

STEP 1: Install Nmap

On Kali Linux

```
sudo apt update
```

```
sudo apt install nmap -y
```

On Ubuntu

```
sudo apt install nmap
```

Verify

```
nmap --version
```

● STEP 2: Find Your IP Address

On Kali / Ubuntu

```
ip a
```

Example:

```
192.168.56.101
```

● STEP 3: Scan Local Network (Host Discovery)

```
nmap -sn 192.168.56.0/24
```

- ✓ Shows **live devices**
- ✓ Identify target IP (example: 192.168.56.105)

 *Take screenshot for lab record*

● STEP 4: Scan Open Ports (Target Machine)

```
nmap 192.168.56.105
```

Sample output:

```
22/tcp open ssh
```

```
80/tcp open http
```

- ✓ Shows **open ports**
-

● STEP 5: Service & Version Detection

```
nmap -sV 192.168.56.105
```

Example:

22/tcp OpenSSH 8.2

80/tcp Apache 2.4.41

- ✓ Identifies **software versions**
-

● **STEP 6: OS Detection (Run as Root)**

sudo nmap -O 192.168.56.105

Example:

Running: Linux 5.x

- ✓ Identifies **Operating System**
-

● **STEP 7: Vulnerability Scan (NSE Scripts)**

sudo nmap --script vuln 192.168.56.105

- ✓ Detects known vulnerabilities
- ✓ Shows CVE references

⚠ Takes time – wait patiently

● **STEP 8: Save Scan Results**

nmap -sV -O 192.168.56.105 -oN nmap_scan.txt

Check file:

cat nmap_scan.txt

- ✓ Required for **report submission**
-

● **STEP 9: Risk Analysis (Write This in Record)**

Finding	Risk
Open SSH	Brute force attacks
Open HTTP	Web vulnerabilities
Outdated service	Exploitable CVEs

● **STEP 10: Conclusion (For Practical File)**

“Using Nmap, network scanning was performed to identify live hosts, open ports, running services, OS details, and vulnerabilities. The results help in understanding the attack surface and improving network security.”