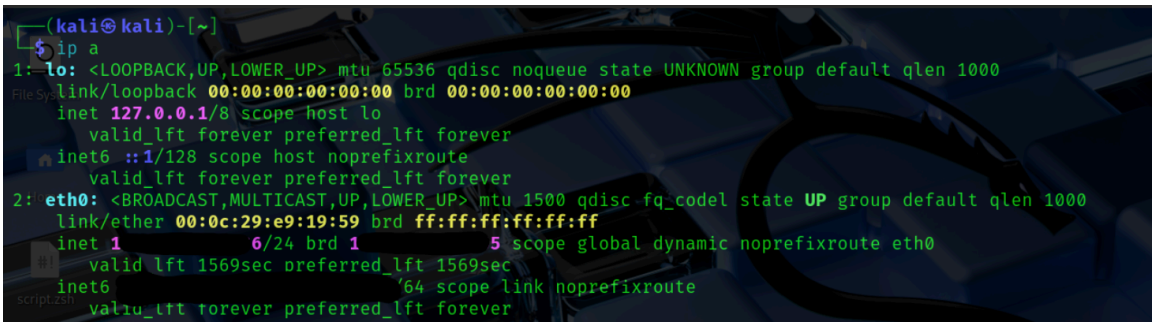
Task-1

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

▼ Define the Scope

To begin with, I started by identifying the IP range of my local network. My network runs on the “ 1##.###.##.##6/24 subnet.



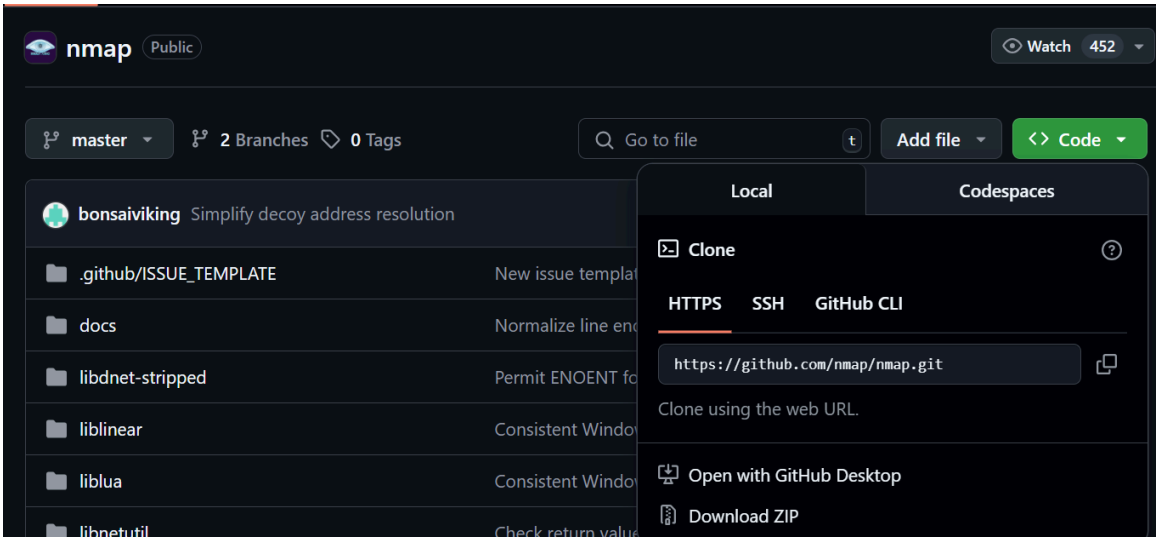
▼ Setting up Tools

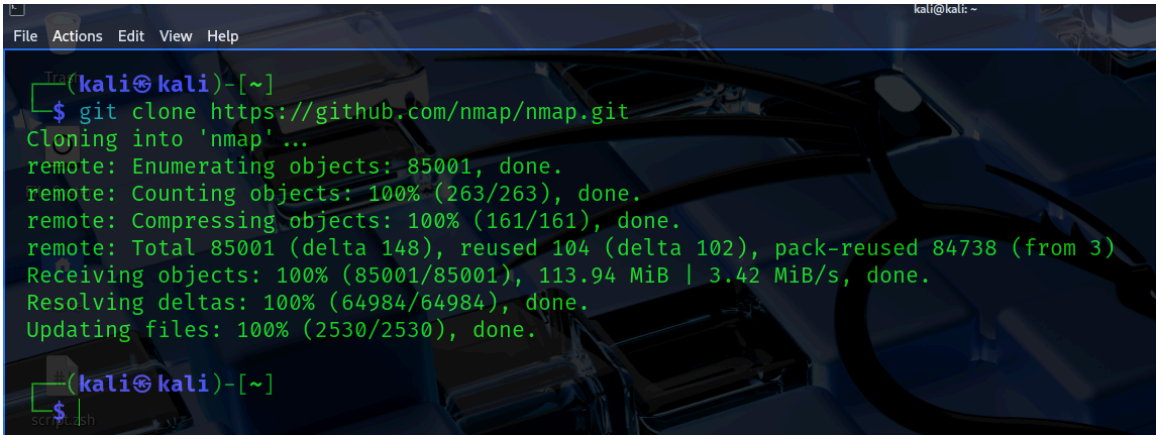
There are wide variety of tools used for network exposure like :-

1. Nmap
2. wireshark
3. Zen map
4. Angry Ip scanner, etc.

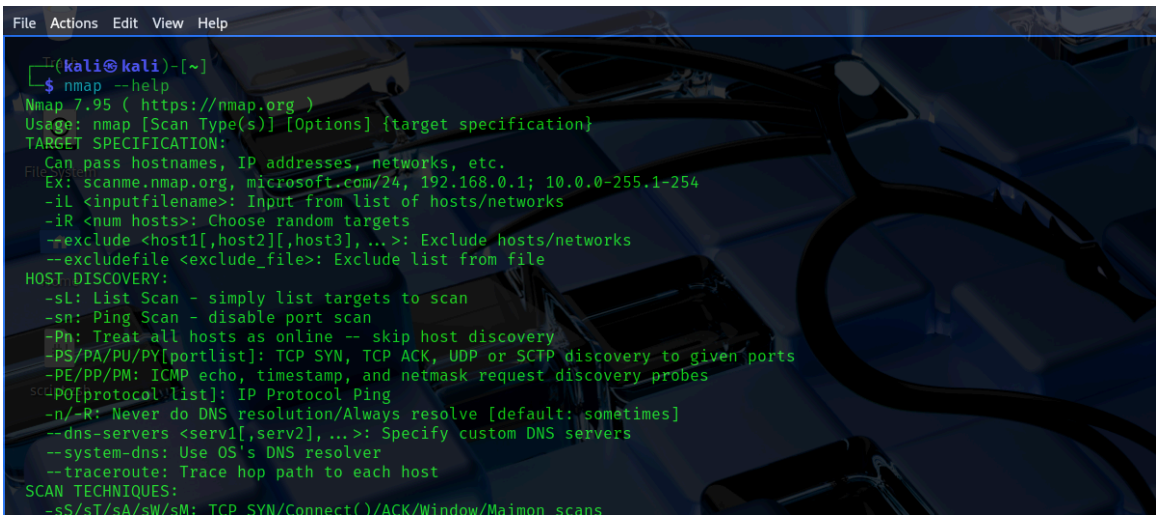
As of today, I am using one of the most recommended tools:
Nmap.

To install Nmap, it can be downloaded using the Git command in the terminal by cloning its official Git repository, which is publicly accessible from various sources or we can run the command “sudo apt-get install nmap” to install it directly.





To explore the available functionalities of Nmap, we can run the command “Nmap - -help”. This will display a list of supported options and provide guidance on how to proceed with using the tool effectively.



▼ Discover Active Devices (Ping Sweep)

To find out which devices are currently active on a network, we can use a technique called a ping sweep. A **ping sweep** helps find active devices on a network by sending ping requests to a range of IPs and checking which ones reply.

Using Nmap with the “-sn” option lets us do this quickly by skipping port scans and only checking which hosts are online. Some devices may not reply if ping is blocked by a firewall.

The result shows the “4 Hosts up” and responsive, so we can proceed with a port scan. There is no need to continue scanning if the host is down, as it will

not respond to any requests.

▼ Scan for Open Ports

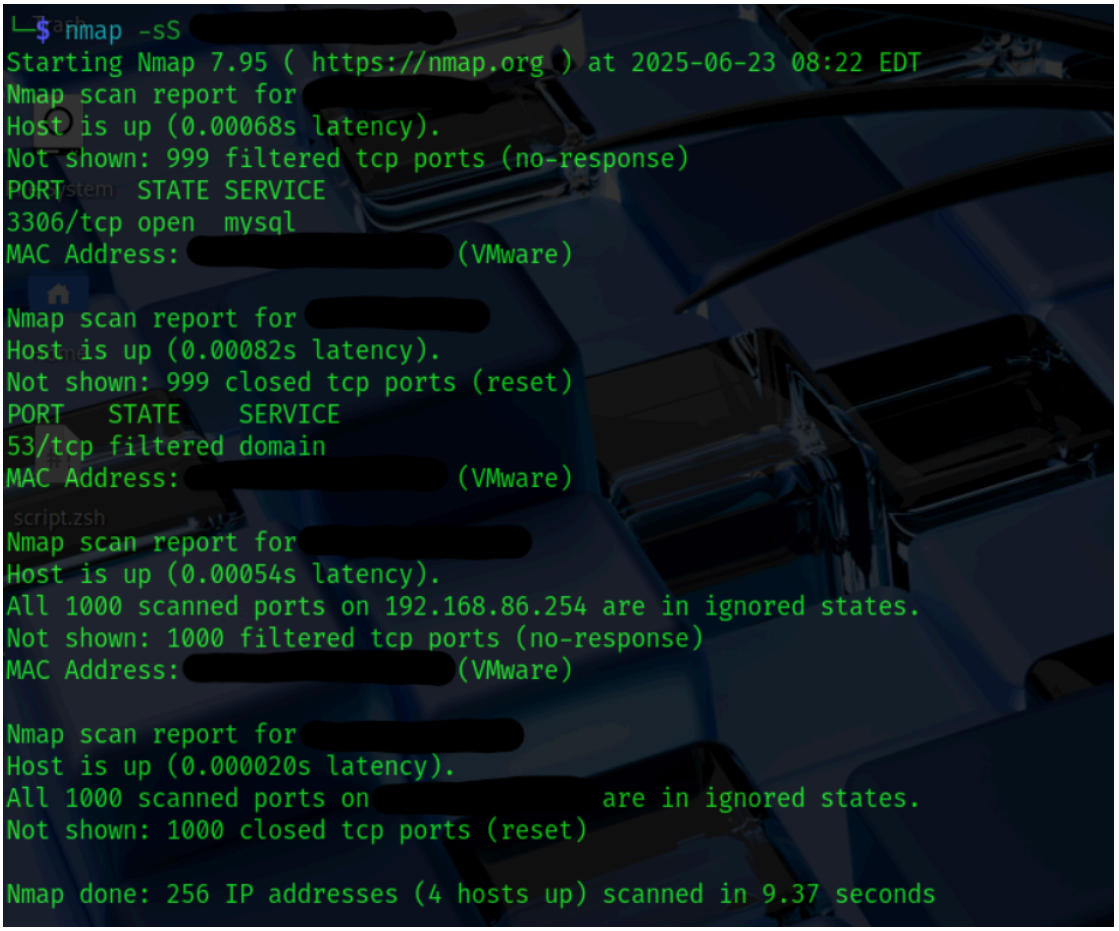
To perform a port scan, Nmap offers several types of scans, each activated by specific command-line flags.

The “-sV” flag tells Nmap to check what services are running on open ports and find their versions. This helps us know what software is there and if there might be security risks.

As we can see, out of 4 hosts we got 2 hosts, where we can see open ports of TCP(Transmission control protocol) with services running on them :-

- The result "3306/tcp open mysql" means port 3306 is open and running a MySQL database. "MySQL (unauthorized)" means the service responded, but we don’t have permission to access it.
- "6646/tcp open tcpwrapped" means port 6646 is open, but the service quickly closed the connection, so Nmap couldn’t identify it. This usually means a firewall or security tool is blocking access.

- "53/tcp filtered domain" means port 53, used for DNS, is blocked or hidden. Nmap didn’t get any response because a firewall or security device is stopping the scan, so it can’t tell if the port is open or closed.



The “-sS” scan sends a quick “hello” to a port without fully connecting. If the port responds, it’s open. This way, the scan is faster and less likely to be noticed.

- When we run the stealth SYN scan “-s”, port 3306 still shows as open running MySQL, with unauthorized access.
- However, port 6646 no longer appears in the results. This likely means that the stealth scan didn’t detect it because the service or firewall is blocking or ignoring SYN probes on that port.
- Port 53 remains filtered, indicating a firewall or security device is blocking responses on the DNS port, so we can’t determine if it’s

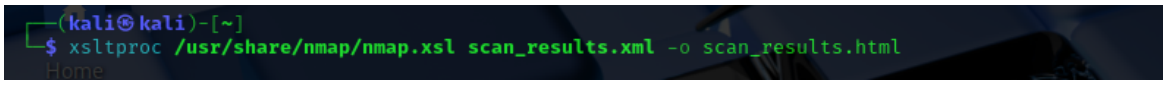
open or closed.

The "-A" option tells Nmap to run an aggressive scan. It does multiple things at once like checking open ports, service versions, operating system info, and running scripts. It gives a lot of detail but can be noisy and easily detected by firewalls or security tools.

- The aggressive scan shows port 3306 is open and running MySQL, but we don’t have permission to access it.
- Port 53 is blocked by a firewall, so the scan can’t tell if it’s open or closed.
- Port 6646 didn’t appear, probably because the service or firewall is hiding it.
- The scan also tried to guess the device type and operating system, like Windows 10 or a VMware virtual machine.

The command "nmap -sS -sV 192.168.86.136/24 -oX scan_results.xml" does the following:

- "sS" tells Nmap to perform a stealth (SYN) scan to check which ports are open without making full connections.
- "sV" tells it to identify what services are running on the open ports and try to find their versions.
- "192.168.86.136/24" means it will scan the local network range, from 192.168.86.1 to 192.168.86.254.
- "oX scan_results.xml" saves the scan results in XML format into a file named scan_results.xml, which can be used in tools or scripts.



This script will helps in converting our xml file in filtered html report.

▼ Potential Security Risks associated with open Ports

1. Port 3306 (MySQL)

- **Service:** MySQL Database
- **Risks:**
  - Exposed databases are frequent targets

- Risk of data theft, injection, or remote code execution
- Can be brute-forced if not protected

2. Port 22 (SSH)

- **Service:** Secure Shell (SSH)
- **Risks:**
  - Brute-force login attacks (especially if using weak passwords)
  - Exploitable SSH vulnerabilities if not updated
  - Misconfigured SSH (e.g., root login enabled, outdated cipher suites)

3. Port 80 (HTTP)

- **Service:** Web server (e.g., Apache, Nginx)
- **Risks:**
  - Exposed to web-based attacks: XSS, SQL injection, directory traversal
  - Leaks sensitive server data through headers
  - Unencrypted (data sent in clear text)