Elevate Labs

Task-1: Scan your local network for open ports.

Internship Questions –

1. What is an open port?

An open port is a network port on a device that is actively accepting incoming connections. It indicates that a specific application or service (like a web server, FTP server, or SSH) is listening for communication on that port.

- For example, if port 80 is open, it usually means an HTTP server is running.
- Open ports are like entry points — they can be legitimate, but if left unprotected, they become attack vectors.

In cybersecurity, identifying open ports is a fundamental step in determining network exposure and potential vulnerabilities.

2. How does Nmap perform a TCP SYN scan?

Nmap uses the TCP SYN scan (-sS) technique, also known as half-open scanning.

How it works:

1. Nmap sends a SYN packet to the target port.
2. If the port is open, the target replies with a SYN-ACK.
3. Nmap immediately sends an RST (reset) instead of completing the handshake, to avoid logging or full connection.

This method is:

- Fast and stealthy (less likely to be logged by the target)
- Useful for scanning hundreds of ports quickly
- Commonly used in penetration testing and network auditing

It mimics what attackers do when silently probing systems.

3. What risks are associated with open ports?

Open ports can be dangerous if:

- The services behind them are vulnerable, outdated, or misconfigured
- They are exposed to the internet without restriction

Real-world risks:

- Port 445 (SMB) → Vulnerable to EternalBlue (WannaCry attack)
- Port 22 (SSH) → Targeted for brute-force attacks
- Port 3306 (MySQL) → Can expose sensitive databases if not secured

Attackers use open ports to:

- Identify potential attack surfaces
- Exploit known vulnerabilities
- Gain unauthorized access to services

Open ports are like open windows — even if you trust them, they must be monitored and locked properly.

4. Explain the difference between TCP and UDP scanning.

Feature	TCP Scanning	UDP Scanning
Connection	Connection-oriented	Connectionless
Feedback	Clear responses (SYN/ACK)	Often silent (no response)
Reliability	More reliable	Less reliable
Speed	Slower	Faster (but inconclusive results)
Example Use Case	Web servers, SSH, FTP	DNS, SNMP, TFTP

- TCP Scan (like SYN scan): Sends SYN packets and waits for a response.
- UDP Scan: Sends UDP packets and hopes for a response. If none, it's hard to tell whether the port is open or just filtered.

UDP scanning is tricky because many open ports don't respond at all unless probed the right way.

5. How can open ports be secured?

Securing open ports involves minimizing exposure and hardening the services running on them:

Security Measures:

- Close unused ports using firewalls
- Enable authentication and access control for services
- Update and patch all running applications
- Use port-knocking or VPNs for private service access
- Run vulnerability scans regularly

Remember: Not every open port is dangerous, but every unmonitored one is a risk.

6. What is a firewall's role regarding ports?

A firewall acts as a traffic filter that controls what data can enter or leave a system based on rules.

Key Roles:

- Block unauthorized ports from being accessed
- Allow only necessary services (e.g., HTTP on port 80)
- Log traffic attempts on sensitive ports
- Protect against port scans and DDoS attacks

Types of firewalls:

- Network Firewalls (like pfSense, Cisco ASA)
- Host Firewalls (like Windows Defender Firewall)

Think of the firewall as the security guard that decides which "doors" (ports) should be open and who can enter them.

7. What is a port scan and why do attackers perform it?

A port scan is a method of probing a system to find open, closed, or filtered ports. It helps determine:

- What services are running
- Which software versions are in use
- The system's potential vulnerabilities

Why attackers scan ports:

- To map the network and identify active hosts
- To discover exploitable services (like Telnet, FTP, SMB)
- As the first stage of a cyber attack (reconnaissance phase)

It's like a burglar walking around a house, checking each door and window to see if it's unlocked.

8. How does Wireshark complement port scanning?

Wireshark helps by showing packet-level visibility during or after a scan.

How it complements:

- You can see the actual SYN packets sent by Nmap
- Observe responses (SYN-ACK, RST) from target systems
- Confirm what Nmap sees under the hood
- Analyze firewall responses, packet drops, or anomalies

Wireshark is useful for:

- Validating Nmap scans
- Troubleshooting network behavior
- Detecting unauthorized scans on your own systems

If Nmap gives the summary, Wireshark shows the proof.