CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Based on a recent security audit, a company discovered the perimeter strategy is inadequate for its recent growth. To address this issue, the company is looking for a solution that includes the following requirements:

1.

Collapse of multiple network security technologies into a single footprint

2.

Support for multiple VPNs with different security contexts

3.

Support for application layer security (Layer 7 of the OSI Model)

Which of the following technologies would be the most appropriate solution given these requirements?

A. NAT gateway

B. Reverse proxy

C. NGFW

D. NIDS

Correct Answer: C

QUESTION 2

An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment\\'s notice. Which of the following should the organization consider FIRST to address this requirement?

A. Implement a change management plan to ensure systems are using the appropriate versions.

B. Hire additional on-call staff to be deployed if an event occurs.

C. Design an appropriate warm site for business continuity.

D. Identify critical business processes and determine associated software and hardware requirements.

Correct Answer: D

When developing a plan, the first thing to consider is the business process and their impact on operations. A warm site does not make sense even if it were to be first, as a warm site does not replicate in a manner that provides "moments notice" fail over.

QUESTION 3

A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections

using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

A. sudo netstat -antu | grep "LISTEN" | awk `{print$5}\\'

B. sudo netstat -nlt -p | grep "ESTABLISHED"

C. sudo netstat -plntu | grep -v "Foreign Address"

D. sudo netstat -pnut -w | column -t -s $\\'\w\\'

E. sudo netstat -pnut | grep -P ^tcp

Correct Answer: E

Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port

QUESTION 4

A security engineer investigates an incident and determines that a rogue device is on the network. Further investigation finds that an employee\\'s personal device has been set up to access company resources and does not comply with standard security controls. Which of the following should the security engineer recommend to reduce the risk of future reoccurrence?

A. Require device certificates to access company resources.

B. Enable MFA at the organization\\'s SSO portal.

C. Encrypt all workstation hard drives.

D. Hide the company wireless SSID.

Correct Answer: A

To reduce the risk of unauthorized devices accessing company resources, requiring device certificates is an effective control. Device certificates can be used to authenticate devices before they are allowed to connect to the network and access resources, ensuring that only devices with a valid certificate, which are typically managed and issued by the organization, can connect.

QUESTION 5

An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely

Which of the following features of these devices MOST likely led to this decision? (Select TWO.)

A. Software-backed keystore

B. Embedded cryptoprocessor

C. Hardware-backed public key storage

D. Support for stream ciphers

E. Decentralized key management

F. TPM 2.0 attestation services

Correct Answer: BC