Module 3 — Ethical Hacking (Viva Questions & Answers)

Q1: What is DNS Spoofing?

A1: DNS Spoofing (DNS cache poisoning) is the act of inserting false DNS information into a resolver's cache so that domain names resolve to attacker-controlled IP addresses, redirecting users to malicious sites.

Q2: How does DNS caching affect spoofing attacks?

A2: DNS caching speeds lookups by storing previous results. If an attacker poisons the cache, the false entries persist until cache expires, potentially redirecting many users until the TTL expires.

Q3: Name two defenses against DNS Spoofing.

A3: Use DNSSEC (digitally sign DNS records) and implement DNS monitoring/response validation. Also keep DNS software patched and apply source authentication where possible.

Q4: What is DHCP and what is a rogue DHCP server?

A4: DHCP (Dynamic Host Configuration Protocol) assigns IP configuration to clients. A rogue DHCP server is an unauthorized server that provides malicious configuration (gateway/DNS) to redirect traffic or enable MITM.

Q5: How can DHCP spoofing enable a Man-in-the-Middle attack?

A5: By offering a malicious default gateway or DNS, a rogue DHCP server causes clients to route traffic through the attacker's device, enabling interception and traffic manipulation.

Q6: How to mitigate DHCP spoofing?

A6: Use DHCP snooping on switches, limit DHCP servers, use static IPs for critical devices, enforce network access controls and segmentation.

Q7: Define a Man-in-the-Middle (MITM) attack.

A7: MITM is when an attacker secretly intercepts or alters communications between two parties, often to steal credentials or inject malicious content.

Q8: Give common techniques used for interception in MITM attacks.

A8: ARP spoofing/poisoning, DNS spoofing, IP spoofing, and rogue Wi■Fi hotspots are common interception techniques.

Q9: What is ARP spoofing and how does it work?

A9: ARP spoofing involves sending forged ARP messages in a LAN to associate the attacker's MAC with another host's IP (e.g., gateway), causing traffic to be redirected to the attacker.

Q10: How can you detect ARP cache poisoning?

A10: Check ARP table with `arp -a` for duplicate MACs for different IPs, use network monitoring tools like Wireshark to spot suspicious ARP replies, or run ARP anomaly detectors on switches.

Q11: List prevention methods for ARP spoofing.

A11: Use static ARP entries for critical devices, enable DHCP snooping/ARP inspection on switches, use packet filtering/IDS, and use VPN encryption for sensitive traffic.

Q12: What is network sniffing and name popular tools.

A12: Network sniffing captures packets on the network. Common tools: Wireshark, tcpdump, NetworkMiner, and EtherApe.

Q13: Differentiate active and passive sniffing.

A13: Passive sniffing captures traffic without injecting packets (common on hubs). Active sniffing injects traffic or manipulates network state (used on switched networks) to intercept flows.

Q14: What is SSL stripping?

A14: SSL stripping downgrades HTTPS to HTTP by intercepting browser requests and removing the secure layer, allowing the attacker to read plaintext data.

Q15: How to defend against SSL stripping and HTTPS hijacking?

A15: Enforce HSTS (HTTP Strict Transport Security), always use HTTPS, validate certificates, and use browser plugins or security gateways that block insecure redirects.

Q16: Define SQL Injection (SQLi).

A16: SQLi is an injection attack where unsanitized user input is included in SQL queries, allowing attackers to run arbitrary SQL commands to read/modify the database.

Q17: Give examples of SQLi entry points.

A17: GET/POST parameters, headers (User-Agent, Referer), cookies, hidden form fields, and any user-controlled input used in dynamic queries.

Q18: Name primary defenses against SQL Injection.

A18: Use prepared statements/parameterized queries, validate and sanitize input, use least-privilege DB accounts, and deploy WAF rules.

Q19: What are brute force attacks and variants?

A19: Brute force attacks try many credential combinations. Variants include dictionary attacks, hybrid attacks, reverse brute force, and credential stuffing.

Q20: How to mitigate brute force attacks?

A20: Use account lockouts, rate limiting, multi-factor authentication (MFA), strong password policies, and monitoring for abnormal login attempts.

Q21: How can SMTP servers be abused by attackers?

A21: Misconfigured SMTP servers (open relays or weak auth) can be used to send spam/phishing, spoof sender domains, or be used in DDoS email floods.

Q22: Name common remote exploitation techniques.

A22: Exploiting unpatched services (RDP, SMB), credential theft (RDP brute force), exploitation frameworks (Metasploit), and DLL/loading vulnerabilities.

Q23: General mitigation strategies for remote exploitation?

A23: Patch management, limit remote access (VPN, 2FA), IDS/IPS, network segmentation, and strong credential policies.

Q24: How to detect a MITM attack in practice?

A24: Watch for certificate warnings, sudden network slowdowns, repeated disconnections, mismatched TLS fingerprints, or unexpected ARP table changes.

Q25: What information should a penetration test report include for these attacks?

A25: Vulnerability description, proof-of-concept steps, impacted assets, risk level, remediation recommendations, and evidence (logs/screenshots).