Free CompTIA Security Plus Practice Test

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

1. Which of the following would be used to detect an employee who is emailing a customer list to a personal account before leaving the company?

(A) DLP
(B) FIM
(C) IDS
(D) EDR

2. A remote employee navigates to a shopping website on their company-owned computer. The employee clicks a link that contains a malicious file. Which of the following would prevent this file from downloading?

(A) DLP
(B) FIM
(C) NAC
(D) EDR

3. An administrator investigating an incident is concerned about the downtime of a critical server due to a failed drive. Which of the following would the administrator use to estimate the time needed to fix the issue?

(A) MTTR
(B) MTBF
(C) RTO
(D) RPO

4. A systems administrator configures a new application. The next day a security analyst reviews the logs and identifies multiple accounts that had been created overnight with administrative privileges and connections from different countries. Which of the following solutions would have prevented this incident?

(A) Applying input validation
(B) Changing the default credentials
(C) Installing a honeynet
(D) Deploying a WAF

5. Which of the following control types describes an alert from a SIEM tool?

(A) Preventive
(B) Corrective
(C) Compensating
(D) Detective

---

6. Which of the following mitigation techniques would a security analyst most likely use to avoid bloatware on devices?

(A) Disabled ports/protocols
(B) Application allow list
(C) Default password changes
(D) Access control permissions

---

7. Which of the following should be used to ensure that a device is inaccessible to a network-connected resource?

(A) Disablement of unused services
(B) Web application firewall
(C) Host isolation
(D) Network-based IDS

---

8. A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

(A) Deploying PowerShell scripts
(B) Pushing GPO update
(C) Enabling PAP
(D) Updating EDR profiles

---

9. A penetration tester, who did not have an access badge, managed to follow a group of employees through multiple badged-access doors and into the data center without being stopped. The tester mentions this finding during the after-action review with the Chief Information Security Officer (CISO). Which of the following issues should the CISO address as a result of this finding?

(A) Role-based access
(B) Shoulder surfing
(C) Insider threat
(D) Social engineering

---

10. A systems administrator is concerned about vulnerabilities within cloud computing instances. Which of the following is most important for the administrator to consider when architecting a cloud computing environment?

(A) SQL injection

(B) TOC/TOU

(C) VM escape

(D) Tokenization

(E) Password spraying