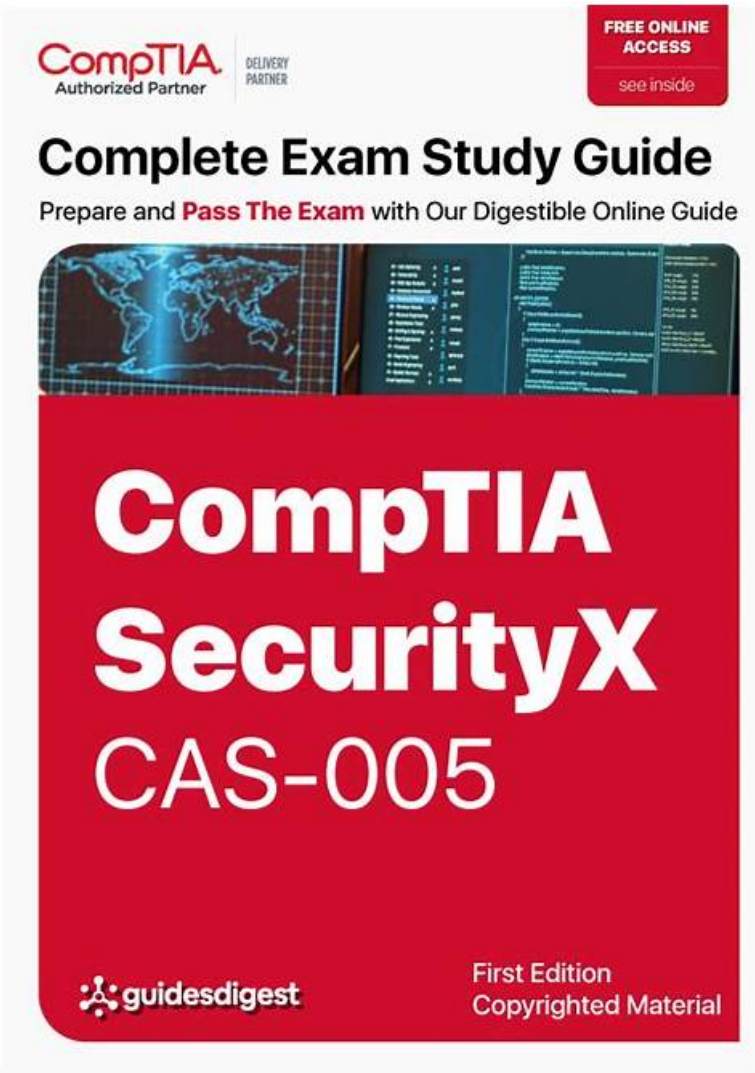
Valid Test CAS-005 Tips & Reliable CAS-005 Exam Bootcamp



P.S. Free 2026 CompTIA CAS-005 dumps are available on Google Drive shared by Exam4Labs: https://drive.google.com/open?id=1lBHehvI3Dk-IwC8u37DTTOgo5AGdpc_n

Our CAS-005 Research materials design three different versions for all customers. These three different versions include PDF version, software version and online version, they can help customers solve any problems in use, meet all their needs. Although the three major versions of our CAS-005 Learning Materials provide a demo of the same content for all customers, they will meet different unique requirements from a variety of users based on specific functionality.

Gone are the days when CAS-005 hadn't their place in the corporate world. With the ever-increasing popularity of the CAS-005 devices and software, now CAS-005 certified professionals are the utmost need of the industry, round the globe. Particularly, advertisement agencies and the media houses have enough room for CAS-005 Certified. CAS-005 dumps promises you to bag your dream CAS-005 certification employing minimum effort and getting the best results you have ever imagined.

>> Valid Test CAS-005 Tips <<

Best Professional CompTIA Valid Test CAS-005 Tips - CAS-005 Free Download

It is well known that certificates are not versatile, but without a CompTIA CAS-005 certification you are a little inferior to the same

competitors in many ways. Compared with the people who have the same experience, you will have the different result and treatment if you have a CompTIA SecurityX Certification Exam CAS-005 Certification.

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	• 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 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 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.

CompTIA SecurityX Certification Exam Sample Questions (Q110-Q115):

NEW QUESTION # 110
A security analyst is reviewingsuspicious log-in activity and sees the following data in the SICM:

Account	Application	Authorization server	Status	Risk
SALES1	Customer manager	LDAP-US	Success	Low
SALES1	Payroll	LDAP-US	Success	Low
ADMIN	Email	LDAP-US	Failure	High
SALES1	Email	LDAP-EU	Unknown	Unknown
MARKET1	Customer manager	LDAP-US	Success	Low
FINANCE1	Payroll	LDAP-EU	Unknown	Unknown

Which of the following is the most appropriate action for the analyst to take?

- A. Block employees from logging in to applications that are not part of their business area.
- B. implement automation to disable accounts that nave been associated with high-risk activity.
- C. Have the admin account owner change their password to avoid credential stuffing.
- D. Update the log configuration settings on the directory server that Is not being captured properly.

Answer: B

Explanation:
The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.
Updating log configuration settings (A) may help in better logging future activities but does not address the immediate threat.
Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.
Blocking employees (C) from logging into non-business applications might help in reducing attack surfaces but doesn't directly address the compromised account issue.
Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.
Reference:
CompTIA SecurityX guide on incident response and account management.
Best practices for handling compromised accounts.
Automation tools and techniques for security operations centers (SOCs).

NEW QUESTION # 111
A security engineer receives an alert from the SIEM platform indicating a possible malicious action on the internal network. The engineer generates a report that outputs the logs associated with the incident:

Date	Time	Action	Details
01/23/2024	08:02:41	Login success	JohnS login attempt into VM001
01/24/2024	08:03:32	Login success	JohnS login attempt into SV002
01/25/2024	08:02:12	Login success	JohnS login attempt into VM001
01/26/2024	08:03:21	Login success	JohnS login attempt into VM001
01/26/2024	23:52:41	Login success	JohnS login attempt into SV002
01/27/2024	08:02:54	Login success	JohnS login attempt into SV002

Which of the following actions best enables the engineer to investigate further?

- A. Querying user behavior analytics data
- B. Searching dark web monitoring resources for exposure
- C. Consulting logs from the enterprise password manager
- D. Reviewing audit logs from privileged actions

Answer: A

NEW QUESTION # 112
An analyst reviews a SIEM and generates the following report:

Host	Rule	Offense Trigger
VM002	Network connection	TCP connection generated to web.corp.local
HOST002	Network connection	Web navigation to comptia.org
HOST002	File download	File download from web browser from web.corp.local
VM002	Network connection	Web navigation to web.corp.local
HOST002	Network connection	Web navigation to comptia.org/files
HOST002	Log-in activity	Log-in successful after two attempts

Only HOST002 is authorized for internet traffic. Which of the following statements is accurate?

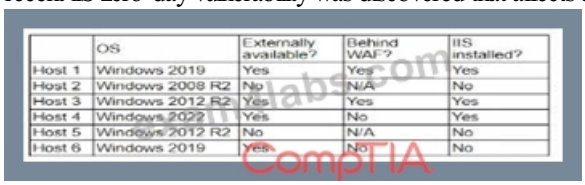
- A. The HOST002 host is under attack, and a security incident should be declared.
- B. The network connection activity is unusual, and a network infection is highly possible.
- C. The SIEM platform is reporting multiple false positives on the alerts.
- D. The VM002 host is misconfigured and needs to be revised by the network team.

Answer: B

Explanation:
Comprehensive and Detailed
Understanding the Security Event:
HOST002 is the only device authorized for internet traffic. However, the SIEM logs show that VM002 is making network connections to web.corp.local.
This indicates unauthorized access, which could be a sign of lateral movement or network infection.
This is a red flag for potential malware, unauthorized software, or a compromised host.
Why Option D is Correct:
Unusual network traffic patterns are often an indicator of a compromised system.
VM002 should not be communicating externally, but it is.
This suggests a possible breach or malware infection attempting to communicate with a command-and-control (C2) server.
Why Other Options Are Incorrect:
A (Misconfiguration): While a misconfiguration could explain the unauthorized connections, the pattern of activity suggests something more malicious.
B (Security incident on HOST002): The issue is not with HOST002. The suspicious activity is from VM002.
C (False positives): The repeated pattern of unauthorized connections makes false positives unlikely.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide: Chapter on SIEM & Incident Analysis MITRE ATT&CK Tactics: Lateral

Movement & Network-based Attacks

NEW QUESTION # 113
A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent llS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:



	OS	Externally available?	Behind WAF?	IIS installed?
Host 1	Windows 2019	Yes	Yes	Yes
Host 2	Windows 2008 R2	No	N/A	No
Host 3	Windows 2012 R2	Yes	Yes	Yes
Host 4	Windows 2022	Yes	No	Yes
Host 5	Windows 2012 R2	No	N/A	No
Host 6	Windows 2019	Yes	No	No

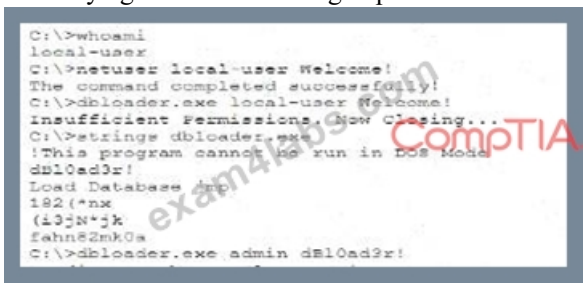
Which of the following hosts should a security analyst patch first once a patch is available?

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4
- F. 5

Answer: A

Explanation:
Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the securityanalyst should patch Host 1 first. Here's why:
Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.
Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.
Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-40: Guide toEnterprise Patch Management Technologies CIS Controls: Control 3 - Continuous Vulnerability Management

NEW QUESTION # 114
Recent repents indicate that a software tool is being exploited Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation.
The analyst generates the following output:



```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>strings dbloader.exe
!This program cannot be run in DOS mode
dBl0ad3r!
Load Database Inp
182(*nx
(i3jN*jk
fahn82mk0a
C:\>dbloader.exe admin dBl0ad3r!
```

Which of the following would the analyst most likely recommend?

- A. Removing hard coded credentials from the source code
- B. Installing appropriate EDR tools to block pass-the-hash attempts
- C. Adding additional time to software development to perform fuzz testing
- D. Not allowing users to change their local passwords

Answer: A

Explanation:
The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access

controls and load the database. The mostlikely recommendation is to remove hard-coded credentials from the source code. Here's why:
Security Best Practices: Hard-coded credentials are a significant security risk because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.
Credential Management: Credentials should be managed securely using environment variables, secure vaults, or configuration management tools that provide encryption and access controls.
Mitigation of Exploits: By eliminating hard-coded credentials, the organization can prevent attackers from easily bypassing authentication mechanisms and gaining unauthorized access to sensitive systems.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
OWASP Top Ten: Insecure Design
NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

NEW QUESTION # 115
.....

More and more people hope to enhance their professional competitiveness by obtaining CAS-005 certification. However, under the premise that the pass rate is strictly controlled, fierce competition makes it more and more difficult to pass the CAS-005 examination. In order to guarantee the gold content of the CAS-005 Certification, the official must also do so. However, it is an indisputable fact that a large number of people fail to pass the CAS-005 examination each year, some of them may choose to give it up while others may still choose to insist.