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

**📌 Objective**

**The goal of this task is to perform a port scan on my local network to identify active hosts and detect open ports.**

**This helps understand how network reconnaissance works and why securing open ports is important in network security.**

**# 🛠 Tools Used**

**- \*Operating System: \* Kali Linux**

**- \*Port Scanning Tool: \* Nmap (7.94SVN)**

**- \*Packet Analyzer: \* Wireshark (optional, not used in this scan)**

**# 📝 Steps Performed**

**--------------------------------------------------------------------------------------------------------------------------------------**

**# 1. Identify Network Information**

**- Opened a terminal in Kali Linux.**

**- Ran the following command to check my IP address and subnet mask:**

**bash: - ifconfig**

**\* Results:**

**\* IP Address: `10.137.128.110`**

**\* Netmask: `255.255.255.0`**

**\* Network Range: `10.137.128.0/24`**

**--------------------------------------------------------------------------------------------------------------------------------------**

**# 2. Perform Nmap TCP SYN Scan**

**\* Executed the following command to perform a TCP SYN scan on my local network:**

**“bash”**

**nmap -sS 10.137.128.0/24**

**\* The `-sS` option performs a stealth SYN scan, which is widely used for reconnaissance.**

**--------------------------------------------------------------------------------------------------------------------------------------**

**# 3. Save Scan Results**

**\* Saved the scan results in a text file using:**

**“bash”**

**nmap -sS 10.137.128.0/24 -oN scan\_results.txt**

**\* This created a file named \*\*scan\\_results.txt\*\* for documentation.**

**--------------------------------------------------------------------------------------------------------------------------------------**

**# 4. Analyze Results**

**\* Found \*2 active hosts\* in my local network:**

**\* \*\*10.137.128.110\*\* → My Kali Linux machine**

**\* \*\*10.137.128.134\*\* → Another device (Intel Corporate MAC)**

**\* Observed that:**

**\* No top 1000 TCP ports were open.**

**\* All ports were either filtered or closed, indicating firewall protection.**

**--------------------------------------------------------------------------------------------------------------------------------------**

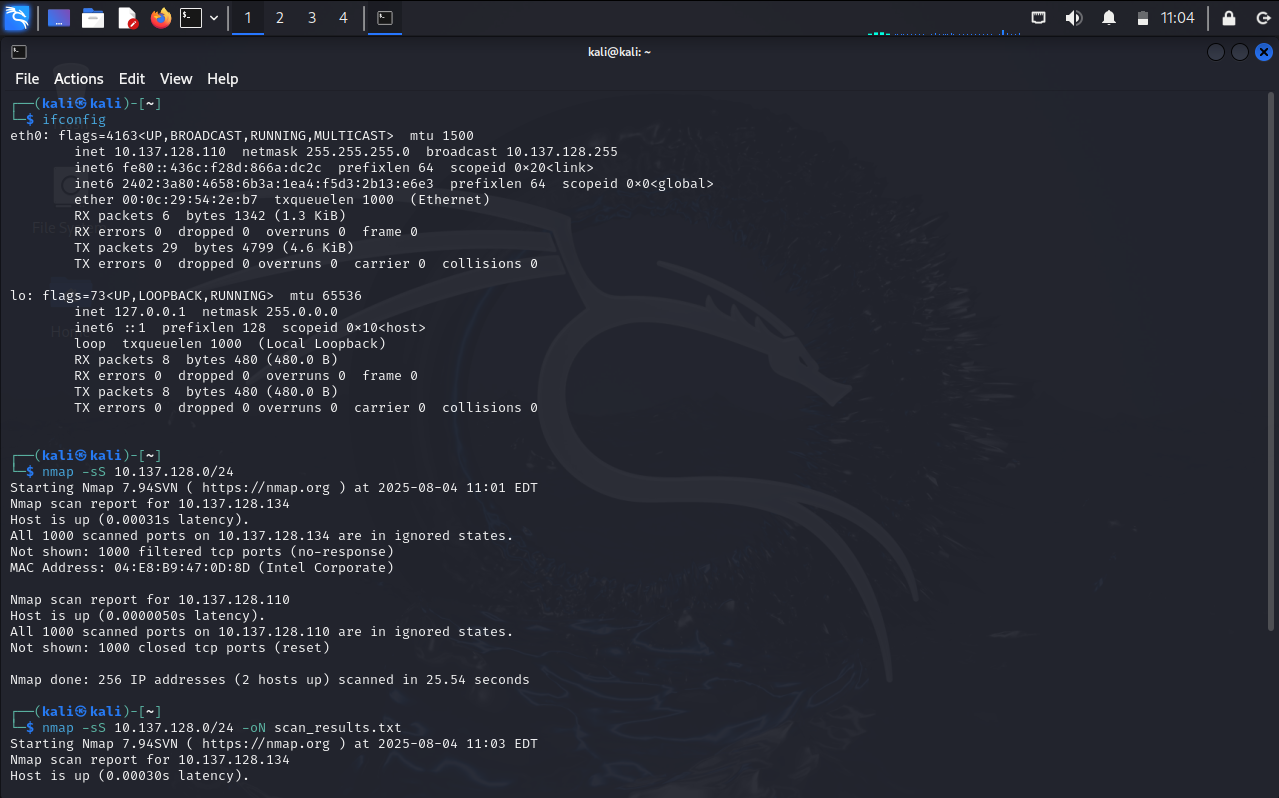
**## 📊 Results**

**# Screenshot of Nmap Scan**

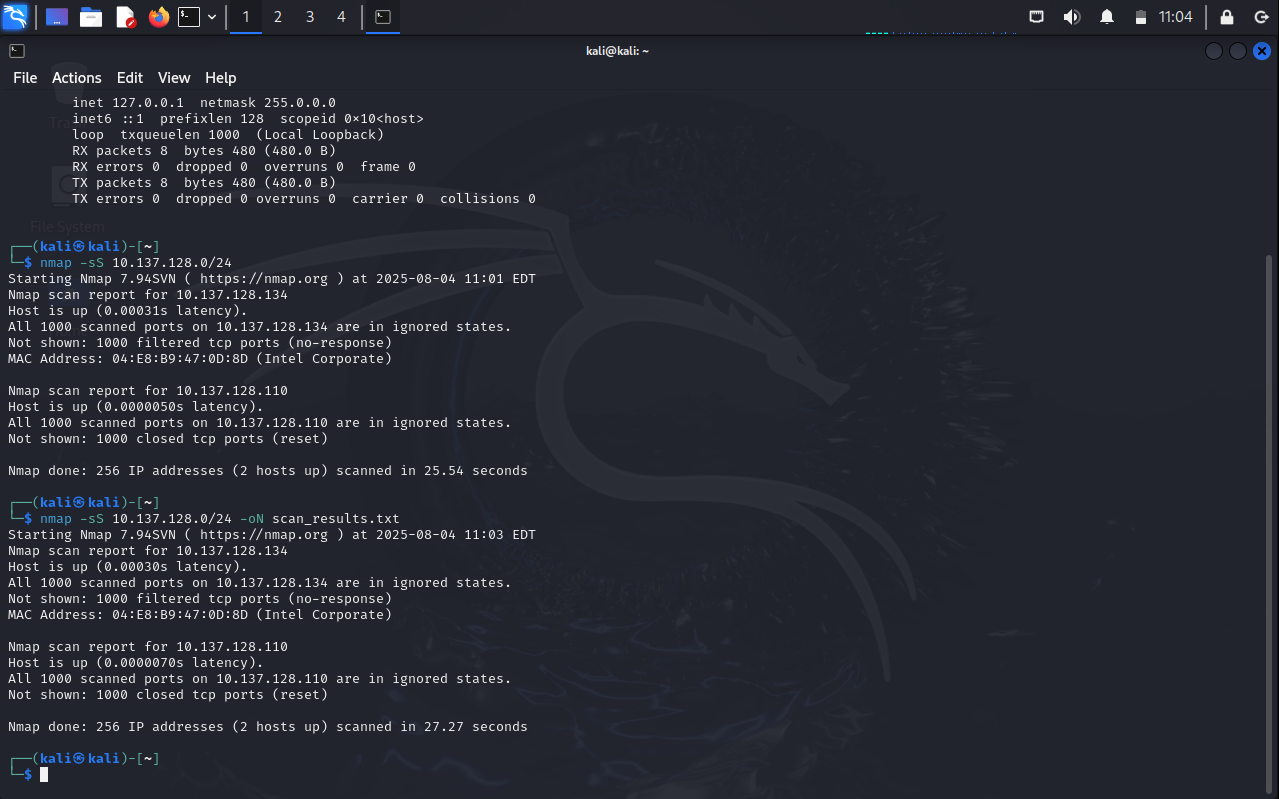
**Here is the screenshot of my Nmap scan results:**

**# 📸 Screenshots of Nmap Sca**

**# Screenshot 1: Finding Network Information**

****

**# Screenshot 2: TCP SYN Scan Results**

****

**# Scan Results File**

**\* Text file with detailed results: [scan\\_results.txt] (scan\_results.txt)**

**--------------------------------------------------------------------------------------------------------------------------------------S**

**# Outcome**

**\* Successfully performed a TCP SYN port scan using Nmap on Kali Linux.**

**\* Detected \*\*2 live hosts\*\* in my local network.**

**\* Observed that no common ports were open, likely due to firewall filtering.**

**\* Gained practical understanding of:**

**\* Port scanning**

**\* Network reconnaissance**

**\* How firewalls protect open ports**

**\* Why monitoring with tools like Wireshark is valuable**

**\*\*Note: \*\* Wireshark analysis was not performed because the task marked it as optional.**

**Since no open ports were detected in the Nmap scan, additional packet analysis with Wireshark**

**was not necessary in this case.**