Features of Three Formats CompTIA CAS-005 Exam Questions

P.S. Free & New CAS-005 dumps are available on Google Drive shared by Pass4Leader: https://drive.google.com/open?id=1Th4sww3JTM78EALSf5XA7C7sGj63I4Sy

In this society, only by continuous learning and progress can we get what we really want. It is crucial to keep yourself survive in the competitive tide. Many people want to get a CAS-005 certification, but they worry about their ability. So please do not hesitate and join our study. Our CAS-005 exam question will help you to get rid of your worries and help you achieve your wishes. So you will have more opportunities than others and get more confidence. Our CAS-005 Quiz guide is based on the actual situation of the customer. Customers can learn according to their actual situation and it is flexible. Next I will introduce the advantages of our CAS-005 test prep so that you can enjoy our products.

CompTIA CAS-005 Exam Syllabus Topics:

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

>> Reliable CAS-005 Test Topics <<

Valid CAS-005 Test Duration, Reliable CAS-005 Study Notes

Pass4Leader CAS-005 Questions have helped thousands of candidates to achieve their professional dreams. Our CompTIA

SecurityX Certification Exam (CAS-005) exam dumps are useful for preparation and a complete source of knowledge. If you are a full-time job holder and facing problems finding time to prepare for the CompTIA CAS-005 Exam Questions, you shouldn't worry more about it.

CompTIA SecurityX Certification Exam Sample Questions (Q318-Q323):

NEW QUESTION # 318
A senior security engineer flags the following log file snippet as having likely facilitated an attacker's lateral movement in a recent breach:
qry_source: 19.27.214.22 TCP/53
qry_dest: 199.105.22.13 TCP/53
qry_type: AXFR
| in comptia.org
---------- directoryserver1 A 10.80.8.10
---------- directoryserver2 A 10.80.8.11
---------- directoryserver3 A 10.80.8.12
---------- internal-dns A 10.80.9.1
---------- www-int A 10.80.9.3
---------- fshare A 10.80.9.4
---------- sip A 10.80.9.5
---------- msn-crit-apcs A 10.81.22.33
Which of the following solutions, if implemented, would mitigate the risk of this issue reoccurring?

- A. Permitting only clients from internal networks to query DNS
- B. Implementing DNS masking on internal servers
- C. Restricting DNS traffic to UDP/53
- D. Disabling DNS zone transfers

Answer: D

Explanation:
Comprehensive and Detailed
The log shows an AXFR (zone transfer) query, which exposed internal DNS records, aiding lateral movement. Let's evaluate:
A . Disabling DNS zone transfers: AXFR allows full DNS zone data to be transferred. Disabling it externally prevents attackers from mapping internal networks, directly mitigating this issue per CAS-005's security operations focus.
B . Restricting to UDP/53: AXFR uses TCP/53, so this wouldn't stop it.
C . DNS masking: Obscures records but isn't a standard term for this fix.
D . Internal-only queries: Helps but doesn't fully prevent external AXFR if misconfigured.

NEW QUESTION # 319
An organization wants to create a threat model to identity vulnerabilities in its infrastructure. Which of the following, should be prioritized first?

- A. External-facing Infrastructure with known exploited vulnerabilities
- B. Internal infrastructure with high-seventy and Known exploited vulnerabilities
- C. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource
- D. External facing Infrastructure with a low risk score and no known exploited vulnerabilities

Answer: A

Explanation:
When creating a threat model to identify vulnerabilities in an organization's infrastructure, prioritizing external-facing infrastructure with known exploited vulnerabilities is critical. Here's why:
Exposure to Attack: External-facing infrastructure is directly exposed to the internet, making it a primary target for attackers. Any vulnerabilities in this layer pose an immediate risk to the organization's security.
Known Exploited Vulnerabilities: Vulnerabilities that are already known and exploited in the wild are of higher concern because they are actively being used by attackers. Addressing these vulnerabilities reduces the risk of exploitation significantly.
Risk Mitigation: By prioritizing external-facing infrastructure with known exploited vulnerabilities, the organization can mitigate the most immediate and impactful threats, thereby improving overall security posture.

NEW QUESTION # 320
An organization determines existing business continuity practices areinadequateto support critical internal process dependencies during a contingency event. Acompliance analystwants the Chief Information Officer (CIO) to identify the level ofresidual riskthat is acceptable to guide remediation activities. Which of the following does the CIO need to clarify?

- A. Impact
- B. Mitigation
- C. Appetite
- D. Likelihood

Answer: C

Explanation:
Understanding Residual Risk:
Residual riskis the amount of risk remainingafter controls and mitigations have been applied.
Risk appetitedefines the level of risk an organization iswilling to acceptbefore taking additional actions.
Why Option D is Correct:
TheCIO must clarify the organization's "Risk Appetite"to determinehow much residual risk is acceptable.
If risk exceeds the appetite,additional security measuresneed to be implemented.
This aligns withISO 31000andNIST Risk Management Framework (RMF).
Why Other Options Are Incorrect:
A (Mitigation):Mitigationrefers toreducing risk, but it doesn't define the acceptable level of residual risk.
B (Impact):Impact assessment measurespotential damage, but it does not determine what is acceptable.
C (Likelihood):Likelihood is theprobability of risk occurring, but not what level isacceptable.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide:Risk Management & Business Continuity NIST SP 800-37:Risk Management Framework ISO 27005:Risk Tolerance & Acceptance

NEW QUESTION # 321
A security engineer must resolve a vulnerability in a deprecated version of Python for a custom-developed flight simul-ation application that is monitored and controlled remotely. The source code is proprietary and built with Python functions running on the Ubuntu operating system. Version control is not enabled for the application in development or production. However, the application must remain online in the production environment using built-in features. Which of the following solutions best reduces theattack surface of these issues and meets the outlined requirements?

- A. Configure version designation within the Python interpreter. Update Python with aptitude, and update modules with pip in a test environment. Deploy the solution to production.
- B. Configure code-signing within the CI/CD pipeline, update Python with aptitude, and update modules with pip in a test environment. Deploy the solution to production.
- C. Enable branch protection in the GitHub repository. Update Python with aptitude, and update modules with pip in a test environment. Deploy the solution to production.
- D. Use an NFS network share. Update Python with aptitude, and update modules with pip in a test environment. Deploy the solution to production.

Answer: B

Explanation:
Code-signing within theCI/CD pipelineensures that only verified and signed code is deployed, mitigating the risk of supply chain attacks. Updating Python withaptitudeand updating modules withpipensures vulnerabilities are patched. Deploying the solution to production after testing maintains application availability while securing the development lifecycle.
* Branch protection (B)applies only to version-controlled environments, which is not the case here.
* NFS network share (C)does not address the deprecated Python vulnerability.
* Version designation (D)does not eliminate security risks from outdated dependencies.
Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 3.0 (Security Engineering), Section onSoftware Assurance and Secure Development

NEW QUESTION # 322

Users are experiencing a variety of issues when trying to access corporate resources examples include
* Connectivity issues between local computers and file servers within branch offices
* Inability to download corporate applications on mobile endpoints wtiilc working remotely
* Certificate errors when accessing internal web applications
Which of the following actions are the most relevant when troubleshooting the reported issues? (Select two).

- A. Restore static content on lite CDN.
- B. Validate MDM asset compliance
- C. Implement advanced WAF rules.
- D. Check IPS rules
- E. Enable secure authentication using NAC
- F. Review VPN throughput

Answer: B,F

Explanation:
The reported issues suggest problems related to network connectivity, remote access, and certificate management:
A . Review VPN throughput: Connectivity issues and the inability to download applications while working remotely may be due to VPN bandwidth or performance issues. Reviewing and optimizing VPN throughput can help resolve these problems by ensuring that remote users have adequate bandwidth for accessing corporate resources.
F . Validate MDM asset compliance: Mobile Device Management (MDM) systems ensure that mobile endpoints comply with corporate security policies. Validating MDM compliance can help address issues related to the inability to download applications and certificate errors, as non-compliant devices might be blocked from accessing certain resources.
B . Check IPS rules: While important for security, IPS rules are less likely to directly address the connectivity and certificate issues described.
C . Restore static content on the CDN: This action is related to content delivery but does not address VPN or certificate-related issues.
D . Enable secure authentication using NAC: Network Access Control (NAC) enhances security but does not directly address the specific issues described.
E . Implement advanced WAF rules: Web Application Firewalls protect web applications but do not address VPN throughput or mobile device compliance.
Reference:
CompTIA Security+ Study Guide
NIST SP 800-77, "Guide to IPsec VPNs"
CIS Controls, "Control 11: Secure Configuration for Network Devices"

NEW QUESTION # 323
.....

Our CAS-005 exam braindump is revised and updated according to the change of the syllabus and the latest development situation in the theory and the practice. The CAS-005 exam torrent is compiled elaborately by the experienced professionals and of high quality. The contents of CAS-005 guide questions are easy to master and simplify the important information. It conveys more important information with less answers and questions, thus the learning is easy and efficient. The language is easy to be understood makes any learners have no obstacles to study and pass the CAS-005 Exam.

- 100% Pass Quiz CAS-005 - CompTIA SecurityX Certification Exam Latest Reliable Test Topics □ Copy URL ▸ www.pdfvce.com ◂ open and search for ➠ CAS-005 □ to download for free □CAS-005 Reliable Test Experience
- Pass Leader CAS-005 Dumps □ Download CAS-005 Fee □ CAS-005 Valid Braindumps Ppt □ Open website □ www.pdfdumps.com □ and search for ⇛ CAS-005 ⇚ for free download □CAS-005 Reliable Test Price
- CAS-005 Valid Braindumps Sheet □ CAS-005 Valid Test Braindumps □ CAS-005 Latest Exam Vce □ Download □ CAS-005 □ for free by simply searching on ▹ www.pdfvce.com ◃ □Pass Leader CAS-005 Dumps
- Latest CAS-005 Exam Questions □ Reliable CAS-005 Exam Papers ✉ Latest CAS-005 Training □ Go to website " www.examdiscuss.com " open and search for 《 CAS-005 》 to download for free □Download CAS-005 Fee
- Frenquent CAS-005 Update □ CAS-005 Valid Braindumps Ppt □ CAS-005 Valid Braindumps Ppt □ Search on 【 www.pdfvce.com 】 for 《 CAS-005 》 to obtain exam materials for free download □Free CAS-005 Vce Dumps
- Latest CAS-005 Training □ Reliable CAS-005 Exam Papers □ Reliable CAS-005 Exam Papers □ Easily obtain □ CAS-005 □ for free download through ➥ www.prepawayexam.com □ □Reliable CAS-005 Exam Papers
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.notebook.ai, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, portfolium.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of Pass4Leader CAS-005 dumps from Cloud Storage: https://drive.google.com/open?id=1Th4sww3JTM78EALSf5XA7C7sGj63I4Sy