1. What is an open port?
   Ans: An open port is a network actively used by a service or application to send or receive over a network. Each port has a unique number (0-65535) and is often associated with a service like HTTP(80) or SSH(22). While essential; for communication, open ports can pose security risks if misconfigured or exposed to in the internet.

2. How does Nmap perform a TCP SYN scan?
   Ans: Nmap performs a TCP SYN scan by sending a SYN packet to a target port to check if it's open. If the port is open, the target replies with a SYN-SCK; if it's closed, it responds with an RST. Nmap then sends an RST instead of completing the handshake, making it a fast and stealthier "half-open" scan.

3. What risks are associated with open ports?
   Ans: Open ports can allow unauthorized access, enabling attackers to exploit vulnerabilities in services or applications and potentially cause data breaches or malware infections. They can also be targeted for Denial of Services (DoS) attacks, overwhelming the systems sand disrupting services. Additionally, misconfigured open ports may expose sensitive data, especially if communication is unencrypted or poorly secured.

4. Explain the differences between TCP and UDP scanning.
   Ans: TCP scanning is used to detect TCP-based services (e.g., web servers, email servers, databases) by initiating

or partially initiating TCP handshake, which makes it reliable because TCP confirms connections.

UDP scanning is used for DNS,DHCP and sends UDP packets without establishing a connection, making it faster but less reliable since there is no handshakes and responses are limited.

5. How can open ports be secured?
   Ans: To secure open ports, first identify and regularly scan them, keeping only those necessary for business operations. Protect them with firewall rules, VPN access, multi-factor authentication, and secure protocols while keeping services updated. Additionally, use network segmentation, monitoring and logging to limit exposure and quickly detect suspicious activity.

6. What is a firewall's role regrading ports?
   Ans: A firewall manages ports by allowing or blocking traffic based on security rules, ensuring only authorized access to services. It filters traffic by port numbers, protocols and IP addresses to prevent unauthorized access and mitigate attacks. This control helps protect sensitive resources and maintain the integrity of the network.

7. What is a port scan and why do attackers perform it?
   Ans: A port scan is used to detect open ports and the services running on them, helping attackers identify potential entry points and vulnerabilities to exploit. Common methods include TCP SYN scans, UDP scans

and stealth scans, which reveal valuable information for planning attacks.

8. How does Wireshark complement port scanning?
   Ans: Wireshark can complement port scanning by capturing and analyzing network traffic to verify scan results, inspect service responses, and detect anomalies that may indicate vulnerabilities or malicious activity. This combination provides deeper insights into network behaviour, confirms port scan findings, and helps indentift potential security risks.