CompTIA Security Plus Exam Answers

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

1. An organization designs an inbound firewall with a fail-open configuration while implementing a website. Which of the following does the organization consider to be the highest priority?

(A) Confidentiality
(B) Non-repudiation
(C) Availability
(D) Integrity

2. Which of the following is the greatest advantage that network segmentation provides?

(A) End-to-end encryption
(B) Decreased resource utilization
(C) Enhanced endpoint protection
(D) Configuration enforcement
(E) Security zones

3. Which of the following features should the company set up? (Select two).

(A) DLP software
(B) DNS filtering
(C) File integrity monitoring
(D) Stateful firewall
(E) Guardrails
(F) Antivirus signatures

4. Which of the following is an internal audit team's function within risk management?

(A) Define an organization's exposure posture.
(B) Implement an organization's regulatory requirements.
(C) Assess an organization's policy compliance.
(D) Define and update an organization's control monitoring.

5. Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?

(A) Unidentified removable devices
(B) Default network device credentials
(C) Spear-phishing emails
(D) Impersonation of business units through typosquatting

---

6. Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?

(A) Recovery site
(B) Cold site
(C) Hot site
(D) Warm site

---

7. A systems administrator creates a script that validates OS version, patch levels, and installed applications when users log in. Which of the following examples best describes the purpose of this script?

(A) Resource scaling
(B) Policy enumeration
(C) Baseline enforcement
(D) Guard rails implementation

---

8. The security team at a company has received reports from employees that the Wi-Fi disconnects intermittently. The team changes the WPA2 passkey and gives it to employees. However, rogue devices are detected on the Wi-Fi network within less than an hour of the passkey change. A security team performs a walkthrough of the office and is unable to find the rogue devices. Which of the following is the most likely root cause of the breach?

(A) Brute force
(B) Trojan virus
(C) Replay attack
(D) Keylogger

---

9. An organization needs to block certain information from view. Which of the following should the organization use to accomplish this task?

(A) Obfuscation
(B) Classification policy
(C) Verification
(D) Block rules

---

10. Which of the following techniques can be used to sanitize the data contained on a hard drive while allowing for the hard drive to be repurposed?

(A) Degaussing

(B) Drive shredder

(C) Retention platform

(D) Wipe tool