

# Internship Project Report

---

Task 1: Basic Network Scanning with Nmap

Name: Sibiraj B

Company: Oasis infobyte

Duration: [July 15 2025 – august 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

```
(scott@notebook)-[~]
$ nmap discord.com -vvv
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-30 08:00 IST
Warning: Hostname discord.com resolves to 5 IPs. Using 162.159.128.233.
Initiating Ping Scan at 08:00
Scanning discord.com (162.159.128.233) [2 ports]
Completed Ping Scan at 08:00, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:00
Completed Parallel DNS resolution of 1 host. at 08:00, 0.07s elapsed
DNS resolution of 1 IPs took 0.07s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 08:00
Scanning discord.com (162.159.128.233) [1000 ports]
Discovered open port 8080/tcp on 162.159.128.233
Discovered open port 80/tcp on 162.159.128.233
Discovered open port 443/tcp on 162.159.128.233
Discovered open port 8443/tcp on 162.159.128.233
Completed Connect Scan at 08:00, 6.32s elapsed (1000 total ports)
Nmap scan report for discord.com (162.159.128.233)
Host is up, received syn-ack (0.062s latency).
Other addresses for discord.com (not scanned): 162.159.137.232 162.159.135.232 162.159.136.232 162.159.138.232
Scanned at 2022-11-30 08:00:39 IST for 6s
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack
443/tcp   open  https  syn-ack
8080/tcp   open  http-proxy syn-ack
8443/tcp   open  https-alt syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
```

## 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.