CS0-002^{Q&As}

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.pass2lead.com/cs0-002.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

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

A. Pause the virtual machine,

B. Shut down the virtual machine.

C. Take a snapshot of the virtual machine.

D. Remove the NIC from the virtual machine.

E. Review host hypervisor log of the virtual machine.

F. Execute a migration of the virtual machine.

Correct Answer: A

If the VM has been compromised then merely taking another snapshot will just add another rollback point \'post compromise\'.

As per the forensic process admin should take a copy. Within the virtual environment this is performed by suspending (pausing) the VM and taking a copy of the folder that the VM and the associated file(s) are located within. This could be used as the start of the chain of custody and could be copied and analysed further.

QUESTION 2

A critical server was compromised by malware, and all functionality was lost. Backups of this server were taken; however, management believes a logic bomb may have been injected by a rootkit. Which of the following should a security analyst perform to restore functionality quickly?

A. Work backward, restoring each backup until the server is clean

B. Restore the previous backup and scan with a live boot anti-malware scanner

C. Stand up a new server and restore critical data from backups

D. Offload the critical data to a new server and continue operations

Correct Answer: C

QUESTION 3

A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website?

![Pass2Lead](https://Pass2Lead.com)
A. VPN

B. Honeypot

C. Whitelisting

D. DMZ

E. MAC filtering

Correct Answer: C

QUESTION 4

A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN

administrator moved a power plug when testing the SAN\\'s fault notification features.

Which of the following should be done to prevent this issue from reoccurring?

A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.

B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.

C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.

D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

Correct Answer: A

QUESTION 5

A network appliance manufacturer is building a new generation of devices and would like to include chipset security improvements. Management wants the security team to implement a method to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. Which of the following would meet this objective?

A. UEFI

B. A hardware security module

C. eFUSE

D. Certificate signed updates

Correct Answer: C

Latest CS0-002 Dumps   CS0-002 Study Guide   CS0-002 Exam Questions