

MIT WORLD PEACE UNIVERSITY

Vulnerability Identification and Penetration Testing
Third Year B. Tech, Semester 6

SCANNING WITH NMAP

ASSIGNMENT 2

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

February 2, 2024

Contents

1 Aim	1
2 Objectives	1
3 Theory	1
4 Introduction to Nmap	1
4.1 Need/Purpose of Nmap	1
4.2 Advantages of Nmap	1
4.3 Disadvantages of Nmap	2
5 Implementation	2
5.1 Get ip Address	2
5.2 Scan 1 port, current IP	3
5.2.1 Syntax	3
5.3 Scan any IP	4
5.3.1 Syntax	4
5.4 Scan a range of IPs	4
5.4.1 Syntax	4
5.5 Scan 1 Port	6
5.5.1 Syntax	6
5.6 Scan a range of ports	6
5.6.1 Syntax	6
5.7 Fragmented Scan	7
5.7.1 Syntax	7
5.8 TCP SYN Scan	8
5.8.1 Syntax	8
5.9 OS Detection	8
5.9.1 Syntax	8
5.10 Syn Scan for specific ports with ping	9
5.10.1 Syntax	10
6 Platform	11
7 Conclusion	11

1 Aim

To perform scanning with nmap.

2 Objectives

1. To learn about nmap.
2. To perform live host scanning.

3 Theory

4 Introduction to Nmap

Nmap, short for Network Mapper, is a widely-used open-source tool designed for network exploration and security auditing. It provides a comprehensive view of a network by discovering hosts and services running on them.

4.1 Need/Purpose of Nmap

Nmap serves various purposes in the field of cybersecurity and network management. Its primary objectives include:

- **Host Discovery:** Identifying active hosts on a network, aiding in network mapping.
- **Port Scanning:** Determining open ports on a system, crucial for understanding potential vulnerabilities.
- **Service Version Detection:** Identifying the version and type of services running on open ports.
- **OS Fingerprinting:** Attempting to determine the operating system of target hosts.
- **Vulnerability Assessment:** Assessing potential security risks and vulnerabilities within a network.

4.2 Advantages of Nmap

Nmap offers several advantages that make it a preferred choice in the cybersecurity community:

- **Versatility:** Nmap can be used for a wide range of network exploration and security auditing tasks.
- **Accuracy:** It provides accurate information about hosts, open ports, and services.
- **Scripting Engine:** Nmap's scripting engine allows users to create custom scripts for specific tasks.
- **Community Support:** Being open-source, Nmap benefits from a large and active user community, ensuring continuous improvement.
- **Platform Independence:** Nmap is available on multiple platforms, making it accessible to a diverse range of users.

4.3 Disadvantages of Nmap

Despite its many strengths, Nmap has some limitations and potential drawbacks:

- **Firewall Interference:** Firewalls may block Nmap scans, limiting the tool's effectiveness.
- **Legal and Ethical Concerns:** Improper use of Nmap for unauthorized scanning may lead to legal and ethical issues.
- **False Positives:** In certain scenarios, Nmap might produce false positives, leading to inaccurate assessments.
- **Resource Intensive:** Intensive scanning can consume significant network resources and slow down target systems.
- **Limited Stealth:** While Nmap offers stealthy scanning options, complete stealth is challenging to achieve in some situations.

5 Implementation

5.1 Get ip Address

Syntax

```
$ifconfig
```

Command

```
$ifconfig
```

Purpose

To get the IP Address of the machine.

Output

```
krishnaraj@Krishnaraj-Arch ~$ ifconfig
enp2s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 54:e1:ad:c9:5a:ba txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9131884 bytes 15562442503 (14.4 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9131884 bytes 15562442503 (14.4 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.38 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2402:e280:3e28:3a0:374:e8a4:8415:b314 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::14ca:3110:e0dc:3c45 prefixlen 64 scopeid 0x20<link>
    inet6 2402:e280:3e28:3a0:1a34:3945:8c34:2563 prefixlen 64 scopeid 0x0<global>
    ether 60:f6:77:52:55:a3 txqueuelen 1000 (Ethernet)
    RX packets 41245372 bytes 34695633022 (32.3 GiB)
    RX errors 0 dropped 24 overruns 0 frame 0
    TX packets 44209237 bytes 32285170928 (30.0 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 1: Get IP Address

5.2 Scan 1 port, current IP

5.2.1 Syntax

```
$ nmap -p <port> <ip>
```

Command

```
$ nmap -p 80 192.168.1.38
```

Purpose

To get the IP Address of the machine.

Output

```
krishnaraj@Krishnaraj-Arch ~$ nmap 192.168.1.38
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:25 IST
Nmap scan report for 192.168.1.38
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.1.38 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

Figure 2: Get IP Address

5.3 Scan any IP

5.3.1 Syntax

```
$ nmap <ip>
```

Command

```
$ nmap 192.168.1.38
```

Purpose

Scan a single ip

Output

```
krishnaraj@Krishnaraj-Arch ~$ nmap www.google.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:30 IST
Nmap scan report for www.google.com (142.250.70.36)
Host is up (0.013s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82a::2004
rDNS record for 142.250.70.36: pnbomb-aa-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

Figure 3: Scan google.com

5.4 Scan a range of IPs

5.4.1 Syntax

```
$ nmap <ip range>
```

Command

```
$ nmap 192.168.1.38-40
```

Purpose

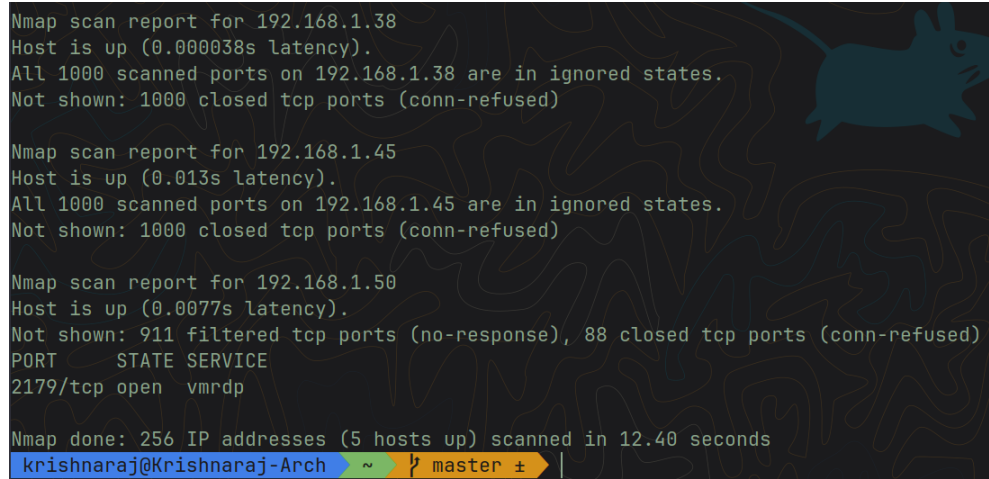
To Scan a range of IPs.

Output

```
krishnaraj@Krishnaraj-Arch ~ } master ± nmap 192.168.1.38/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 12:20 IST
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
21/tcp    open       ftp
22/tcp    filtered  ssh
53/tcp    open       domain
80/tcp    open       http
443/tcp   open       https

Nmap scan report for 192.168.1.33
Host is up (0.0068s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
21/tcp    filtered  ftp
23/tcp    filtered  telnet
53/tcp    filtered  domain
110/tcp   filtered  pop3
135/tcp   filtered  msrpc
256/tcp   filtered  fw1-secureremote
995/tcp   filtered  pop3s
1720/tcp  filtered  h323q931
5900/tcp  filtered  vnc
8888/tcp  filtered  sun-answerbook
```

Figure 4: scan range of ips.



```

Nmap scan report for 192.168.1.38
Host is up (0.000038s latency).
All 1000 scanned ports on 192.168.1.38 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.1.45
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.45 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.1.50
Host is up (0.0077s latency).
Not shown: 911 filtered tcp ports (no-response), 88 closed tcp ports (conn-refused)
PORT      STATE SERVICE
2179/tcp  open  vmrpd

Nmap done: 256 IP addresses (5 hosts up) scanned in 12.40 seconds
krishnaraj@Krishnaraj-Arch ~ } master ±

```

Figure 5: scan range of ips.

5.5 Scan 1 Port

5.5.1 Syntax

```
$ nmap -p <port> <ip>
```

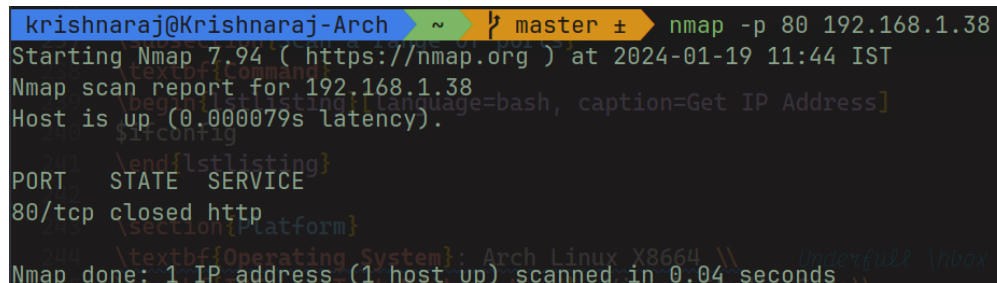
Command

```
$ nmap -p 80 www.example.com
```

Purpose

To perform a scan on a single port.

Output



```

krishnaraj@Krishnaraj-Arch ~ } master ± nmap -p 80 192.168.1.38
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:44 IST
Nmap scan report for 192.168.1.38
Host is up (0.000079s latency).
PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds

```

Figure 6: Scan a single port

5.6 Scan a range of ports

5.6.1 Syntax

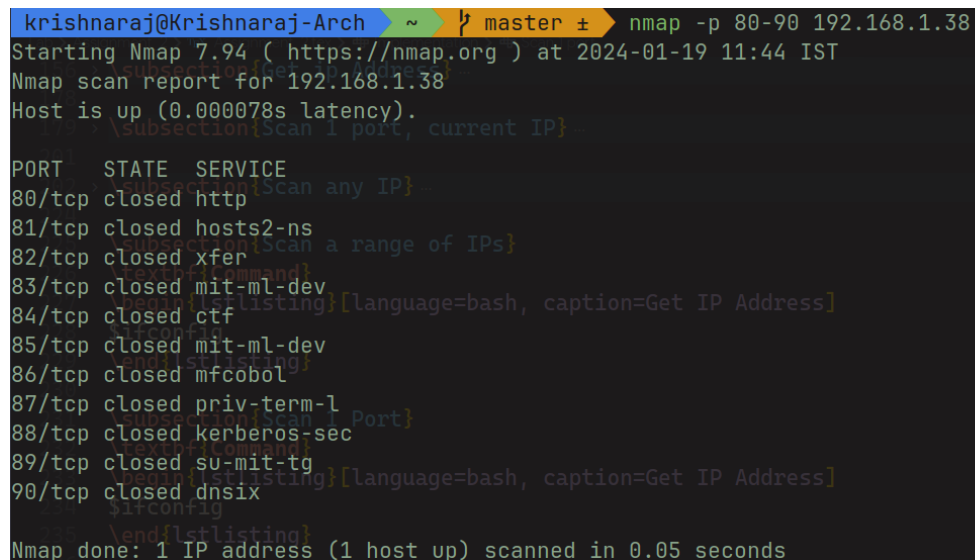
```
$ nmap -p <port range> <ip>
```


Command

```
$ nmap -p 1-100 www.example.com
```

Purpose

To perform a scan on a range of ports.

Output

```
krishnaraj@Krishnaraj-Arch ~$ nmap -p 80-90 192.168.1.38
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:44 IST
Nmap scan report for 192.168.1.38
Host is up (0.000078s latency).
PORT      STATE SERVICE
80/tcp    closed http
81/tcp    closed hosts2-ns
82/tcp    closed xfer
83/tcp    closed mit-ml-dev
84/tcp    closed ctf
85/tcp    closed mit-ml-dev
86/tcp    closed mfcobol
87/tcp    closed priv-term-l
88/tcp    closed kerberos-sec
89/tcp    closed su-mit-tg
90/tcp    closed dnsix
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Figure 7: Scan a range of ports

5.7 Fragmented Scan

5.7.1 Syntax

```
$ nmap -F <ip>
```

Command

```
$ nmap -F www.example.com
```

Purpose

Fragmented Scan is used to evade firewalls.

Output

```
krishnaraj@Krishnaraj-Arch ~$ sudo nmap -F 192.168.1.38
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:49 IST
Nmap scan report for 192.168.1.38
Host is up (0.000015s latency).
All 100 scanned ports on 192.168.1.38 are in ignored states.
Not shown: 100 closed tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Figure 8: Perform a fragmented scan.

5.8 TCP SYN Scan

5.8.1 Syntax

```
$ nmap -sS <ip>
```

Command

```
$ nmap -sS www.example.com
```

Purpose

To scan a host for open ports using TCP SYN scan.

Output

```
krishnaraj@Krishnaraj-Arch ~$ sudo nmap -sS www.example.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:59 IST
Nmap scan report for www.example.com (93.184.216.34)
Host is up (0.25s latency).
Other addresses for www.example.com (not scanned): 2606:2800:220:1:248:1893:25c8:1946
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1119/tcp  closed bnetgame
1935/tcp  closed rtmp
Nmap done: 1 IP address (1 host up) scanned in 16.14 seconds
```

Figure 9: Check if tcp syn scan is possible on a host.

5.9 OS Detection

5.9.1 Syntax

```
$ nmap -O <ip>
```

Command

```
$ nmap -O www.example.com
```

Purpose

To scan operating system of a host.

Output

```
krishnaraj@Krishnaraj-Arch ~$ sudo nmap -O www.example.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 12:05 IST
Nmap scan report for www.example.com (93.184.216.34)
Host is up (0.24s latency).
Other addresses for www.example.com (not scanned): 2606:2800:220:1:248:1893:25c8:1946
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1119/tcp  closed bnetgame
1935/tcp  closed rtmp
Device type: general purpose|phone
Running (JUST GUESSING): OpenBSD 4.X (87%), Google Android 5.X (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:google:android:5.0.1
Aggressive OS guesses: OpenBSD 4.0 (87%), Android 5.0.1 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.79 seconds
```

Figure 10: Scan Operating System of example.com

```
krishnaraj@Krishnaraj-Arch ~$ sudo nmap -O 192.168.1.38/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 12:05 IST
Nmap scan report for 192.168.1.1
Host is up (0.0039s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: B4:3D:08:08:D7:90 (GX International BV)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Nmap scan report for 192.168.1.33
Host is up (0.023s latency).
All 1000 scanned ports on 192.168.1.33 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: EC:30:B3:33:46:5C (Xiaomi Communications)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figure 11: Scan Operating System of host

5.10 Syn Scan for specific ports with ping

add diagram also

5.10.1 Syntax

```
$ sudo nmap -sS -p< <ip>
```

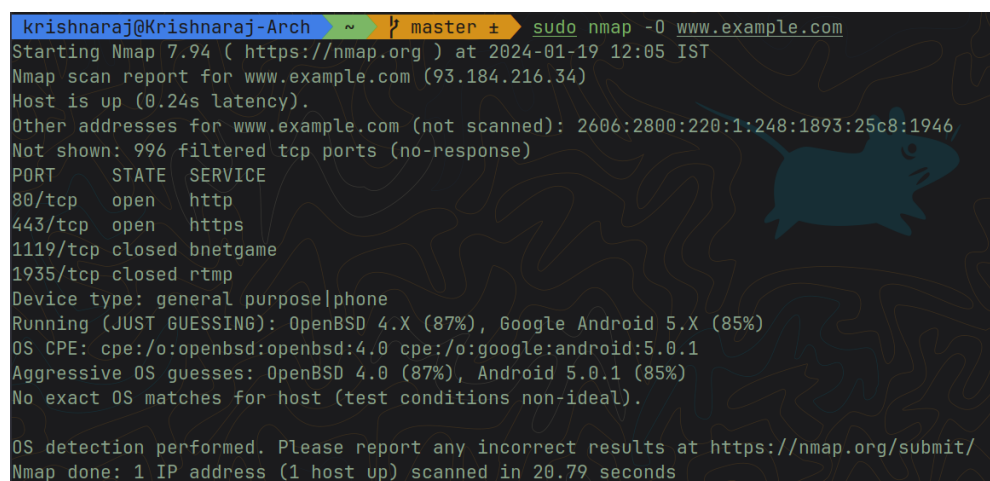
Command

```
$ sudo nmap -sS -p80-90 172.16.182.162
```

Purpose

To scan operating system of a host.

Output



```
krishnaraj@Krishnaraj-Arch ~$ sudo nmap -O www.example.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 12:05 IST
Nmap scan report for www.example.com (93.184.216.34)
Host is up (0.24s latency).
Other addresses for www.example.com (not scanned): 2606:2800:220:1:248:1893:25c8:1946
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1119/tcp  closed bnetgame
1935/tcp  closed rtmp
Device type: general purpose|phone
Running (JUST GUESSING): OpenBSD 4.X (87%), Google Android 5.X (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:google:android:5.0.1
Aggressive OS guesses: OpenBSD 4.0 (87%), Android 5.0.1 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.79 seconds
```

Figure 12: Scan Operating System of example.com

```
krishnaraj@Krishnaraj-Arch ~$ sudo nmap -O 192.168.1.38/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 12:05 IST
Nmap scan report for 192.168.1.1
Host is up (0.0039s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: B4:3D:08:08:D7:90 (GX International BV)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Nmap scan report for 192.168.1.33
Host is up (0.023s latency).
All 1000 scanned ports on 192.168.1.33 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: EC:30:B3:33:46:5C (Xiaomi Communications)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figure 13: Scan Operating System of host

next command

with ping `sudo nmap -sS -p80-90 172.16.182.162`

less time no ping `sudo nmap -sS -Pn -p40-6000 172.16.182.162`

with t

6 Platform

Operating System: Arch Linux X8664

IDEs or Text Editors Used: Visual Studio Code

7 Conclusion

Thus, we have successfully performed scanning with nmap, and learnt about the various options available with nmap.