CompTIA Security Plus Example Questions

Section: CompTIA Security Plus Certification Exams • **Total Questions:** 10 • **Format:** Verified Q&A

1. Which of the following is a one-way function that provides assurance of data integrity?

(A) Hashing
(B) Salting
(C) Segmentation
(D) Tokenization

2. A company wants to track modifications to the code that is used to build new virtual servers. Which of the following will the company most likely deploy?

(A) Change management ticketing system
(B) Behavioral analyzer
(C) Collaboration platform
(D) Version control tool

3. Which of the following is a risk of conducting a vulnerability assessment?

(A) A disruption of business operations
(B) Unauthorized access to the system
(C) Reports of false positives
(D) Finding security gaps in the system

4. Which of the following outlines the configuration, maintenance, and security roles between a cloud service provider and the customer?

(A) Service-level agreement
(B) Responsibility matrix
(C) Memorandum of understanding
(D) Non-disclosure agreement

5. A few weeks after deploying additional email servers, a company begins to receive complaints from employees that messages they send are going into their recipients' spam folders. Which of the following needs to be updated in order to resolve this issue?

(A) CNAME
(B) SMTP
(C) DLP
(D) SPF

---

6. Which of the following is a use of CVSS?

(A) To determine the cost associated with patching systems
(B) To identify unused ports and services that should be closed
(C) To analyze code for defects that could be exploited
(D) To prioritize the remediation of vulnerabilities

---

7. A Chief Security Officer signs off on a request to allow inbound SMB and RDP from the internet to a single VLAN. Which of the following is the most likely explanation for this activity?

(A) The company built a new file-sharing site
(B) The organization is preparing for a penetration test
(C) The security team is integrating with an SASE platform
(D) The security team created a honeynet

---

8. A security manager wants to reduce the number of steps required to identify and contain basic threats. Which of the following will help achieve this goal?

(A) SOAR
(B) SIEM
(C) DMARC
(D) NIDS

---

9. Which of the following is the best way to securely store an encryption key for a data set in a manner that allows multiple entities to access the key when needed?

(A) Public key infrastructure
(B) Open public ledger
(C) Public key encryption
(D) Key escrow

---

10. Which of the following best describes a common use of OSINT?

(A) Monitoring internal systems and network traffic to detect abnormal behavior

(B) Installing and configuring security patches to fix known vulnerabilities

(C) Collecting information from public platforms to find possible security exposures

(D) Encrypting sensitive company data and storing it securely in the cloud