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.pass4itsure.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 company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration

B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat

C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats

D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Correct Answer: A

QUESTION 2

A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

A. Reconfigure the firewall to block external UDP traffic.

B. Establish a security baseline on the IDS.

C. Block echo reply traffic at the firewall.

D. Modify the edge router to not forward broadcast traffic.

Correct Answer: B

QUESTION 3

A small retail company recently deployed a new point of sale (POS) system to all 67 stores. The core of the POS is an extranet site, accessible only from retail stores and the corporate office over a split-tunnel VPN. An additional split-tunnel VPN provides bi-directional connectivity back to the main office, which provides voice connectivity for store VoIP phones. Each store offers guest wireless functionality, as well as employee wireless. Only the staff wireless network has access to the POS VPN. Recently, stores are reporting poor response times when accessing the POS application from store computers as well as degraded voice quality when making phone calls. Upon investigation, it is determined that three store PCs are hosting malware, which is generating excessive network traffic. After malware removal, the information security department is asked to review the configuration and suggest changes to prevent this from happening again. Which of the following denotes the BEST way to mitigate future malware risk?

A. Deploy new perimeter firewalls at all stores with UTM functionality.

B. Change antivirus vendors at the store and the corporate office.

C. Move to a VDI solution that runs offsite from the same data center that hosts the new POS solution.

D. Deploy a proxy server with content filtering at the corporate office and route all traffic through it.

Correct Answer: A

A perimeter firewall is located between the local network and the Internet where it can screen network traffic flowing in and out of the organization. A firewall with unified threat management (UTM) functionalities includes anti-malware capabilities.

QUESTION 4

A security analyst works for a defense contractor that produces classified research on drones. The contractor faces nearly constant attacks from sophisticated nation-state actors and other APIs. Which of the following would help protect the confidentiality of the research data?

A. Use diverse components in layers throughout the architecture

B. Implement non-heterogeneous components at the network perimeter

C. Purge all data remnants from client devices\\' volatile memory at regularly scheduled intervals

D. Use only in-house developed applications that adhere to strict SDLC security requirements

Correct Answer: A

QUESTION 5

Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization\\'s incident response capabilities. Which of the following activities has the incident team lead executed?

A. Lessons learned review

B. Root cause analysis

C. Incident audit

D. Corrective action exercise

Correct Answer: A