CAS-002$^{\text{Q\&As}}$

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.pass2lead.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 security manager is concerned about performance and patch management, and, as a result, wants to implement a virtualization strategy to avoid potential future OS vulnerabilities in the host system. The IT manager wants a strategy that would provide the hypervisor with direct communications with the underlying physical hardware allowing the hardware resources to be paravirtualized and delivered to the guest machines. Which of the following recommendations from the server administrator BEST meets the IT and security managers\\' requirements? (Select TWO).

A. Nested virtualized hypervisors

B. Type 1 hypervisor

C. Hosted hypervisor with a three layer software stack

D. Type 2 hypervisor

E. Bare metal hypervisor with a software stack of two layers

Correct Answer: BE

QUESTION 2

A high-tech company dealing with sensitive data seized the mobile device of an employee suspected of leaking company secrets to a competitive organization. Which of the following is the BEST order for mobile phone evidence extraction?

A. Device isolation, evidence intake, device identification, data processing, verification of data accuracy, documentation, reporting, presentation and archival.

B. Evidence intake, device identification, preparation to identify the necessary tools, device isolation, data processing, verification of data accuracy, documentation, reporting, presentation and archival.

C. Evidence log, device isolation ,device identification, preparation to identify the necessary tools, data processing, verification of data accuracy, presentation and archival.

D. Device identification, evidence log, preparation to identify the necessary tools, data processing, verification of data accuracy, device isolation, documentation, reporting, presentation and archival.

Correct Answer: B

QUESTION 3

A new malware spreads over UDP Port 8320 and several network hosts have been infected. A new security administrator has determined a possible cause, and the infected machines have been quarantined. Which of the following actions could a new security administrator take to further mitigate this issue?

A. Limit source ports on the firewall to specific IP addresses.

B. Add an explicit deny-all and log rule as the final entry of the firewall rulebase.

C. Implement stateful UDP filtering on UDP ports above 1024.

D. Configure the firewall to use IPv6 by default.

Correct Answer: B

QUESTION 4

The IT department of a pharmaceutical research company is considering whether the company should allow or block access to social media websites during lunch time. The company is considering the possibility of allowing access only through the company\\'s guest wireless network, which is logically separated from the internal research network. The company prohibits the use of personal devices; therefore, such access will take place from company owned laptops.

Which of the following is the HIGHEST risk to the organization?

A. Employee\\'s professional reputation

B. Intellectual property confidentiality loss

C. Downloaded viruses on the company laptops

D. Workstation compromise affecting availability

Correct Answer: B

QUESTION 5

A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks

B. Job rotation

C. Least privilege

D. Employee termination procedures

Correct Answer: B