can effectively reduce the risk of phishing attacks.

231. Frage

.....

Wollen Sie größere Errungenschaften in der IT-Branche erzielen, dann ist es richtig, ZertPruefung zu wählen. Die Schulungsunterlagen zur CompTIA CAS-005 Zertifizierungsprüfung aus ZertPruefung werden von den erfahrenen Experten durch ständige Praxis und Forschung bearbeitet. Sie verfügen über hohe Genauigkeiten und große Reichweite. Haben Sie die Schulungsunterlagen zur CompTIA CAS-005 Zertifizierungsprüfung aus ZertPruefung, dann haben Sie den Schlüssel zum Erfolg.

CAS-005 Prüfungsfrage: https://www.zertpruefung.ch/CAS-005_exam.html

Laden Sie die neuesten ZertPruefung CAS-005 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1LErwjflYW2ybzXk0GVHFfG2BlKg_wxrH