

# Nmap Scanning Project

## Objective:

Identify the operating system, running services, and potential vulnerabilities on the target IP **192.168.88.123** to understand its infrastructure and assess security measures.

## Tools Used:

- Nmap (Network mapper)
- Kali Linux (running on VirtualBox)
- Target: local machine with IP 192.168.174.123

## Methodology:

### 1. Ping Scan:

- Purpose: Verify if the target is active on the network.
- Command: `nmap -sn 192.168.174.123`
- Process: Sends ICMP echo requests to check if the host is up.

### 2. Port Scan:

#### I. To scan all 65535 ports

- Purpose: Identify open ports on the target system.
- Command: `nmap -p- 192.168.88.123`
- Process: Scans all 65535 ports for open or filtered states.

#### II. To scan multiple specific ports

- Purpose: Identify specific open ports on the target system
- Command: `nmap -p 22,80,443 192.168.88.123`
- Process: Scans port no 22,80,443 ports for open or filtered states

#### III. To scan a range of ports

- Purpose: Identify the specific range of open ports on the target system.
- Command: `nmap -p 1-1535 192.168.88.123`
- Process: Scans only port 1 to port 1535 for open or filtered states.

### 3. UDP Port Scan:

- Purpose: Discover open UDP ports on the target.
- Command: `nmap -sU 192.168.88.123`
- Process: Scans for active UDP-based services which are often missed by standard TCP scans.

### 4. Service Version Detection:

- Purpose: Identify active services and their versions to understand the target's network landscape.
- Command: `nmap -sV 192.168.88.123`
- Process: This command scans open ports and attempts to determine the version of services running on them.

## 5. OS Detection:

- Purpose: Identify the target's operating system for further exploitation or system analysis.
- Command: `nmap -O 192.168.88.123`
- Process: Uses TCP/IP stack fingerprinting to guess the operating system.

## 6. Firewall/IDS Detection:

- Purpose: Detect the presence of firewalls or intrusion detection systems (IDS) that may block scanning attempts. –
- Command: `nmap --script firewall-bypass 192.168.88.123`
- Process: Executes scripts designed to identify and attempt to bypass firewall rules.

## 7. Aggressive Scan:

- Purpose: Perform a comprehensive scan combining service detection, OS detection, and traceroute.
- Command: `nmap -A 192.168.88.123`
- Process: This command conducts a detailed assessment by combining multiple scanning techniques.

## 8. Vulnerability Scan:

- Purpose: Identify known vulnerabilities in detected services.
- Command: `nmap --script=vuln 192.168.88.123`
- Process: Runs Nmap's vulnerability detection scripts to find potential weaknesses.

## Findings:

### 1. Ping Scan (`nmap -sn 192.168.50.19`)

- Host is up and reachable on the network.

```
(root@Kali)-[~]
# nmap -sn 192.168.50.19

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 13:36 IST
Nmap scan report for 192.168.50.19
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

### 2. Port Scan (`nmap -p- 192.168.50.19`)

#### I. Port Scan (`nmap -p- 192.168.50.19`)

- All 65,535 TCP ports are closed. No active services detected on any port.

```
(root@Kali)-[~]
# nmap -p- 192.168.50.19

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 13:42 IST
Nmap scan report for 192.168.50.19
Host is up (0.0000030s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
```

- II. Specific Port Scan (nmap -p 22,80,443 192.168.50.19)
- Common service ports (SSH, HTTP, HTTPS) are closed. No services are running on ports 22, 80, or 443.

```
(root@Kali)-[~]
# nmap -p 22,80,443 192.168.50.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 13:38 IST
Nmap scan report for 192.168.50.19
Host is up (0.000031s latency).

PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    closed http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

- III. Port Range Scan (nmap -p 1-10000 192.168.50.20)
- Host is up with low latency. Port **8080/tcp** is open and running **http-proxy**. All other ports in the range are closed.

```
(root@Kali)-[~]
# nmap -p 1-10000 192.168.50.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 14:16 IST
Nmap scan report for 192.168.50.20
Host is up (0.0000030s latency).
Not shown: 9999 closed tcp ports (reset)
PORT      STATE SERVICE
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

3. UDP Port Scan (nmap -sU 192.168.50.20)

- Host is up with low latency. Ports **68/udp (dhcpc)** and **3702/udp (ws-discovery)** are in an *open/filtered* state, meaning Nmap couldn't determine whether they are truly open or just filtered by a firewall. All other 998 UDP ports are closed.

```
(root@Kali)-[~]
# nmap -sU 192.168.50.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 14:19 IST
Nmap scan report for 192.168.50.20
Host is up (0.0000030s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT      STATE SERVICE
68/udp    open|filtered dhcpc
3702/udp  open|filtered ws-discovery

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
```

4. Service Version Detection (nmap -sV 192.168.50.20)

- Host is up with low latency. Port **8080/tcp** is open, running **SimpleHTTPServer 0.6** (Python 3.12.7). All other scanned TCP ports are closed.

```
(root@Kali)-[~]
# nmap -sV 192.168.50.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 14:20 IST
Nmap scan report for 192.168.50.20
Host is up (0.0000030s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8080/tcp  open  http      SimpleHTTPServer 0.6 (Python 3.12.7)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.28 seconds
```

## 5. OS Detection (nmap -O 192.168.50.20)

- Host is up with low latency. The device is running **Linux 2.6.32**. It is detected as a general-purpose Linux system with the Linux kernel version 2.6.X. All other scanned TCP ports are closed.

```
(root@Kali)~# nmap -O 192.168.50.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 14:22 IST
Nmap scan report for 192.168.50.20
Host is up (0.000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
8080/tcp   open  http-proxy
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

## 6. Firewall Bypass Script (nmap --script firewall-bypass 192.168.56.1)

- Host seems down, possibly due to blocking ICMP (ping) requests or firewall restrictions. To bypass this, use the **-Pn** option to assume the host is up. The scan didn't proceed as expected due to this network configuration.

```
(root@Kali)~# nmap --script firewall-bypass 192.168.56.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-25 10:37 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.26 seconds
```

## 7. Aggressive Scan (nmap -A 127.0.0.1)

- Host is up (0.000067s latency).
- All 1000 TCP ports on 127.0.0.1 are in ignored states.
- No open ports detected (all ports closed or filtered).
- OS Detection: Too many fingerprints match this host, unable to specify OS.
- Network Distance: 0 hops (localhost).

```
(root@Kali)~# nmap -A 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 14:28 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000067s latency).
All 1000 scanned ports on localhost (127.0.0.1) 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 2.32 seconds
```

## 8. Vulnerability Scan (nmap --script=vuln 127.0.0.1)

- Host is up (0.0000020s latency).
- All 1000 TCP ports on 127.0.0.1 are in ignored states.
- No open ports detected (all ports closed or filtered).
- No vulnerabilities found (since no open ports were detected).

```
(root@kali)~# nmap --script=vuln 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 14:31 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 10.31 seconds
```