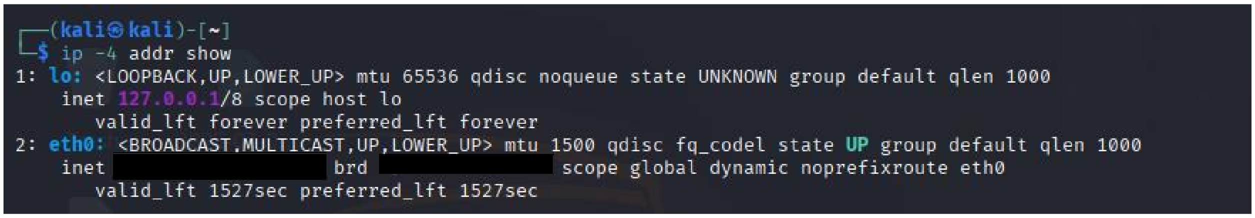
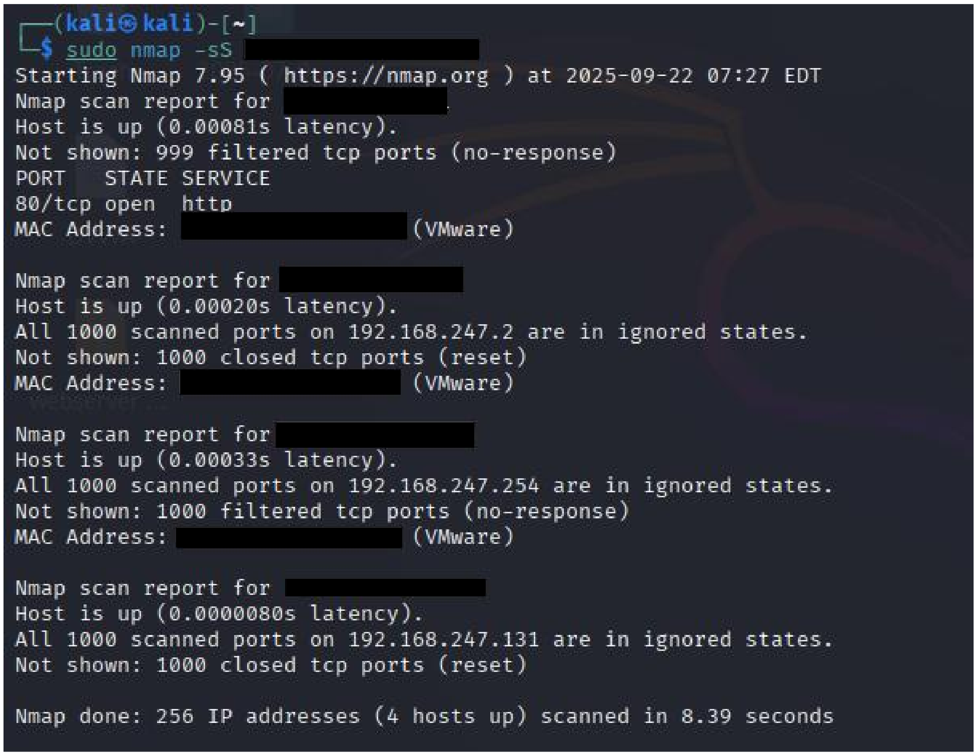
Task 1: Scan Your Local Network for Open Ports

2.



```
┌──(kali㉿kali)-[~]
└─$ ip -4 addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet [redacted] brd [redacted] scope global dynamic noprefixroute eth0
       valid_lft 1527sec preferred_lft 1527sec
```

3.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 07:27 EDT
Nmap scan report for [redacted]
Host is up (0.00081s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: [redacted] (VMware)

Nmap scan report for [redacted]
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.247.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: [redacted] (VMware)

Nmap scan report for [redacted]
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.247.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: [redacted] (VMware)

Nmap scan report for [redacted]
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.247.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.39 seconds
```

6. Common ports & typical services:

- 22 — SSH (remote shell)
- 21 — FTP
- 23 — Telnet (insecure)
- 25 — SMTP
- 53 — DNS
- 80 — HTTP
- 443 — HTTPS
- 139/445 — SMB/CIFS (Windows file sharing)
- 3306 — MySQL
- 3389 — RDP (Windows Remote Desktop)
- 5900 — VNC

7. Identify potential security risks & what they mean

Examples of typical findings and risk levels:

- Open SSH (22): Low-to-medium risk if patched + strong auth. Risk increases if password auth or weak keys are allowed.
  Fix: enforce key-based auth, disable password login, use fail2ban, change default port only as noise reduction.
- Open HTTP (80) / outdated web server: Medium risk — may expose web apps with vulnerabilities (XSS, SQLi, remote code exec).
  Fix: patch server/app, run web app scans (Burp/ZAP), use WAF.
- SMB (139/445): High risk on unpatched Windows (e.g., wormable exploits).
  Fix: disable if not needed, patch, restrict via firewall, require SMB signing.
- Open RDP (3389): High risk — brute force, exposed RDP vulnerabilities.
  Fix: put behind VPN, use NLA, enforce MFA, limit source IPs.
- Telnet / FTP (21/23): High risk — cleartext credentials.
  Fix: replace with SSH/SFTP, disable services.
- Database ports (3306 etc.) exposed: High risk — data exfiltration.
  Fix: bind DB to localhost or private network, firewall rules, authentication, TLS.

8. # Nmap 7.95 scan initiated Mon Sep 22 07:31:35 2025 as: /usr/lib/nmap/nmap -sS -sV -oN scan_results.txt [redacted]

```
Nmap scan report for 192.168.247.1
Host is up (0.0013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd [redacted]
MAC Address: [redacted] (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for [redacted]
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.247.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: [redacted] (VMware)

Nmap scan report for [redacted]
Host is up (0.00033s latency).
All 1000 scanned ports on [redacted] are in ignored states.
```

```
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: [redacted] (VMware)

Nmap scan report for [redacted]
Host is up (0.0000080s latency).
All 1000 scanned ports on [redacted] are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Sep 22 07:31:50 2025 -- 256 IP addresses (4 hosts up) scanned in
15.09 seconds
```