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.leads4pass.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

A facilities manager requests approval to deploy a new key management system that integrates with logical network access controls to provide conditional access. The security analyst who is assessing the risk has no experience with the category of products.

Which of the following is the FIRST step the analyst should take to begin the research?

A. Seek documented industry best practices.

B. Review the preferred vendor\\'s white papers.

C. Compare the product function to relevant RFCs

D. Execute a non-disclosure agreement with the vendor

Correct Answer: A

QUESTION 2

The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

A. Review the flow data against each server\\'s baseline communications profile.

B. Configure the server logs to collect unusual activity including failed logins and restarted services.

C. Correlate data loss prevention logs for anomalous communications from the server.

D. Setup a packet capture on the firewall to collect all of the server communications.

Correct Answer: A

Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day exploits. Having knowledge of each host\\'s communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zero-day and APT (advance persistent threat) malware and agents. Data intelligence allows forensic analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network.

QUESTION 3

A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure

confidentiality of individual operating system data?

A. Encryption of each individual partition

B. Encryption of the SSD at the file level

C. FDE of each logical volume on the SSD

D. FDE of the entire SSD as a single disk

Correct Answer: A

In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.

Therefore, the solution is to encrypt each individual partition separately.

QUESTION 4

As part of an organization\\'s ongoing vulnerability assessment program, the Chief Information Security Officer (CISO) wants to evaluate the organization\\'s systems, personnel, and facilities for various threats As part of the assessment the CISO plans to engage an independent cybersecurity assessment firm to perform social engineering and physical penetration testing against the organization\\'s corporate offices and remote locations. Which of the following techniques would MOST likely be employed as part of this assessment? (Select THREE).

A. Privilege escalation

B. SQL injection

C. TOC/TOU exploitation

D. Rogue AP substitution

E. Tailgating

F. Vulnerability scanning

G. Vishing

H. Badge skimming

Correct Answer: EGH

QUESTION 5

A security administrator wants to stand up a NIPS that is multilayered and can incorporate many security technologies into a single platform The product should have diverse capabilities, such as antivirus, VPN, and firewall services, and be able to be updated in a timely manner to meet evolving threats. Which of the following network prevention system types can be used to satisfy the requirements?

A. Application firewall

B. Unified threat management

C. Enterprise firewall

D. Content-based IPS

Correct Answer: A