Port Scanning & Security - Quick Guide

1. What is an open port?

An open port is a network port that is actively accepting connections or data, indicating a running service or application.

2. How does Nmap perform a TCP SYN scan?

Nmap sends a SYN packet to a port; if it gets a SYN-ACK, the port is open. It then sends a RST to avoid completing the handshake (stealth scan).

3. What risks are associated with open ports?

Open ports can expose vulnerable services, leading to data breaches, unauthorized access, or malware infections.

4. Explain the difference between TCP and UDP scanning.

TCP Scan: Actively tries to connect (e.g., SYN or full handshake).

UDP Scan: Sends a datagram and waits for a response or ICMP error. Slower and less reliable.

5. How can open ports be secured?

Close unused ports

Use firewalls

Apply patches

Restrict access using IP whitelisting

Enable encryption (TLS/SSL) where needed

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

A firewall filters traffic by allowing or blocking ports based on security rules, preventing unauthorized access.

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

A port scan is a probe of ports to find open ones. Attackers use it to identify targets and vulnerabilities for exploitation.

8. How does Wireshark complement port scanning?

Wireshark captures and analyzes network packets, helping you see the scan in action, verify traffic behavior, and detect suspicious scans.