? EASY (Q1–Q10)

Q1. Physical security primarily protects:
A. Software applications
B. Physical assets and infrastructure
C. Network protocols
D. Encryption keys

Q2. Physical security is important because it:
A. Replaces cybersecurity
B. Complements cybersecurity controls
C. Eliminates cyber attacks
D. Improves software performance

Q3. Which is a physical security control?
A. Firewall
B. CCTV camera
C. Antivirus
D. IDS

Q4. Confidentiality in physical security refers to:
A. System uptime
B. Preventing unauthorized physical access
C. Data accuracy
D. Network speed

Q5. Access control systems manage:
A. File permissions
B. Physical entry and exit
C. Network traffic
D. Malware detection

Q6. Environmental controls protect against:
A. Hackers
B. Fire, flood, and temperature issues
C. Password theft
D. Network attacks

Q7. Tailgating is an example of:
A. Network attack
B. Social engineering
C. Malware infection
D. DoS attack

Q8. Physical barriers include:
A. Encryption
B. Locks and fences
C. IDS rules
D. VPNs

Q9. Physical security mainly impacts which CIA component?
A. Integrity only
B. Availability only
C. All CIA components
D. Authentication only

Q10. Surveillance systems are used to:
A. Encrypt data
B. Monitor and record activities
C. Control traffic
D. Patch systems

□ MEDIUM (Q11–Q25)

Q11. The scope of physical security includes:
A. Only buildings
B. People, assets, and facilities
C. Software code
D. Network packets

Q12. Unauthorized physical access can lead to:
A. Hardware theft
B. Data compromise
C. Service disruption
D. All of the above

Q13. Insider threats in physical security involve:
A. External attackers only
B. Authorized personnel misusing access
C. Malware
D. Network sniffing

Q14. Biometric access control improves physical security by:
A. Using passwords
B. Verifying physical traits
C. Blocking networks
D. Encrypting data

Q15. Physical security policies define:
A. Software bugs
B. Rules for access and behavior
C. Network routing
D. Encryption algorithms

Q16. Security guards provide:
A. Logical access
B. Human-based physical control
C. Malware protection
D. Network monitoring

Q17. Penetration testing methodologies start with:
A. Exploitation
B. Reconnaissance
C. Privilege escalation
D. Reporting

Q18. Scanning and enumeration aim to:
A. Destroy systems
B. Identify vulnerabilities and services
C. Patch systems
D. Encrypt data

Q19. Exploitation phase involves:
A. Identifying assets
B. Gaining unauthorized access
C. Writing reports
D. Monitoring logs

Q20. Post-exploitation focuses on:
A. Maintaining access and assessing impact
B. Installing antivirus
C. Encrypting disks
D. Blocking users

Q21. Ethical penetration testing requires:
A. No authorization
B. Legal permission and defined scope
C. Public targets
D. Anonymous execution

Q22. Physical penetration testing may involve:
A. Phishing emails
B. Lock picking and badge cloning (authorized)
C. Malware deployment
D. SQL injection

Q23. Security awareness training reduces risk of:
A. Hardware failure
B. Social engineering attacks
C. Natural disasters
D. Power outages

Q24. Detection of physical breaches relies on:
A. Logs only
B. Surveillance and access logs
C. Encryption
D. IDS only

Q25. Physical security audits help organizations to:
A. Ignore threats
B. Identify gaps and weaknesses
C. Replace cybersecurity
D. Increase attack surface

🔴 HARD (Q26–Q40)

Q26. Physical security failures can completely bypass cybersecurity because:
A. Firewalls block attacks
B. Direct hardware access allows full compromise
C. Encryption stops attackers
D. IDS detects all threats

Q27. Layered physical security is effective because:
A. One control is sufficient
B. Multiple barriers delay and deter attackers
C. It removes human error
D. It eliminates insider threats

Q28. Environmental threats impact availability by:
A. Encrypting data
B. Damaging infrastructure
C. Stealing credentials
D. Spoofing identities

Q29. Social engineering exploits which factor most?
A. Hardware
B. Human trust and behavior
C. Encryption
D. Network speed

Q30. Physical access control logs are important for:
A. Encryption
B. Forensic investigations
C. Performance tuning
D. Backup creation

Q31. Penetration testing methodologies emphasize reporting because:
A. Attacks are irrelevant
B. Findings must guide remediation
C. Exploitation is illegal
D. Tools require logs

Q32. Physical penetration tests differ from cyber tests because they:
A. Use malware
B. Involve real-world access attempts
C. Require no planning
D. Are automated

Q33. A badge cloning attack exploits:
A. Network protocols
B. Weak RFID or access card security
C. Antivirus flaws
D. Encryption algorithms

Q34. CCTV systems support integrity by:
A. Preventing access
B. Providing evidence of events
C. Encrypting footage
D. Blocking intrusions

Q35. Physical security risk assessment considers:
A. Only cyber threats
B. Asset value, threats, and vulnerabilities
C. Network speed
D. Software versions

Q36. Tailgating prevention includes:
A. Open doors
B. Turnstiles and awareness training
C. Encryption
D. Firewalls

Q37. Physical security controls are weakest when:
A. Policies exist
B. Human compliance is poor
C. Surveillance is active
D. Access logs are reviewed

Q38. Ethical hacking principles apply to physical testing by ensuring:
A. Maximum damage
B. Authorization and minimal disruption
C. No documentation
D. Anonymous testing

Q39. Penetration testing improves security posture by:
A. Increasing attacks
B. Identifying real-world weaknesses
C. Removing controls
D. Reducing visibility

Q40. Physical security must be aligned with cybersecurity to:
A. Replace IT teams
B. Provide holistic protection
C. Slow operations
D. Reduce usability