CAS-003 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

https://www.passapply.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A security engineer reviews the table below: The engineer realizes there is an active attack occurring on the network. Which of the following would BEST reduce the risk of this attack reoccurring the future?

Switchport	MAC address	IP address	Lease start	Lease length
Gi1/0	EB:04:18:20:18:54	192.168.1.5	4/16 14:00	24 hours
Gi1/0	EB:04:18:20:18:55	192.168.1.6	4/16 14:00	24 hours
Gi1/0	EB:04:18:20:18:56	192.168.1.8	4/16 14:00	24 hours
Gi1/0	EB:04:18:20:18:57	192.168.1.9	4/16 14:00	24 hours
Gi1/0	EB:04:18:20:18:58	192.168.1.13	4/16 14:00	24 hours
Gi1/0	EB:04:18:20:18:59	192.168.1.14	4/16 14:00	24 hours
Gi1/1	01:49:D9:B2:22:F6	192.168.1.11	4/15 17:30	24 hours
Gi1/2	C3:59:29:B9:A2:F3	192.168.1.4	4/15 12:30	24 hours
Gi1/2	98:82:11:F1:E9:AA	192.168.1.7	4/16 9:20	24 hours
Gi1/2	28:48:29:CA:B2:31	192.168.1.2	4/16 11:15	24 hours
Gi1/3	E3:FA:B0:82:18:BD	192.168.1.12	4/15 18:29	24 hours
Gi1/4	DB:29:D7:A3:32:03	192.168.1.3	4/15 22:30	24 hours

A. Upgrading device firmware

B. Enabling port security

C. Increasing DHCP pool size

D. Disabling dynamic trucking

E. Reducing DHCP lease length

Correct Answer: B

QUESTION 2

A company is migrating systems from an on-premises facility to a third-party managed datacenter. For continuity of operations and business agility, remote access to all hardware platforms must be available at all times. Access controls need to be very robust and provide an audit trail. Which of the following security controls will meet the company\\'s objectives? (Select two.)

A. Integrated platform management interfaces are configured to allow access only via SSH

B. Access to hardware platforms is restricted to the systems administrator\\'s IP address

C. Access is captured in event logs that include source address, time stamp, and outcome

D. The IP addresses of server management interfaces are located within the company\\'s extranet

E. Access is limited to interactive logins on the VDi

F. Application logs are hashed cryptographically and sent to the SIEM

Correct Answer: CE

QUESTION 3

A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer\\'s company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

A. DLP

B. Mail gateway

C. Data flow enforcement

D. UTM

Correct Answer: A

QUESTION 4

A company\\'s existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh.

Which of the following is the BEST way to address these issues and mitigate risks to the organization?

A. Purchase the SSL, decryption license for the firewalls and route traffic back to the proxies for end-user categorization and malware analysis.

B. Roll out application whitelisting to end-user desktops and decommission the existing proxies, freeing up network ports.

C. Use an EDP solution to address the malware issue and accept the diminishing role of the proxy for URL categorization in the short team.

D. Accept the current risk and seek possible funding approval in the next budget cycle to replace the existing proxies with ones with more capacity.

Correct Answer: B

QUESTION 5

An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

- Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
- SSL Medium Strength Cipher Suites Supported
- Vulnerability in DNS Resolution Could Allow Remote Code Execution
- SMB Host SIDs allows Local User Enumeration

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker

B. Port scanner

C. Account enumerator

D. Exploitation framework

Correct Answer: A