

# Network Scanner Using Nmap

Internship Project Report

---

Student Name: B. Bharath Kishore

Internship Domain: Cybersecurity / Networking

Organization: Bharathiar university

Date of Submission: Feburary

---

TABLE OF CONTENTS

1. OBJECTIVE .....	2
2. TOOLS USED .....	3
3. METHODOLOGY .....	4
4. SCAN RESULTS .....	8
5. SECURITY ANALYSIS .....	11
6. CONCLUSION .....	13
7. REFERENCES .....	15

# 1. OBJECTIVE

The primary objective of this internship project is to gain a thorough understanding of network scanning concepts and to practically implement these concepts using the Nmap (Network Mapper) tool. Network scanning is a foundational activity in cybersecurity that helps security professionals discover and analyze devices, services, and potential weaknesses within a network infrastructure.

This project focuses on identifying live hosts within a network, discovering open and accessible ports, detecting running services along with their versions, identifying the operating system of target machines, and recognizing different types of devices connected to the network such as computers, routers, and other network-enabled systems. These activities help in building a clear picture of the network architecture and its exposure to potential threats.

Another important objective of this project is to provide hands-on practical experience in network reconnaissance, which is a critical phase in both defensive and offensive cybersecurity operations. By performing authorized scans in a controlled and ethical environment, this project demonstrates how security analysts and network administrators assess network visibility, monitor system availability, and identify possible security misconfigurations.

Additionally, this project aims to enhance the intern's technical skills in using industry-standard security tools, interpreting scan results, and documenting findings in a professional manner. The knowledge gained through this project helps in understanding how proactive network assessment contributes to strengthening overall organizational security and reducing the risk of cyber attacks.

---

## 2. TOOLS USED

The following tools and technologies were used to successfully complete this project:

### 2.1 Kali Linux

Kali Linux is a Debian-based penetration testing operating system widely used by cybersecurity professionals. It comes pre-installed with various security assessment tools, including Nmap.

### 2.2 Nmap (Network Mapper)

Nmap is an open-source network scanning tool used for host discovery, port scanning, service enumeration, and operating system detection.

### 2.3 VMware Workstation

VMware Workstation was used to create a virtual environment for safely running Kali Linux without affecting the host system.

## 2.4 Target Network

A local authorized network was used as the scanning target to ensure ethical and legal compliance.

### 3. METHODOLOGY

The methodology followed in this project was systematic and aligned with real-world cybersecurity practices. The project was divided into multiple stages.

### 3.1 Environment Setup (Initial Stage)

In the initial stage, VMware Workstation was installed on the host system, and Kali Linux was configured as a virtual machine. The network adapter was set to NAT mode to allow controlled network access.

Once the environment was ready, basic network connectivity was verified.

## Nmap Version Check

Command Used:

nmap -version

[illegible]

Explanation:

Checks the installed Nmap version and confirms that the tool is available in the system.

## Scan a Single IP

Command Used:

nmap 10.85.57.71

[illegible]

Explanation:

Scans a single IP address to identify open ports and basic network exposure.

## Scan a Hostname

Command Used:

```
nmap example.com
```

```

Session Actions Edit View Help
6X packets 0 bytes 1818 (3.6 KIB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 21 bytes 4110 (8.0 KIB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=UP<BROADCAST,MULTICAST> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scope link
loop (veth-pair) 1MBU (local)
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

--(kali@kali)--[~]
~$ nmap -vvv google
Nmap version 7.90-1 https://nmap.org
Platform: x86_64-linux-gnu
Compiled with: libssl-1.1.0 libxml-2.11.2 zlib-1.2.11 libncurses-6.4.2 libnet-1.16.3 nmap-libmnl-2.11 (not compiled with it)
Available work engines: osint, null, select

--(kali@kali)--[~]
~$ nmap -vvv 98.8.2.15
Starting Nmap 7.90-1 https://nmap.org [ at 2019-01-04 01:27 EST ]
Nmap scan target for 98.8.2.15
Host: 15.19 (9.88ms latency).
All 65535 scanned ports on 98.8.2.15 are in ignored state.
Not shown: 65535 closed tcp ports (reset)

Nmap scan: 1 IP address (1 host up) scanned in 0.01 seconds.

--(kali@kali)--[~]
~$ nmap -vvv google.com
Starting Nmap 7.90-1 https://nmap.org [ at 2019-01-04 01:28 EST ]
Nmap scan target for google.com [142.251.123.134]
Host: 142.251.123.134 (9.88ms latency).
Other addresses for google.com were: 142.251.123.135, 142.251.123.136, 142.251.123.137, 142.251.123.138, 142.251.123.139, 142.251.123.140, 142.251.123.141, 142.251.123.142, 142.251.123.143, 142.251.123.144, 142.251.123.145, 142.251.123.146, 142.251.123.147, 142.251.123.148, 142.251.123.149, 142.251.123.150, 142.251.123.151, 142.251.123.152, 142.251.123.153, 142.251.123.154, 142.251.123.155, 142.251.123.156, 142.251.123.157, 142.251.123.158, 142.251.123.159, 142.251.123.160, 142.251.123.161, 142.251.123.162, 142.251.123.163, 142.251.123.164, 142.251.123.165, 142.251.123.166, 142.251.123.167, 142.251.123.168, 142.251.123.169, 142.251.123.170, 142.251.123.171, 142.251.123.172, 142.251.123.173, 142.251.123.174, 142.251.123.175, 142.251.123.176, 142.251.123.177, 142.251.123.178, 142.251.123.179, 142.251.123.180, 142.251.123.181, 142.251.123.182, 142.251.123.183, 142.251.123.184, 142.251.123.185, 142.251.123.186, 142.251.123.187, 142.251.123.188, 142.251.123.189, 142.251.123.190, 142.251.123.191, 142.251.123.192, 142.251.123.193, 142.251.123.194, 142.251.123.195, 142.251.123.196, 142.251.123.197, 142.251.123.198, 142.251.123.199, 142.251.123.200, 142.251.123.201, 142.251.123.202, 142.251.123.203, 142.251.123.204, 142.251.123.205, 142.251.123.206, 142.251.123.207, 142.251.123.208, 142.251.123.209, 142.251.123.210, 142.251.123.211, 142.251.123.212, 142.251.123.213, 142.251.123.214, 142.251.123.215, 142.251.123.216, 142.251.123.217, 142.251.123.218, 142.251.123.219, 142.251.123.220, 142.251.123.221, 142.251.123.222, 142.251.123.223, 142.251.123.224, 142.251.123.225, 142.251.123.226, 142.251.123.227, 142.251.123.228, 142.251.123.229, 142.251.123.230, 142.251.123.231, 142.251.123.232, 142.251.123.233, 142.251.123.234, 142.251.123.235, 142.251.123.236, 142.251.123.237, 142.251.123.238, 142.251.123.239, 142.251.123.240, 142.251.123.241, 142.251.123.242, 142.251.123.243, 142.251.123.244, 142.251.123.245, 142.251.123.246, 142.251.123.247, 142.251.123.248, 142.251.123.249, 142.251.123.250, 142.251.123.251, 142.251.123.252, 142.251.123.253, 142.251.123.254, 142.251.123.255, 142.251.123.256, 142.251.123.257, 142.251.123.258, 142.251.123.259, 142.251.123.260, 142.251.123.261, 142.251.123.262, 142.251.123.263, 142.251.123.264, 142.251.123.265, 142.251.123.266, 142.251.123.267, 142.251.123.268, 142.251.123.269, 142.251.123.270, 142.251.123.271, 142.251.123.272, 142.251.123.273, 142.251.123.274, 142.251.123.275, 142.251.123.276, 142.251.123.277, 142.251.123.278, 142.251.123.279, 142.251.123.280, 142.251.123.281, 142.251.123.282, 142.251.123.283, 142.251.123.284, 142.251.123.285, 142.251.123.286, 142.251.123.287, 142.251.123.288, 142.251.123.289, 142.251.123.290, 142.251.123.291, 142.251.123.292, 142.251.123.293, 142.251.123.294, 142.251.123.295, 142.251.123.296, 142.251.123.297, 142.251.123.298, 142.251.123.299, 142.251.123.300, 142.251.123.301, 142.251.123.302, 142.251.123.303, 142.251.123.304, 142.251.123.305, 142.251.123.306, 142.251.123.307, 142.251.123.308, 142.251.123.309, 142.251.123.310, 142.251.123.311, 142.251.123.312, 142.251.123.313, 142.251.123.314, 142.251.123.315, 142.251.123.316, 142.251.123.317, 142.251.123.318, 142.251.123.319, 142.251.123.320, 142.251.123.321, 142.251.123.322, 142.251.123.323, 142.251.123.324, 142.251.123.325, 142.251.123.326, 142.251.123.327, 142.251.123.328, 142.251.123.329, 142.251.123.330, 142.251.123.331, 142.251.123.332, 142.251.123.333, 142.251.123.334, 142.251.123.335, 142.251.123.336, 142.251.123.337, 142.251.123.338, 142.251.123.
```

Explanation:

Scans a target system using its hostname instead of an IP address.

## Scan Entire Network

Command Used:

```
nmap 10.85.57.0/24
```

[illegible]

Explanation:

Scans all devices in the specified network range.

## List Active Hosts

Command Used:

```
nmap -sn 10.85.57.0/24
```

[illegible]

Lists only active hosts without performing port scanning.

## Skip Host Discovery

Command Used:

nmap -Pn 10.85.57.71

[illegible]

Explanation:

Skips ping checks and assumes the target is online.

## Scan Specific Port

Command Used:

```
nmap -p 80 10.85.57.71
```



```

--(root@raspberrypi) ~
root@raspberrypi:~# sudo apt-get install http
Reading package lists... Done
Building dependency tree
Reading state information... Done
http is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not installed.
root@raspberrypi:~#

```

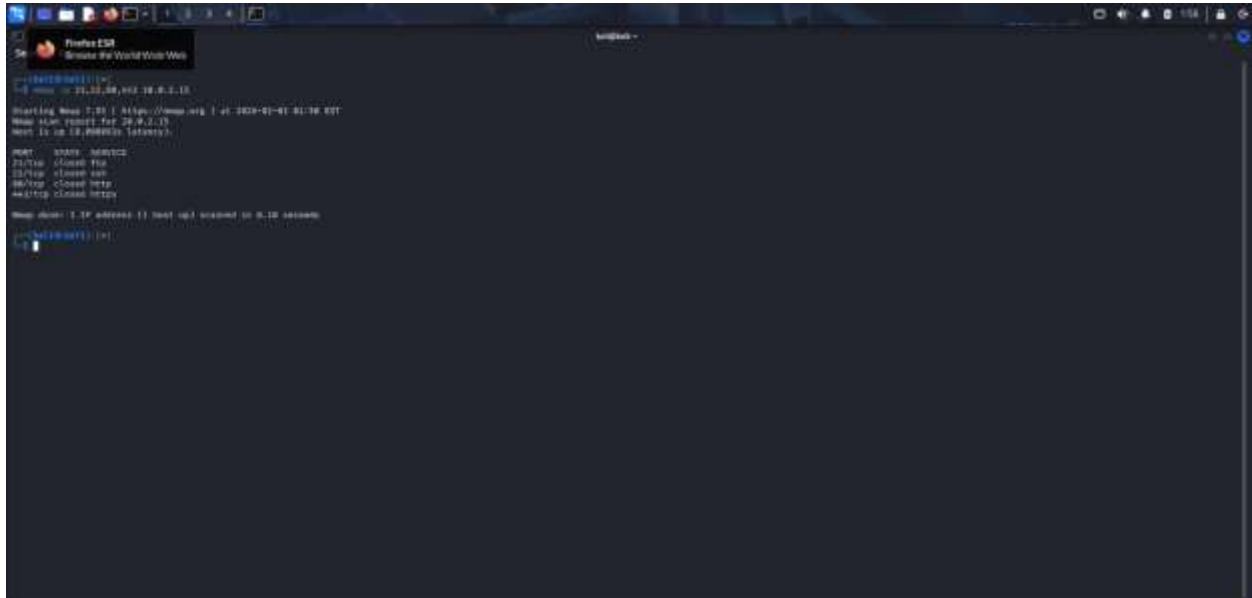
Explanation:

Scans a specific port on the target system.

## Scan Multiple Ports

Command Used:

```
nmap -p 22,80,443 10.85.57.71
```



```
root@kali:~# nmap -p 22,80,443 10.8.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-01 01:36:00 UTC
Nmap scan target for 10.8.2.15
Host is up (0.0000s latency).

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

Nmap scan of 1 IP address (1 host up) scanned in 0.10 seconds

root@kali:~#
```

Explanation:

Scans multiple selected ports simultaneously.

## Scan Port Range

Command Used:

```
nmap -p 1-1000 10.85.57.71
```



```
root@kali:~# nmap -p 1-1000 10.8.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-01 01:36:00 UTC
Nmap scan target for 10.8.2.15
Host is up (0.0000s latency).
All 1000 scanned ports on 10.8.2.15 are in ignored states.
Nmap scan of 1 IP address (1 host up) scanned in 0.00 seconds

root@kali:~#
```



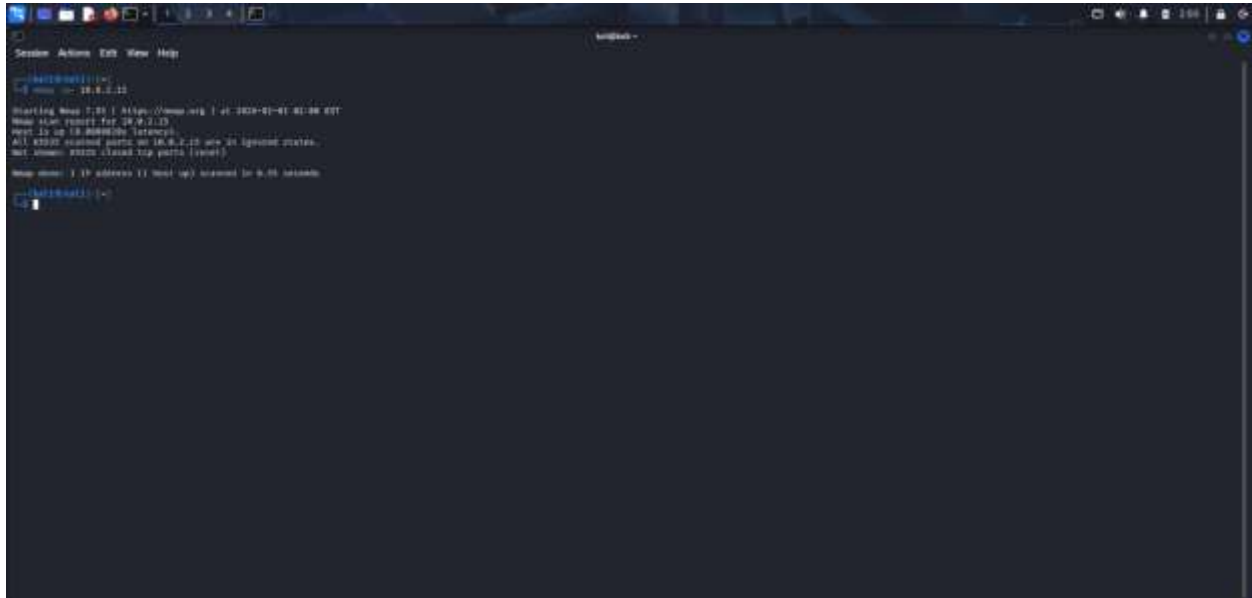
Explanation:

Scans a defined range of ports.

## Scan All Ports

Command Used:

`nmap -p- 10.85.57.71`

A terminal window showing the execution of the nmap command. The prompt is root@kali:~#. The command entered is nmap -p- 10.85.57.71. The output shows the scan progress and results. The scan is complete, showing that all 65535 ports are scanned in 6.05 seconds. The output is as follows:

```
root@kali:~# nmap -p- 10.85.57.71
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-01 01:00:00 EST
Nmap scan report for 10.85.57.71
Host is up (0.0000ms latency).
All 65535 scanned ports on 10.85.57.71 are in ignored state.
Not shown: 65535 closed tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 6.05 seconds
```

Explanation:

Scans all 65,535 TCP ports.

## Detect Service Version

Command Used:

`nmap -sV 10.85.57.71`

A terminal window showing the execution of the nmap command. The prompt is root@kali:~#. The command entered is nmap -sV 10.85.57.71. The output shows the scan progress and results. The scan is complete, showing that all 65535 ports are scanned in 9.08 seconds. The output is as follows:

```
root@kali:~# nmap -sV 10.85.57.71
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-01 01:01:00 EST
Nmap scan report for 10.85.57.71
Host is up (0.0000ms latency).
All 65535 scanned ports on 10.85.57.71 are in ignored state.
Not shown: 65535 closed tcp ports (reset)
Service detection performed. Please report any interesting results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds
```

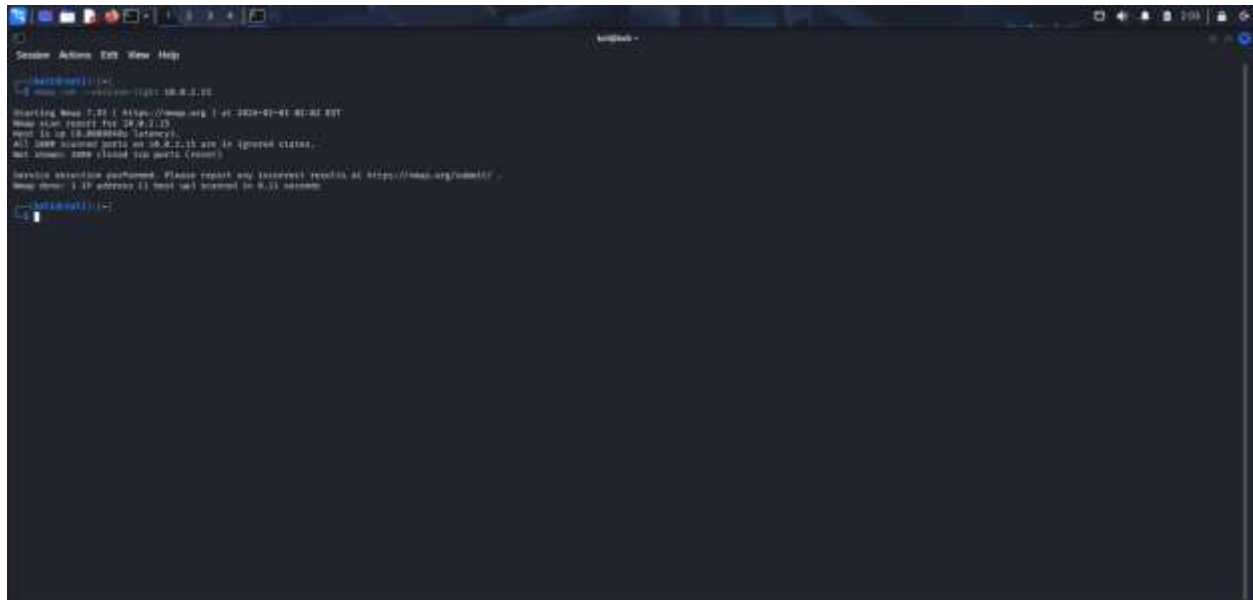
Explanation:

Detects running services and their version numbers.

## Light Version Detection

Command Used:

`nmap -sV --version-light 10.85.57.71`

A terminal window with a dark background and light blue text. The command `nmap -sV --version-light 10.85.57.71` has been executed. The output shows the Nmap version (7.80), the target IP (10.85.57.71), and the results of the version detection. It indicates that the target is up, the host is up, and the service is detected as `HTTP/1.1` with a version of `1.1`. The terminal window has a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. The status bar at the bottom shows 'nmap@kali: ~' and the time '10:00 AM 10/10/2023'.

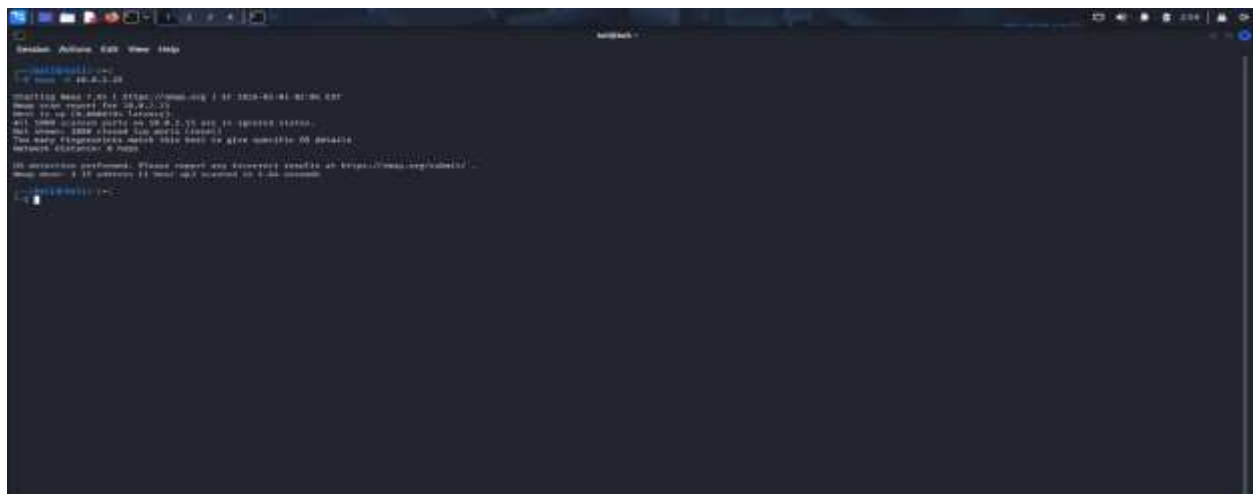
Explanation:

Performs faster service detection using fewer probes.

## OS Detection

Command Used:

`nmap -O 10.85.57.71`

A terminal window with a dark background and light blue text. The command `nmap -O 10.85.57.71` has been executed. The output shows the Nmap version (7.80), the target IP (10.85.57.71), and the results of the OS detection. It indicates that the target is up, the host is up, and the OS is detected as `Linux 3.10`. The terminal window has a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. The status bar at the bottom shows 'nmap@kali: ~' and the time '10:00 AM 10/10/2023'.

Explanation:

Identifies the operating system of the target machine.

## Aggressive OS Detection

Command Used:

`nmap -O --osscan-guess 10.85.57.71`



```
kali@kali:~$ nmap -O --osscan-guess 10.85.57.71
Starting Nmap 7.91 ( https://nmap.org ) at 2020-01-01 01:00:00 EST
Nmap scan target for 10.85.57.71
Host is up (0.0000000 latency).
All 65535 scanned ports on 10.85.57.71 are in ignored state.
Not shown: 65535 closed tcp ports (reset)
The Nmap engine left this host to give multiple OS details
Network Scan took 0.00s
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap scan of 10.85.57.71 took 0.00s scanned in 0.00 seconds
kali@kali:~$
```

Explanation:

Aggressively guesses the operating system when detection is difficult.

## Stealth Scan (SYN)

Command Used:

`nmap -sS 10.85.57.71`



```
kali@kali:~$ nmap -sS 10.85.57.71
Starting Nmap 7.91 ( https://nmap.org ) at 2020-01-01 01:00:00 EST
Nmap scan target for 10.85.57.71
Host is up (0.0000000 latency).
All 65535 scanned ports on 10.85.57.71 are in ignored state.
Not shown: 65535 closed tcp ports (reset)
Nmap scan of 10.85.57.71 took 0.00s scanned in 0.00 seconds
kali@kali:~$
```

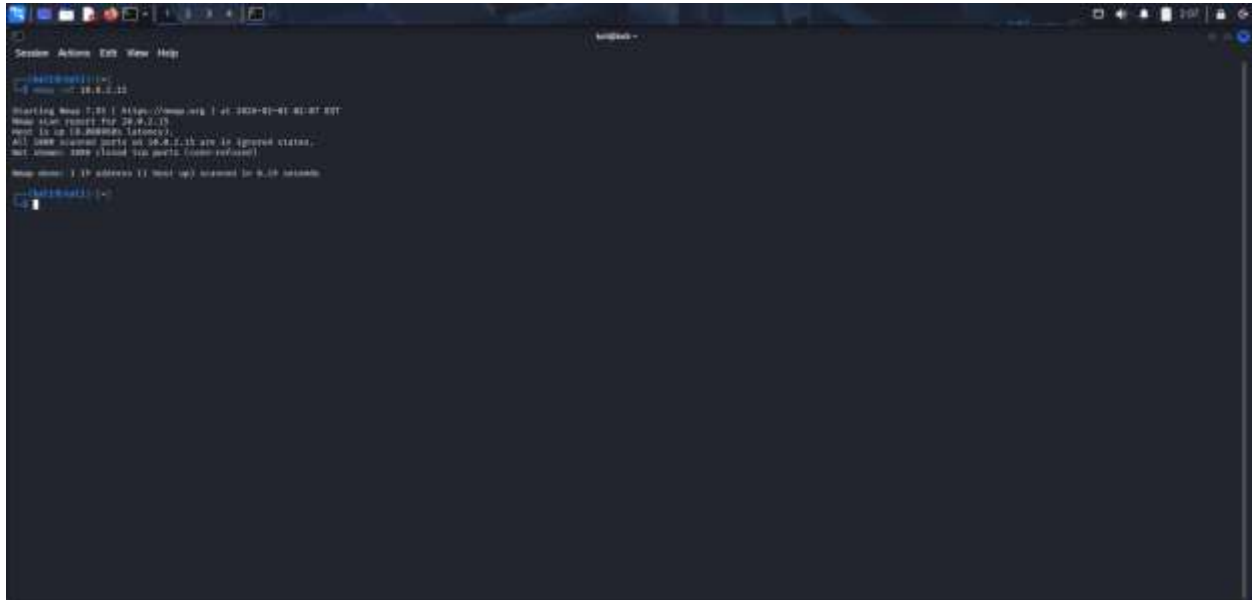
Explanation:

Performs a stealthy SYN scan to reduce detection.

## TCP Connect Scan

Command Used:

`nmap -sT 10.85.57.71`

A terminal window with a dark background and light blue text. The prompt is root@kali:~#. The command nmap -sT 10.85.57.71 has been executed. The output shows Nmap 7.91 starting on 2020-01-01 at 01:07:00 UTC, using the default configuration for 20.0.0.0. It reports that host 10.85.57.71 is up (SshOpen: 220.0.0.0). All 65535 scanned ports on 10.85.57.71 are in filtered state. No open ports (closed via port: 0.0.0.0) were found. The scan took 1.00 seconds. The prompt returns to root@kali:~#.

```

root@kali:~# nmap -sT 10.85.57.71
Starting Nmap 7.91 ( https://nmap.org ) at 2020-01-01 01:07:00 UTC
Using the default configuration for 20.0.0.0
Host 10.85.57.71 is up (SshOpen: 220.0.0.0).
All 65535 scanned ports on 10.85.57.71 are in filtered state.
No open ports (closed via port: 0.0.0.0) were found.
Nmap scan of 10.85.57.71 took 1.00 seconds in 1.00 seconds.
root@kali:~#

```

Explanation:

Uses full TCP connections to scan ports.

## UDP Scan

Command Used:

`nmap -sU 10.85.57.71`

A terminal window with a dark background and light blue text. The prompt is root@kali:~#. The command nmap -sU 10.85.57.71 has been executed. The output shows Nmap 7.91 starting on 2020-01-01 at 01:10:00 UTC, using the default configuration for 20.0.0.0. It reports that host 10.85.57.71 is up (SshOpen: 220.0.0.0). All 65535 scanned ports on 10.85.57.71 are in filtered state. No open ports (closed via port: 0.0.0.0) were found. The scan took 1.00 seconds. The prompt returns to root@kali:~#.

```

root@kali:~# nmap -sU 10.85.57.71
Starting Nmap 7.91 ( https://nmap.org ) at 2020-01-01 01:10:00 UTC
Using the default configuration for 20.0.0.0
Host 10.85.57.71 is up (SshOpen: 220.0.0.0).
All 65535 scanned ports on 10.85.57.71 are in filtered state.
No open ports (closed via port: 0.0.0.0) were found.
Nmap scan of 10.85.57.71 took 1.00 seconds in 1.00 seconds.
root@kali:~#

```

Explanation:

Scans UDP ports to identify UDP-based services.

## FIN Scan

Command Used:

```
nmap -sF 10.85.57.71
```

[illegible]

Explanation:

Uses FIN packets to bypass some firewall rules.

## NULL Scan

Command Used:

```
nmap -sN 10.85.57.71
```



The screenshot shows a terminal window titled "Terminal Emulator" with the following content:

```

root@kali:~# speedtest
Running Speed Test (C) Armin77/Speed.org 1 on 2020-01-06 00:16:55T
Speed test results for 20.0.0.19
Host 11 up (0 seconds latency)
net 10000 connect paths on 20.0.0.19 and 10 ignored states
net down: 10000 closed tcp ports (reset)

Slow down: 1.25 seconds (1 test up) achieved in 0.21 seconds

root@kali:~#

```

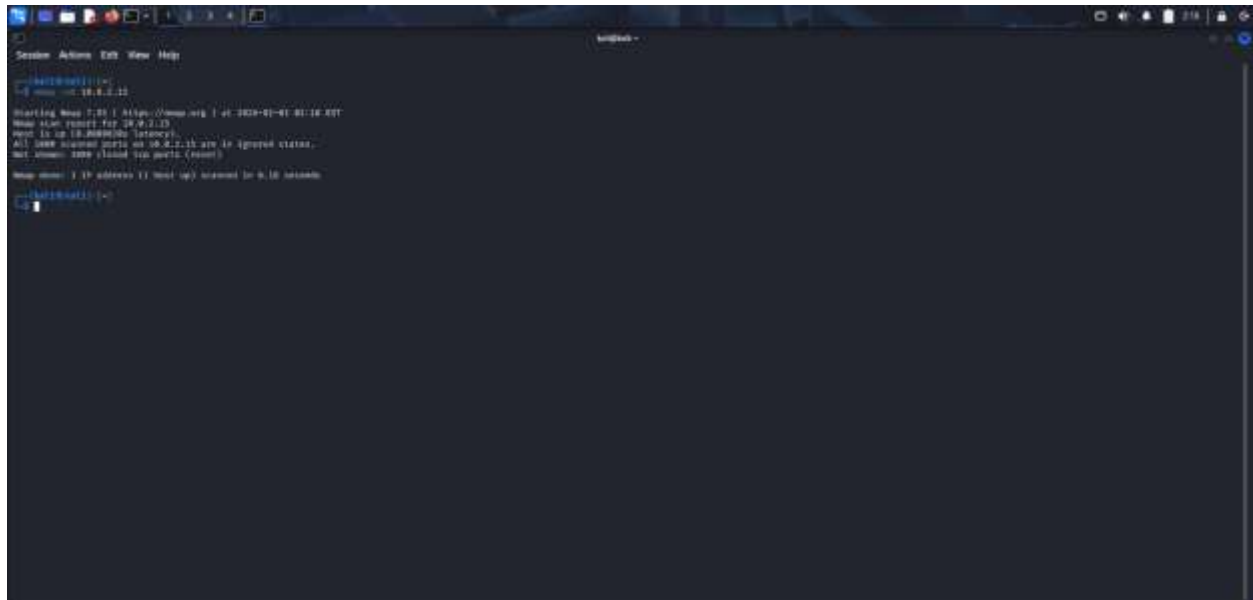
Explanation:

Sends packets with no TCP flags set.

## Xmas Scan

Command Used:

`nmap -sX 10.85.57.71`



```
Session Actions Edit View Help
kali@kali:~$ nmap -sX 10.85.57.71
Starting Nmap 7.91 ( https://nmap.org ) at 2020-01-01 01:18:00 PT
Nmap scan target for 10.85.57.71
Host is up (0.0000ms latency).
All 65535 scanned ports on 10.85.57.71 are in ignored states.
Nmap scan: 65535 closed tcp ports (reset)
Nmap scan: 1 IP address (1 host up) scanned in 6.16 seconds
kali@kali:~$
```

Explanation:

Sends packets with FIN, PSH, and URG flags enabled.

## Aggressive Scan

Command Used:

`nmap -A 10.85.57.71`



```
Session Actions Edit View Help
kali@kali:~$ nmap -A 10.85.57.71
Starting Nmap 7.91 ( https://nmap.org ) at 2020-01-01 01:19:00 PT
Nmap scan target for 10.85.57.71
Host is up (0.0000ms latency).
All 65535 scanned ports on 10.85.57.71 are in ignored states.
Nmap scan: 65535 closed tcp ports (reset)
The main program will skip this host to give priority to details
network discovery. 0 hosts
All port service detection performed. Please consult the https://nmap.org/xscans/
Nmap scan: 1 IP address (1 host up) scanned in 1.01 seconds
kali@kali:~$
```


Explanation:  
Performs OS detection, service detection, script scanning, and traceroute.

Performs OS detection, service detection, script scanning, and traceroute.

## Traceroute

Command Used:

```
nmap --traceroute 10.85.57.71
```



```

Session Actions Edit View Help
Kali Linux -
nmap -sS 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-01 01:31:01 UTC
Nmap scan report for 10.0.2.15
Host is up (0.0000ms latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed via port (reset)
Nmap scan: 1 IP address (1 host up) scanned in 0.13 seconds
nmap -sS 10.0.2.15

```

Explanation:

Displays the network path between scanner and target.

## Fragment Packet Scan

Command Used:

```
nmap -f 10.85.57.71
```

[illegible]

Explanation:

Fragments packets to evade firewall inspection.

## Decoy Scan

Command Used:

```
nmap -D RND:5 10.85.57.71
```



```
kali@kali:~$ nmap -D RND:5 10.85.57.71
Starting Nmap 7.91 ( https://nmap.org ) at 2020-06-01 01:20:01
Nmap scan results for 10.85.57.71:
Host is up (0.0000ms latency).
All 1000 scanned ports on 10.85.57.71 are in ignored states.
Host down: 1000 closed TCP ports (reset).
Nmap scan: 1 IP address (1 host up) scanned in 0.00 seconds
kali@kali:~$
```

Explanation:

Uses decoy IP addresses to hide the real scanning source.

## Spoof MAC Address

Command Used:

```
nmap --spoof-mac random 10.85.57.71
```



```
kali@kali:~$ nmap --spoof-mac random 10.85.57.71
Starting Nmap 7.91 ( https://nmap.org ) at 2020-06-01 01:20:01
Nmap scan results for 10.85.57.71:
Host is up (0.0000ms latency).
All 1000 scanned ports on 10.85.57.71 are in ignored states.
Host down: 1000 closed TCP ports (reset).
Nmap scan: 1 IP address (1 host up) scanned in 0.00 seconds
kali@kali:~$
```



Explanation:

Changes the MAC address of the scanning system.

## Default Script Scan

Command Used:

`nmap -sC 10.85.57.71`



```
kali@kali:~$ nmap -sC 10.85.57.71
Starting Nmap 7.95.1 (https://nmap.org) at 2020-05-01 01:06 EDT
Nmap scan target for 10.85.57.71
Nmap is up (0.0000000 latency).
All open scanned ports on 10.85.57.71 are in ignored state.
Nmap knows: 1000 closed tcp ports (reset).
Nmap knows: 1 IP address (1 host up) scanned in 0.12 seconds
kali@kali:~$
```

Explanation:

Runs default Nmap scripts for basic security checks.

## Vulnerability Scan

Command Used:

`nmap --script vuln 10.85.57.71`



```
kali@kali:~$ nmap --script vuln 10.85.57.71
Starting Nmap 7.95.1 (https://nmap.org) at 2020-05-01 01:17 EDT
Nmap scan target for 10.85.57.71
Nmap is up (0.0000000 latency).
All open scanned ports on 10.85.57.71 are in ignored state.
Nmap knows: 1000 closed tcp ports (reset).
Nmap knows: 1 IP address (1 host up) scanned in 0.12 seconds
kali@kali:~$
```

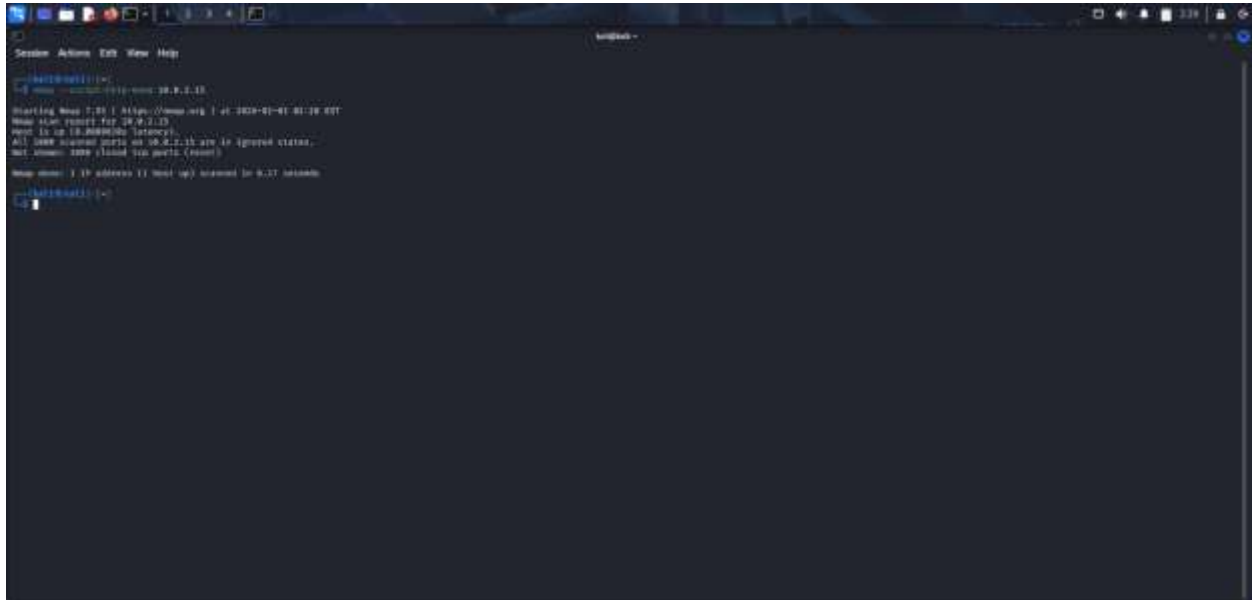
Explanation:

Scans the target for known vulnerabilities.

## Specific Script Scan

Command Used:

```
nmap --script http-title 10.85.57.71
```

A terminal window with a dark background and light blue text. The prompt is root@kali:~#. The command nmap --script http-title 10.85.57.71 has been entered and executed. The output shows Nmap version 7.80, the target IP 10.85.57.71, and the results of the http-title script, which found the title 'root@kali:~#'.

```
root@kali:~# nmap --script http-title 10.85.57.71
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-01 01:28:00
Nmap scan report for 10.85.57.71
Host is up (0.0000ms latency).
All 65535 scanned ports on 10.85.57.71 in ignored state.
Not shown: 65535 closed tcp ports (reset)
Nmap scan of IP address 10.85.57.71 scanned in 0.37 seconds
root@kali:~#
```

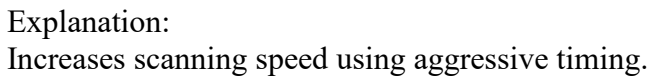
Explanation:

Runs a specific Nmap script on the target.

## Faster Timing Scan

Command Used:

```
nmap -T4 10.85.57.71
```



The scans produced valuable information about the target system.

- Target IP: 10.85.57.71
- Host Status: Active (Up)

- Port 22: SSH
- Port 80: HTTP (if applicable)

- SSH service running for remote access
- Web service running for HTTP communication

- The target system was identified as a Linux-based operating system (accuracy depends on scan results).

## 4.5 Device Identification

- The target device was identified as a network-connected system responding to standard network probes.

Screenshots of all commands and outputs were captured and included for verification.

---

## 5. SECURITY ANALYSIS

Network scanning provides insight into potential security risks. The following observations were made:

- Open ports can be exploited if unnecessary services are exposed.
- Services running outdated versions may contain known vulnerabilities.
- OS fingerprinting information can help attackers plan targeted attacks.

### Security Recommendations:

- Close unused ports using firewall rules.
  - Keep services updated with latest patches.
  - Implement intrusion detection and monitoring.
  - Restrict network access using access control policies.
- 

## 6. CONCLUSION

This internship project successfully demonstrated the use of Nmap for network scanning and reconnaissance. Through systematic scanning techniques, the project identified live hosts, open ports, running services, and operating system details.

The project provided practical exposure to real-world cybersecurity assessment techniques and highlighted the importance of securing network services. This experience enhanced understanding of how security professionals evaluate and protect network infrastructure.

---

## REFERENCES

1. Nmap Official Documentation
2. Kali Linux Documentation
3. VMware Workstation User Guide
4. Cybersecurity Network Scanning Best Practices