Part – A (2 Marks Each) 10 x 2 = 20

1. Describe the role of a penetration tester in an organization. A penetration tester (or ethical hacker) is responsible for legally and systematically probing an organization's network, applications, and physical security to find vulnerabilities. Their primary goal is to identify weaknesses before malicious actors do and provide actionable recommendations to mitigate those risks. $(2\ \text{marks})$

2. Identify any two objectives of ethical hacking. $(2\ \text{marks})$

- **To identify vulnerabilities:** Finding security gaps in systems and software.
- **To test security posture:** Evaluating the effectiveness of an organization's existing security controls and defensive mechanisms.

3. Illustrate the importance of the TCP/IP model in solving communication delays/failures. $(2\ \text{marks})$

The TCP/IP model provides a structured framework for data transmission. It helps in troubleshooting by isolating issues to specific layers (e.g., checking physical connectivity at the Network Access layer vs. error-checking at the Transport layer). This "divide and conquer" approach ensures reliable, sequenced delivery of data packets.

4. Differentiate between network attacks and malware attacks. $(2\ \text{marks})$

- **Network Attacks:** These target the infrastructure or communication protocols (e.g., DoS, Man-in-the-Middle) to intercept data or disrupt service.
- **Malware Attacks:** These involve malicious software (e.g., viruses, ransomware) installed on a host to damage files, steal data, or gain unauthorized access.

5. Describe the concept of footprinting in cyber security. Footprinting is the initial phase of information gathering where an attacker (or ethical hacker) collects as much data as possible about a target network. This includes IP addresses, domain names, employee details, and network blocks to create a "blueprint" of the target's security profile. $(2\ \text{marks})$

6. Identify any two tools used for footprinting through search engines and web services. $(2\ \text{marks})$

- Google Hacking Database (GHDB) / Google Dorks
- Whois Lookup

7. Distinguish between port scanning and network scanning. $(2\ \text{marks})$

- **Network Scanning:** Used to identify active hosts (live IP addresses) on a network.

- **Port Scanning:** Performed on a specific live host to identify which services (ports) are open, closed, or filtered (e.g., HTTP on port 80).

8. Illustrate why scanning techniques are important in vulnerability detection. (2 marks)
Scanning automates the discovery of open doors and known weaknesses. It allows administrators to proactively find unpatched software, misconfigured services, or weak entry points, enabling them to apply security patches before an exploit occurs.

9. Describe the role of NetBIOS enumeration in information gathering. NetBIOS enumeration allows an attacker to fetch details like the list of computers belonging to a domain, shared resources (files/printers), and device names. It helps in mapping the internal network structure of Windows-based systems. (2 marks)

10. Identify any two vulnerability assessment techniques used for desktop and server OS. (2 marks)

- **Credentialed Scanning:** Scanning with administrative access to find deep-seated configuration issues.
- **Non-Credentialed Scanning:** Scanning from the outside to see what a hacker would see without prior access.