Part – A (2 Marks Each)

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. Identify any two objectives of ethical hacking.

- **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.

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.

- **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.

6. Identify any two tools used for footprinting through search engines and web services.

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

7. Distinguish between port scanning and network scanning.

- **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. 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.

10. Identify any two vulnerability assessment techniques used for desktop and server OS.

- **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.

Part- B (16 marks)

11 (a) Penetration Testing Methodology & TCP/IP Layer Analysis

1. Introduction to the Methodology (2 Marks)

A comprehensive penetration test follows a standardized lifecycle to ensure all vulnerabilities are identified without disrupting business operations.

- **Pre-engagement:** Defining the scope (web apps, data transmission, internet connectivity).
- **Information Gathering:** Collecting data about the target.
- **Vulnerability Analysis:** Identifying flaws.
- **Exploitation:** Attempting to bypass security controls.
- **Post-Exploitation & Reporting:** Documenting findings and mitigation strategies.

2. TCP/IP Layer Analysis & Vulnerability Identification (8 Marks)

To address the company's specific incidents (web apps, data transmission, internet connectivity), the test must be broken down by the **TCP/IP layers**:

TCP/IP Layer	Focus Area	Specific Vulnerabilities to Identify
Application Layer	Web Applications, Email, File Transfer	SQL Injection, Cross-Site Scripting (XSS), insecure APIs, weak authentication, and unpatched web server software.
Transport Layer	End-to-end communication (TCP/UDP)	Use of clear-text protocols (Telnet/HTTP instead of SSH/HTTPS), open ports, and vulnerabilities in SSL/TLS handshakes.
Internet Layer	Routing and IP Addressing	IP spoofing, ICMP redirect attacks, and misconfigured firewall rules allowing unauthorized traffic.
Network Access Layer	Physical/Data Link (MAC, Ethernet)	ARP poisoning, MAC flooding, and insecure wireless access points (WAPs).

3. Implementation Steps (Practical Workflow) (3 Marks)

1. **Reconnaissance:** Use tools like Nmap for port scanning and Whois for domain info.
2. **Scanning:** Use Nessus or OpenVAS to find known vulnerabilities in the web apps and servers.
3. **Exploitation:** Use the Metasploit Framework to simulate an attack on a detected vulnerability (e.g., a buffer overflow in a transport protocol).
4. **Data Analysis:** Determine if sensitive data (from "data transmission") can be intercepted using packet sniffers like Wireshark.

4. Mitigation Strategies (3 Marks)

- **Application Layer:** Implement a **Web Application Firewall (WAF)** and enforce **Input Validation** to prevent injection attacks.
- **Transport Layer:** Enforce **Encryption (TLS 1.3)** for all data in transit to solve the "data transmission failures" mentioned in the prompt.
- **Internet Layer:** Deploy **Intrusion Detection/Prevention Systems (IDS/IPS)** and implement **Network Segmentation** to limit the lateral movement of an attacker.
- **Network Access Layer:** Use **Port Security** (MAC filtering) and **VPNs** for secure remote connectivity.

11 (b) Malware Detection and Incident Response Strategy

1. Incident Response Framework (3 Marks)

To handle the repeated attacks, the organization must follow the standard **SANS/NIST Incident Response Lifecycle**:

- **Preparation:** Hardening systems and setting up monitoring tools before an attack.
- **Identification:** Detecting the malware or intruder activity via logs or alerts.
- **Containment:** Isolating infected systems to prevent lateral movement.
- **Eradication:** Removing the root cause (malware files, backdoors).
- **Recovery:** Restoring systems to normal operation.
- **Lessons Learned:** Analyzing the attack to prevent recurrence.

---

2. Detection and Analysis (6 Marks)

The "Demonstration" part of the question requires identifying the presence of the intruder and the malware behavior:

- **Network Detection (Intruders):**
    - **Tool: Wireshark / TCPDump**.
    - **Method:** Analyze traffic for unusual patterns like unauthorized port scanning, large data exfiltration (data leakage), or connections to known malicious C2 (Command and Control) servers.
- **Host-Based Detection (Malware):**
    - **Tool: Process Explorer / Autoruns**.
    - **Method:** Check for suspicious processes running in the background, unauthorized registry changes, or new files in startup folders.
- **Log Analysis:**
    - **Tool: SIEM (e.g., Splunk / ELK Stack)**.
    - **Method:** Correlate login failures (potential brute force) and account escalations.

3. Practical Security Mechanisms (4 Marks)

To stop the "repeated" nature of these attacks, the following mechanisms must be demonstrated:

- **Endpoint Detection and Response (EDR):** Deploying agents on all desktops/servers to monitor behavior and automatically kill malicious processes.
- **Intrusion Prevention Systems (IPS):** Configuring signatures to automatically drop packets identified as known malware payloads or exploit attempts.
- **Data Loss Prevention (DLP):** Implementing DLP rules to monitor and block the "data leakage" mentioned in the scenario by scanning outgoing traffic for sensitive patterns (e.g., credit card numbers, proprietary code).
- **Access Control (Zero Trust):** Implementing Multi-Factor Authentication (MFA) to ensure that even if an intruder has credentials, they cannot access the system.

4. Mitigation & Response Summary (3 Marks)

- **Short-term:** Disconnect infected hosts from the VLAN, reset all administrative passwords, and block the attacker's IP at the firewall.
- **Long-term:** Patch the vulnerabilities that allowed the malware in (e.g., unpatched software or weak phishing defenses) and conduct regular security awareness training for employees.

12 (a) Footprinting and Information Gathering Methodology

1. Introduction to Footprinting (2 Marks)

Footprinting is the first step in the reconnaissance phase of a penetration test. It involves gathering as much information as possible about a target organization to identify its security posture. For this startup, the goal is to assess "online exposure" and "digital footprint" before their product launch.

2. Information Gathering Techniques (6 Marks)

Since the requirement is to perform information gathering **without directly interacting with their systems**, we use **Passive Footprinting**:

- **Search Engine Discovery:**
    - **Method:** Using Advanced Google Hacking (Google Dorks) to find sensitive directories, exposed documents (PDF/Docx), or subdomains.

    - **Queries:** site:startup.com filetype:pdf or intitle:"index of".
- **Social Networking Platforms:**
    - **Platforms:** LinkedIn, X (Twitter), and Facebook.
    - **Method:** Analyzing employee profiles to identify the technology stack (e.g., "Experience in AWS/React"), organizational hierarchy, and potential email naming conventions.
- **Web Services & Domain Research:**
    - **Whois Lookup:** To find domain ownership details, registration dates, and technical contact information.
    - **Netcraft / BuiltWith:** To identify the web server type, OS, and CMS without sending a single packet to the startup's server.

3. Application of Intelligence Gathering (4 Marks)

To evaluate potential security risks for the startup, the gathered data is analyzed as follows:

- **Domain Name System (DNS) Analysis:** Using tools like DNSdumpster to map the startup's infrastructure (mail servers, name servers) to find "hidden" staging or development servers.
- **Email Harvesting:** Using tools like theHarvester to collect email addresses from public sources, which could be used for social engineering or phishing tests.
- **Leaked Credentials Check:** Searching databases (like HaveIBeenPwned or specialized breach repositories) to see if any employee emails have already been compromised.

4. Evaluation of Security Risks (4 Marks)

Based on the footprinting results, the following risks are assessed:

- **Information Leakage:** Are internal documents or private API endpoints visible to search engines?
- **Social Engineering Vulnerability:** Do employees share too much technical detail on LinkedIn that could help an attacker craft a convincing spear-phishing email?

- **Shadow IT:** Are there unmanaged subdomains or legacy systems (e.g., dev.startup.com) that are unpatched and exposed?

12 (b) Network Reconnaissance and Port Scanning Methodology

1. Introduction to Network Reconnaissance (2 Marks)

Network reconnaissance is the process of identifying active hosts, open ports, and services running on a target network to find potential entry points for an attack. In this scenario, it is used to detect misconfigured services that attackers might exploit.

2. Step-by-Step Process of Network Reconnaissance (8 Marks)

A systematic approach involves moving from broad network discovery to specific service identification:

- **Step 1: Live Host Discovery:**
    - **Method:** Performing an ICMP Echo Request (Ping Sweep) or ARP ping to see which IP addresses are active.
    - **Tool:** Nmap -sn or fping.
- **Step 2: Port Scanning:**
    - **Method:** Probing the discovered live hosts to see which TCP/UDP ports are open. This identifies "doors" into the system.
    - **Techniques:**
        - **TCP Connect Scan (-sT):** Completes the 3-way handshake. Reliable but easily logged.
        - **SYN Stealth Scan (-sS):** Sends a SYN packet but resets before the handshake completes. Harder to detect.
- **Step 3: Service Version Detection:**
    - **Method:** Sending specific probes to open ports to determine the exact software and version running (e.g., Apache 2.4.41).
    - **Tool:** Nmap -sV.
- **Step 4: OS Fingerprinting:**
    - **Method:** Analyzing how the target's network stack responds to specific packets to guess the Operating System (Linux, Windows, etc.).

- **Tool:** Nmap -O.

3. Identification of Weaknesses (3 Marks)

After scanning, the results are interpreted to find vulnerabilities:

- **Open Ports:** Unnecessary ports like 21 (FTP) or 23 (Telnet) that should be closed.
- **Misconfigured Services:** Services running with default credentials or outdated versions with known vulnerabilities (CVEs).
- **Firewall Weaknesses:** If a port like 3389 (RDP) is open to the public internet, it indicates a major firewall misconfiguration.

4. Tools and Techniques Summary (3 Marks)

Technique	Purpose	Common Tool
Ping Sweep	Identify live hosts	Nmap, Angry IP Scanner
Port Scanning	Find open entry points	Nmap, Masscan
Banner Grabbing	Identify service versions	Telnet, Netcat
Vulnerability Scanning	Automated flaw detection	Nessus, OpenVAS

13 (a) NetBIOS Enumeration for Vulnerability Assessment

1. Introduction to NetBIOS Enumeration (2 Marks)

NetBIOS (Network Basic Input/Output System) enumeration is a technique used to extract sensitive information from Windows-based systems. It allows a security analyst to identify resources being shared over a local network, which is critical for the "information gathering" phase mentioned in your scenario.

2. NetBIOS Enumeration Techniques (4 Marks)

To collect detailed system and resource information, the following techniques are applied:

- **Finding Computer Names:** Identifying the NetBIOS name of the target machine to understand its role (e.g., HR-PC vs. DB-SERVER).
- **Enumerating Shared Resources:** Listing shared files, folders, and printers that might be poorly secured.
- **Identifying User Accounts:** Fetching the names of users currently logged in or accounts existing on the machine.

- **Extracting MAC Addresses:** Obtaining the hardware address of the network interface for further spoofing or mapping.

3. Impact on Vulnerability Assessment (2 Marks)

NetBIOS information supports attack planning by:

- **Identifying High-Value Targets:** Pinpointing servers that hold sensitive data based on their shared folders.
- **Credential Attacks:** Using discovered usernames for password spraying or brute-force attacks.
- **Protocol Weaknesses:** Identifying if the system is running older, insecure versions of NetBIOS or SMB (Server Message Block) that are susceptible to exploits like EternalBlue.

13 (b) SNMP, LDAP, and DNS Enumeration

1. Enumeration Overview (2 Marks)

In a corporate data center, services like SNMP, LDAP, and DNS often hold the "keys to the kingdom." Enumerating these services helps a security professional identify misconfigurations and exposed services without needing a password.

2. Demonstration of Enumeration Techniques (4 Marks)

Service	Enumeration Technique	Information Extracted
SNMP (Simple Network Management Protocol)	Using **SNMPwalk** with "public" or "private" community strings.	Router tables, device temperatures, system uptime, and even clear-text passwords stored in device configs.
LDAP (Lightweight Directory Access Protocol)	Querying the directory service using tools like ldapsearch.	Usernames, email addresses, department structures, and group memberships (Active Directory info).
DNS (Domain Name System)	Attempting a **Zone Transfer (AXFR)**.	A complete list of all internal hostnames and IP addresses, revealing "hidden" servers like backup-db.internal.

Service	Enumeration Technique	Information Extracted
SMTP (Simple Mail Transfer Protocol)	Using the VRFY and EXPN commands.	Verifying if a specific user exists on the mail server to build a targeted phishing list.

3. Exploitation and Risk Analysis (2 Marks)

Attackers exploit this information in the following ways:

- **Network Mapping:** Using DNS and SNMP data to create a perfect map of the internal data center layout.
- **Privilege Escalation:** Using LDAP data to identify high-privilege users (Domain Admins) to target specifically.
- **Service Exploitation:** Knowing the exact version of an SMTP or SNMP service allows an attacker to search for specific exploits (CVEs) to gain unauthorized access.