**❓ Interview Questions & Answers**

**1. What is an open port?**

An open port is a network port that is configured to accept connections. It can be accessed remotely and may expose services running on the device.

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

Nmap sends SYN packets (like the start of a TCP handshake) and waits for a SYN-ACK response. If received, the port is considered open.

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

Open ports can expose sensitive services, be used by attackers to exploit vulnerabilities, or allow unauthorized access.

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

* TCP scan checks connection-based services and expects responses.
* UDP scan checks connectionless services and may be slower due to lack of response.

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

* Close unnecessary ports
* Use firewalls
* Implement intrusion detection systems (IDS)
* Disable unused services

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

A firewall filters network traffic based on rules and can block or allow ports to secure a device from unwanted access.

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

A port scan probes a system to find open ports and services. Attackers use it to map vulnerabilities and plan exploits.

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

Wireshark helps visualize packet-level data, confirming scan behavior and detecting unusual or malicious activity.