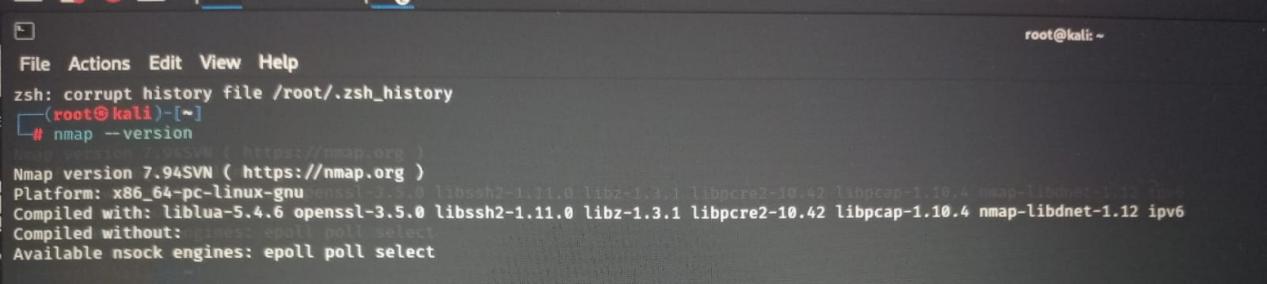
**Network Reconnaissance using Nmap (Task 1 Report)**

**Objective**The goal of this task is to **scan the local network for open ports** to understand network exposure and possible security risks. This demonstrates the use of **Nmap** for basic network reconnaissance.

**Step 1: Verify Nmap Installation**

Since Kali Linux usually comes with Nmap pre‑installed, I checked the version:

nmap --version



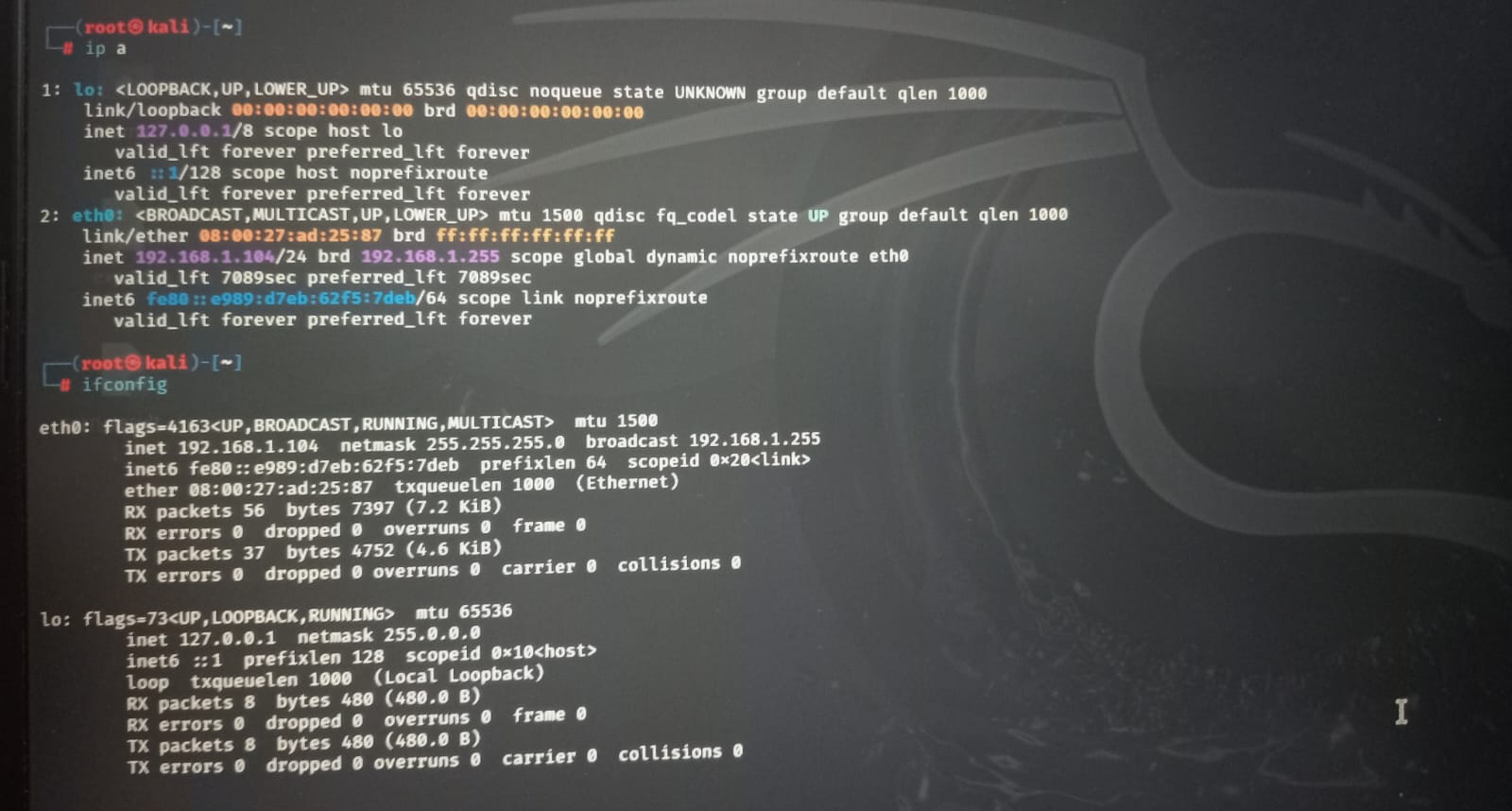
Nmap is installed and ready to use.

**Step 2: Identify Local IP and Network Range**

To find my IP address and subnet, I used the following commands:

ip a  
or

ifconfig

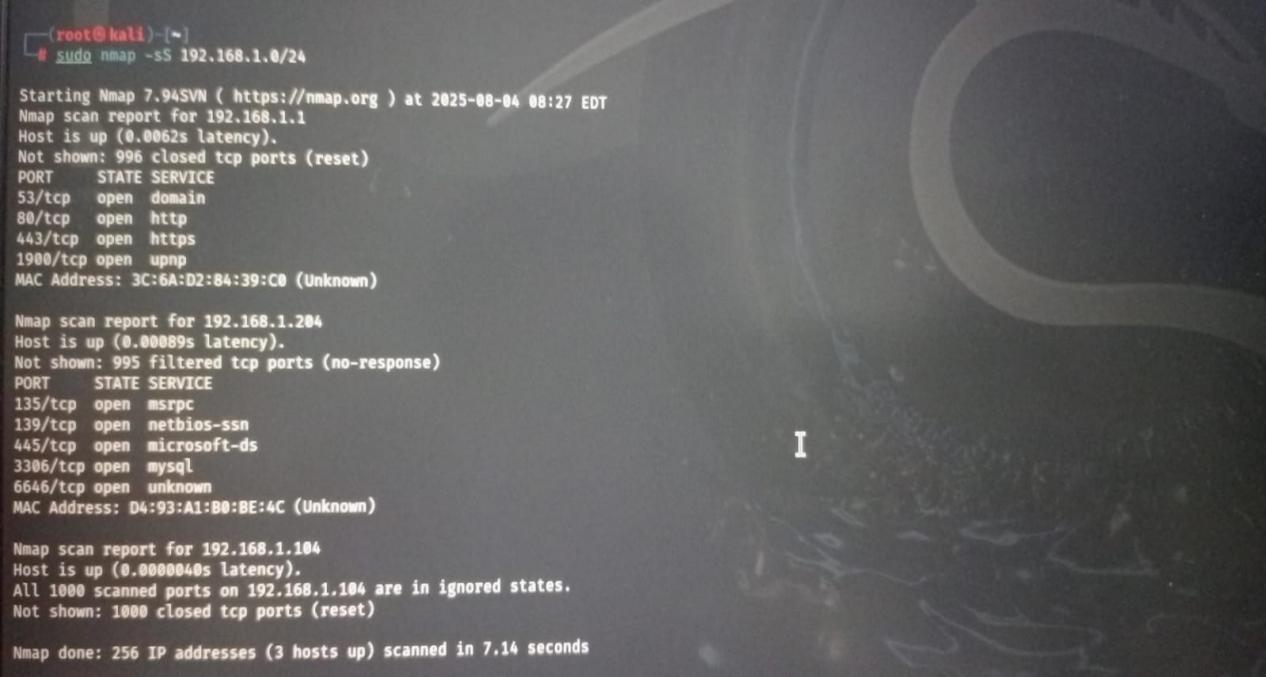


My system IP = **192.168.1.104**  
 Subnet mask = **/24**  
 Therefore, the network range = **192.168.1.0/24**

**Step 3: Perform TCP SYN Scan**

Now I scanned the entire local subnet to discover devices and open ports:

sudo nmap -sS 192.168.1.0/24



sudo → required for privileged SYN scans

-sS → TCP SYN scan (also called half‑open or stealth scan)

192.168.1.0/24 → scans all devices from 192.168.1.1 to 192.168.1.254

**Step 4: Scan Results**

The scan discovered **3 active hosts**

1.Host: **192.168.1.1** (Router)

**53/tcp open domain**

**80/tcp open http**

**443/tcp open https**

**1900/tcp open upnp**

This is likely the network router. It has web services (HTTP, HTTPS), DNS, and UPnP enabled.

**2.**Host: **192.168.1.204** (Windows/Database Server)

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**3306/tcp open mysql**

**6646/tcp open unknown**

This system is exposing multiple ports: SMB (NetBIOS, Microsoft‑DS), MySQL database, and one unknown service on port 6646.

These can be potential security risks if not properly secured.

1. Host: **192.168.1.104** (My Kali Machine)

All 1000 scanned ports on 192.168.1.104 are closed

No open ports found → This machine is secure.

## Security Analysis

**Router (192.168.1.1)** → Normal open services, but UPnP may be risky if exposed externally.

**Windows/DB Host (192.168.1.204)** → SMB ports (445, 139) are commonly exploited in ransomware attacks. MySQL (3306) should not be exposed without strong authentication.

**My Kali Machine (192.168.1.104)** → Safe, no open ports detected.

## Outcome

Learned to identify IP range in local network.

Performed **TCP SYN scan** using Nmap.

Discovered 3 devices and analyzed their open ports.

Gained awareness about potential security issues related to open ports.