**Task 1: Scan Your Local Network for Open Ports**

**Objective**

**Learn to discover open ports on devices in your local network to understand network exposure.**

**Tools**

* **Nmap (free)**
* **Wireshark (optional, not used in this scan)**

**Steps Performed**

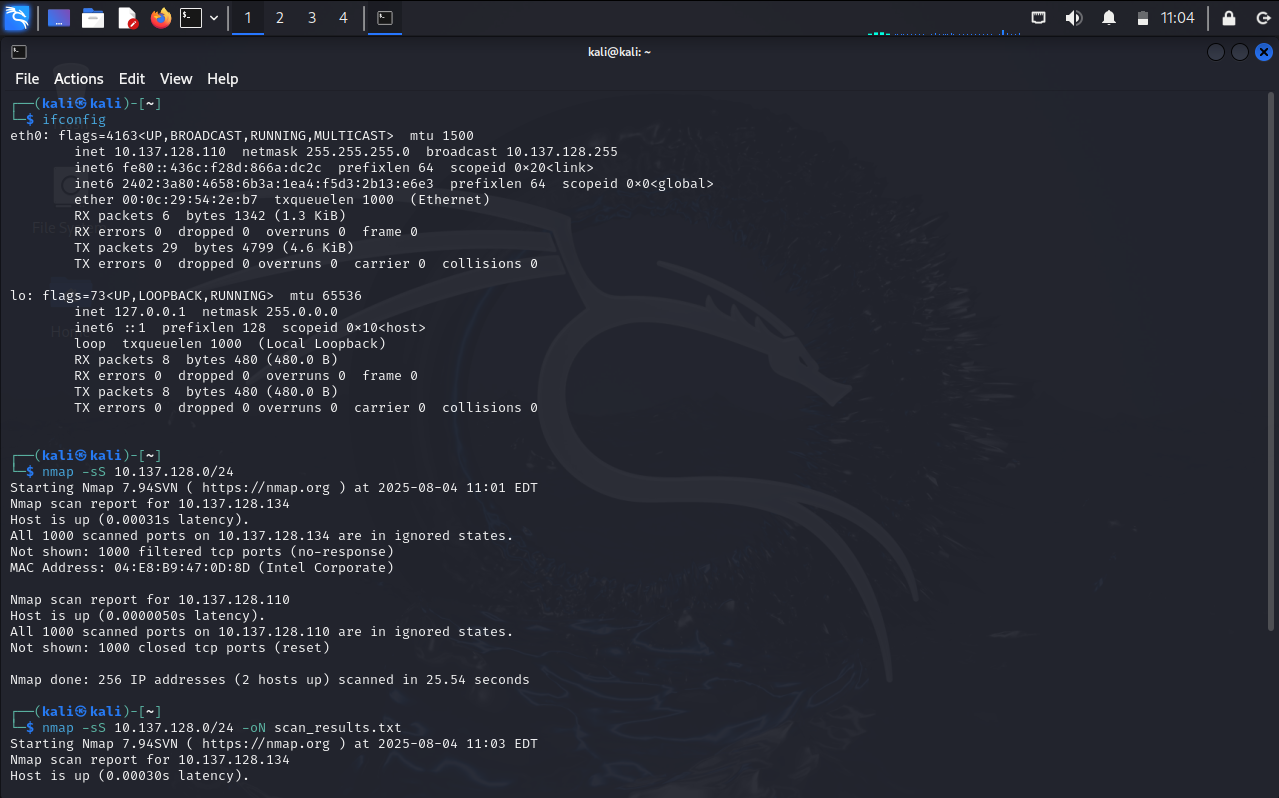
1. **Installed Nmap**
   * **Used the preinstalled Nmap on Kali Linux.**
2. **Found Local IP Range**
   * **Ran the following command to check my IP and subnet mask:**
   * **ifconfig**
   * **Result:**
     + **IP Address: 10.137.128.110**
     + **Netmask: 255.255.255.0**
     + **Network Range: 10.137.128.0/24**
3. **Performed TCP SYN Scan**
   * **Executed:**
   * **nmap -sS 10.137.128.0/24**
   * **The -sS option performs a stealth SYN scan, widely used for reconnaissance.**
4. **Noted IP Addresses and Open Ports**
   * **Discovered 2 active hosts in my local network.**
   * **Observed that:**
     + **All 1000 scanned ports were either closed or filtered.**
     + **No open ports were found, likely due to firewall filtering.**
5. **(Optional) Wireshark Analysis**
   * **Skipped since no open ports were detected.**
6. **Researched Common Services**
   * **Reviewed that normally open ports may include:**
     + **Port 80 (HTTP)**
     + **Port 443 (HTTPS)**
     + **Port 22 (SSH)**
7. **Identified Security Risks**
   * **Since no open ports were found, no immediate risk was detected.**
   * **Firewalls appear to be actively filtering inbound traffic.**
8. **Saved Results**
   * **Exported scan results to a text file for submission:**
   * **nmap -sS 10.137.128.0/24 -oN scan\_results.txt**

**Outcome**

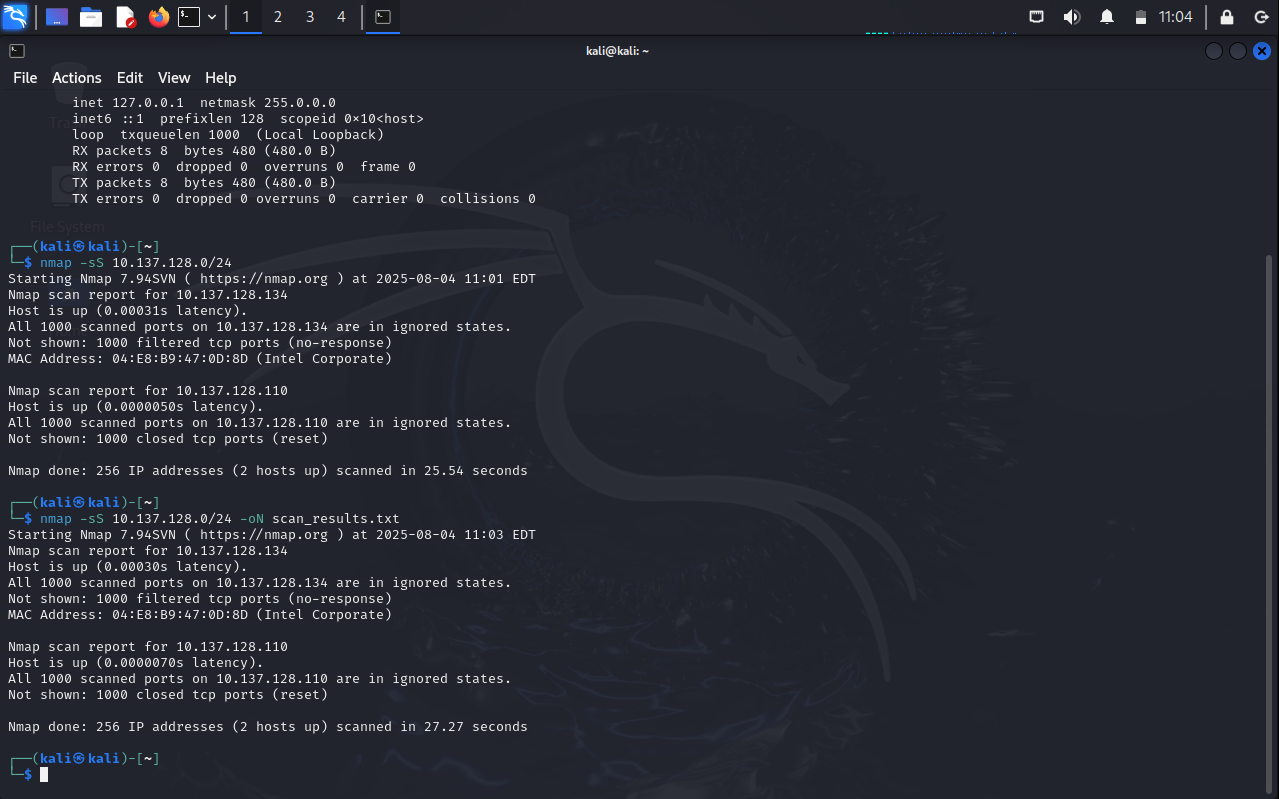
* **Successfully performed a TCP SYN port scan using Nmap.**
* **Detected 2 live hosts in the local network.**
* **No open ports were found — all were closed or filtered.**
* **Gained understanding of:**
  + **Port scanning techniques**
  + **How firewalls filter traffic**
  + **Basics of network reconnaissance and exposure**

**📌 Screenshots to Add**

* **Screenshot of ifconfig output (to show IP range)**

****

* **Screenshot of Nmap scan results**

****