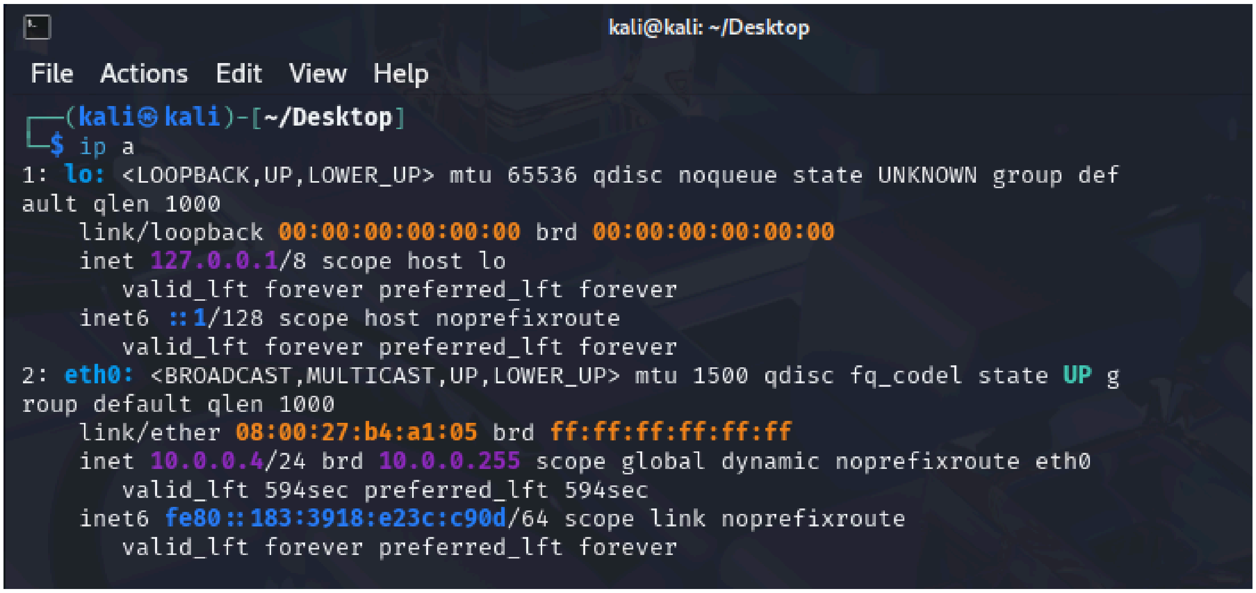
Task 1: Scan Your Local Network for Open Ports

1.Install Nmap from the official website.

- Already comes installed in kali linux.

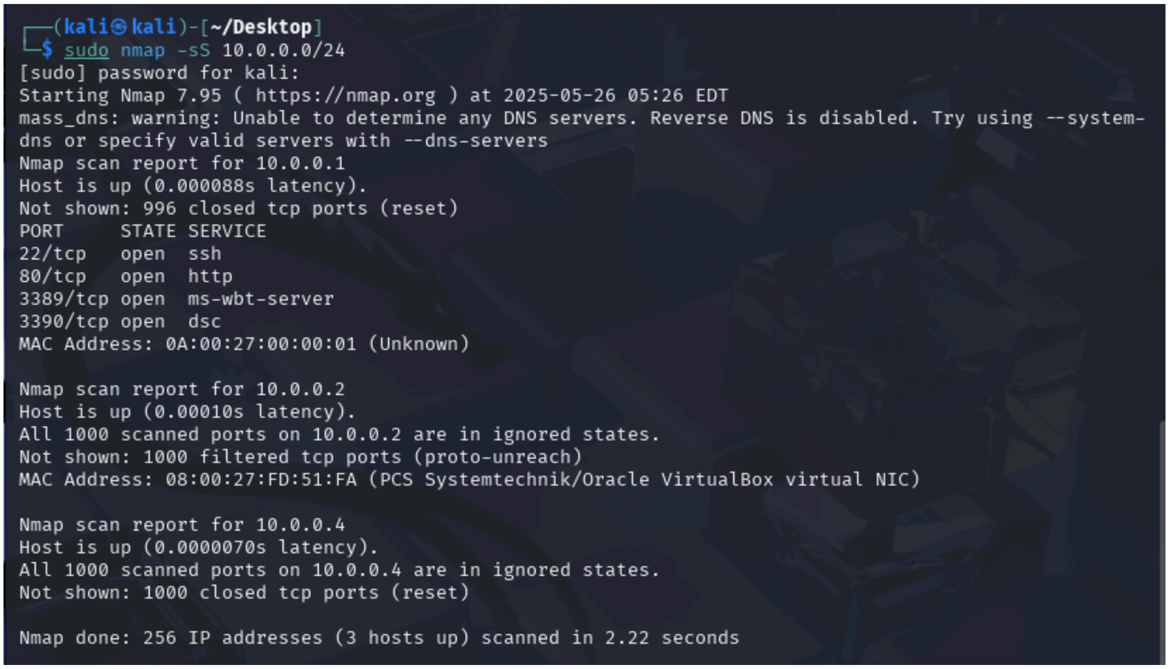
2.Find your local IP range (e.g., 192.168.1.0/24).



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.4/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 594sec preferred_lft 594sec
    inet6 fe80::183:3918:e23c:c90d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- Device IP is 10.0.0.4/24, so local IP range is 10.0.0.0/24

3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS 10.0.0.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 05:26 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.1
Host is up (0.000088s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3389/tcp open  ms-wbt-server
3390/tcp open  dsc
MAC Address: 0A:00:27:00:00:01 (Unknown)

Nmap scan report for 10.0.0.2
Host is up (0.00010s latency).
All 1000 scanned ports on 10.0.0.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:FD:51:FA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.0.4
Host is up (0.0000070s latency).
All 1000 scanned ports on 10.0.0.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.22 seconds
```

4.Note down IP addresses and open ports found.

- IP 10.0.0.1 is found with ssh(22), http(80), ms-wbt-server(3389), and dsc(3390) open. IP 10.0.0.2 and 10.0.0.4 is found with no ports open.

6.Research common services running on those ports.
The Nmap scan revealed the following open ports and services on IP `10.0.0.1`:

- **Port 22 (SSH)**:
  SSH (Secure Shell) is commonly used for remote login and command execution. It encrypts traffic and is widely used for secure administration of servers and network devices.

- **Port 80 (HTTP)**:
  HTTP is used to serve web pages and is the foundation of communication on the World Wide Web. Traffic on this port is **unencrypted**, making it susceptible to eavesdropping.

- **Port 3389 (ms-wbt-server / RDP)**:
  Microsoft Remote Desktop Protocol allows users to connect to a Windows machine remotely. It is commonly used for remote administration and virtual desktops.

- **Port 3390 (DSC or Alternate RDP)**:
  Often used for alternate Remote Desktop configurations or Windows Remote Management (e.g., Desired State Configuration). It may be manually configured or used by other management tools.

7.Identify potential security risks from open ports.
Each open port represents a **possible entry point** for attackers. The risks include:

- **SSH (22)**:

    - **Brute-force login attempts** using default or weak credentials.

    - If root login or password-based auth is enabled, the system is more vulnerable.

    - **Mitigation**: Use key-based authentication, disable root login, enable fail2ban.

- **HTTP (80)**:

    - **Sensitive data can be exposed** due to unencrypted communication.

    - Vulnerable or outdated web applications on this port can be exploited.

    - **Mitigation**: Use HTTPS (TLS), patch web server/CMS regularly.

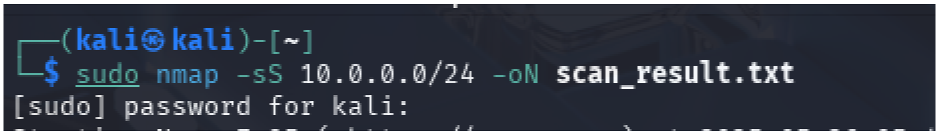
- **RDP (3389) and 3390**:

    - **Highly targeted by attackers** (e.g., brute-force, ransomware attacks).

    - Vulnerabilities in RDP can allow remote code execution.

    - **Mitigation**: Restrict access (via firewall or VPN), use strong passwords and 2FA, keep system updated.

8.Save scan results as a text or HTML file.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.0.0.0/24 -oN scan_result.txt
[sudo] password for kali:
```