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.pass2lead.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 Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit utilized in the banking industry and whether attribution is possible. The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO\\'s request?

A. 1. Perform the ongoing research of the best practices2. Determine current vulnerabilities and threats3. Apply Big Data techniques4. Use antivirus control

B. 1. Apply artificial intelligence algorithms for detection2. Inform the CERT team3. Research threat intelligence and potential adversaries4. Utilize threat intelligence to apply Big Data techniques

C. 1. Obtain the latest IOCs from the open source repositories2. Perform a sweep across the network to identify positive matches3. Sandbox any suspicious files4. Notify the CERT team to apply a future proof threat model

D. 1. Analyze the current threat intelligence2. Utilize information sharing to obtain the latest industry IOCs3. Perform a sweep across the network to identify positive matches4. Apply machine learning algorithms

Correct Answer: C

QUESTION 2

An organization is concerned that its hosted web servers are not running the most updated version of software. Which of the following would work BEST to help identify potential vulnerabilities?

A. hping3 -S comptia.org -p 80

B. nc -1 -v comptia.org -p 80

C. nmap comptia.org -p 80 -sV

D. nslookup -port=80 comptia.org

Correct Answer: C

QUESTION 3

During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization\\'s reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards.

Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

A. Air gaps

B. Access control lists

C. Spanning tree protocol

D. Network virtualization

E. Elastic load balancing

Correct Answer: D

QUESTION 4

A security manager wants to implement a policy that will management with the ability to monitor employees\\' activities with minimum impact to productivity.

Which of the following policies Is BEST suited for this scenario?

A. Separation of duties

B. Mandatory vacations

C. Least privilege

D. Incident response

Correct Answer: A

QUESTION 5

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

A. vTPM

B. HSM

C. TPM

D. INE

Correct Answer: A

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the

remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout

its lifetime on the platform.

CAS-003 Practice Test CAS-003 Study Guide CAS-003 Braindumps