**1. What is an Open Port?**

* An open port is a network port that is actively listening for incoming connections.
* It allows data to flow between devices and services using specific protocols (e.g., HTTP on port 80).
* Open ports are essential for communication but can be exploited if not properly secured.

**2. How Does Nmap Perform a TCP SYN Scan?**

* Nmap sends a **SYN** packet to the target port (first step of TCP handshake).
* If the port is **open**, it replies with **SYN-ACK**; Nmap then sends a **RST** to avoid completing the handshake.
* If the port is **closed**, it responds with a **RST**.
* This method is called a **half-open scan** and is stealthier than a full TCP connection.

**3. What Risks Are Associated with Open Ports?**

* **Unauthorized Access**: Hackers can exploit services running on open ports.
* **Malware Infections**: Open ports can be entry points for malicious payloads.
* **DDoS Attacks**: Attackers may flood open ports to disrupt services.
* **Data Exfiltration**: Sensitive data can be siphoned through exposed ports.

**4. Explain the Difference Between TCP and UDP Scanning**

| **Feature** | **TCP Scanning** | **UDP Scanning** |
| --- | --- | --- |
| Protocol Type | Connection-oriented | Connectionless |
| Reliability | High (3-way handshake) | Low (no handshake) |
| Detection | Easier to detect | Harder to detect |
| Speed | Slower due to handshake | Faster but less reliable |
| Use Case | Web, SSH, FTP | DNS, SNMP, VoIP |
| Tools | Nmap -sS, -sT | Nmap -sU |

**5. How Can Open Ports Be Secured?**

* **Close Unused Ports**: Reduce attack surface.
* **Use Firewalls**: Block unauthorized traffic.
* **Enable VPNs**: Restrict access to trusted users.
* **Apply Patches**: Keep services updated.
* **Use IDS/IPS**: Detect and prevent suspicious activity.

**6. What Is a Firewall's Role Regarding Ports?**

* Firewalls **monitor and control** traffic based on port rules.
* They **allow, block, or filter** traffic to specific ports.
* Firewalls can be **host-based** or **network-based**, and help enforce security policies.

**7. What Is a Port Scan and Why Do Attackers Perform It?**

* A port scan sends packets to various ports to identify which are open, closed, or filtered.
* Attackers use it for **reconnaissance** to find vulnerable services.
* Common scan types: SYN, FIN, XMAS, UDP, and Ping scans.
* Ethical hackers also use port scans for **security assessments**.

**8. How Does Wireshark Complement Port Scanning?**

* Wireshark captures and analyzes **live packet data**.
* It helps verify **port scan results** by showing actual traffic.
* You can filter by port (e.g., tcp.port == 443) to inspect service behavior.
* Useful for **deep packet inspection**, protocol analysis, and troubleshooting.