**Elevate Labs Internship**

Task: 1

Interview Questions

1. What is an open port?

English — Answer:  
A port is a logical endpoint on a host used for network communication. An open port means a service or application on that host is listening for incoming connections on that port (e.g., TCP 80 → an HTTP server).  
Easy example: If a shop has its door open and a shopkeeper is waiting, customers can enter — that’s like an open port where clients can connect.

**2. How does Nmap perform a TCP SYN scan?**

**English — Answer:**  
A TCP SYN scan (-sS) is a “half-open” scan. Nmap sends a SYN to a port:

* If the host replies **SYN/ACK**, the port is **open** → Nmap responds with **RST** (so TCP handshake is not completed).
* If the host replies **RST**, the port is **closed**.
* If there is no reply or an ICMP unreachable, the port is **filtered** (firewall/ACL likely).  
  This is fast and stealthier than completing full handshakes.

**Easy example:** Think of knocking on a door (SYN). If someone peeks and waves you in (SYN/ACK), you step back without entering (send RST). If nobody answers or a “do not enter” sign is shown, you know the situation without going inside.

**3. What risks are associated with open ports?**

**English — Answer:**  
Open ports expose running services — risks include:

* **Unauthorized access** (if service has weak auth).
* **Exploitation of unpatched vulnerabilities** (remote code execution).
* **Information leakage** (service banners reveal versions).
* **Lateral movement** — attacker uses one compromised service to reach others.
* **Denial-of-service** — services exposed to flooding.  
  Impact severity depends on the service, configuration, and network controls.

**Easy example:** An unlocked door lets burglars enter, look for valuables, or use that room as a path to other rooms.

**4. Explain the difference between TCP and UDP scanning.**

**English — Answer:**

* **TCP** is connection-oriented (handshake). TCP scans (SYN, connect) check port states based on handshake responses — usually reliable and produce clear open/closed answers.
* **UDP** is connectionless. UDP scans send UDP datagrams and infer state from replies: an ICMP port unreachable → closed; no reply → open|filtered (ambiguous). UDP scanning is **slower**, **less reliable**, and more prone to false negatives because many services don’t reply or are rate-limited.

**Easy example:** TCP is like calling and getting a live reply; UDP is like dropping a letter and hoping for a return receipt — you may not receive any reply even if someone got it.

**5. How can open ports be secured?**

**English — Answer:**  
Best practices:

* **Close unused ports** (stop or uninstall unused services).
* **Apply patches** and keep software up to date.
* **Restrict access** with firewall rules / allowlists (limit by IP, VPN).
* **Use strong authentication & encryption** (TLS, SSH keys, MFA).
* **Run services with least privilege** and isolate via network segmentation.
* **Use IDS/IPS and rate-limiting** and monitor/log access.
* **Hide version banners** and limit error details to avoid information leakage.

**Easy example:** Keep only necessary doors unlocked, install sturdy locks, allow only known guests, and keep logbooks of visitors.

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

**English — Answer:**  
A firewall controls network traffic by **allowing, denying, or filtering** packets based on rules (ports, protocols, IPs). It can:

* Block unwanted incoming/outgoing ports.
* Implement allowlists or blocklists.
* Perform NAT (hide internal port mapping).
* Enforce application-layer policies (web application firewall).
* Log and alert on suspicious access attempts.

**Easy example:** A firewall is like a security guard at a building who checks IDs and only lets authorized visitors through specific doors.

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

**English — Answer:**  
A **port scan** is a technique to probe a host’s ports to discover which are open, closed, or filtered. Attackers perform port scans to:

* **Enumerate available services** and their versions.
* **Find weak or vulnerable services** to exploit.
* Map the network (identify hosts, firewalls, ACLs).
* Stage further attacks (credential stuffing, RCE, lateral movement).  
  Port scanning is reconnaissance — the first step before exploitation.

**Easy example:** A burglar walking past houses and checking which windows/doors are open before choosing a target.

**8. How does Wireshark complement port scanning?**

**English — Answer:**  
Wireshark is a packet-capture and analysis tool. It complements port scans by allowing you to:

* **Capture network traffic** during/after a scan to see real packet-level responses.
* **Verify service behavior** (actual protocol exchanged, TLS handshake details, headers).
* **Detect anomalous or malicious traffic** that a simple port scan can’t show.
* **Troubleshoot false positives/negatives** from scans (e.g., retransmissions, ICMP messages).  
  Use Wireshark when you need deep inspection of what happened on the wire.

**Easy example:** Nmap is like scanning doors to see which are open; Wireshark is like standing by the door with a camera to record exactly who knocked, what they said, and who answered.