CompTIA CAS-005 Practice Test Prepare for Success

BTW, DOWNLOAD part of PracticeDump CAS-005 dumps from Cloud Storage: https://drive.google.com/open?id=1I6ea_PCZrOFsFSr9PtB2UnAKc2fcyUIp

If you want to clear CompTIA real exams but doubt to us, you can download the free demo of CAS-005 dumps pdf to check. We will provide the one-year free update once you purchase our CAS-005 Practice Questions. I will give you my support if you have any problems and doubts when you learn the CompTIA CASP study materials.

CompTIA CAS-005 Exam Syllabus Topics:

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

>> CAS-005 Valid Test Test <<

CAS-005 Valid Test Discount & Latest CAS-005 Learning Material

Nowadays, so many internet professionals agree that CompTIA exam certificate is a stepping stone to the peak of our life. CAS-

005 exam is an exam concerned by lots of internet professionals. Close to 100% passing rate is the best gift that our customers give us. We also hope our CAS-005 exam materials can help more and more ambitious people pass the CAS-005 exam. Our professional team checks the update of exam materials every day, so please rest assured that the CAS-005 Exam software you are using must contain the latest and most information. We are a team of the exam questions providers CAS-005 exam in internet that ensured you can pass actual test 100%. We have experienced and professional experts to create the latest CAS-005 exam questions and answers many times which are approach to the CAS-005 exam.

CompTIA SecurityX Certification Exam Sample Questions (Q168-Q173):

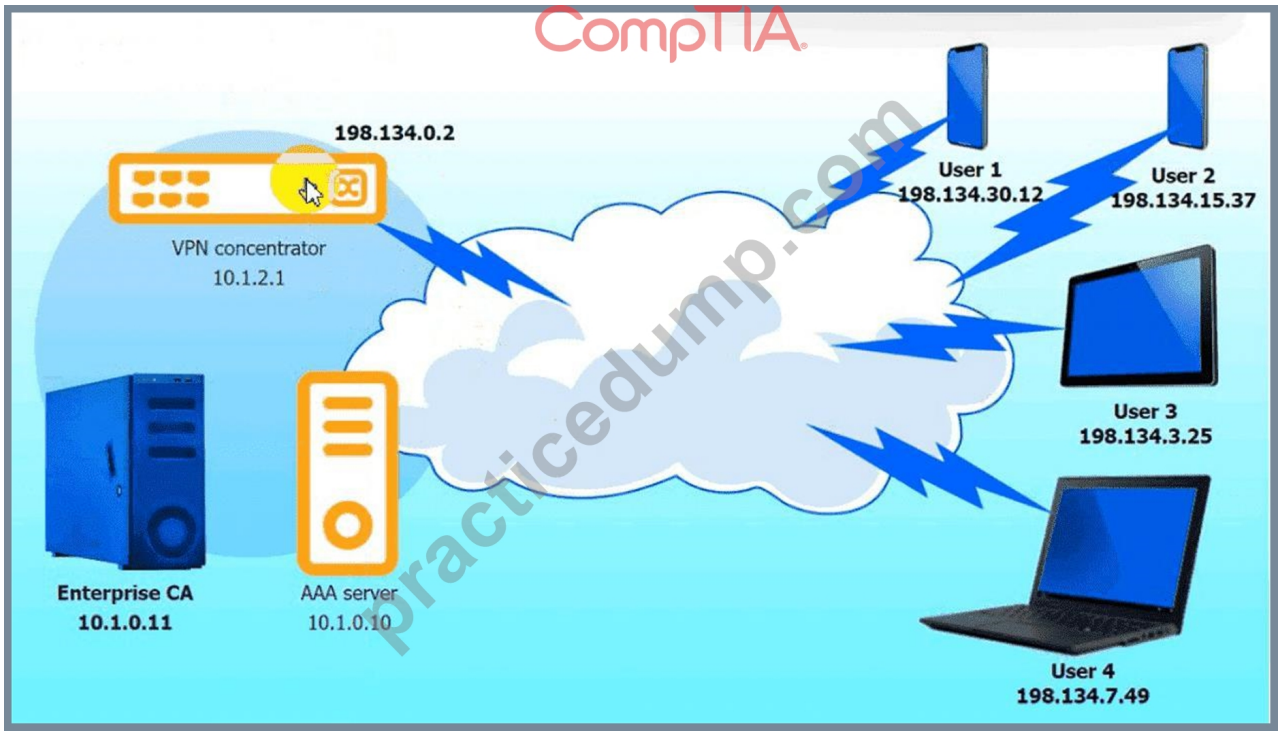
NEW QUESTION # 168
An organization is increasing its focus on training that addresses new social engineering and phishing attacks.
Which of the following is the organization most concerned about?

- A. Generative AI tools increasing the quality of exploits
- B. Meeting existing regulatory compliance
- C. Overreliance on AI support bots
- D. Differential analysis using AI models

Answer: A

Explanation:
The organization is most concerned about Generative AI improving phishing and social engineering attacks.
Tools like ChatGPT can generate highly convincing phishing emails, fake websites, and human-like interactions that bypass traditional detection methods. Employees who were trained to spot poor grammar or obvious scams may now struggle to detect AI-crafted exploits.
Option A relates to compliance but not AI-driven threats. Option B (overreliance on AI bots) is operational risk, not phishing. Option D (differential analysis) applies to AI privacy issues, not phishing.
CAS-005 emphasizes adapting training to emerging threats, including AI-enabled social engineering. This ensures users remain resilient against modern attacks, making C the correct answer.

NEW QUESTION # 169
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:
* The EAP method must use mutual certificate-based authentication (With issued client certificates).
* The IKEv2 Cipher suite must be configured to the MOST secure
authenticated mode of operation,
* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimumlength requirement of eight characters, INSTRUCTIONS Click on the AAA server and VPN concentrator to complete the configuration.
Fill in the appropriate fields and make selections from the drop-down menus.



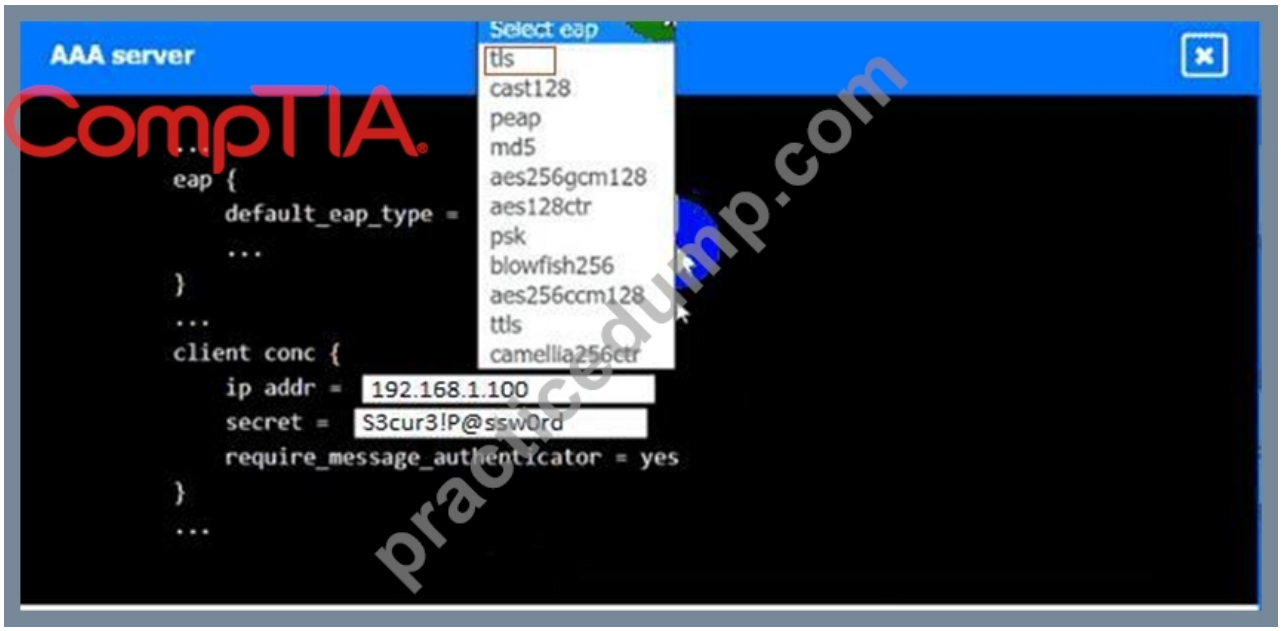
VPN Concentrator:

AAA Server:

Answer:

Explanation:
See the answer below in Explanation.
Explanation:
VPN Concentrator:
A screenshot of a computer Description automatically generated

AAA Server:
A screenshot of a computer Description automatically generated



NEW QUESTION # 170
A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:

```
11 Dec 16:03:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (Windows NT 5.1) Gecko
11 Dec 16:33:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0(Windows NT 5.1) Gecko
11 Dec 22:30:23 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
11 Dec 23:00:23 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
11 Dec 23:05:43 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
11 Dec 23:35:43 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
12 Dec 00:30:53 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
```

A security architect is onboarding a new EDR agent on servers that traditionally do not have internet access.
In order for the agent to receive updates and report back to the management console, some changes must be made. Which of the following should the architect do to best accomplish this requirement? (Select two).

- A. Create a firewall rule to only allow traffic from the subnet to the internet to fully qualified names that are not identified as malicious by the firewall vendor.
- B. Configure a proxy policy that blocks only lists of known-bad, fully qualified domain names.
- C. Configure a proxy policy that blocks all traffic on port 443.
- D. Configure a proxy policy that allows only fully qualified domain names needed to communicate to a portal.
- E. Create a firewall rule to only allow traffic from the subnet to the internet via a proxy.
- F. Create a firewall rule to only allow traffic from the subnet to the internet via port 443.

Answer: D,E

Explanation:
SecurityX CAS-005 endpoint security and network control objectives emphasize least privilege network access.
* Creating a firewall rule to allow outbound traffic only via a proxy (A) ensures centralized inspection and control.
* Configuring the proxy to allow only the required FQDNs for EDR management communication (C) limits exposure to necessary destinations.Options D and E allow broader access than necessary, and B would block required communications entirely. F relies on blocklists instead of allowlists, which is less secure for high-assurance environments.

NEW QUESTION # 171
An auditor is reviewing the logs from a web application to determine the source of an incident. The web application architecture includes an internet-accessible application load balancer, a number of web servers in a private subnet, application servers, and one

database server in a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:
Web server logs:
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET /bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "GET / HTTP/1.1" 200 453 Safari/536.36 Application server logs:
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing Database server logs:
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size1 unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self-signed.
Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

- A. Use stored procedures on the database server.
- B. Install a software-based HIDS on the application servers.
- C. Enable the X-Forwarded-For header at the load balancer.
- D. Install a certificate signed by a trusted CA.
- E. Store the value of the $_SERVER['REMOTE_ADDR'] received by the web servers.

Answer: C

Explanation:
The issue is tracing the original source of requests in a tiered architecture with a load balancer. The web server logs show internal IPs (192.168.1.10), not the external client IPs, because the load balancer forwards requests without preserving the source. Enabling theX-Forwarded-Forheader on the load balancer adds the client's original IP to the HTTP request headers, allowing downstream servers to log it. This ensures traceability without altering the architecture significantly.
* Option A:Correct-X-Forwarded-For is the standard solution for preserving client IPs through load balancers.
* Option B:A Host-based Intrusion Detection System (HIDS) detects anomalies but doesn't address IP traceability.
* Option C:A trusted CA certificate fixes the self-signed warning but is unrelated to source tracking.
* Option D:Stored procedures improve database security but don't help with IP logging.
* Option E:Storing $_SERVER['REMOTE_ADDR'] captures the load balancer's IP, not the client's, unless X-Forwarded-For is enabled.

NEW QUESTION # 172
A security administrator has isolated a computer system because it was targeted by a ransomware attack. Which of the following should the security administrator do to recover from this attack in the most secure way?

- A. Restore the system from a baseline snapshot.
- B. Determine if the encryption key can be recovered. If it can, restore the files.
- C. Check if file versioning is enabled and restore the files.
- D. Seek approval from senior leadership to pay the ransom and unencrypt the files with the provided key.

Answer: A

Explanation:
Restoring from a known-good, immutable snapshot ensures you return the system to a clean, pre-infection state without any residual ransomware artifacts or potential backdoors. Snapshots are typically protected from tampering and provide a trusted recovery point, making this the most secure and reliable remediation method.

NEW QUESTION # 173
.....

Environment

- Free PDF 2026 CompTIA CAS-005: CompTIA SecurityX Certification Exam Latest Valid Test Test □ Search for ➠ CAS-005 □ and obtain a free download on ➽ www.troytecdumps.com □ □Exam Dumps CAS-005 Free
- CAS-005 Visual Cert Exam □ CAS-005 Test Price □ Real CAS-005 Testing Environment □ Download [CAS-005] for free by simply entering 「 www.pdfvce.com 」 website □CAS-005 Study Materials Review
- Free CAS-005 Pdf Guide □ Real CAS-005 Testing Environment □ CAS-005 Test Price □ Immediately open □ www.practicevce.com □ and search for ▸ CAS-005 ◂ to obtain a free download □Dump CAS-005 Torrent
- Providing You Fantastic CAS-005 Valid Test Test with 100% Passing Guarantee □ Search on 「 www.pdfvce.com 」 for ➥ CAS-005 □ to obtain exam materials for free download □CAS-005 Visual Cert Exam
- Practice CAS-005 Online □ CAS-005 Test Price □ CAS-005 Test Price □ Search for ⇛ CAS-005 ⇚ and obtain a free download on 《 www.testkingpass.com 》 □CAS-005 Valid Exam Guide
- Free Download CAS-005 Valid Test Test - Leading Offer in Qualification Exams - Trustworthy CAS-005 Valid Test Discount 🖕 Open website ➽ www.pdfvce.com □ and search for □ CAS-005 □ for free download □CAS-005 Test Price
- First-rank CAS-005 Practice Materials Stand for Perfect Exam Dumps - www.pass4test.com ❤ Download 「 CAS-005 」 for free by simply searching on { www.pass4test.com } □New CAS-005 Test Format
- Free PDF 2026 CompTIA CAS-005: CompTIA SecurityX Certification Exam Latest Valid Test Test □ Search on 【 www.pdfvce.com 】 for □ CAS-005 □ to obtain exam materials for free download □CAS-005 Valid Vce
- Quiz CompTIA - CAS-005 - Useful CompTIA SecurityX Certification Exam Valid Test Test □ Enter ➤ www.practicevce.com □ and search for ➥ CAS-005 □ to download for free □Real CAS-005 Testing Environment
- teganlkyd689291.vblogetin.com, jaysondpyl350392.blog-a-story.com, elainecvoo500094.blogdosaga.com, katrinarzft423618.dekaronwiki.com, naturalbookmarks.com, extrabookmarking.com, monicamtmg697394.gynoblog.com, robertpkwj660043.blogoxo.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, yiwnhua.com, Disposable vapes

BONUS!!! Download part of PracticeDump CAS-005 dumps for free: https://drive.google.com/open?id=1I6ea_PCZrOFsFSr9PtB2UnAKc2fcyUIp