🔍 Network Reconnaissance using Nmap | Cybersecurity Task

🧩 Step 1: Task Objective

Discover open ports and live devices on the local network using Nmap. Analyze security exposure and optional packet behavior with Wireshark.

🖥️ Step 2: Tools Used

Tool	Purpose
Nmap	**Port scanning**
Wireshark	**Packet capture and analysis (optional)**
GitHub	**Documentation and submission**
Terminal/CLI	**Command execution**

🌐 Step 3: Identify Local IP Range

Run the following command to find your local IP:

ipconfig # Windows
ifconfig # Linux/macOS

📍 **Example:**
IPv4 Address: 192.168.137.128

✳️ This means your **subnet** is:
192.168.137.0/24 (i.e., 192.168.137.1 to 192.168.137.254)

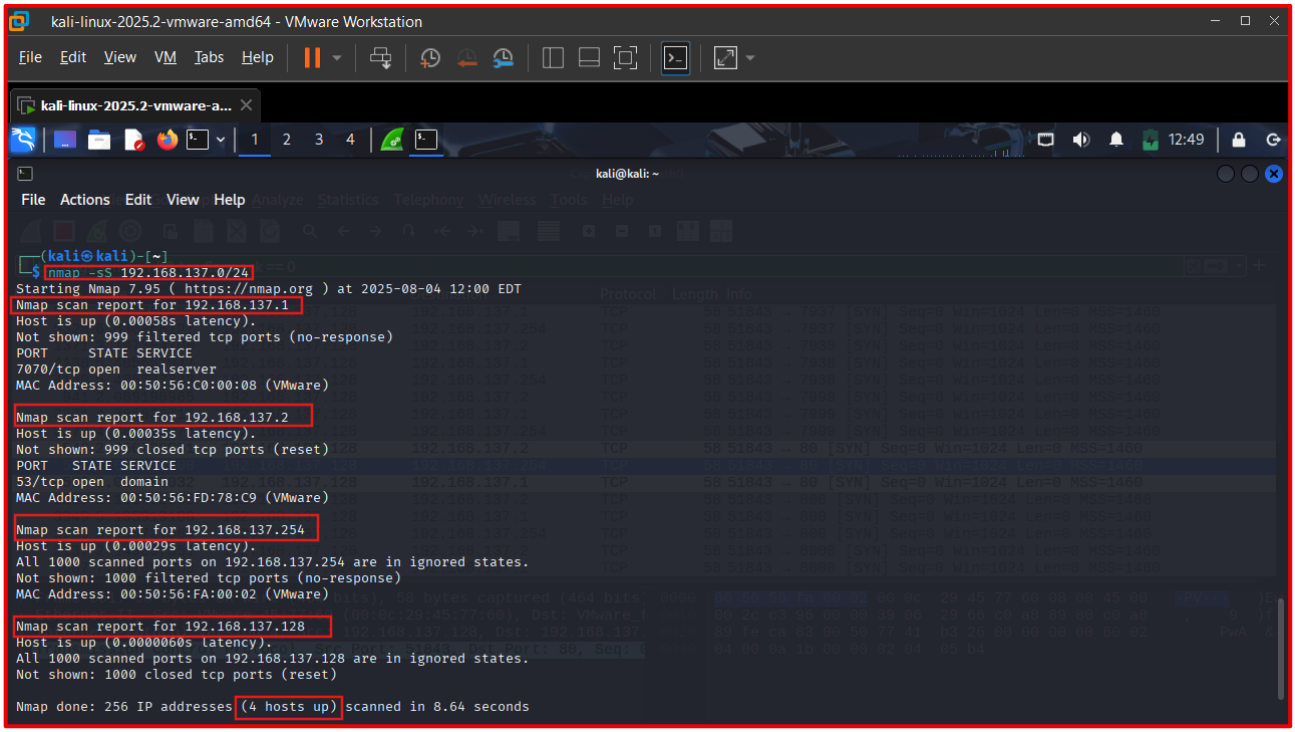
🔍 Step 4: Run TCP SYN Scan with Nmap

Use the following command:

nmap -sS 192.168.137.0/24

- **-sS: TCP SYN scan (stealth scan)**

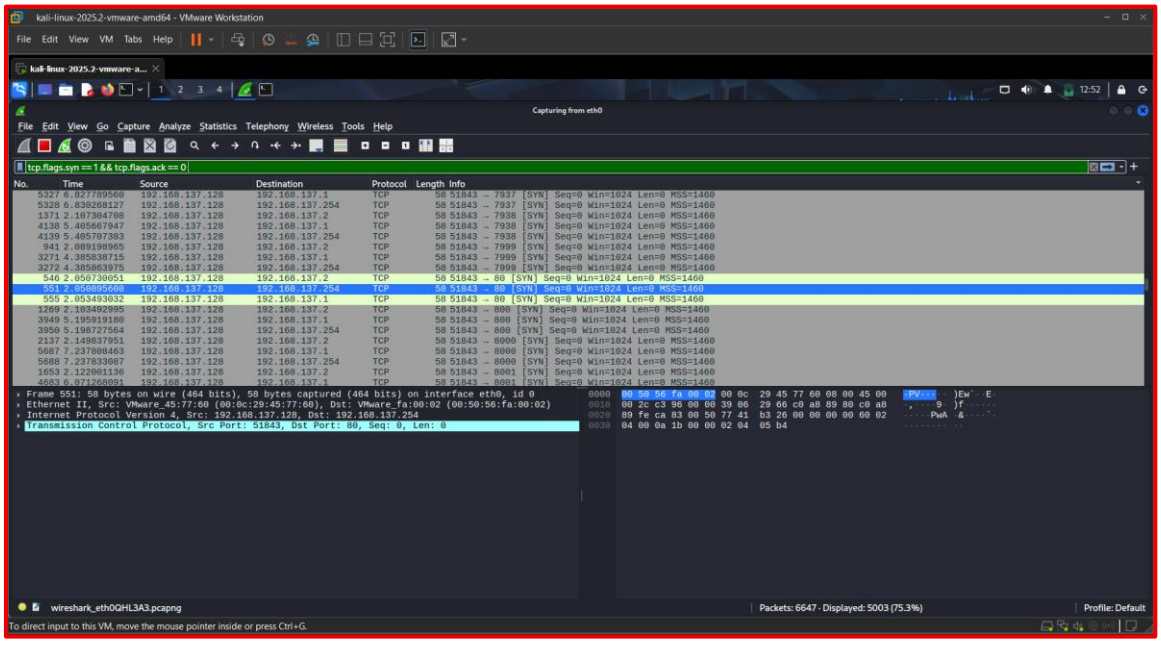
POC:



Step 5: (Optional) Capture Packets with Wireshark

1. Start Wireshark and choose your network adapter.
2. Begin capture.
3. While capturing, run the same Nmap command.
4. Apply filters to view Nmap activity: ***tcp.flags.syn == 1 && tcp.flags.ack == 0***

POC:



📊 Step 6: Analyze Results

Extracted from scan_results.txt:

IP Address	Open Ports	Service	Risk Level	Notes
192.168.137.1	7070	realserver	Medium	Streaming port; should be disabled if unused.
192.168.137.2	53	domain (DNS)	High	DNS service; vulnerable if exposed externally.
192.168.137.128	None	—	Low	All ports closed. Secure.
192.168.137.254	None	—	Unknown	All ports filtered. May be firewalled.

🔐 Step 7: Security Learnings

- Unused open ports should be closed.
- Essential ports (like DNS) should be protected with firewall rules.
- Port filtering is useful but may indicate hidden services.
- SYN scans are stealthy and widely used in real-world recon.

❓ Interview Questions & Answers

1. What is an open port?

An **open port** is a network port that is actively listening for incoming connections. It indicates that a service (like HTTP, SSH, or DNS) is running on that port and is accessible over the network. Open ports are essential for communication, but they can also pose security risks if left exposed unnecessarily.

---

2. How does Nmap perform a TCP SYN scan?

A **TCP SYN scan** (also known as a "stealth scan") works by sending a SYN (synchronize) packet to a target port.

- If the port is **open**, the system responds with a SYN-ACK.
- Nmap then immediately sends a RST (reset) packet to avoid completing the handshake — this helps avoid detection.
- If the port is **closed**, the system responds with a RST.
- If there's no response or it's filtered by a firewall, Nmap marks it as **filtered**.

This technique is fast, stealthy, and does not fully open a connection.

---

3. What risks are associated with open ports?

Open ports can be entry points for attackers if they expose:

- **Outdated or vulnerable services**
- **Unnecessary services** running by default
- **Unsecured protocols** like FTP or Telnet

If misconfigured, they can lead to:

- **Unauthorized access**
- **Data leakage**
- **Remote code execution**
- **Denial of Service (DoS)** attacks

That's why it's crucial to minimize the number of open ports and secure the ones that are needed.

---

4. Explain the difference between TCP and UDP scanning.

TCP Scanning	UDP Scanning
Connection-oriented	Connectionless
Easier to detect (logs, firewalls)	Harder to detect, but slower
More reliable results	Many ports may appear closed even if open (due to no response)
Used for services like HTTP, SSH	Used for services like DNS, SNMP

TCP scan completes or simulates a handshake to detect status, while **UDP scan** relies on lack of responses or ICMP errors, making it less accurate but still valuable for identifying services.

---

5. How can open ports be secured?

To secure open ports:

- **Close unused ports** using firewall or service configuration
- **Use firewalls** (host-based or network) to restrict access
- **Restrict access** using IP whitelisting or VPNs
- **Enable service authentication and encryption**
- **Regularly patch services** to fix vulnerabilities
- **Monitor logs** for suspicious access attempts

Security is not just about closing ports but managing them smartly.

---

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

A **firewall** acts as a filter between your network and outside traffic. It allows or blocks traffic based on predefined rules.

Regarding ports, a firewall:

- **Blocks unused or unauthorized ports**
- **Allows only necessary services** to communicate
- **Detects and logs unusual access patterns**
- **Protects against port scanning and brute-force attacks**

It’s a critical component in network security to control and monitor exposure.

---

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

A **port scan** is a method used to discover which ports are open on a target system and which services are running.

Attackers use port scanning to:

- Identify vulnerable services
- Map a network before launching an attack
- Find misconfigured or exposed systems

While port scanning is a legitimate tool for defenders (ethical hackers), it's often a **precursor to exploitation** when used by attackers.

---

8. How does Wireshark complement port scanning?

Wireshark helps you **see actual packet traffic** during a scan. It can:

- Confirm if SYN or ACK packets are sent and received
- Reveal hidden ports or traffic patterns
- Help detect **network filtering or firewall behavior**
- Provide evidence during forensic or security analysis

While Nmap gives **results**, Wireshark shows **how** those results happened at the packet level.