非常好的CAS-005資訊和資格考試的領導者以及100％的合格率CAS-005：CompTIA SecurityX Certification Exam

P.S. PDFExamDumps在Google Drive上分享了免費的2026 CompTIA CAS-005考試題庫：https://drive.google.com/open?id=1xEEo7fCd_EirBGA-sU3L8-IG2jqYo8YC

根據過去的考試題和答案的研究，PDFExamDumps提供的CompTIA CAS-005練習題和真實的考試試題有緊密的相似性。PDFExamDumps是可以承諾您能100%通過你第一次參加的CompTIA CAS-005 認證考試。

CompTIA CAS-005 考試大綱：

主題	簡介
主題 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.
主題 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.
主題 3	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.
主題 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.

>> CAS-005資訊 <<

快速下載的CAS-005資訊 |第一次嘗試輕鬆學習並通過考試並且有效的CAS-005：CompTIA SecurityX Certification Exam

在談到CAS-005考試認證，很難忽視的是可靠性，PDFExamDumps的CAS-005考試培訓資料是特別設計，以最大限度的提高你的工作效率，本站在全球範圍內執行這項考試通過率最大化。

最新的 CompTIA CASP CAS-005 免費考試真題 (Q581-Q586):

問題 #581
During DAST scanning, applications are consistently reporting code defects in open-source libraries that were used to build web applications. Most of the code defects are from using libraries with known vulnerabilities. The code defects are causing product deployment delays.
Which of the following is the best way to uncover these issues earlier in the life cycle?

- A. Modifying the WAF polices to block against known vulnerabilities
- B. Using a software dependency management solution
- C. Completing an IAST scan against the web application
- D. Directing application logs to the SIEM for continuous monitoring

答案：B

問題 #582
A security engineer discovers that some legacy systems are still in use or were not properly decommissioned. After further investigation, the engineer identifies that an unknown and potentially malicious server is also sending emails on behalf of the company.
The security engineer extracts the following data for review:

Server IP	DNS	Status	Auth. pass rate
200.100.50.25	marketing.company.com	Authorized	97%
200.50.25.10	29mail.mycrosoft.info	Unauthorized	0%
210.20.20.5	mail.google.com	Authorized	100%

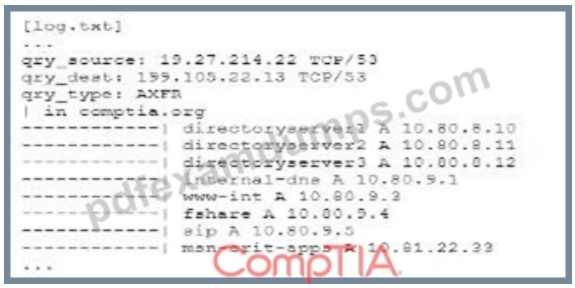
Which of the following actions should the security engineer take next? (Select two).

- A. Change the DMARC policy to reject and remove references to the server.
- B. Rotate the DKIM selector to use another key.
- C. Change the DMARC policy to none and monitor email flow to establish a new baseline.
- D. Change the SPF record to enforce the hard fail parameter.
- E. Remove the unnecessary servers from the SPF record.
- F. Update the MX record to contain only the primary email server.

答案：D,E

解題說明：
The presence of an unauthorized server (29mail.mycrosoft.info) sending emails on behalf of the company indicates a potential spoofing or phishing attempt. To mitigate this:
Remove the unnecessary servers from the SPF record (Option C): The Sender Policy Framework (SPF) specifies which mail servers are authorized to send emails on behalf of a domain. Removing unauthorized or unnecessary servers from the SPF record helps prevent spoofed emails from passing SPF checks.
Change the SPF record to enforce the hard fail parameter (Option D): Setting the SPF policy to a hard fail (-all) ensures that emails from unauthorized servers are rejected, enhancing email security.
Implementing these changes strengthens the domain's email authentication mechanisms, reducing the risk of successful phishing or spoofing attacks.

問題 #583
A senior security engineer flags me following log file snippet as hawing likely facilitated an attacker's lateral movement in a recent breach:



Which of the following solutions, if implemented, would mitigate the nsk of this issue reoccurnnp?

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

答案：B

解題說明：
The log snippet indicates a DNS AXFR (zone transfer) request, which can be exploited by attackers to gather detailed information about an internal network's infrastructure. Disabling DNS zone transfers is the best solution to mitigate this risk. Zone transfers should generally be restricted to authorized secondary DNS servers and not be publicly accessible, as they can reveal sensitive network information that facilitates lateral movement during an attack.
References:
* CompTIA SecurityX Study Guide: Discusses the importance of securing DNS configurations, including restricting zone transfers.
* NIST Special Publication 800-81, "Secure Domain Name System (DNS) Deployment Guide":
Recommends restricting or disabling DNS zone transfers to prevent information leakage.

問題 #584
Several unlabeled documents in a cloud document repository contain cardholder information.
Which of the following configuration changes should be made to the DLP system to correctly label these documents in the future?

- A. Watermarking
- B. Network traffic decryption
- C. Digital rights management
- D. Regular expressions

答案：D

解題說明：
Data Loss Prevention (DLP) systems can use regular expressions to identify and classify sensitive information, such as cardholder data, based on patterns (e.g., patterns for credit card numbers). By configuring the DLP system with appropriate regular expressions, the system can correctly identify and label documents containing such information in the future, ensuring compliance and enhancing security.

問題 #585
A security team is responding to malicious activity and needs to determine the scope of impact the malicious activity appears to affect certain version of an application used by the organization Which of the following actions best enables the team to determine the scope of Impact?

- A. Inspecting egress network traffic
- B. Performing a port scan
- C. Reviewing the asset inventory
- D. Analyzing user behavior

答案：C

解題說明：
Reviewing the asset inventory allows the security team to identify all instances of the affected application versions within the organization. By knowing which systems are running the vulnerable versions, the team can assess the full scope of the impact, determine which systems might be compromised, and prioritize them for further investigation and remediation.
Performing a port scan (Option A) might help identify open ports but does not provide specific information about the application versions. Inspecting egress network traffic (Option B) and analyzing user behavior (Option D) are important steps in the incident response process but do not directly identify which versions of the application are affected.
References:
* CompTIA Security+ Study Guide
* NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"
* CIS Controls, "Control 1: Inventory and Control of Hardware Assets" and "Control 2: Inventory and Control of Software Assets"

問題 #586
.....