Module 2 — Ethical Hacking (Viva Questions & Answers)

Q1: What is ethical hacking?

A1: Ethical hacking is the authorized practice of probing systems and networks to find security weaknesses, report them, and help fix them before malicious actors exploit them.

Q2: List the five phases of ethical hacking.

A2: Reconnaissance (passive/active), Scanning, Gaining Access (exploitation), Maintaining Access (post■exploitation), and Covering Tracks/Reporting.

Q3: Difference between white■hat, black■hat and grey■hat hackers.

A3: White■hat: authorized security testers; Black■hat: malicious attackers; Grey■hat: fall between (may find vulnerabilities without permission but not for malicious gain).

Q4: What legal and ethical considerations must a tester follow?

A4: Obtain written permission, follow scope/constraints, avoid unnecessary harm, protect sensitive data, and report findings responsibly to stakeholders.

Q5: What is footprinting? Give examples.

A5: Footprinting gathers publicly available info about a target: WHOIS, DNS records, social media, company websites, employee emails, IP ranges, and Google dorks.

Q6: Define scanning and name common scanning tools.

A6: Scanning probes hosts to discover live systems, open ports, and services. Tools: Nmap, Masscan, Nessus (vulnerability scanner).

Q7: What information does an Nmap TCP SYN scan reveal?

A7: SYN scan (half-open) identifies open/closed/filtered TCP ports without completing the TCP handshake, useful for stealthy discovery.

Q8: What is banner grabbing and why is it useful?

A8: Banner grabbing retrieves service/version info sent by network services, aiding fingerprinting and identifying vulnerable versions.

Q9: Describe vulnerability assessment vs penetration testing.

A9: Vulnerability assessment finds and lists vulnerabilities (usually non-exploitative). Penetration testing attempts to exploit vulnerabilities to assess real-world risk and impact.

Q10: What is privilege escalation?

A10: Privilege escalation is gaining higher access rights (e.g., user → root) by exploiting OS/service vulnerabilities or misconfigurations.

Q11: Give basic defenses against common web vulnerabilities.

A11: Input validation, output encoding, parameterized queries, authentication controls, secure session management, and using WAFs.

Q12: What is password cracking and common tools?

A12: Password cracking recovers plaintext passwords from hashes or login endpoints using brute-force or dictionaries. Tools: John the Ripper, Hashcat, Hydra.

Q13: Explain social engineering with an example.

A13: Social engineering manipulates people to reveal info or take actions. Example: phishing email prompting users to enter credentials on a fake site.

Q14: What is two-factor authentication (2FA) and its importance?

A14: 2FA requires two authentication factors (e.g., password + OTP), significantly reducing the risk of account compromise from stolen credentials.

Q15: Define cryptography, symmetric vs asymmetric.

A15: Cryptography secures data. Symmetric uses same key for encrypt/decrypt (AES); asymmetric uses key pairs (public/private) for encryption and digital signatures (RSA).

Q16: What is hashing and how is it different from encryption?

A16: Hashing produces a fixed-size digest from input (one-way). Encryption is reversible with a key. Hashing used for integrity and password storage (with salt).

Q17: What is a buffer overflow vulnerability?

A17: Buffer overflow occurs when a program writes more data than allocated buffer, potentially overwriting control data (return addresses) enabling arbitrary code execution.

Q18: What is the purpose of Metasploit?

A18: Metasploit is an exploitation framework with modules for scanning, exploiting, payload generation, and post-exploitation to validate vulnerabilities.

Q19: How should sensitive findings be reported?

A19: Report clearly with description, severity, proof-of-concept, affected assets, remediation steps, and evidence (screenshots, logs). Keep reports confidential to authorized parties.

Q20: What is risk assessment (in brief)?

A20: Risk assessment identifies threats, vulnerabilities, and potential impacts to calculate risk level and prioritize remediation based on likelihood and impact.

Q21: Explain the concept of 'least privilege'.

A21: Least privilege gives users/processes minimum rights necessary to perform tasks, reducing potential damage from compromised accounts.

Q22: How to secure remote access services like SSH and RDP?

A22: Use strong authentication (keys/2FA), change default ports if desired, limit access via IP whitelisting, apply rate-limiting, and keep software patched.

Q23: What is a security baseline? Why is it important?

A23: A security baseline is a set of configuration standards for systems to ensure consistent, secure settings (patch levels, services disabled). It reduces misconfigurations.

Q24: What is data exfiltration and how to detect it?

A24: Data exfiltration is unauthorized data transfer out of a network. Detect via DLP tools, unusual outbound traffic, spikes in data transfer, and monitoring/logging.

Q25: Mention three preventive controls to reduce successful attacks.

A25: Regular patching, network segmentation (limit lateral movement), and multi-factor authentication (MFA).