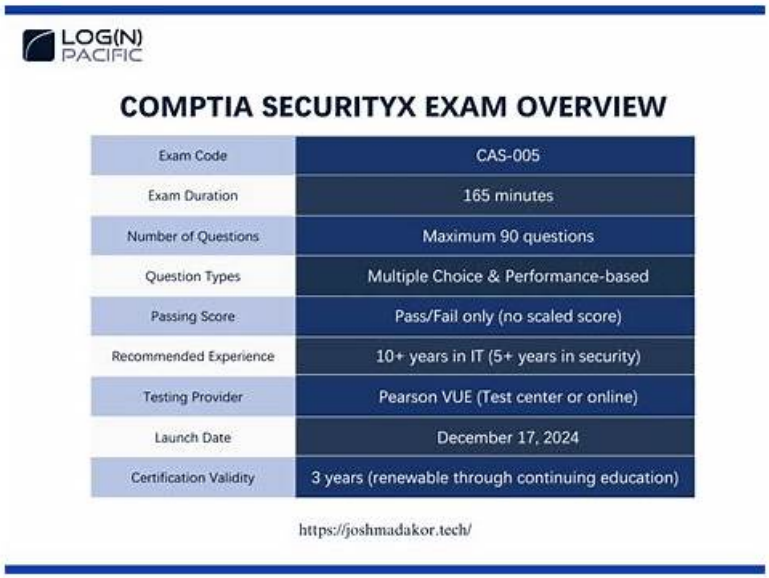
CAS-005 Exam Questions - CompTIA SecurityX Certification Exam Torrent Prep & CAS-005 Test Guide



What's more, part of that DumpExam CAS-005 dumps now are free: https://drive.google.com/open?id=1AIAaFeEASWNOBb1BTYd-9_Yyi7XG3i9v

DumpExam gives you unlimited online access to CAS-005 certification practice tools. You can instantly download the CAS-005 test engine and install it on your PDF reader, laptop or phone, then you can study it in the comfort of your home or while at office. Our CAS-005 test engine allows you to study anytime and anywhere. In addition, you can set the time for each test practice of CAS-005 simulate test. The intelligence and customizable CAS-005 training material will help you get the CAS-005 certification successfully.

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

>> CAS-005 Latest Test Labs <<

Exam Sample CAS-005 Online, Valid CAS-005 Test Materials

Although the CAS-005 exam prep is of great importance, you do not need to be over concerned about it. With scientific review and arrangement from professional experts as your backup, and the most accurate and high quality content of our CAS-005 Study Materials, you will cope with it like a piece of cake. So our CAS-005 learning questions will be your indispensable practice materials during your way to success.

CompTIA SecurityX Certification Exam Sample Questions (Q13-Q18):

NEW QUESTION # 13
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 the following is the best action for the security analyst to take?

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

Answer: C

Explanation:
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.

NEW QUESTION # 14
After a leak of important documents, a company decides to implement a data protection program to avoid similar incidents in the future. Which of the following should the company do first?

- A. Perform data storage hardening.
- B. Develop data labeling standards.
- C. Deploy a data loss prevention policy.
- D. Implement data encryption.

Answer: B

Explanation:
Developing data labeling standards is the first step in a data protection program. It ensures that data is classified according to sensitivity, which then informs the appropriate encryption, storage hardening, and DLP policies to apply.

NEW QUESTION # 15
A product development team has submitted code snippets for review prior to release.
INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1
Code Snippet 2
Vulnerability 1:
* SQL injection

* Cross-site request forgery
* Server-side request forgery
* Indirect object reference
* Cross-site scripting
Fix 1:
* Perform input sanitization of the userid field.
* Perform output encoding of queryResponse,
* Ensure usex:ia belongs to logged-in user.
* Inspect URLS and disallow arbitrary requests.
* Implement anti-forgery tokens.
Vulnerability 2
1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind
variables.
B) Remove the serve_forever instruction.
C) Prevent the "authenticated" value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

Answer:

Explanation:
Code Snippet 1
Vulnerability 1: SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1: Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.
Code Snippet 2
Vulnerability 2: Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2: Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti- forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

NEW QUESTION # 16
A security analyst notices a number of SIEM events that show the following activity:
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop HinDctend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptidcasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell -> 40.90.23.154:443
Which of the following response actions should the analyst take first?

- A. Disable local administrator privileges on the endpoints
- B. Configure the forward proxy to block 40.90.23.154
- C. Disable powershell.exe on all Microsoft Windows endpoints
- D. Restart Microsoft Windows Defender

Answer: B

Explanation:
The first immediate action in an active incident iscontainment.Blocking the IP address (40.90.23.154)at the network edge prevents further communication with the malicious external server. Disabling PowerShell or removing local admin privileges are valid hardening steps, but containment by network control is the highest priority during an active compromise to stop data exfiltration or further command and control activity.
Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply incident response techniques focusing on immediate containment actions.

NEW QUESTION # 17
After an organization met with its ISAC, the organization decided to test the resiliency of its security controls against a small number of advanced threat actors. Which of the following will enable the security administrator to accomplish this task?

- A. Reliability factors
- B. Internal reconnaissance
- C. Deployment of a honeypot
- D. Adversary emulation

Answer: D

Explanation:
Comprehensive and Detailed Explanation:
Adversary emulation simulates specific advanced persistent threat (APT) behaviors and techniques to test an organization's security posture. In SecurityX CAS-005, this is part of red-teaming and purple-teaming strategies for realistic resilience testing.
* Reliability factors (B) relate to operational uptime, not threat simulation.
* Honeypots (C) attract attackers but do not directly emulate specific adversaries.
* Internal reconnaissance (D) is one phase of an attack simulation, not the full emulation of advanced threat actors.

NEW QUESTION # 18
.....

and easily obtain a free download on ▶ www.pdfvce.com ◀ □CAS-005 Study Group

- Use CompTIA CAS-005 Exam Questions And Get Excellent Marks □ Download ☀ CAS-005 □☀□ for free by simply entering ☀ www.vce4dumps.com □☀□ website □CAS-005 Valid Study Plan
- zakarianima714669.shivawiki.com, yesbookmarks.com, businessbookmark.com, lms.sitekit.id, finniantfzo967362.bloggactif.com, deaconnogf802941.wikicarrier.com, bookmarklinking.com, linkedbookmarker.com, socialwebconsult.com, arungxpq168301.livebloggs.com, Disposable vapes

P.S. Free & New CAS-005 dumps are available on Google Drive shared by DumpExam: https://drive.google.com/open?id=1AIAaFeEASWNOBb1BTYd-9_Yyi7XG3i9v