GAQM®
Global Association for Quality Management

Sample Exam

Exam Name: Certified Advanced Penetration Tester (CAPT)

Exam Code: CAPT-001

1. Which of the following best defines the primary purpose of physical security in cybersecurity?

A. To ensure digital firewalls are updated regularly
B. To safeguard hardware, personnel, and infrastructure from physical threats
C. To monitor online user behavior in real-time
D. To encrypt sensitive data during transmission

Correct Answer: B

---

2. Which of the following is NOT one of the three core elements of physical security?

A. Deterrence
B. Detection
C. Encryption
D. Response

Correct Answer: C

---

3. Tailgating is an example of which category of physical breach technique?

A. Hardware manipulation
B. Lock-based bypassing
C. Social engineering
D. Electronic exploitation

Correct Answer: C

---

4. What is the main objective of deterrence in physical security?

A. To instantly block unauthorized individuals
B. To alert security personnel of every access attempt
C. To discourage intruders by increasing perceived risk
D. To track employee movements within a facility

Correct Answer: C

---

5. Which tool is commonly used to test the security of RFID-based access systems?

A. USB data blocker
B. Lock picking set
C. RFID cloner
D. Biometric recorder

Correct Answer: C

---

6. Impersonation as a physical breach technique relies primarily on:

A. Technical exploitation of alarm systems
B. Weaknesses in biometric authentication
C. Exploiting trust and authority to bypass controls
D. Using advanced surveillance tools

Correct Answer: C

---

7. Which of the following best describes the purpose of dumpster diving in physical penetration testing?

A. To identify outdated hardware
B. To retrieve improperly disposed sensitive information
C. To test employee awareness during recycling
D. To measure the organization’s waste disposal efficiency

Correct Answer: B

---

8. When assessing security controls, why is simulating attack scenarios important?

A. It ensures security staff remain polite
B. It reveals vulnerabilities that routine checks may miss
C. It reduces the need for compliance audits
D. It eliminates the need for security policies

Correct Answer: B

---

9. Which of the following is a key practice for improving physical security concerning visitors?

A. Allowing visitors to move unescorted for efficiency
B. Granting permanent access cards to frequent visitors
C. Requiring sign-in and escorting visitors at all times
D. Disabling CCTV cameras in visitor waiting areas

Correct Answer: C

---

10. Which of the following best highlights the relationship between physical and digital security?

A. They operate independently and do not overlap
B. Physical security replaces the need for cybersecurity
C. Weak physical security can undermine digital protections
D. Digital security eliminates physical access risks entirely

Correct Answer: C

Case Scenario Question – Physical Security Testing

A penetration tester is hired to evaluate the physical security of a financial company's headquarters. During the assessment, the tester observes that employees frequently hold open the main entrance door for anyone walking behind them, especially during peak hours. The building uses RFID access cards, but the entry turnstiles are often left unlocked by the security staff to "speed up traffic" in the morning. CCTV cameras are installed, but their coverage leaves a blind spot near the employee lounge. During the test, the

penetration tester successfully enters the facility by walking closely behind an employee and later retrieves sensitive printed reports from a recycling bin located in the blind spot area.

Which of the following is the MOST critical security failure demonstrated in this scenario?

A. Insufficient CCTV coverage near the employee lounge
B. Improper disposal of documents in recycling bins
C. Tailgating enabled by unlocked turnstiles and employee behavior
D. Excessive employee traffic during morning hours

Correct Answer: C

A diagram of an Android mobile application architecture shows:

- UI Layer
- Business Logic Layer
- Data Layer
- The app also requests permissions for:
    - Camera
    - Microphone
    - Contacts
    - Location

Only the Camera permission line is connected to an actual app feature (QR scanning).

The other three permissions (Microphone, Contacts, Location) show no linked features in the architecture.

What is the most accurate security concern based on the diagram?

A. Excessive permissions increase the attack surface for malware or data harvesting
B. QR scanning functionality is insecure by default
C. The business logic layer improperly stores sensitive data
D. The UI layer has insufficient authentication controls

Correct Answer: A