CAS-003$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

A. Capture process ID data and submit to anti-virus vendor for review.

B. Reboot the Linux servers, check running processes, and install needed patches.

C. Remove a single Linux server from production and place in quarantine.

D. Notify upper management of a security breach.

E. Conduct a bit level image, including RAM, of one or more of the Linux servers.

Correct Answer: E

Incident management (IM) is a necessary part of a security program. When effective, it mitigates business impact, identifies weaknesses in controls, and helps fine-tune response processes.

In this question, an attack has been identified and confirmed. When a server is compromised or used to commit a crime, it is often necessary to seize it for forensics analysis. Security teams often face two challenges when trying to remove a physical server from service: retention of potential evidence in volatile storage or removal of a device from a critical business process.

Evidence retention is a problem when the investigator wants to retain RAM content. For example, removing power from a server starts the process of mitigating business impact, but it also denies forensic analysis of data, processes, keys, and possible footprints left by an attacker.

A full a bit level image, including RAM should be taken of one or more of the Linux servers. In many cases, if your environment has been deliberately attacked, you may want to take legal action against the perpetrators. In order to preserve this option, you should gather evidence that can be used against them, even if a decision is ultimately made not to pursue such action. It is extremely important to back up the compromised systems as soon as possible. Back up the systems prior to performing any actions that could affect data integrity on the original media.

QUESTION 2

An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

A. Port security

B. Rogue device detection

C. Bluetooth

D. GPS

Correct Answer: D

QUESTION 3

While traveling to another state, the Chief Financial Officer (CFO) forgot to submit payroll for the company The CFO quickly gained access to the corporate network through the high-speed wireless network provided by the hotel and

completed the task. Upon returning from the business trip, the CFO was told no one received their weekly pay due to a malware attack on the system.

Which of the following is the MOST likely cause of the secunty breach?

A. The security manager did not enforce automatic VPN connection.

B. The company\\'s server did not have endpoint security enabled.

C. The hotel did not require a wireless password to authenticate.

D. The laptop did not have the host-based firewall properly configured.

Correct Answer: A

QUESTION 4

The SOC has noticed an unusual volume of traffic coming from an open WiFi guest network that appears correlated with a broader network slowdown The network team is unavailable to capture traffic but logs from network services are available

1.

No users have authenticated recently through the guest network\\'s captive portal

2.

DDoS mitigation systems are not alerting

3.

DNS resolver logs show some very long domain names

Which of the following is the BEST step for a security analyst to take next?

A. Block all outbound traffic from the guest network at the border firewall

B. Verify the passphrase on the guest network has not been changed.

C. Search antivirus logs for evidence of a compromised company device

D. Review access pent fogs to identify potential zombie services

Correct Answer: A

QUESTION 5

A security analyst has requested network engineers integrate sFlow into the SOC\\'s overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

A. Effective deployment of network taps

B. Overall bandwidth available at Internet PoP

C. Optimal placement of log aggregators

D. Availability of application layer visualizers

Correct Answer: D