

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

As part of a systems modernization program, the use of a weak encryption algorithm is identified in a web services API. The client using the API is unable to upgrade the system on its end which would support the use of a secure algorithm. As a temporary workaround, the client provides its IP space and the network administrator limits access to the API via an ACL to only the IP space held by the client. Which of the following is the use of the ACL in this situation an example of?

- A. Avoidance
- B. Transference
- C. Mitigation
- D. Acceptance
- E. Assessment

Correct Answer: C

QUESTION 2

Company.org has requested a black-box security assessment be performed on key cyber terrain. One area of concern is the company's SMTP services. The security assessor wants to run reconnaissance before taking any additional action and wishes to determine which SMTP server is Internet-facing.

Which of the following commands should the assessor use to determine this information?

- A. `dnsrecon -d company.org -t SOA`
- B. `dig company.org mx`
- C. `nc -v company.org`
- D. `whois company.org`

Correct Answer: A

QUESTION 3

A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones

continue to sync email while traveling.

Which of the following is the MOST likely explanation? (Choose two.)

- A. Outdated geographic IP information
- B. Privilege escalation attack

- C. VPN on the mobile device
- D. Unrestricted email administrator accounts
- E. Client use of UDP protocols
- F. Disabled GPS on mobile devices

Correct Answer: AC

QUESTION 4

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.

QUESTION 5

A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

- A. Code review
- B. Penetration testing
- C. Grey box testing
- D. Code signing

E. White box testing

Correct Answer: AE

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.

White box testing assumes that the penetration test team has full knowledge of the network and the infrastructure per se thus rendering the testing to follow a more structured approach.

[Latest CAS-003 Dumps](#)

[CAS-003 Study Guide](#)

[CAS-003 Braindumps](#)