CAS-002 Q&As

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

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

QUESTION 1

News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial exploit network mapping and fingerprinting occurs in preparation for further exploitation. Which of the following is the MOST effective solution to protect against unrecognized malware infections, reduce detection time, and minimize any damage that might be done?

A. Remove local admin permissions from all users and change anti-virus to a cloud aware, push technology.

B. Implement an application whitelist at all levels of the organization.

C. Deploy a network based heuristic IDS, configure all layer 3 switches to feed data to the IDS for more effective monitoring.

D. Update router configuration to pass all network traffic through a new proxy server with advanced malware detection.

Correct Answer: B

QUESTION 2

A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

A. Use AES in Electronic Codebook mode

B. Use RC4 in Cipher Block Chaining mode

C. Use RC4 with Fixed IV generation

D. Use AES with cipher text padding

E. Use RC4 with a nonce generated IV

F. Use AES in Counter mode

Correct Answer: EF

QUESTION 3

A security architect is seeking to outsource company server resources to a commercial cloud service provider. The provider under consideration has a reputation for poorly controlling physical access to datacenters and has been the victim of multiple social engineering attacks. The service provider regularly assigns VMs from multiple clients to the same physical resources. When conducting the final risk assessment which of the following should the security architect take into consideration?

A. The ability to implement user training programs for the purpose of educating internal staff about the dangers of social engineering.

B. The cost of resources required to relocate services in the event of resource exhaustion on a particular VM.

C. The likelihood a malicious user will obtain proprietary information by gaining local access to the hypervisor platform.

D. Annual loss expectancy resulting from social engineering attacks against the cloud service provider affecting corporate network infrastructure.

Correct Answer: C

QUESTION 4

A security administrator is investigating the compromise of a SCADA network that is not physically connected to any other network. Which of the following is the MOST likely cause of the compromise?

A. Outdated antivirus definitions

B. Insecure wireless

C. Infected USB device

D. SQL injection

Correct Answer: C

QUESTION 5

A security consultant is evaluating forms which will be used on a company website. Which of the following techniques or terms is MOST effective at preventing malicious individuals from successfully exploiting programming flaws in the website?

A. Anti-spam software

B. Application sandboxing

C. Data loss prevention

D. Input validation

Correct Answer: D