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.leads4pass.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An organization does not have visibility into when company-owned assets are off network or not connected via a VPN. The lack of visibility prevents the organization from meeting security and operational objectives. Which of the following cloud-hosted solutions should the organization implement to help mitigate the risk?

A. Antivirus

B. UEBA

C. EDR

D. HIDS

Correct Answer: C

QUESTION 2

In a shared responsibility model for PaaS, which of the following is a customer\\'s responsibility?

A. Network security

B. Physical security

C. OS security

D. Host infrastructure

Correct Answer: C

QUESTION 3

A security engineer is assessing a legacy server and needs to determine if FTP is running and on which port. The service cannot be turned off, as it would impact a critical application\\'s ability to function. Which of the following commands would provide the information necessary to create a firewall rule to prevent that service from being exploited?

A. service --status-all | grep ftpd

B. chkconfig --list

C. netstat --tulpn

D. systemctl list-unit-file --type service ftpd

E. service ftpd status

Correct Answer: C

-t : Display TCP connections.

-u : Display UDP connections.

-l : Display listening socket (services).

-p : Display the process associated with the service.

-n : Display numerical addresses instead of resolving hostnames.

The output of this command will show all active network connections and listening ports along with the associated processes. You can then identify if FTP is running and on which port.

QUESTION 4

During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels. Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.

B. Perform ASIC password cracking on the host.

C. Read the /etc/passwd file to extract the usernames.

D. Initiate unquoted service path exploits.

E. Use the UNION operator to extract the database schema.

Correct Answer: A

Reference: https://docs.rapid7.com/insightvm/elevating-permissions/

QUESTION 5

A company provides guest WiFi access to the Internet and physically separates the guest network from the company\\'s internal WiFi. Due to a recent incident in which an attacker gained access to the company\\'s internal WiFi, the company

plans to configure WPA2 Enterprise in an EAP-TLS configuration.

Which of the following must be installed on authorized hosts for this new configuration to work properly?

A. Active Directory GPOs

B. PKI certificates

C. Host-based firewall

D. NAC persistent agent

Correct Answer: B