RC0-C02[Q&As]

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

https://www.geekcert.com/rc0-c02.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A security analyst at Company A has been trying to convince the Information Security Officer (ISO) to allocate budget towards the purchase of a new intrusion prevention system (IPS) capable of analyzing encrypted web transactions. Which of the following should the analyst provide to the ISO to support the request? (Select TWO).

A. Emerging threat reports

B. Company attack trends

C. Request for Quote (RFQ)

D. Best practices

E. New technologies report

Correct Answer: AB

QUESTION 2

A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user\\'s ongoing communication be retained in the user\\'s account for future investigations. Which of the following will BEST meet the goals of law enforcement?

A. Begin a chain-of-custody on for the user\\'s communication. Next, place a legal hold on the user\\'s email account.

B. Perform an e-discover using the applicable search terms. Next, back up the user\\'s email for a future investigation.

C. Place a legal hold on the user\\'s email account. Next, perform e-discovery searches to collect applicable emails.

D. Perform a back up of the user\\'s email account. Next, export the applicable emails that match the search terms.

Correct Answer: C

A legal hold is a process that an organization uses to maintain all forms of pertinent information when legal action is reasonably expected. E-discovery refers to discovery in litigation or government investigations that manages the exchange of electronically stored information (ESI). ESI includes email and office documents, photos, video, databases, and other filetypes.

QUESTION 3

A data processing server uses a Linux based file system to remotely mount physical disks on a shared SAN. The server administrator reports problems related to processing of files where the file appears to be incompletely written to the disk. The network administration team has conducted a thorough review of all network infrastructure and devices and found everything running at optimal performance. Other SAN customers are unaffected. The data being processed consists of millions of small files being written to disk from a network source one file at a time. These files are then accessed by a local Java program for processing before being transferred over the network to a SELinux host for processing. Which of the following is the MOST likely cause of the processing problem?

A. The administrator has a PERL script running which disrupts the NIC by restarting the CRON process every 65 seconds.

B. The Java developers accounted for network latency only for the read portion of the processing and not the write process.

C. The virtual file system on the SAN is experiencing a race condition between the reads and writes of network files.

D. The Linux file system in use cannot write files as fast as they can be read by the Java program resulting in the errors.

Correct Answer: D

QUESTION 4

In order to reduce costs and improve employee satisfaction, a large corporation is creating a BYOD policy. It will allow access to email and remote connections to the corporate enterprise from personal devices; provided they are on an approved device list. Which of the following security measures would be MOST effective in securing the enterprise under the new policy? (Select TWO).

A. Provide free email software for personal devices.

B. Encrypt data in transit for remote access.

C. Require smart card authentication for all devices.

D. Implement NAC to limit insecure devices access.

E. Enable time of day restrictions for personal devices.

Correct Answer: BD

In this question, we are allowing access to email and remote connections to the corporate enterprise from personal devices. When providing remote access to corporate systems, you should always ensure that data travelling between the corporate network and the remote device is encrypted. We need to provide access to devices only if they are on an approved device list. Therefore, we need a way to check the device before granting the device access to the network if it is an approved device. For this we can use NAC (Network Access Control). When a computer connects to a computer network, it is not permitted to access anything unless it complies with a business defined policy; including anti-virus protection level, system update level and configuration. While the computer is being checked by a pre- installed software agent, it can only access resources that can remediate (resolve or update) any issues. Once the policy is met, the computer is able to access network resources and the Internet, within the policies defined within the NAC system. NAC solutions allow network operators to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them in switches, routers, and network middleboxes.

QUESTION 5

Which of the following BEST constitutes the basis for protecting VMs from attacks from other VMs hosted on the same physical platform?

A. Aggressive patch management on the host and guest OSs.

B. Host based IDS sensors on all guest OSs.

C. Different antivirus solutions between the host and guest OSs.

D. Unique Network Interface Card (NIC) assignment per guest OS.

Correct Answer: A

This question is asking "Which of the following BEST constitutes the basis for protecting VMs from attacks from other VMs hosted on the same physical platform. In other words, what is the primary method protecting VMs.

The first thing we should do to protect the VMs is to ensure that the guest OS\\'s are patched and ensure that the host is patched. The host provides the virtualization software to enable the running of the virtual machines. Any floors in the

virtualization software that affect the VM separation enabling an attack between VMs running on the host would hopefully be fixed by the virtualization software vendor in a patch. The most important step and therefore "the basis" for protecting

VMs would be aggressive patch management.