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.geekcert.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

As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back

up and match their gold image. If they find any inconsistencies, they must formally document the information.

Which of the following BEST describes this test?

A. Walk through

B. Full interruption

C. Simulation

D. Parallel

Correct Answer: C

QUESTION 2

A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wife transfer Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

A. Implementing a sandboxing solution for viewing emails and attachments

B. Limiting email from the finance department to recipients on a pre-approved whitelist

C. Configuring email client settings to display all messages in plaintext when read

D. Adding a banner to incoming messages that identifies the messages as external

Correct Answer: D

QUESTION 3

A security analyst determines that several workstations are reporting traffic usage on port 3389. All workstations are running the latest OS patches according to patch reporting. The help desk manager reports some users are getting logged off of their workstations, and network access is running slower than normal. The analyst believes a zero-day threat has allowed remote attackers to gain access to the workstations. Which of the following are the BEST steps to stop the threat without impacting all services? (Choose two.)

A. Change the public NAT IP address since APTs are common.

B. Configure a group policy to disable RDP access.

C. Disconnect public Internet access and review the logs on the workstations.

D. Enforce a password change for users on the network.

E. Reapply the latest OS patches to workstations.

F. Route internal traffic through a proxy server.

Correct Answer: BD

QUESTION 4

An analyst is responding 10 an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the held. Maiware was loaded on the device via the installation of a third-party software package The analyst has baselined the device.

Which of the following should the analyst do to BEST mitigate future attacks?

A. Implement MDM

B. Update the maiware catalog

C. Patch the mobile device\\'s OS

D. Block third-party applications

Correct Answer: A

QUESTION 5

An analyst has initiated an assessment of an organization\\'s security posture. As a part of this review, the analyst would like to determine how much information about the organization is exposed externally. Which of the following techniques would BEST help the analyst accomplish this goal? (Select two.)

A. Fingerprinting

B. DNS query log reviews

C. Banner grabbing

D. Internet searches

E. Intranet portal reviews

F. Sourcing social network sites

G. Technical control audits

Correct Answer: DF

Latest CS0-002 Dumps CS0-002 Exam Questions CS0-002 Braindumps