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

January 19, 2024

Contents

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

```
1 $ifconfig
```
Listing 1: Get IP Address

Command

```
1 $ifconfig
```
Listing 2: Get IP Address

Purpose

To get the IP Address of the machine.

Output

Figure 1: Get IP Address

5.2 Scan 1 port, current IP

5.2.1 Syntax

```
1 $ nmap -p <port> <ip>
```

Listing 3: Get IP Address

Command

```
1 $ nmap -p 80 192.168.1.38
```

Listing 4: Get IP Address

Purpose

To get the IP Address of the machine.

Output

Figure 2: Get IP Address

5.3   Scan any IP

5.3.1   Syntax

```
1 $ nmap <ip>
```

Listing 5: Get IP Address

Command

```
1 $ nmap 192.168.1.38
```

Listing 6: Get IP Address

Purpose

Scan a single ip

Output

Figure 3: Scan google.com

5.4   Scan a range of IPs

5.4.1   Syntax

```
1 $ nmap <ip range>
```

Listing 7: Get IP Address
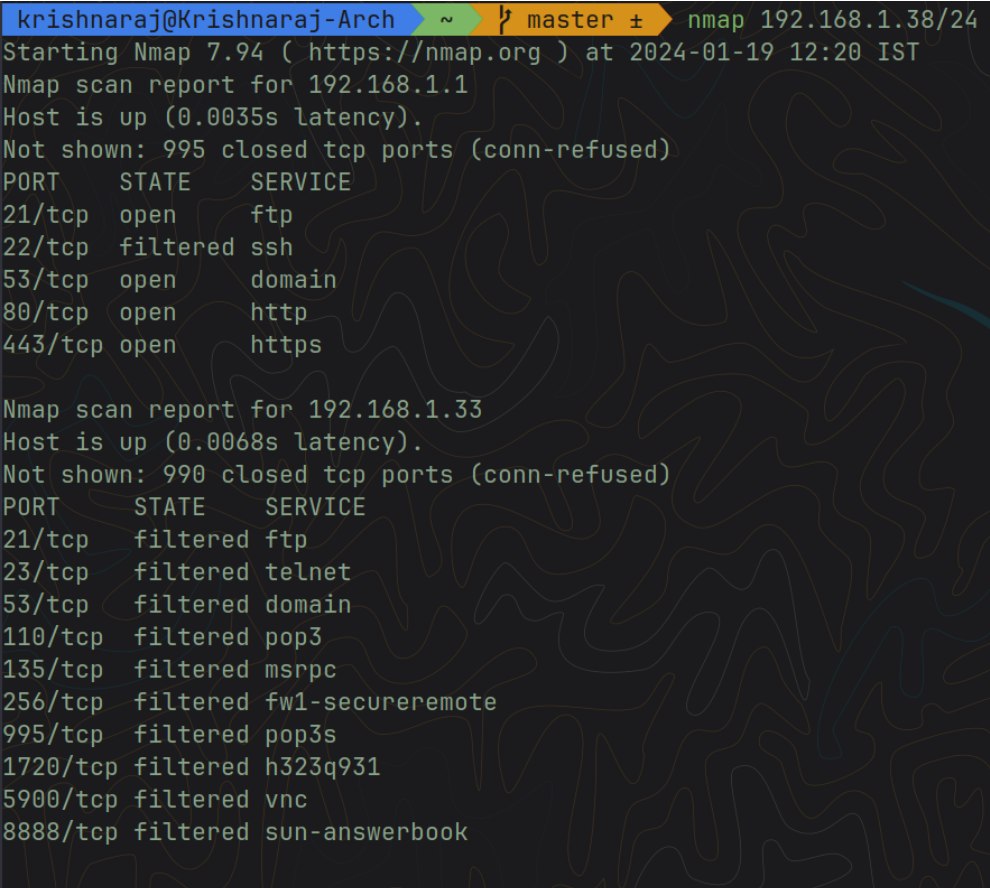
Command

```
1 $ nmap 192.168.1.38-40
```

Listing 8: Get IP Address

Purpose

To Scan a range of IPs.

Output

Figure 4: scan range of ips.

Figure 5: scan range of ips.

5.5   Scan 1 Port

5.5.1   Syntax

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

Listing 9: Get IP Address

Command

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

Listing 10: Get IP Address

Purpose

To perform a scan on a single port.

Output

Figure 6: Scan a single port

5.6   Scan a range of ports

5.6.1   Syntax

```
1 $ nmap -p <port range> <ip>
```

<div align="center">Listing 11: Get IP Address</div>

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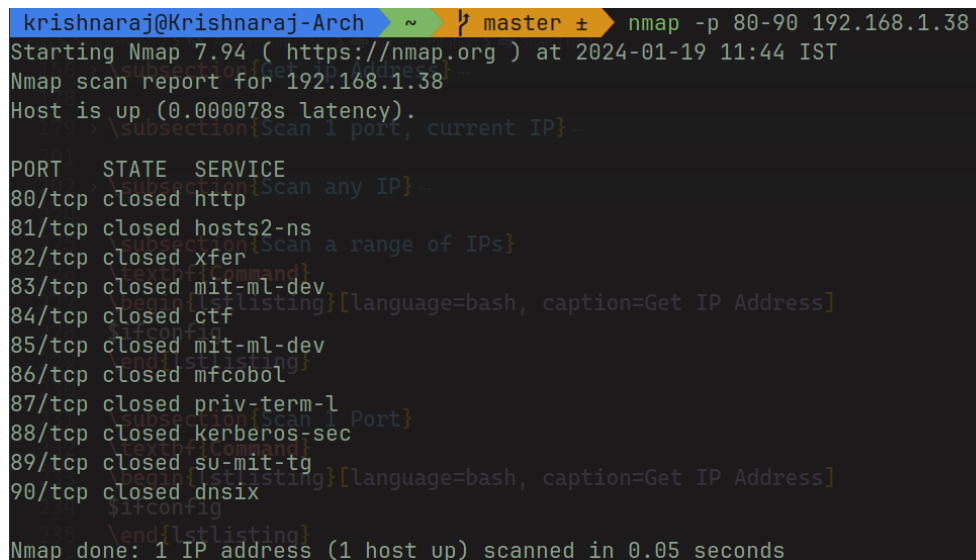
```
1 $ nmap -p 1-100 www.example.com
```

<div align="center">Listing 12: Get IP Address</div>

Purpose

To perform a scan on a range of ports.

Output

<div align="center">Figure 7: Scan a range of ports</div>

5.7   Fragmented Scan

5.7.1   Syntax

```
1 $ nmap -F <ip>
```

<div align="center">Listing 13: Get IP Address</div>

Command

```
1 $ nmap -F www.example.com
```

<div align="center">Listing 14: Get IP Address</div>

Purpose

Fragmented Scan is used to evade firewalls.

Output

Figure 8: Perform a fragmented scan.

5.8   TCP SYN Scan

5.8.1   Syntax

```
1 $ nmap -sS <ip>
```

Listing 15: Get IP Address

Command

```
1 $ nmap -sS www.example.com
```

Listing 16: Get IP Address

Purpose

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

Output

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

5.9 OS Detection

5.9.1 Syntax

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

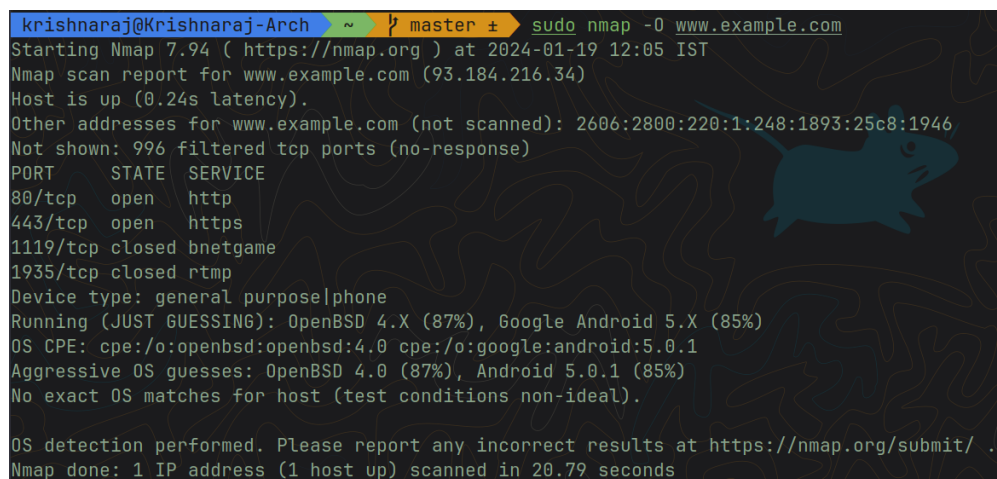<div align="center">Listing 17: Get IP Address</div>

Command

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

<div align="center">Listing 18: Get IP Address</div>

Purpose

To scan operating system of a host.

Output

<div align="center">Figure 10: Scan Operating System of example.com</div>

Figure 11: Scan Operating System of host

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.