CAS-002 Q&As

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

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

https://www.passapply.com/cas-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A vulnerability research team has detected a new variant of a stealth Trojan that disables itself when it detects that it is running on a virtualized environment. The team decides to use dedicated hardware and local network to identify the Trojan\\'s behavior and the remote DNS and IP addresses it connects to. Which of the following tools is BEST suited to identify the DNS and IP addresses the stealth Trojan communicates with after its payload is decrypted?

A. HIDS

B. Vulnerability scanner

C. Packet analyzer

D. Firewall logs

E. Disassembler

Correct Answer: C

QUESTION 2

A manager who was attending an all-day training session was overdue entering bonus and payroll information for subordinates. The manager felt the best way to get the changes entered while in training was to log into the payroll system, and then activate desktop sharing with a trusted subordinate. The manager granted the subordinate control of the desktop thereby giving the subordinate full access to the payroll system. The subordinate did not have authorization to be in the payroll system. Another employee reported the incident to the security team. Which of the following would be the MOST appropriate method for dealing with this issue going forward?

A. Provide targeted security awareness training and impose termination for repeat violators.

B. Block desktop sharing and web conferencing applications and enable use only with approval.

C. Actively monitor the data traffic for each employee using desktop sharing or web conferencing applications.

D. Permanently block desktop sharing and web conferencing applications and do not allow its use at the company.

Correct Answer: A

QUESTION 3

An administrator at a small company replaces servers whenever budget money becomes available. Over the past several years the company has acquired and still uses 20 servers and 50 desktops from five different computer manufacturers. Which of the following are management challenges and risks associated with this style of technology lifecycle management?

A. Decreased security posture, decommission of outdated hardware, inability to centrally manage, and performance bottlenecks on old hardware.

B. Increased mean time to failure rate of legacy servers, OS variances, patch availability, and ability to restore to dissimilar hardware.

C. OS end-of-support issues, ability to backup data, hardware parts availability, and firmware update availability and management.

D. Inability to use virtualization, trusted OS complexities, and multiple patch versions based on OS dependency.

Correct Answer: B

QUESTION 4

A team is established to create a secure connection between software packages in order to list employee\\'s remaining or unused benefits on their paycheck stubs. Which of the following business roles would be MOST effective on this team?

A. Network Administrator, Database Administrator, Programmers

B. Network Administrator, Emergency Response Team, Human Resources

C. Finance Officer, Human Resources, Security Administrator

D. Database Administrator, Facilities Manager, Physical Security Manager

Correct Answer: C

QUESTION 5

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC. Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

A. Static and dynamic analysis is run as part of integration

B. Security standards and training is performed as part of the project

C. Daily stand-up meetings are held to ensure security requirements are understood

D. For each major iteration penetration testing is performed

E. Security requirements are story boarded and make it into the build

F. A security design is performed at the end of the requirements phase

Correct Answer: AD