The CompTIA CAS-005 Online Practice Test Engine

BONUS!!! Download part of TestInsides CAS-005 dumps for free: https://drive.google.com/open?id=1LbgdF_-F9EsRYEznqYS8sCWVEX4w93e2

Eliminates confusion while taking the CompTIA CAS-005 certification exam. Prepares you for the format of your CAS-005 exam dumps, including multiple-choice questions and fill-in-the-blank answers. Comprehensive, up-to-date coverage of the entire CompTIA SecurityX Certification Exam (CAS-005) certification curriculum. CompTIA CAS-005 practice questions are based on recently released CAS-005 exam objectives.

For years our team has built a top-ranking brand with mighty and main which bears a high reputation both at home and abroad. The sales volume of the CAS-005 Study Materials we sell has far exceeded the same industry and favorable rate about our products is approximate to 100%. Why the clients speak highly of our CAS-005 study materials? Our dedicated service, high quality and passing rate and diversified functions contribute greatly to the high prestige of our products. We provide free trial service before the purchase, the consultation service online after the sale, free update service and the refund service in case the clients fail in the test.

>> CAS-005 Practice Exams Free <<

Reliable CAS-005 Exam Tips & CAS-005 Valid Test Registration

Practice tests (desktop and web-based) provide an CompTIA CAS-005 examination scenario so your preparation for the CompTIA SecurityX Certification Exam (CAS-005) exam becomes quite easier. Since the real CAS-005 examination costs a high penny, TestInsides provide a free demo of CompTIA CAS-005 Exam Dumps before your purchase. The free demo of the CompTIA SecurityX Certification Exam (CAS-005) exam prep material is helpful to remove your doubts about it. The product is available in three versions which are PDF, Web-based practice test, and Desktop practice test software.

CompTIA CAS-005 Exam Syllabus Topics:

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

CompTIA SecurityX Certification Exam Sample Questions (Q88-Q93):

NEW QUESTION # 88
During a vulnerability assessment, a scan reveals the following finding:
Windows Server 2016 Missing hotfix KB87728 - CVSS 3.1 Score: 8.1 [High] - Affected host 172.16.15.2 Later in the review process, the remediation team marks the finding as a false positive. Which of the following is the best way toavoid this issue on future scans?

- A. Configuring the sensor with an advanced policy for fingerprinting servers
- B. Coordinating the scan execution with the remediation team early in the process
- C. Performing an authenticated scan on the servers
- D. Getting an up-to-date list of assets from the CMDB

Answer: C

Explanation:
Authenticated scans allow the scanner to verify installed patches and configurations, reducing false positives.
Other options:
A (CMDB updates) improve asset tracking but do not validate patch installations.
C (Advanced fingerprinting) improves accuracy but does not replace authentication.
D (Coordination with teams) is good practice but does not prevent false positives.
Reference: CASP+ CAS-005 - Vulnerability Scanning and RiskManagement

NEW QUESTION # 89
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. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA
- B. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA
- C. Removing support for CBC-based key exchange and signing algorithms
- D. Disallowing cipher suites that use ephemeral modes of operation for key agreement
- E. Implementing HIPS rules to identify and block BEAST attack attempts
- F. Adding TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256

Answer: C,F

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:
* B. 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.
* C. 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.
References:
* CompTIA Security+ Study Guide

* NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"
* OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

NEW QUESTION # 90
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?
Supply chain attack B. Cipher substitution attack C. Side-channel analysis D. On-path attack E. Pass-the-hash attack Explanation:
Step by Step Explanation:
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:

- A. On-path attack (formerly man-in-the-middle): This attack involves intercepting and potentially altering communication between two parties. While important, it's not theprimary focus of the registry.
- B. 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.
- C. 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.
- D. Supply chain attack: This type of attack involves compromising the software supply chain by injecting malicious code into legitimate software packages.
  Reference: CASP+ objectives often emphasize supply chain security due to its growing importance. The scenario directly relates to this type of attack, as the registry helps ensure that software packages haven't been tampered with during the supply chain process.
- E. 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.

Answer: D

Explanation:
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.

NEW QUESTION # 91
A company's help desk is experiencing a large number of calls from the finance department slating access issues to www bank com The security operations center reviewed the following security logs:
Which of the following is most likely the cause of the issue?

- A. DNS traffic is being sinkholed.
- B. The DNS record has been poisoned.
- C. The DNS was set up incorrectly.

- D. Recursive DNS resolution is failing

Answer: A

Explanation:
Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.
In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.
Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.
DNS poisoning (B) could result in usersbeing directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.
Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.
By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.
Reference:
CompTIA SecurityX study materials on DNS security mechanisms.
Standard HTTP status codes and their implications.

NEW QUESTION # 92
A cloud engineer configured mail security protocols to support email authenticity and wants to enable the flow of email security information to a third-party platform for further analysis. Which of the following must be configured correctly?

- A. SPF
- B. DMARC
- C. DKIM
- D. TLS

Answer: B

NEW QUESTION # 93
.....

- Exam Dumps CAS-005 Free CAS-005 Sample Questions Reliable CAS-005 Test Labs Easily obtain ➽ CAS-005 for free download through ➠ www.pdfvce.com CAS-005 Books PDF
- Updated CAS-005 Test Cram Download CAS-005 Fee CAS-005 Test Tutorials Simply search for ➤ CAS-005 for free download on ☀ www.testkingpass.com ☀ New CAS-005 Real Test
- Latest CAS-005 Practice Exams Free Covers the Entire Syllabus of CAS-005 Search for ➽ CAS-005 and easily obtain a free download on www.pdfvce.com Updated CAS-005 Test Cram
- CAS-005 Complete Exam Dumps Updated CAS-005 Test Cram Exam Dumps CAS-005 Free Download ➥ CAS-005 for free by simply searching on www.prep4away.com CAS-005 Test Review
-