Module 4 — Ethical Hacking (Viva Questions & Answers)

Q1: Define a router and its primary functions.

A1: A router connects two or more packet■switched networks and forwards data packets to their intended IP addresses; it manages traffic between LANs and WANs and allows multiple devices to share a single Internet connection. ■filecite■turn2file10■

Q2: Name three specialized types of routers.

A2: Core routers (inside large networks), edge routers (connect to external networks and use BGP), and virtual routers (software-based routing). ■filecite■turn2file10■

Q3: What is NAT and why is it used?

A3: Network Address Translation (NAT) lets multiple LAN devices share one public IP by translating private IPs to a public address; it conserves IPv4 addresses and hides internal addresses from the Internet. ■filecite■turn2file10■

Q4: List three security risks related to routers.

A4: Unpatched firmware vulnerabilities, default/admin credentials left unchanged, and routers being overwhelmed by DDoS attacks. ■filecite■turn2file10■

Q5: What is a firewall and its main purpose?

A5: A firewall monitors and filters incoming/outgoing network traffic based on security policies; it acts as a barrier between an internal network and the public Internet to allow safe traffic and block threats. ■filecite■turn2file9■

Q6: Give types of modern firewalls.

A6: Packet-filtering firewalls, application-layer (stateful) firewalls, and Next-Generation Firewalls (NGFW) that include IPS, application and identity controls. ■filecite■turn2file9■

Q7: How do firewalls and IDS/IPS differ?

A7: Firewalls filter/allow traffic per policy; IDS (Intrusion Detection System) monitors and alerts on suspicious activity, while IPS (Intrusion Prevention System) can actively block or stop detected malicious traffic. ■filecite■turn2file9■

Q8: What are common IDS detection methods?

A8: Signature-based detection (matches known attack patterns) and anomaly-based detection (flags deviations from learned normal behavior, often using ML). ■filecite■turn2file9■

Q9: Define a honeypot and its purpose.

A9: A honeypot is a decoy system that appears attractive to attackers to capture, study, and divert malicious activity; used for detection, research, and threat intelligence. ■filecite■turn2file9■

Q10: Types of honeypots and deployment considerations.

A10: Low-interaction (simulate services), high-interaction (full systems for deep analysis), honeynets (multiple honeypots) and placement (DMZ or isolated networks); VMs often host honeypots. ■filecite■turn2file9■

Q11: How can honeypots be abused by attackers?

A11: Attackers may hijack honeypots to pivot attacks or use them to collect intelligence about defenders; careful isolation and monitoring are required. ■filecite■turn2file9■

Q12: Explain DHCP spoofing and its risks.

A12: A rogue DHCP server responds to client DHCP requests with malicious network settings (gateway/DNS), enabling MITM, traffic interception, or DoS. ■filecite■turn2file16■

Q13: How to mitigate DHCP and ARP based MITM attacks?

A13: Use DHCP snooping, dynamic ARP inspection, static ARP entries for critical hosts, VPNs, and network segmentation. ■filecite■turn2file16■turn2file17■

Q14: How to detect ARP spoofing?

A14: Check ARP table (`arp -a`) for duplicate MAC entries, use Wireshark to spot suspicious ARP replies, and deploy network monitoring/IDS. ■filecite■turn2file17■

Q15: What should a viva answer include when reporting a router or firewall vulnerability?

A15: Brief description, impact, proof-of-concept steps, affected assets, severity, and remediation recommendations (patching, config changes, access control). ■filecite■turn2file10■turn2file9■