? EASY (Q1–Q10)

Q1. Cyber security primarily focuses on protecting:
A. Only hardware
B. Only software
C. Information systems and data
D. Internet connections only

Q2. Which of the following best defines confidentiality?
A. Ensuring data accuracy
B. Ensuring data availability
C. Preventing unauthorized data access
D. Ensuring system uptime

Q3. The CIA triad consists of:
A. Control, Integrity, Authorization
B. Confidentiality, Integrity, Availability
C. Confidentiality, Identification, Authentication
D. Control, Investigation, Accountability

Q4. Which of the following is an example of malware?
A. Firewall
B. Antivirus
C. Worm
D. IDS

Q5. Which attack mainly targets availability of systems?
A. Phishing
B. SQL Injection
C. Denial of Service
D. Sniffing

Q6. Ethical hacking is performed to:
A. Steal sensitive data
B. Disrupt systems
C. Identify and fix vulnerabilities
D. Bypass security permanently

Q7. Which hacker works with legal permission?
A. Black-hat hacker
B. White-hat hacker
C. Hacktivist
D. Script kiddie

Q8. Which of the following is NOT a cyber threat?
A. Trojan

B. Virus
C. Firewall
D. Worm

Q9. A vulnerability refers to:
A. A malicious actor
B. A weakness in a system
C. An attack technique
D. A security control

Q10. Which domain deals with security policies and governance?
A. Network security
B. Application security
C. Information security management
D. Malware analysis

□ MEDIUM (Q11–Q25)

Q11. Integrity ensures that information is:
A. Accessible
B. Accurate and unaltered
C. Confidential
D. Encrypted

Q12. Which security control is used to detect incidents?
A. Preventive
B. Detective
C. Corrective
D. Administrative

Q13. Which attack uses deceptive emails to steal credentials?
A. Spoofing
B. Phishing
C. Sniffing
D. Flooding

Q14. Which hacker category has minimal technical skills?
A. Black-hat
B. White-hat
C. Script kiddie
D. Insider

Q15. Risk in information security is calculated as:
A. Threat + Asset

B. Vulnerability − Threat
C. Threat × Vulnerability
D. Asset ÷ Threat

Q16. Which phase comes first in ethical hacking?
A. Exploitation
B. Reporting
C. Reconnaissance
D. Scanning

Q17. IDS is primarily used to:
A. Prevent attacks
B. Detect intrusions
C. Encrypt data
D. Block users

Q18. Which of the following is a preventive control?
A. Audit logs
B. Alerts
C. Firewall
D. Incident report

Q19. A zero-day vulnerability is:
A. Already patched
B. Publicly disclosed
C. Unknown to the vendor
D. Hardware related

Q20. Which attack intercepts communication between two parties?
A. Phishing
B. Spoofing
C. Man-in-the-Middle
D. Brute force

Q21. Which tool is commonly used for packet analysis?
A. Metasploit
B. Nmap
C. Wireshark
D. Nessus

Q22. Availability ensures:
A. Data secrecy
B. System performance
C. Access when required
D. Encryption strength

Q23. Which of the following is an example of social engineering?
A. SQL Injection
B. Buffer Overflow
C. Phishing
D. Port Scanning

Q24. Ethical hackers must strictly follow:
A. Criminal law only
B. Organizational ethics
C. Code of ethics and legal authorization
D. No rules

Q25. Which framework provides best practices for information security management?
A. TCP/IP
B. ISO 27001
C. HTTP
D. DNS

HARD (Q26–Q40)

Q26. Defense-in-depth refers to:
A. Single strong security control
B. Multiple layered security controls
C. Physical security only
D. Network security only

Q27. Which attack compromises confidentiality and integrity simultaneously?
A. DoS
B. Sniffing
C. Man-in-the-Middle
D. Flooding

Q28. Threat modeling helps organizations to:
A. Improve performance
B. Identify attack paths and risks
C. Install security tools
D. Encrypt databases

Q29. Which security control restores systems after an incident?
A. Preventive
B. Detective
C. Corrective
D. Administrative

Q30. Which of the following best describes an insider threat?
A. External attacker
B. Trusted user misusing access
C. Anonymous hacker
D. Script kiddie

Q31. Which attack primarily exploits human psychology?
A. SQL Injection
B. Buffer Overflow
C. Social Engineering
D. SYN Flood

Q32. Which tool is mainly used for vulnerability scanning?
A. Wireshark
B. Nessus
C. Netcat
D. Tcpdump

Q33. Governance in cyber security focuses on:
A. Network design
B. Security tools
C. Policies, risk, and compliance
D. Malware detection

Q34. A risk treatment option that transfers risk is:
A. Risk avoidance
B. Risk mitigation
C. Risk acceptance
D. Risk insurance

Q35. Which attack aims to exhaust system resources?
A. Phishing
B. XSS
C. DDoS
D. SQL Injection

Q36. Which principle enforces minimal access rights?
A. Separation of duties
B. Least privilege
C. Defense-in-depth
D. Risk acceptance

Q37. Ethical hacking without permission is considered:
A. Legal
B. Ethical
C. Illegal
D. Administrative

Q38. Which metric evaluates overall security strength of an organization?
A. Network speed
B. Security posture
C. CPU utilization
D. Uptime

Q39. Which domain integrates people, process, and technology?
A. Malware analysis
B. Network security
C. Information security management
D. Application security

Q40. Which activity is performed LAST in ethical hacking?
A. Scanning
B. Exploitation
C. Reporting
D. Reconnaissance