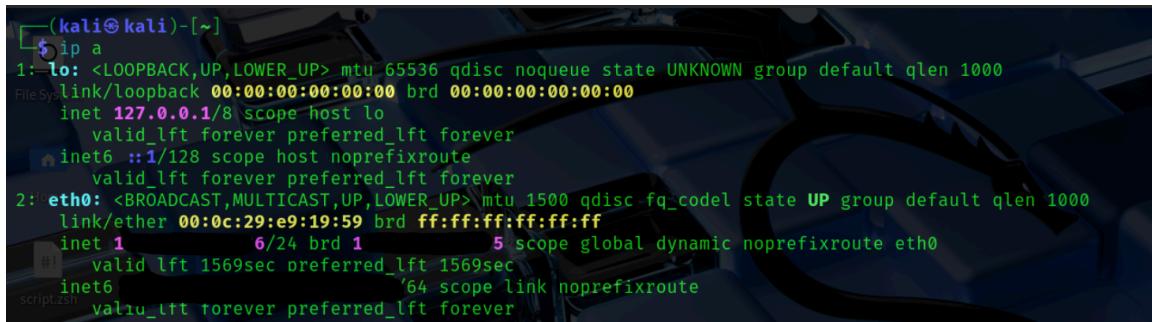


Task-1

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.

A terminal window titled '(kali㉿kali)-[~]' showing the output of the 'ip a' command. The output lists two interfaces: 'lo' (loopback) and 'eth0' (ethernet). The 'lo' interface has an IPv4 address of 127.0.0.1/8. The 'eth0' interface has an IPv4 address of 192.168.1.6/24 and an IPv6 address of fe80::c29:e9ff:fe19:59/64. Both interfaces have a MTU of 1500 and 1569sec valid_lft and preferred_lft values.

▼ Setting up Tools

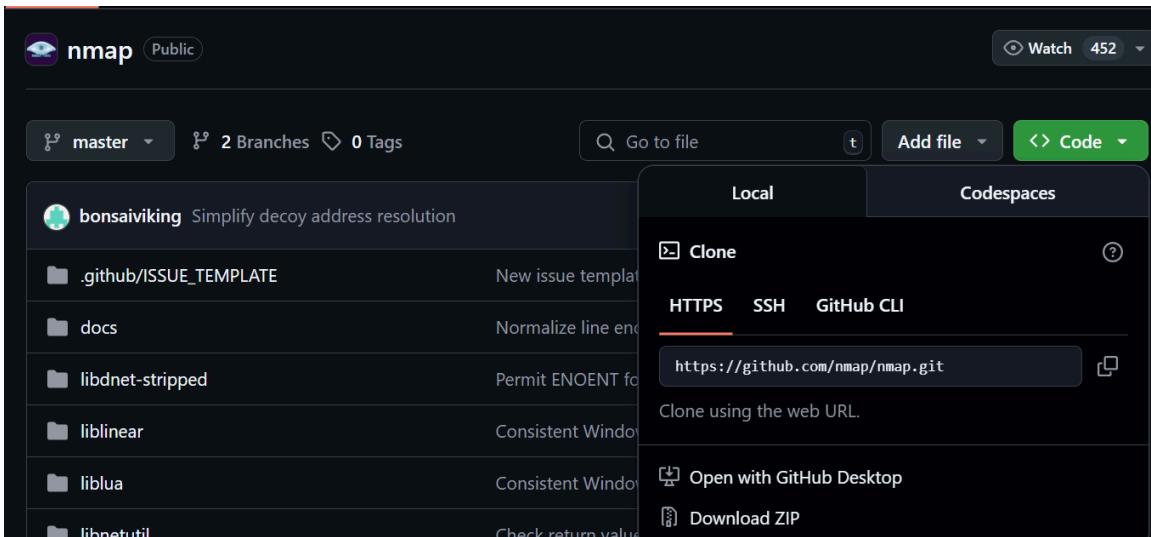
There are wide variety of tools used for network exposure like :-

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.



```
$ git clone https://github.com/nmap/nmap.git
Cloning into 'nmap'...
remote: Enumerating objects: 85001, done.
remote: Counting objects: 100% (263/263), done.
remote: Compressing objects: 100% (161/161), done.
remote: Total 85001 (delta 148), reused 104 (delta 102), pack-reused 84738 (from 3)
Receiving objects: 100% (85001/85001), 113.94 MiB | 3.42 MiB/s, done.
Resolving deltas: 100% (64984/64984), done.
Updating files: 100% (2530/2530), done.
```

```
$ sudo apt-get install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.95+dfsg-3kali1).
nmap set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 85 not upgraded.
```

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.

```
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ nmap --help
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -S<PO[protocol\list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/-sT/-sA/-sW/-sM: TCP SYN/Connect() /ACK/Window/Maimon scans
```

▼ 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.

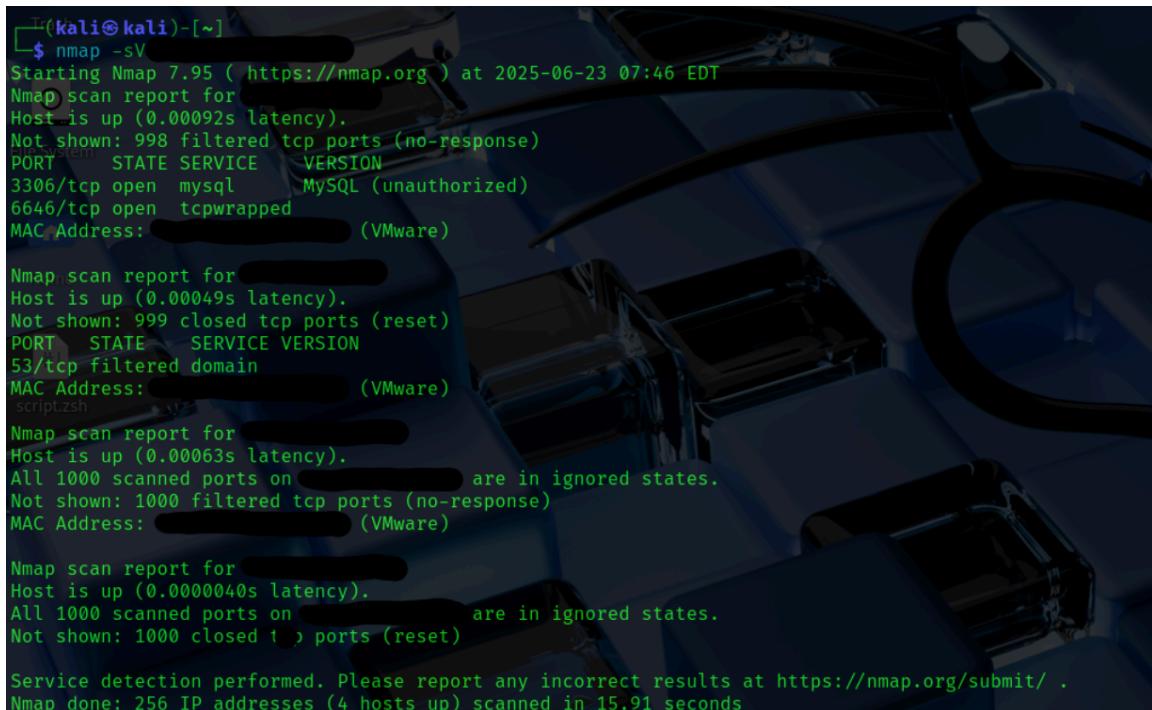
```
└──(kali㉿kali)-[~]
$ nmap -sn [REDACTED]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 07:53 EDT
Nmap scan report for [REDACTED]
Host is up (0.00054s latency).
MAC Address: [REDACTED] (VMware)
Nmap scan report for [REDACTED]
Host is up (0.00078s latency).
MAC Address: [REDACTED] (VMware)
Nmap scan report for [REDACTED]
Host is up (0.00072s latency).
MAC Address: [REDACTED] (VMware)
Nmap scan report for [REDACTED]
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.32 seconds
```

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.



```
[root@kali kali]-[~]
└─$ nmap -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 07:46 EDT
Nmap scan report for [REDACTED]
Host is up (0.00092s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql    MySQL (unauthorized)
6646/tcp  open  tcpwrapped
MAC Address: [REDACTED] (VMware)

Nmap scan report for [REDACTED]
Host is up (0.00049s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    filtered domain
MAC Address: [REDACTED] (VMware)
script[zsh]

Nmap scan report for [REDACTED]
Host is up (0.00063s 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 (0.0000040s 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: 256 IP addresses (4 hosts up) scanned in 15.91 seconds
```

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.

```

└─$ nmap -sS
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 08:22 EDT
Nmap scan report for [REDACTED]
Host is up (0.00068s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3306/tcp  open  mysql
MAC Address: [REDACTED] (VMware)

Nmap scan report for [REDACTED]
Host is up (0.00082s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: [REDACTED] (VMware)

script.zsh
Nmap scan report for [REDACTED]
Host is up (0.00054s latency).
All 1000 scanned ports on 192.168.86.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: [REDACTED] (VMware)

Nmap scan report for [REDACTED]
Host is up (0.000020s latency).
All 1000 scanned ports on [REDACTED] are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 9.37 seconds

```

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.



```
[kali㉿kali: ~]
$ nmap -A
Nmap 7.95 ( https://nmap.org ) at 2025-06-23 08:46 EDT
--=-
Scanning 192.168.1.15 ( https://nmap.org ) with 252 hosts completed (3 up), 3 undergoing Script Scan
NSE Timing: About 96.99% done; ETC: 08:46 (0:00:00 remaining)
Nmap scan report for
Host is up (0.0004s latency).
No shown filtered TCP ports (no-response)
PORT      STATE SERVICE VERSION
3306/tcp  open  MySQL   MySQL (unauthorized)
MAC Address: (VMware)
Warning: OScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux (Unknown)
OS CPE: cpe:/o:canonical:ubuntu_server_12.04
Aggressive OS guesses: Microsoft Windows 11 21H2 (91%), FreeBSD 12.0-RELEASE-p6 (85%), Microsoft Windows 10 (80%), Microsoft Windows Server 2008 or 2008 Beta 3 (85%), Microsoft Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1  0.94 ms  [REDACTED]

Nmap scan report for
Host is up (0.0005s latency).
No shown 999 closed ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    filtered domain
MAC Address: (VMware)
Warning: OScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running: VMware Player
OS CPE: cpe:/o:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1  0.55 ms  [REDACTED]
```

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.



```
(kali㉿kali)-[~]
$ nmap -sS -sV -oX scan_results.xml
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 09:37 EDT
Nmap scan report for [REDACTED]
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql  MySQL (unauthorized)
MAC Address: [REDACTED] (VMware)

Nmap scan report for [REDACTED]
Host is up (0.00083s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    filtered domain
MAC Address: [REDACTED] (VMware)

Nmap scan report for [REDACTED]
Host is up (0.00075s 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 (0.000031s latency).
All 1000 scanned ports on [REDACTED] are in ignored states.
Not shown: 1000 closed tcp ports (reset)

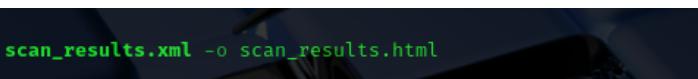
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 10.39 seconds

(kali㉿kali)-[~]
$ ls
```

The terminal window shows the execution of the Nmap command, which performs a SYN scan (-sS) and identifies services (-sV) on the local network range (-oX scan_results.xml). The output includes reports for four hosts, detailing open ports, service names, and versions. The final command listed is 'ls'.

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.



```
(kali㉿kali)-[~]
$ xsltproc /usr/share/nmap/nmap.xsl scan_results.xml -o scan_results.html
```

The terminal window shows the execution of the xsltproc command, which converts the XML scan results into an HTML report ('scan_results.html').

This script will help in converting our XML file into a 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)