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

An **open port** is a communication endpoint on a computer or server that is configured to accept incoming network connections. It is a logical number assigned to a specific process or service, allowing it to "listen" for and respond to network traffic. When a port is "open," it means a service is actively running on it, ready to communicate.

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

A **TCP SYN scan**, also known as a "stealth scan," is a method used by Nmap to determine if a port is open without completing the full TCP three-way handshake. The process is as follows:

1. **SYN Packet:** Nmap sends a TCP SYN (synchronize) packet to the target port.
2. **SYN-ACK Response (Open Port):** If the port is open, the target system responds with a TCP SYN-ACK (synchronize-acknowledge) packet.
3. **RST Packet:** Instead of sending the final ACK packet to complete the handshake, Nmap sends a TCP RST (reset) packet. This immediately tears down the connection.

This method is "stealthy" because the connection is never fully established, making it less likely to be logged by the target system's security monitoring.

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

Open ports are a significant security risk because they represent potential entry points for attackers. The risks include:

* **Unauthorized Access:** Attackers can exploit vulnerabilities in services running on open ports to gain unauthorized access to a system.
* **Malware Infections:** Ports can be used as a vector for malware, which can spread automatically by scanning for and exploiting vulnerable open ports.
* **Information Leakage:** Open ports can reveal the services, versions, and operating system of a host, providing valuable information for attackers to plan a more targeted attack.
* **Denial-of-Service (DoS) Attacks:** Attackers can flood an open port with a large volume of traffic to overload and crash the service, making it unavailable to legitimate users.

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

* **TCP (Transmission Control Protocol) Scanning:** TCP is a connection-oriented protocol that establishes a reliable connection before data is transferred. TCP scans, like the SYN scan, rely on the three-way handshake and subsequent responses to determine if a port is open. This method is generally more reliable for identifying open ports.
* **UDP (User Datagram Protocol) Scanning:** UDP is a connectionless protocol, which means it doesn't establish a handshake. A UDP scan works by sending a UDP packet to a port. If the port is open, the service may or may not send a response. If the port is closed, the target system will typically send back an ICMP (Internet Control Message Protocol) "Port Unreachable" error. The absence of this error usually indicates that the port is open.

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

Securing open ports is a critical part of network defense. Key measures include:

* **Principle of Least Privilege:** Close all ports that are not absolutely necessary for a service to function.
* **Firewalls:** Use a firewall to filter incoming and outgoing traffic, creating rules that only allow connections to specific ports from trusted IP addresses.
* **Regular Patching:** Keep all software and services running on open ports up to date with the latest security patches to fix known vulnerabilities.
* **Strong Authentication:** Implement strong, unique passwords, and consider two-factor authentication for any service that is exposed to the internet.

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

A firewall's primary role regarding ports is to act as a gatekeeper, controlling what traffic is allowed to enter and exit a network. It uses a set of predefined rules to:

* **Block Unwanted Traffic:** It can block all traffic to non-essential ports, making them invisible to external scanners.
* **Filter Traffic by Source:** It can be configured to only allow connections from specific IP addresses or networks, denying access to everyone else.

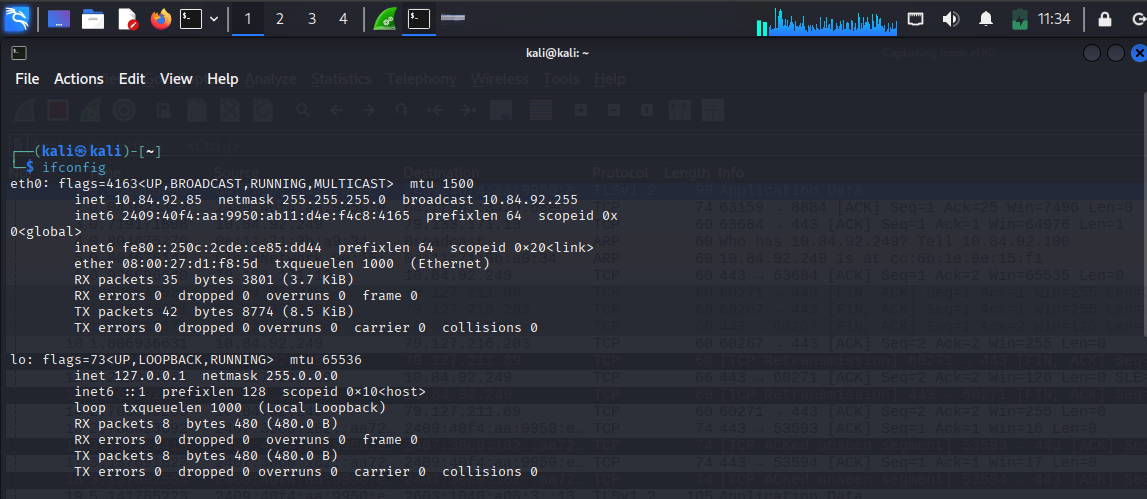
**7. What is a port scan and why do attackers perform it?**

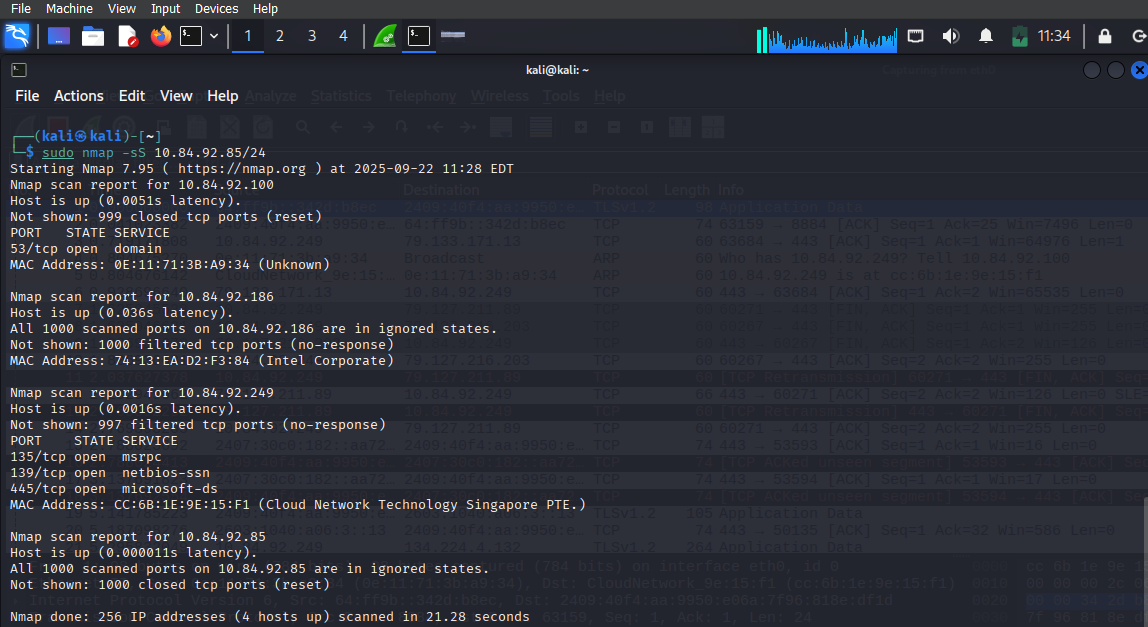
A **port scan** is an attack method used to identify active ports and services on a host. Attackers perform it for **network reconnaissance**. The goal is to gather information about a target's network to find potential entry points. By identifying open ports, attackers can determine what services are running and search for known vulnerabilities in those services.

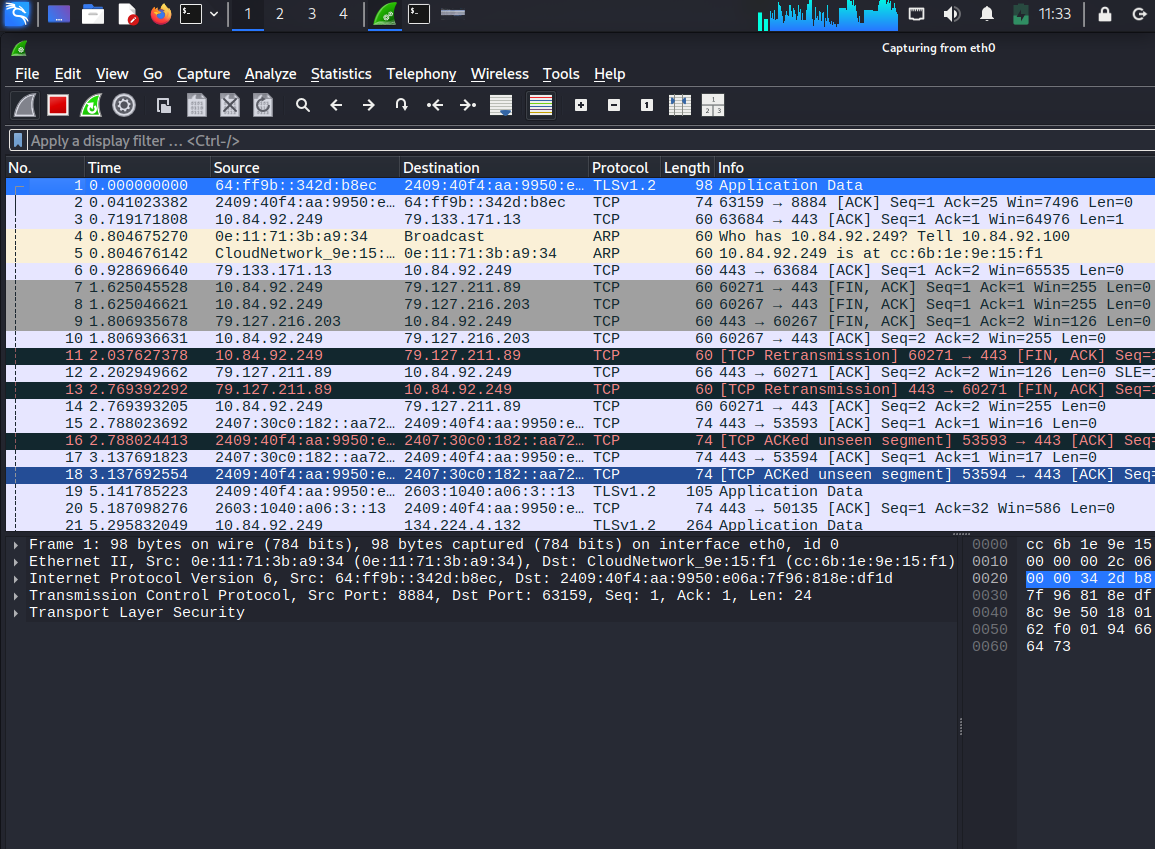
**8. How does Wireshark complement port scanning?**

Wireshark is a packet analyzer that complements port scanning by providing a detailed, low-level view of the network traffic. While Nmap actively scans and reports on open ports, Wireshark passively captures and visualizes the actual packets being sent and received. This allows a security professional to:

* **Verify Scan Results:** See the exact SYN, SYN-ACK, and RST packets Nmap sends, confirming how the scan works.
* **Troubleshoot and Debug:** Understand why a port is behaving a certain way (e.g., if a firewall is silently dropping packets).

**TASK-1 screenshots: **

****

****