Internship Project Report

Task 1: Basic Network Scanning with Nmap

Name: Sibiraj B

Company: Oasis infobyte

Duration: [July 15 2025 – augest 15 2025]

Submitted as part of the internship program

1. Objective

The objective of this project is to perform basic network scanning using Nmap to identify live hosts, open ports, running services, and basic operating system detection within a controlled and authorized environment.

2. Description

This project focuses on using the Nmap (Network Mapper) tool for basic network scanning. The aim is to understand how to perform different scanning techniques, interpret results, and analyze the implications of discovered hosts and services. All activities were performed on a safe, authorized lab network.

3. Tools & Technologies

- Tool: Nmap

- Operating System: Kali Linux / Windows

- Target: Authorized lab network

- Protocols: TCP, UDP, ICMP

4. Scope

1. Host discovery using Ping Sweep (-sn)

2. TCP SYN Scan (-sS)

3. Service Version Detection (-sV)

4. Operating System Detection (-O)

5. Combined Scans with Aggressive Mode (-A)

5. Implementation Steps

Step 1: Host Discovery

Command:

```
nmap -sn 192.168.1.0/24
```

Description: Used to identify active devices on the network.

Step 2: TCP SYN Scan

Command:

```
nmap -sS 192.168.1.10
```

Description: Stealth scan to detect open TCP ports.

Step 3: Service Version Detection

Command:
```
nmap -sV 192.168.1.10
```

Description: Detects versions of running services.

Step 4: Operating System Detection

Command:
```
nmap -O 192.168.1.10
```

Description: Identifies the operating system of the target host.

Step 5: Aggressive Scan

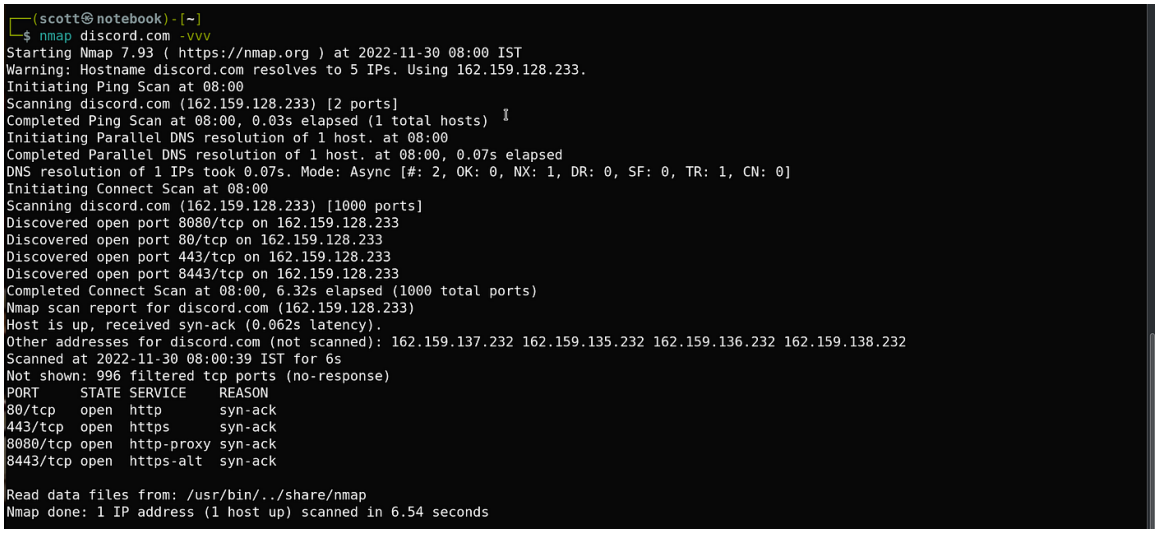
Command:
```
nmap -A 192.168.1.10
```

Description: Combines OS detection, version detection, script scanning, and traceroute.

6. Sample Results Summary

Example table of scan results:

Host IP	Status	Open Ports	Services	OS Guess
192.168.1.10	Up	22, 80	SSH, HTTP	Linux Kernel 5.x
192.168.1.15	Up	3389	Microsoft RDP	Windows 10 Pro



7. Ethical Considerations

All scans were performed only on authorized lab networks. No unauthorized systems were targeted, ensuring full compliance with ethical hacking principles.

8. Conclusion

The project successfully demonstrated the use of Nmap for basic network scanning, providing insights into host discovery, port scanning, and service identification. This serves as a foundation for more advanced scanning and vulnerability assessment techniques.