

# Nmap Network Recon – Cybersecurity Internship Project

---

Name: Shashvat Singh

Date: June 19, 2025

## Objective:

Use Nmap to scan your local network, identify active hosts, detect open ports, and analyze potential vulnerabilities.

## Tools Used:

- Linux (Kali / Ubuntu / Parrot OS)
- Nmap

## Step 1: Check Your IP Address

Identifying local IP address: 192.168.64.2/24

```
(shashvat@shashvat)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 group default qlen 1000
    link/ether c2:8c:b8:e5:35:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.64.2/24 brd 192.168.64.255 scope global dynamic noprefixroute eth0
        valid_lft 2522sec preferred_lft 2522sec
    inet6 fd03:f4cc:8eb:dd23:f55e:4be9:70a6:8d9/64 scope global temporary dynamic
        valid_lft 603724sec preferred_lft 85200sec
    inet6 fd03:f4cc:8eb:dd23:c08c:b8ff:fee5:3561/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 2591936sec preferred_lft 604736sec
    inet6 fe80::c08c:b8ff:fee5:3561/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

## Step 2: Discover Live Devices

Nmap ping sweep showing multiple hosts on loopback

```
(shashvat@shashvat)-[~]
$ nmap -sn 127.0.0.1/8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 04:59 EDT
Nmap scan report for 127.0.0.0
Host is up.
Nmap scan report for localhost (127.0.0.1)
Host is up.
Nmap scan report for 127.0.0.2
Host is up.
Nmap scan report for 127.0.0.3
Host is up.
Nmap scan report for 127.0.0.4
Host is up.
Nmap scan report for 127.0.0.5
Host is up.
Nmap scan report for 127.0.0.6
Host is up.
Nmap scan report for 127.0.0.7
Host is up.
Nmap scan report for 127.0.0.8
Host is up.
Nmap scan report for 127.0.0.9
Host is up.
Nmap scan report for 127.0.0.10
Host is up.
Nmap scan report for 127.0.0.11
Host is up.
Nmap scan report for 127.0.0.12
Host is up.
Nmap scan report for 127.0.0.13
Host is up.
Nmap scan report for 127.0.0.14
Host is up.
Nmap scan report for 127.0.0.15
Host is up.
```

### Step 3: Run Intense Scan on a Target

Detected closed ports and performed OS fingerprinting

```
(shashvat@shashvat)-[~]
$ nmap -A -T4 127.0.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 05:02 EDT
Nmap scan report for 127.0.0.2
Host is up (0.000068s latency).
All 1000 scanned ports on 127.0.0.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds
```

## Step 4: Run Vulnerability Scan

Vulnerability scan – detected CVE-2011-1002 (Avahi DoS)

```
(shashvat@shashvat)-[~]
$ nmap --script vuln 127.0.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 05:02 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 127.0.0.2
Host is up (0.0000060s latency).
All 1000 scanned ports on 127.0.0.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
test.sh
Nmap done: 1 IP address (1 host up) scanned in 34.65 seconds
```

## Recommendations:

- Patch or disable SMB services
- Enforce HTTPS using TLS and redirect HTTP
- Use SSH key authentication and fail2ban
- Upgrade Apache & Samba to latest versions