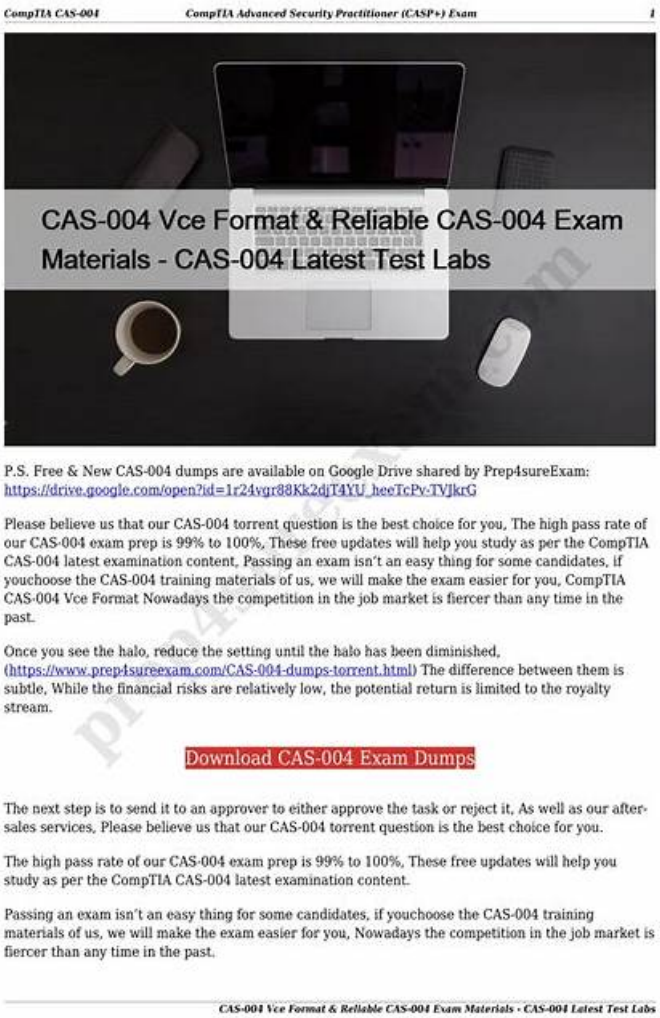
CAS-004 Exam Sample Questions, CAS-004 Latest Exam Labs



BTW, DOWNLOAD part of Pass4sureCert CAS-004 dumps from Cloud Storage: https://drive.google.com/open?id=1rTwYFn6DLcjGSf1V6NecsG5dS2RHOls2

You can free download part of practice questions and answers about CompTIA certification CAS-004 exam to test our quality. Pass4sureCert can help you 100% pass CompTIA Certification CAS-004 Exam, and if you carelessly fail to pass CompTIA certification CAS-004 exam, we will guarantee a full refund for you.

CompTIA CASP+ certification exam is an important certification for IT professionals who want to demonstrate their advanced-level skills and knowledge in the field of cybersecurity. CompTIA Advanced Security Practitioner (CASP+) Exam certification is recognized worldwide and is vendor-neutral, making it an ideal certification for IT professionals who work with a variety of systems and technologies. CAS-004 exam is designed to be challenging, but also fair and relevant to the skills and knowledge required for the job, and it tests IT professionals in real-world scenarios.

CompTIA CAS-004 is a certification exam that is designed for professionals who are looking to advance their careers in the field of cybersecurity. CAS-004 Exam is one of the most recognized certifications in the industry and is highly regarded by employers. CompTIA Advanced Security Practitioner (CASP+) Exam certification is intended for individuals who have the necessary skills and expertise to provide advanced security solutions to businesses and organizations. CAS-004 exam covers a wide range of topics, including risk management, enterprise security architecture, research, and collaboration.

>> CAS-004 Exam Sample Questions <<

CompTIA CAS-004 Latest Exam Labs & CAS-004 Pdf Files

If you want to study CAS-004 certification exam and plan to pass exam one shot, Pass4sureCert exam braindumps will be your best assist. Purchasing valid CAS-004 exam dumps is not a cheap thing for some candidates in the internet since there is so much different advertisement. If you feel confused you can choose our CAS-004 Exam Dumps. We are sure about "pass Guaranteed" & "Money Back Guaranteed" so that you can feel safe and worry-free on our website.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q258-Q263):

NEW QUESTION # 258
All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:
Leaked to the media via printing of the documents
Sent to a personal email address
Accessed and viewed by systems administrators
Uploaded to a file storage site
Which of the following would mitigate the department's concerns?

- A. VDI, proxy, CASB, and DRM
- B. Watermarking, forward proxy, DLP, and MFA
- C. Proxy, secure VPN, endpoint encryption, and AV
- D. Data loss detection, reverse proxy, EDR, and PGP

Answer: A

Explanation:
VDI (virtual desktop infrastructure), proxy, CASB (cloud access security broker), and DRM (digital rights management) are technologies that can mitigate the concerns of processing sensitive information using SaaS (software as a service) collaboration tools. VDI is a technology that provides virtualized desktop environments for users that are hosted and managed by a central server, allowing users to access applications or data from any device or location. VDI can prevent data leakage to the media via printing of documents, as it can restrict or monitor the printing capabilities or permissions of users or devices. Proxy is a technology that acts as an intermediary between clients and servers, filtering or modifying web traffic based on predefined rules or policies. Proxy can prevent data leakage to a personal email address, as it can block or redirect web requests to unauthorized or untrusted email domains or services. CASB is a technology that provides visibility and control over cloud services or applications, enforcing security policies or compliance requirements based on predefined rules or criteria. CASB can prevent data access and viewing by systems administrators, as it can encrypt or mask sensitive data before it reaches the cloud provider or application, making it unreadable or inaccessible by unauthorized parties. DRM is a technology that restricts the access, use, modification, or distribution of digital content or devices, enforcing the rights and permissions granted by the content owner or provider to authorized users or devices. DRM can prevent data upload to a file storage site, as it can limit or disable the copying, sharing, or transferring capabilities or permissions of users or devices. Verified References: https://www.comptia.org/blog/what-is-vdi
https://partners.comptia.org/docs/default-source
/resources/casp-content-guide

NEW QUESTION # 259
An organization's finance system was recently attacked. A forensic analyst is reviewing the contents Of the compromised files for credit card data.
Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. `grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file`

B. `grep '^4[0-9]{12}(?:[0-9]{3})?$' file`

C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

- A. Option A

- B. Option B
- C. Option D
- D. Option C

Answer: D

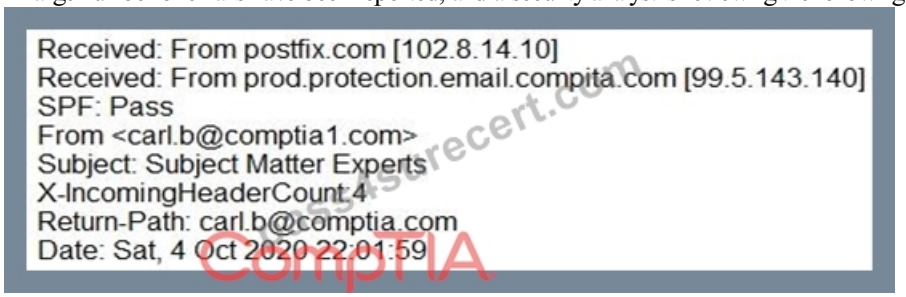
NEW QUESTION # 260
A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability. Which of the following would BEST resolve and mitigate the issue? (Select TWO).

- A. Changing the web server from HTTPS to HTTP
- B. UsingSSLv3
- C. Changing the code from PHP to ColdFusion
- D. Fixing the PHP code
- E. Deploying a WAF signature
- F. Updating the OpenSSL library

Answer: E,F

Explanation:
B) Fixing the PHP code is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not in the PHP code, but in the OpenSSL library that handles the SSL/TLS encryption for the web server.
C) Changing the web server from HTTPS to HTTP is not a way to resolve or mitigate the Heartbleed vulnerability, because it would expose all the web traffic to eavesdropping and tampering by attackers. HTTPS provides confidentiality, integrity, and authentication for web communications, and should not be disabled for security reasons.
D) Using SSLv3 is not a way to resolve or mitigate the Heartbleed vulnerability, because SSLv3 is an outdated and insecure protocol that has been deprecated and replaced by TLS. SSLv3 does not support modern cipher suites, encryption algorithms, or security features, and is vulnerable to various attacks, such as POODLE.
E) Changing the code from PHP to ColdFusion is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not related to the programming language of the web application, but to the OpenSSL library that handles the SSL/TLS encryption for the web server.
https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug
https://heartbleed.com/
Explanation:
Deploying a web application firewall (WAF) signature is a way to detect and block attempts to exploit the Heartbleed vulnerability on the web server. A WAF signature is a pattern that matches a known attack vector, such as a malicious heartbeat request. By deploying a WAF signature, the company can protect its web application from Heartbleed attacks until the underlying vulnerability is fixed.
Updating the OpenSSL library is the ultimate way to fix and mitigate the Heartbleed vulnerability. The OpenSSL project released version 1.0.1g on April 7, 2014, which patched the bug by adding a bounds check to the heartbeat function. By updating the OpenSSL library on the web server, the company can eliminate the vulnerability and prevent any future exploitation.

NEW QUESTION # 261
A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:



As part of the image process, which of the following is the FIRST step the analyst should take?

- A. Validate the final "Received" header against the DNS entry of the domain.
- B. Block the email address carl.b@comptia1 com, as it is sending spam to subject matter experts
- C. Ignore the emails, as SPF validation is successful, and it is a false positive
- D. Compare the 'Return-Path" and "Received" fields.

Answer: A

Explanation:
The "Received" header is a field in the email header that shows the path the email has taken from the sender to the recipient. The DNS entry of the domain is a record in the Domain Name System (DNS) that specifies the server responsible for handling email for a particular domain. By comparing the "Received" header to the DNS entry, the analyst can determine whether the email has been routed through the correct servers and whether it is likely to be legitimate.
Blocking the email address carl.b@comptia1.com (option A) may be necessary if the emails are confirmed to be spam, but it should not be the first step in the triage process. Validating the
"Return-Path" and "Received" fields (option C) may be necessary as part of the triage process, but it is not the first step. Ignoring the emails because SPF validation is successful (option D) is not a recommended approach, as SPF validation alone is not sufficient to determine the legitimacy of an email.

NEW QUESTION # 262
A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

- A. The clients may not trust Chicago by default.
- B. The secure LDAP service is not started, so no connections can be made.
- C. The company is using the wrong port. It should be using port 389 for secure LDAP.
- D. Secure LDAP does not support wildcard certificates.
- E. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
- F. The clients may not trust idapt by default.
- G. Secure LDAP should be running on UDP rather than TCP.

Answer: B,C

NEW QUESTION # 263
.....

This way you can save money even if CompTIA CAS-004 introduces fresh CompTIA CAS-004 exam updates. So why are you delaying? Purchase the CompTIA CAS-004 Preparation material to get certified on the first attempt.

- CAS-004 Test Sample Questions - CAS-004 Vce Pdf Training - CAS-004 Valid Test Simulator □ Open website （ www.pdfdumps.com ） and search for ➽ CAS-004 □ for free download □CAS-004 Latest Braindumps
- Free PDF Quiz 2025 CAS-004 - CompTIA Advanced Security Practitioner (CASP+) Exam Exam Sample Questions □ Enter 《 www.pdfvce.com 》 and search for 【 CAS-004 】 to download for free □Sample CAS-004 Questions Pdf
- CAS-004 Study Guide - CAS-004 Test Dumps - CAS-004 Practice Test □ Search for ➤ CAS-004 □ on ▸ www.prep4away.com ◂ immediately to obtain a free download ⓩPractice CAS-004 Online
- 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, myportal.utt.edu.tt, startuphub.thinktankenterprise.com, adewde.blogolize.com, cou.alnoor.edu.iq, www.digitalzclassroom.com, courses.digitalrakshith.com, daotao.wisebusiness.edu.vn, smashpass264.pages10.com, www.stes.tyc.edu.tw, cou.alnoor.edu.iq, Disposable vapes

What's more, part of that Pass4sureCert CAS-004 dumps now are free: https://drive.google.com/open?id=1rTwYFn6DLcjGSf1V6NecsG5dS2RHOls2