CS0-001 Q&As

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

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

QUESTION 1

A security engineer has been asked to reduce the attack surface on an organization\\'s production environment. To limit access, direct VPN access to all systems must be terminated, and users must utilize multifactor authentication to access a constrained VPN connection and then pivot to other production systems form a bastion host. The MOST appropriate way to implement the stated requirement is through the use of a:

A. sinkhole.

B. multitenant platform.

C. single-tenant platform.

D. jump box

Correct Answer: D

QUESTION 2

Three similar production servers underwent a vulnerability scan. The scan results revealed that the three servers had two different vulnerabilities rated "Critical".

The administrator observed the following about the three servers:

The servers are not accessible by the Internet AV programs indicate the servers have had malware as recently as two weeks ago The SIEM shows unusual traffic in the last 20 days Integrity validation of system files indicates unauthorized modifications

Which of the following assessments is valid and what is the most appropriate NEXT step? (Select TWO).

A. Servers may have been built inconsistently

B. Servers may be generating false positives via the SIEM

C. Servers may have been tampered with

D. Activate the incident response plan

E. Immediately rebuild servers from known good configurations

F. Schedule recurring vulnerability scans on the servers

Correct Answer: CD

QUESTION 3

A security analyst is creating ACLs on a perimeter firewall that will deny inbound packets that are from internal addresses, reversed external addresses, and multicast addresses. Which of the following is the analyst attempting to prevent?

A. Broadcast storms

B. Spoofing attacks

C. DDoS attacks

D. Man-in-the-middle attacks

Correct Answer: B

QUESTION 4

An insurance company employs quick-response team drivers that carry corporate-issued mobile devices with the insurance company\\'s app installed on them. Devices are configuration-hardened by an MDM and kept up to date. The employees use the app to collect insurance claim information and process payments. Recently, a number of customers have filed complaints of credit card fraud against the insurance company, which occurred shortly after their payments were processed via the mobile app. The cyber-incident response team has been asked to investigate. Which of the following is MOST likely the cause?

A. The MDM server is misconfigured.

B. The app does not employ TLS.

C. USB tethering is enabled.

D. 3G and less secure cellular technologies are not restricted.

Correct Answer: B

QUESTION 5

A security analyst is assisting with a computer crime investigation and has been asked to secure a PC and deliver it to the forensic lab. Which of the following items would be MOST helpful to secure the PC? (Choose three.)

A. Tamper-proof seals

B. Faraday cage

C. Chain of custody form

D. Drive eraser

E. Write blockers

F. Network tap

G. Multimeter

Correct Answer: ABC