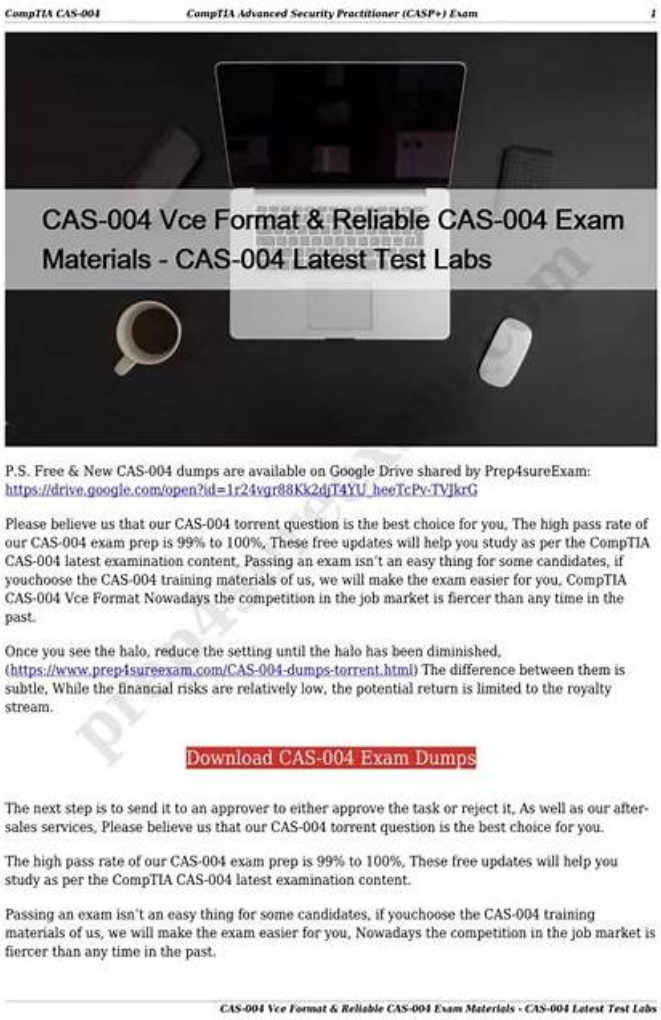
Reliable CAS-004 Exam Blueprint - CAS-004 Latest Test Discount



P.S. Free 2025 CompTIA CAS-004 dumps are available on Google Drive shared by ActualVCE: https://drive.google.com/open?id=1TfisHX3JBcTUqyJ-CNg-2L2JoiQCPmq_

As we all know, the world does not have two identical leaves. People's tastes also vary a lot. So we have tried our best to develop the three packages of our CAS-004 exam braindumps for you to choose. Now we have free demo of the CAS-004 study materials exactly according to the three packages on the website for you to download before you pay for the CAS-004 Practice Engine, and the free demos are a small part of the questions and answers. You can check the quality and validity by them.

CompTIA CASP+ certification is recognized worldwide as a validation of advanced-level security skills and knowledge. It is a vendor-neutral certification, which means that it is not tied to any specific hardware or software platform. This makes it an ideal certification for IT professionals who work with a variety of systems and technologies.

>> Reliable CAS-004 Exam Blueprint <<

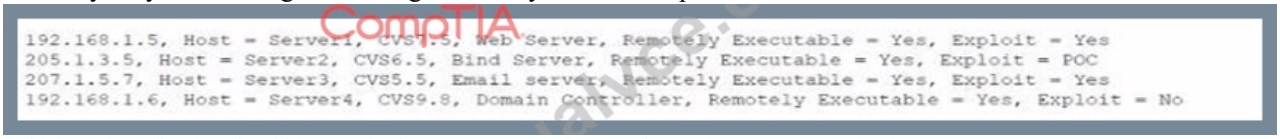
100% Pass Quiz 2025 Pass-Sure CompTIA Reliable CAS-004 Exam Blueprint

It is not easy for you to make a decision of choosing the CAS-004 prep guide from our company, because there are a lot of study materials about the exam in the market. However, if you decide to buy the CAS-004 test practice files from our company, we are going to tell you that it will be one of the best decisions you have made in recent years. As is known to us, the CAS-004 study

braindumps from our company are designed by a lot of famous experts and professors in the field. There is no doubt that the CAS-004 prep guide has the high quality beyond your imagination. Choosing the CAS-004 study braindumps from our company can but prove beneficial to all people. We believe that our products, at all events, worth a trial.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q137-Q142):

NEW QUESTION # 137
A security analyst is reviewing the following vulnerability assessment report:



Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

- A. Server 3
- B. Server2
- C. Servers
- D. Server1

Answer: D

NEW QUESTION # 138
A security manager wants to transition the organization to a zero trust architecture. To meet this requirement, the security manager has instructed administrators to remove trusted zones, role- based access, and one-time authentication. Which of the following will need to be implemented to achieve this objective? (Choose three.)

- A. IaaS
- B. Firewall
- C. Least privilege
- D. Policy automation
- E. VPN
- F. Continuous integration
- G. Continuous validation
- H. PKI

Answer: C,D,G

Explanation:
To achieve a zero trust architecture, the following measures will need to be implemented:
Least privilege: The principle of least privilege should be applied to ensure that users and devices only have access to the resources they need to perform their functions. This involves granting the minimum level of access required and then gradually increasing access privileges as needed.
Policy automation: Policies for access control, authentication, and authorization should be automated to reduce the risk of human error and to ensure that policies are consistently applied across the organization.
Continuous validation: Continuous monitoring and validation of user and device behavior is necessary to detect and respond to any anomalies or suspicious activity that may indicate a security breach.

NEW QUESTION # 139
A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregate and allows remote access to MSSP analyst.
Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud. The data is then sent from the log aggregate to a public IP address in the MSSP datacenter for analysis.
A security engineer is concerned about the security of the solution and notes the following.
* The critical devise send cleartext logs to the aggregator.
* The log aggregator utilize full disk encryption.
* The log aggregator sends to the analysis server via port 80.
* MSSP analysis utilize an SSL VPN with MFA to access the log aggregator remotely.

* The data is compressed and encrypted prior to being achieved in the cloud.
Which of the following should be the engineer's GREATEST concern?

- A. Network bridging from a remote access VPN
- B. Hardware vulnerabilities introduced by the log aggregate server
- C. Multinancy and data remnants in the cloud
- D. Encryption of data in transit

Answer: D

Explanation:
Explanation
Encryption of data in transit should be the engineer's greatest concern regarding the security of the solution.
Data in transit refers to data that is being transferred over a network or between devices. If data in transit is not encrypted, it can be intercepted, modified, or stolen by attackers who can exploit vulnerabilities in the network protocols or devices. The solution in the question sends logs from the critical devices to the aggregator in cleartext and from the aggregator to the analysis server via port 80, which are both insecure methods that expose the data to potential attacks. Verified References:
https://www.comptia.org/training/books/casp-cas-004-study-guide , https://us-cert.cisa.gov/ncas/tips/ST04-019

NEW QUESTION # 140
A security researcher detonated some malware in a lab environment and identified the following commands running from the EDR tool:

```
netsh advfirewall set allprofiles firewall policy blockinbound, blockoutbound
netsh advfirewall set allprofiles state on
init.ps1 -win32_shadow copy
```

With which of the following MITRE ATT&CK TTPs is the command associated? (Choose two.)

- A. Network denial of service
- B. OS credential dumping
- C. System information discovery
- D. External remote services
- E. Indirect command execution
- F. Inhibit system recovery

Answer: B,C

Explanation:
OS credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software.
System information discovery is the process of gathering information about the system, such as hostname, IP address, OS version, running processes, etc. Both of these techniques are commonly used by adversaries to gain access to sensitive data and resources on the target system. The command shown in the image is using Mimikatz, a tool that can dump credentials from memory, and also querying the system information using WMIC.

NEW QUESTION # 141
A user in the finance department uses a laptop to store a spreadsheet that contains confidential financial information for the company.
Which of the following would be the best way to protect the file while the user brings the laptop between locations? (Choose two.)

- A. Place an ACL on the file to only allow access to specified users.
- B. Enable access logging on the file.
- C. Place an ACL on the file to deny access to everyone.
- D. Store the file in the user profile.
- E. Back up the file to an encrypted flash drive.
- F. Encrypt the hard drive with full disk encryption.

Answer: E,F

Explanation:
To protect confidential financial information on a laptop that is frequently moved between locations, full disk encryption (FDE) is a

strong security measure that ensures that all data on the hard drive is encrypted. This means that if the laptop is lost or stolen, the data remains inaccessible without the encryption key. Additionally, backing up the file to an encrypted flash drive provides an extra layer of security and ensures that there is a secure copy of the file in case the laptop is compromised.

NEW QUESTION # 142

......

Students are given a fixed amount of time to complete each test, thus CompTIA Exam Questions candidate's ability to control their time and finish the CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004) exam in the allocated time is a crucial qualification. Obviously, this calls for lots of practice. Taking ActualVCE CAS-004 Practice Exam helps you get familiar with the CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004) exam questions and work on your time management skills in preparation for the real CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004) exam.

CAS-004 Latest Test Discount: https://www.actualvce.com/CompTIA/CAS-004-valid-vce-dumps.html

- Get CompTIA CAS-004 Practice Test For Quick Preparation [2025] □ Search for " CAS-004 " and easily obtain a free download on { www.prep4away.com } □CAS-004 Top Questions
- CAS-004 Valid Learning Materials □ Valid CAS-004 Dumps □ CAS-004 Reliable Exam Blueprint □ Go to website □ www.pdfvce.com □ open and search for ➤ CAS-004 □ to download for free □CAS-004 Latest Exam
- 100% Pass 2025 CompTIA High Pass-Rate Reliable CAS-004 Exam Blueprint □ Search on 《 www.lead1pass.com 》 for ➠ CAS-004 □ to obtain exam materials for free download □CAS-004 Exam Simulator Online
- Practice CAS-004 Engine □ Pass4sure CAS-004 Study Materials □ CAS-004 Top Questions □ Search for □ CAS-004 □ and easily obtain a free download on ⇛ www.pdfvce.com ⇚ □CAS-004 Latest Exam
- CAS-004 Test Simulates: CompTIA Advanced Security Practitioner (CASP+) Exam - CAS-004 Study Guide □ Search for ➻ CAS-004 □ on 《 www.prep4pass.com 》 immediately to obtain a free download □CAS-004 Valid Learning Materials
- CAS-004 Test Simulates: CompTIA Advanced Security Practitioner (CASP+) Exam - CAS-004 Study Guide □ Open ➡ www.pdfvce.com □□□ enter □ CAS-004 □ and obtain a free download □CAS-004 Latest Braindumps Pdf
- Free PDF Quiz 2025 CompTIA Pass-Sure CAS-004: Reliable CompTIA Advanced Security Practitioner (CASP+) Exam Exam Blueprint □ ➻ www.pass4test.com □ is best website to obtain " CAS-004 " for free download □CAS-004 Latest Exam
- Want to Get CompTIA CAS-004 Certified? Rely on Pdfvce's Exam Questions for Easy Success □ Open website " www.pdfvce.com " and search for （ CAS-004 ） for free download □CAS-004 Latest Dumps Book
- Latest Online CompTIA CAS-004 Practice Tests □ Open ☀ www.actual4labs.com □☀□ and search for 「 CAS-004 」 to download exam materials for free □CAS-004 Practice Exam
- Get CompTIA CAS-004 Practice Test For Quick Preparation [2025] □ Simply search for □ CAS-004 □ for free download on ☀ www.pdfvce.com □☀□ □CAS-004 New Dumps Questions
- Free PDF 2025 CompTIA Latest Reliable CAS-004 Exam Blueprint □ Easily obtain free download of 《 CAS-004 》 by searching on 《 www.pdfdumps.com 》 □CAS-004 Valid Examcollection
- kareyed271.daneblogger.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, myportal.utt.edu.tt, tedcole945.qodsblog.com, motionentrance.edu.np, pct.edu.pk, 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, study.stcs.edu.np, myportal.utt.edu.tt, Disposable vapes

P.S. Free & New CAS-004 dumps are available on Google Drive shared by ActualVCE: https://drive.google.com/open?id=1TfisHX3JBcTUqyJ-CNg-2L2JoiQCPmq_