1. **What is an open port?**  
   An open port is a numbered network endpoint on a device that is actively *listening* for network connections. When a service (like SSH, a web server, or file sharing) runs on a device it opens a port (e.g., 22 for SSH, 80 for HTTP). An open port means *something is reachable there* — which is necessary for legitimate use but also creates an attack surface if the service is vulnerable or misconfigured.
2. **How does Nmap perform a TCP SYN scan?**  
   A TCP SYN scan (-sS) sends a TCP **SYN** packet to a target port:

* If the target replies **SYN/ACK**, Nmap marks the port **open** and typically sends a **RST** to avoid completing the handshake.
* If the target replies **RST**, Nmap marks the port **closed**.
* If there is no reply or an ICMP unreachable, Nmap marks the port **filtered**.  
  SYN scan is fast and less intrusive because it doesn’t complete full TCP connections (it only probes the handshake).

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

* **Unpatched services**: known vulnerabilities can be remotely exploited.
* **Misconfiguration**: default credentials, weak auth, or excessive privileges.
* **Data exposure**: services might leak sensitive data.
* **Network entry points**: attackers can use open services to pivot/scan deeper into a network.
* **Automated attacks**: bots scan the Internet and try common exploits on open ports.

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

* **TCP** is connection-oriented (SYN → SYN/ACK → ACK). TCP scans (like SYN or connect) get clear replies (SYN/ACK = open, RST = closed), so they are usually reliable and faster.
* **UDP** is connectionless. Many UDP services don’t reply when closed, so scanners rely on ICMP “port unreachable” or timeout heuristics — making UDP scans **slower** and prone to **false negatives** (open ports that look closed). UDP scanning often requires more patience and retries.

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

* **Close or disable** services you don’t need.
* **Patch** services and OS regularly.
* **Restrict access** with firewalls and ACLs (allow only required IPs).
* **Use strong auth** (SSH keys, MFA) and change default credentials.
* **Run services with least privilege** and inside containers/VLANs if possible.
* **Expose admin services** only via VPN or jump-hosts, not directly to the internet.
* **Monitor** logs and use IDS/IPS to detect abnormal access attempts.

1. **What is a firewall's role regarding ports?**  
   A firewall controls which ports and addresses can communicate with a host or network. It can block or allow traffic by port, protocol, source/destination IPs and be **stateful** (track connection state) or **stateless**. Firewalls reduce the exposed attack surface by preventing unauthorized access to open services.
2. **What is a port scan and why do attackers perform it?**  
   A port scan probes hosts to discover which ports/services are reachable. Attackers scan to map an environment, find accessible services and their versions, and identify likely vulnerabilities to exploit. Defensive teams perform scans too — for asset discovery and to find and fix exposures.
3. **How does Wireshark complement port scanning?**  
   Wireshark captures the actual network packets so you can *see* what happened during a scan — e.g., your SYN packet, the target’s SYN/ACK or RST, dropped packets, or suspicious payloads. This proves Nmap’s findings, helps debug weird results (filtered vs. no-reply), and lets you inspect protocol details and banners at packet level for more accurate analysis.