Ethical Hacking — Module 1

Viva Questions & Answers (English Only)

Q1. What is Information Security?

A1. Information security is the practice of protecting information and information systems from unauthorized access, disclosure, alteration, and destruction.

Q2. Name the five core elements of information security.

A2. Confidentiality, Integrity, Availability, Authenticity, Non-repudiation.

Q3. Explain Confidentiality.

A3. Ensures data is accessible only to authorized users; protected by encryption, access control, classification.

Q4. Explain Integrity.

A4. Integrity ensures information remains accurate, complete and unaltered except by authorized actions (checksums, access control).

Q5. Explain Availability.

A5. Availability means systems and data are accessible to authorized users when needed (redundancy, backups, DDoS protection).

Q6. What is Authenticity?

A6. Authenticity confirms identity of users and source of information (biometrics, certificates, tokens).

Q7. What is Non-repudiation?

A7. Assurance that a sender cannot deny sending a message and the receiver cannot deny receipt (digital signatures, logs).

Q8. Define Hacker and difference between Hacker and Cracker.

A8. Hacker: person who explores or breaks into systems (intent varies). Cracker: hacker with malicious intent (data theft, damage).

Q9. List types of hackers.

A9. White hat, Black hat, Grey hat, Script kiddies, Green hat, Blue hat, Red hat, State-sponsored, Hacktivists, Malicious insiders.

Q10. What is an Ethical Hacker?

A10. A security professional authorized to test systems to find vulnerabilities before malicious actors do.

Q11. Why do organizations hire ethical hackers?

A11. To discover vulnerabilities, test defenses, prepare for attacks, and improve security posture.

Q12. What are Penetration Testing models?

A12. White box (full info), Black box (no info), Grey box (partial info).

Q13. List the phases of Penetration Testing.

A13. Reconnaissance (data collection), Vulnerability assessment, Exploitation (actual exploit), Reporting & analysis.

Q14. Name popular pentesting methodologies mentioned.

A14. OSSTMM, NIST framework, OWASP (for web apps).

Q15. What is OWASP Top 10? Give examples of some items.

A15. OWASP Top 10 highlights the most critical web app security risks (Injection, Broken Authentication, XSS, Sensitive Data Exposure, etc.).

Q16. Explain Vulnerability Assessment vs Penetration Testing.

A16. Vulnerability Assessment finds and lists vulnerabilities (broad, often automated). Penetration Testing attempts to exploit them to show real risk (depth, manual).

Q17. What is Social Engineering? Give examples.

A17. Manipulating people to reveal confidential info (phishing emails, pretexting, tailgating).

Q18. Mention legal/ethical considerations for pentesting.

A18. Always get written authorization (NDA/engagement letter), respect scope, report findings responsibly; unauthorized testing is illegal.

Q19. Name common tools and environment for pentesters.

A19. Kali Linux, Nmap, Metasploit, Burp Suite, Wireshark, Nikto, OWASP ZAP.

Q20. How should a pentest report be structured?

A20. Executive summary, scope, methodology, findings (with severity), proof-of-concept, remediation recommendations, conclusion.

Generated for viva preparation — Ethical Hacking Module 1.