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

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.

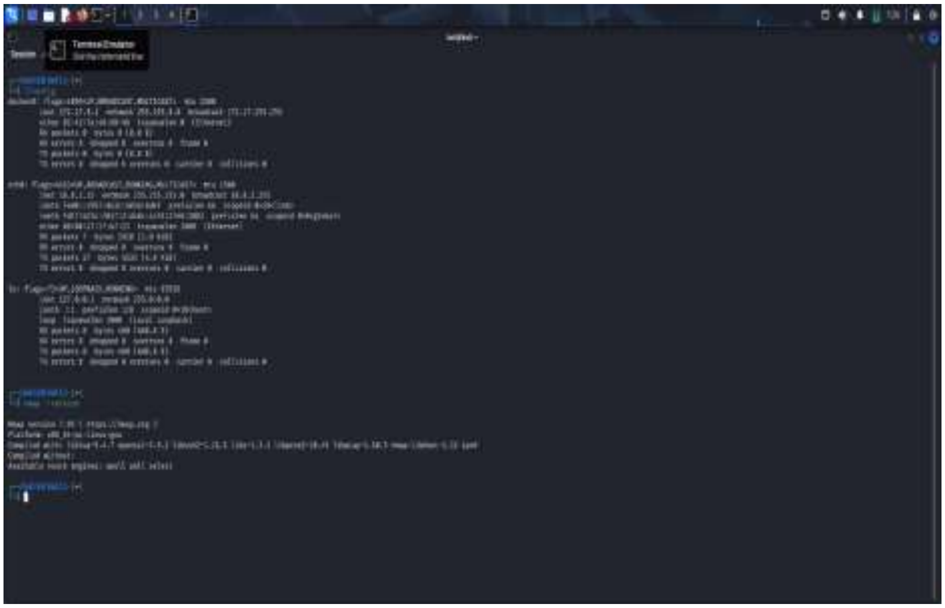
3.1 Environment Setup (Initial Stage)

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

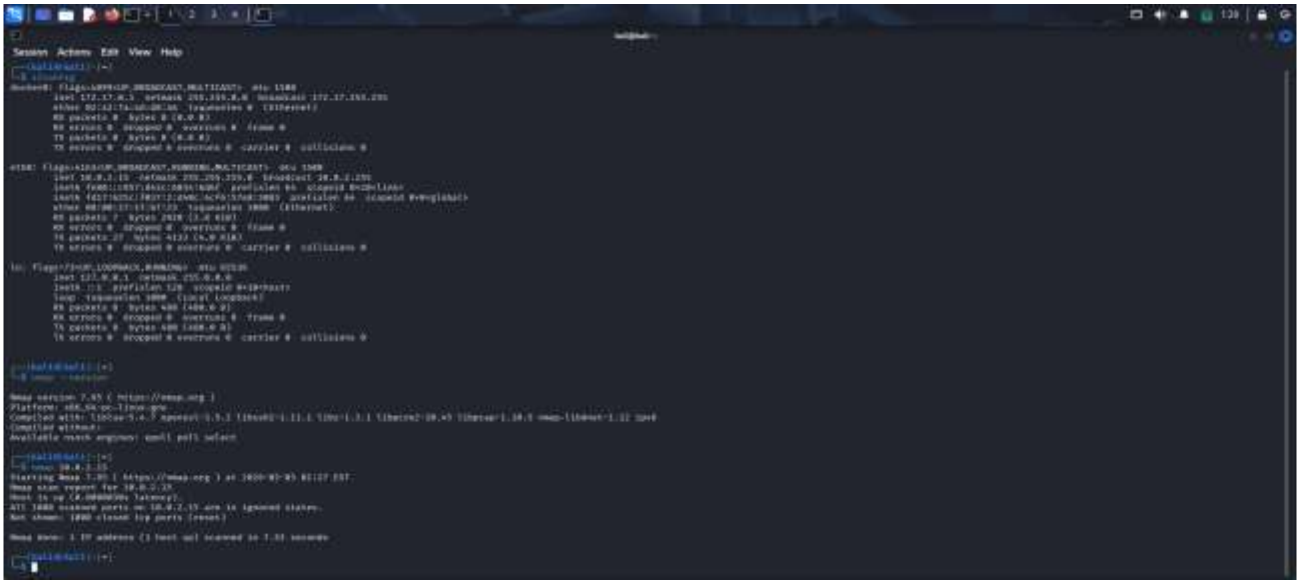


```
[illegible]

Nmap version [illegible] ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: [illegible]
Compiled without:
Available nsock engines: epoll poll select
```

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

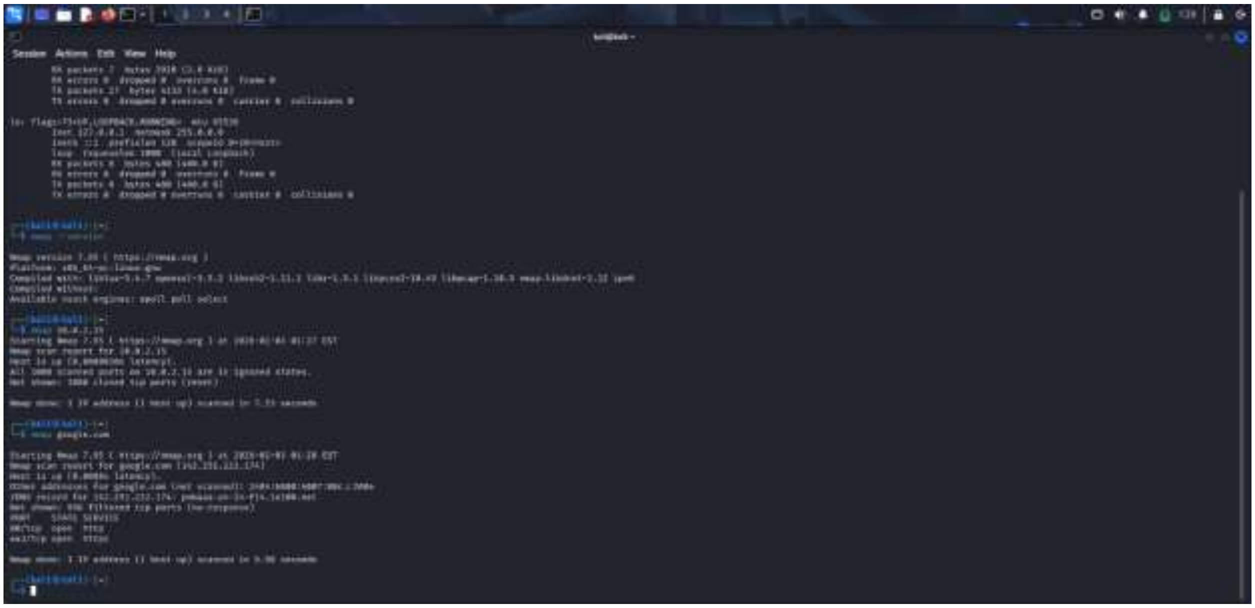


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:7a:[illegible]  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::[illegible]  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:[illegible]  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:[illegible]  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2028 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 4122 (4.0 KiB)
        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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ nmap --version

Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.2 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-05 01:27 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 7.33 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

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

Scan a Hostname

Command Used:
nmap example.com

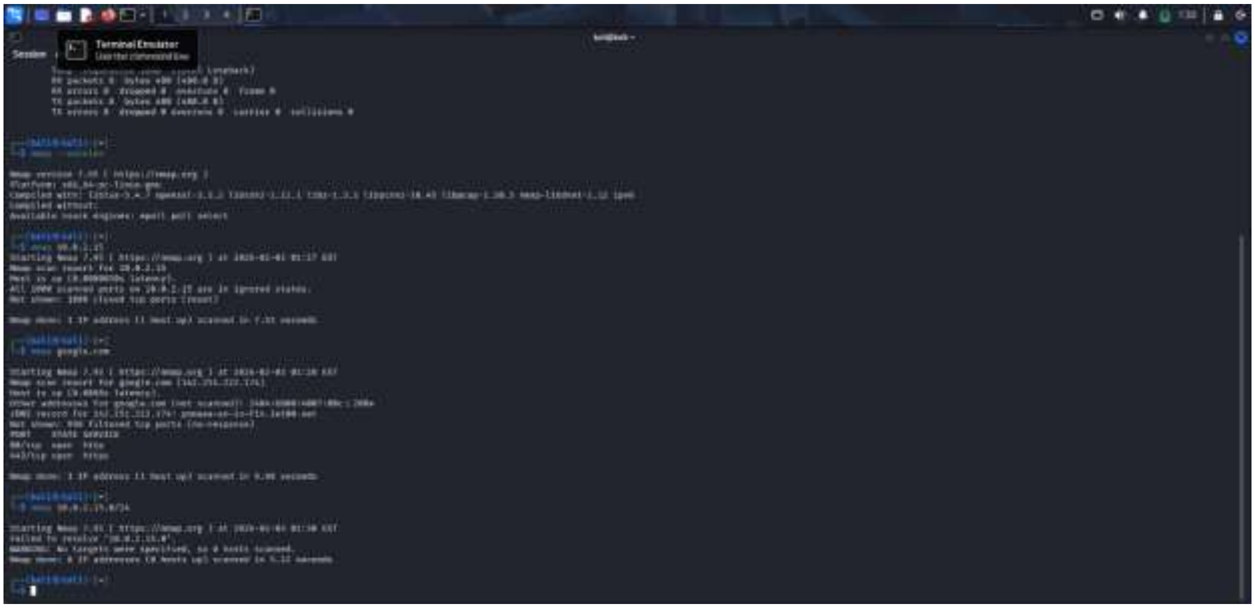


```
        RX packets 7  bytes 2028 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 4122 (4.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ nmap --version

Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.2 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-05 01:27 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 7.33 seconds

┌──(kali㉿kali)-[~]
└─$ nmap google.com

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-05 01:28 EST
Nmap scan report for google.com (142.251.222.174)
Host is up (0.0088s latency).
Other addresses for google.com (not scanned): 2404:6800:4007:80c::200e
rDNS record for 142.251.222.174: [illegible].1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.90 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

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

Scan Entire Network

Command Used:
nmap 10.85.57.0/24

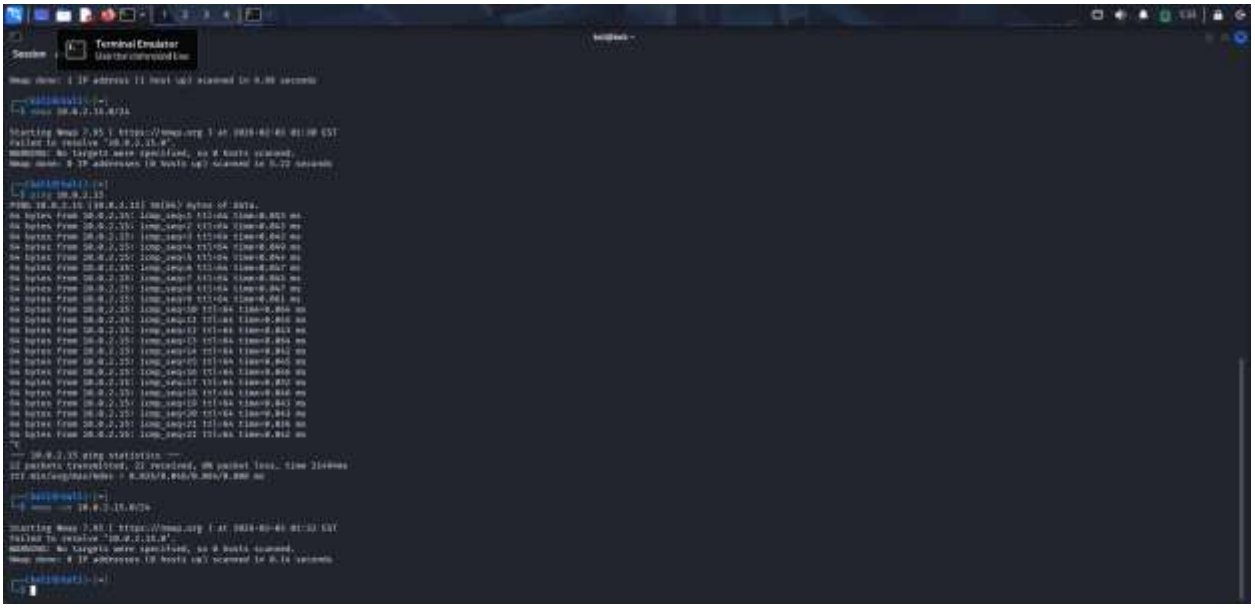


```
        [illegible] (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ nmap --version

Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.2 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:17 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 7.33 seconds

┌──(kali㉿kali)-[~]
└─$ nmap google.com

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:18 EST
Nmap scan report for google.com (142.251.222.174)
Host is up (0.0065s latency).
Other addresses for google.com (not scanned): 2404:6800:4007:80c::200e
rDNS record for 142.251.222.174: pnmaaa-aa-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:30 EST
Failed to resolve "10.0.2.15.0".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 5.12 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Explanation:
Scans all devices in the specified network range.

List Active Hosts

Command Used:
nmap -sn 10.85.57.0/24

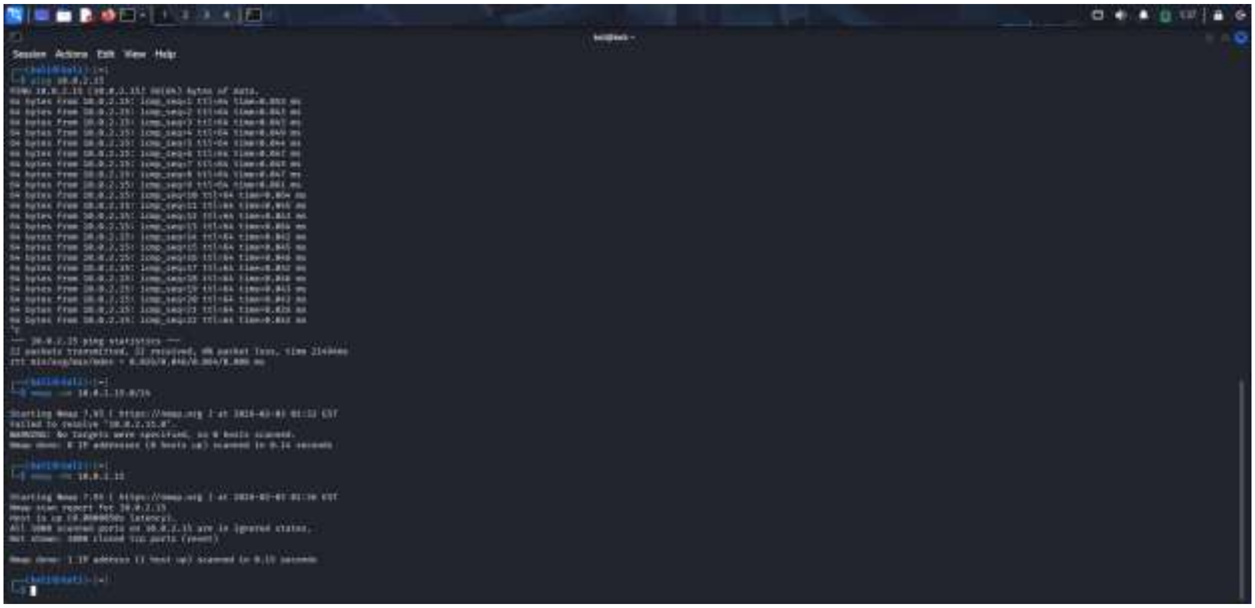


```
Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:30 EST
Failed to resolve "10.0.2.15.0".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 5.22 seconds

┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.042 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.049 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.044 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.047 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.043 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.047 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.061 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.044 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.055 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.013 ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=0.054 ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=0.042 ms
64 bytes from 10.0.2.15: icmp_seq=15 ttl=64 time=0.045 ms
64 bytes from 10.0.2.15: icmp_seq=16 ttl=64 time=0.046 ms
64 bytes from 10.0.2.15: icmp_seq=17 ttl=64 time=0.032 ms
64 bytes from 10.0.2.15: icmp_seq=18 ttl=64 time=0.044 ms
64 bytes from 10.0.2.15: icmp_seq=19 ttl=64 time=0.043 ms
64 bytes from 10.0.2.15: icmp_seq=20 ttl=64 time=0.043 ms
64 bytes from 10.0.2.15: icmp_seq=21 ttl=64 time=0.036 ms
64 bytes from 10.0.2.15: icmp_seq=22 ttl=64 time=0.042 ms
^C
--- 10.0.2.15 ping statistics ---
22 packets transmitted, 22 received, 0% packet loss, time 21494ms
rtt min/avg/max/mdev = 0.025/0.046/0.065/0.008 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.0.2.15.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:32 EST
Failed to resolve "10.0.2.15.0".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.16 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Explanation:
Lists only active hosts without performing port scanning.

Skip Host Discovery

Command Used:
nmap -Pn 10.85.57.71

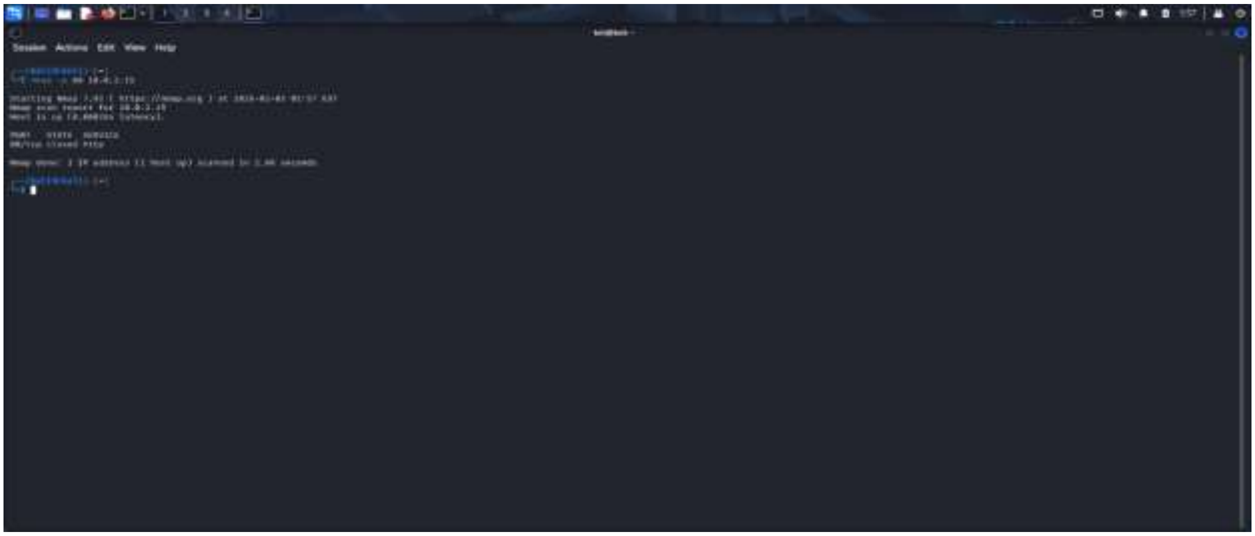


```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=15 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=16 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=17 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=18 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=19 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=20 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=21 ttl=64 time=[illegible] ms
64 bytes from 10.0.2.15: icmp_seq=22 ttl=64 time=[illegible] ms
^C
--- 10.0.2.15 ping statistics ---
22 packets transmitted, 22 received, 0% packet loss, time [illegible]ms
rtt min/avg/max/mdev = [illegible] ms

┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.0.2.15.0/24

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Failed to resolve "10.0.2.15.0".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible] latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$
```

Explanation:
Skips ping checks and assumes the target is online.

Scan Specific Port

Command Used:
nmap -p 80 10.85.57.71

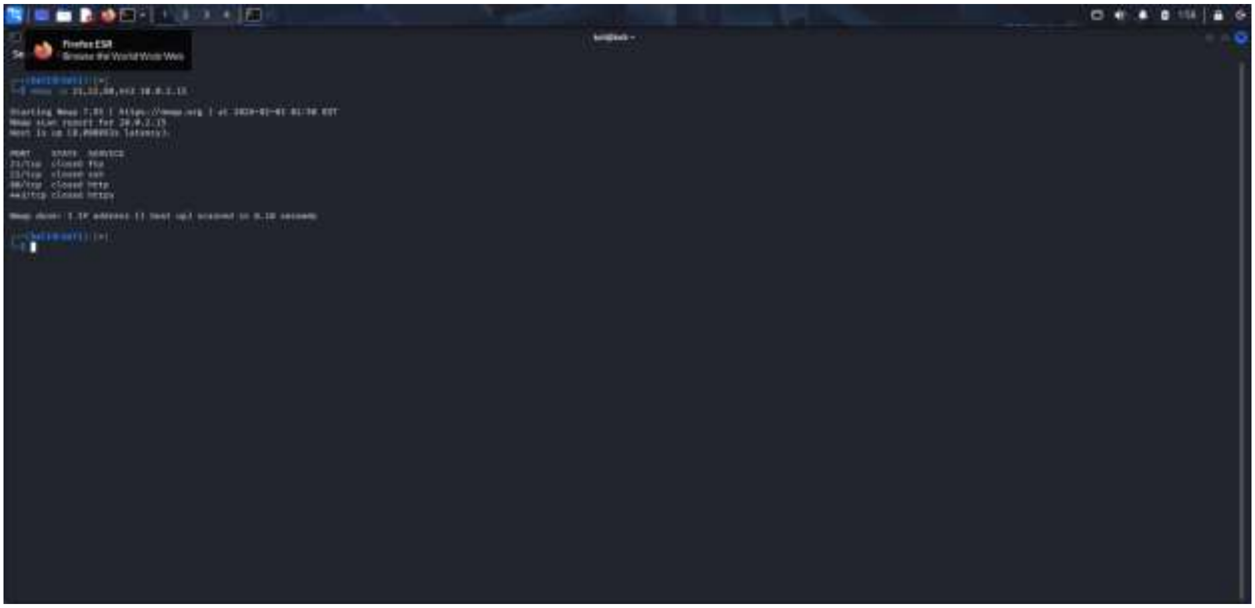


```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible] latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$
```

Explanation:
Scans a specific port on the target system.

Scan Multiple Ports

Command Used:
nmap -p 22,80,443 10.85.57.71

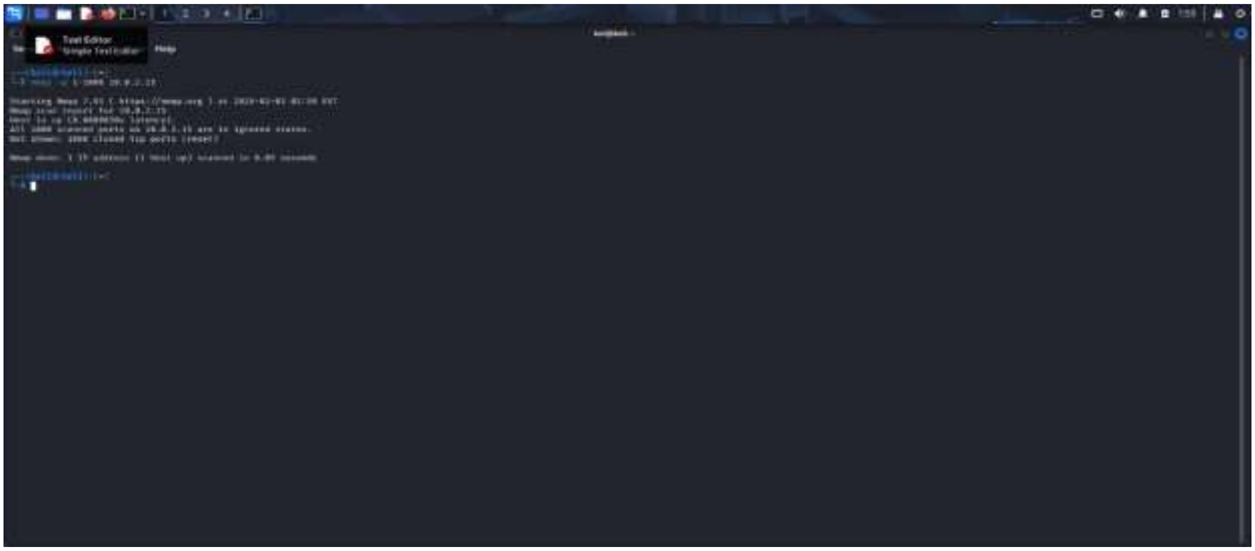


```
┌──(kali㉿kali)-[~]
└─$ nmap -p 21,22,80,443 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:50 EST
Nmap scan report for 10.0.2.15
Host is up (0.000053s latency).

PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  closed ssh
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds

┌──(kali㉿kali)-[~]
└─$
```

Explanation:
Scans multiple selected ports simultaneously.

Scan Port Range

Command Used:
nmap -p 1-1000 10.85.57.71

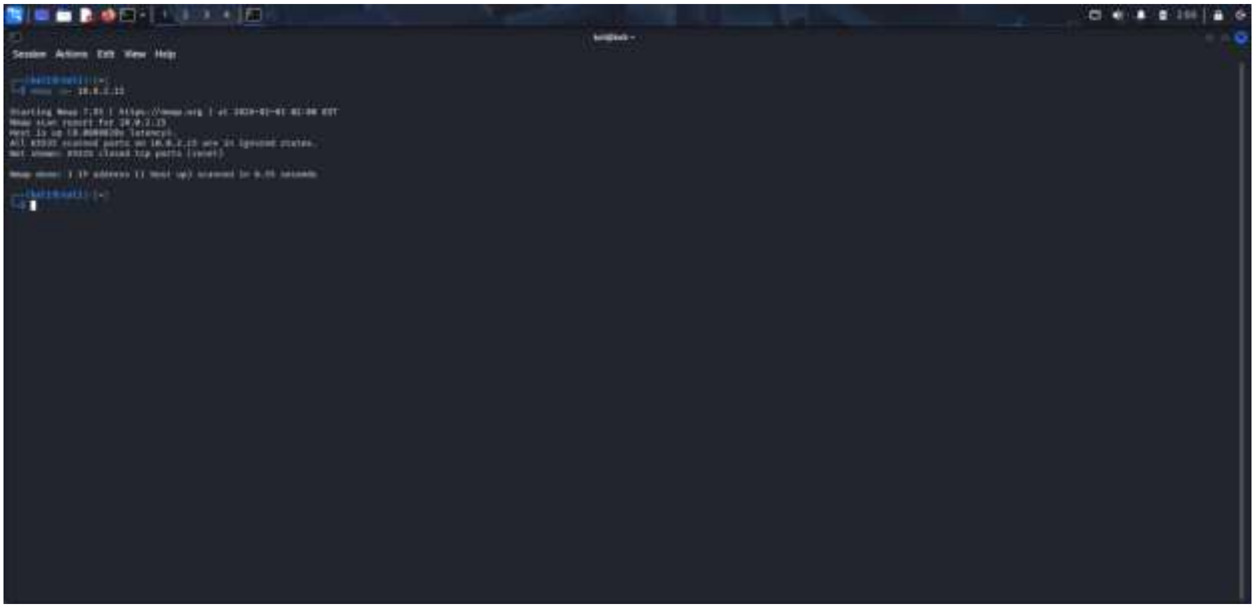


```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-1000 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:56 EST
Nmap scan report for 10.0.2.15
Host is up (0.000036s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds

┌──(kali㉿kali)-[~]
└─$
```

Explanation:
Scans a defined range of ports.

Scan All Ports

Command Used:
nmap -p- 10.85.57.71

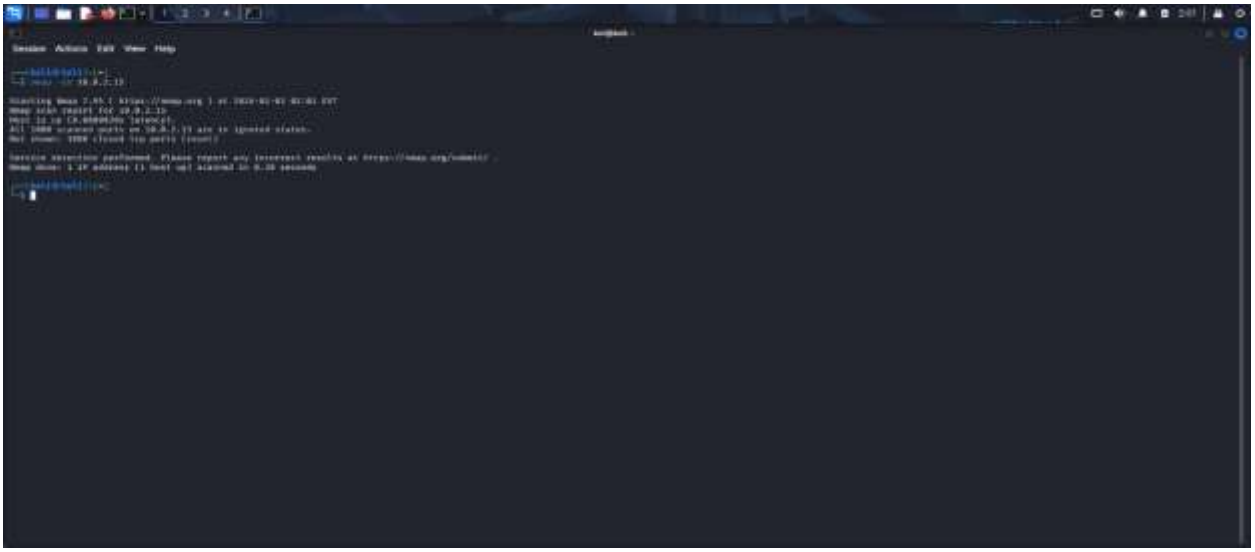


```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible]s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Scans all 65,535 TCP ports.

Detect Service Version

Command Used:
nmap -sV 10.85.57.71

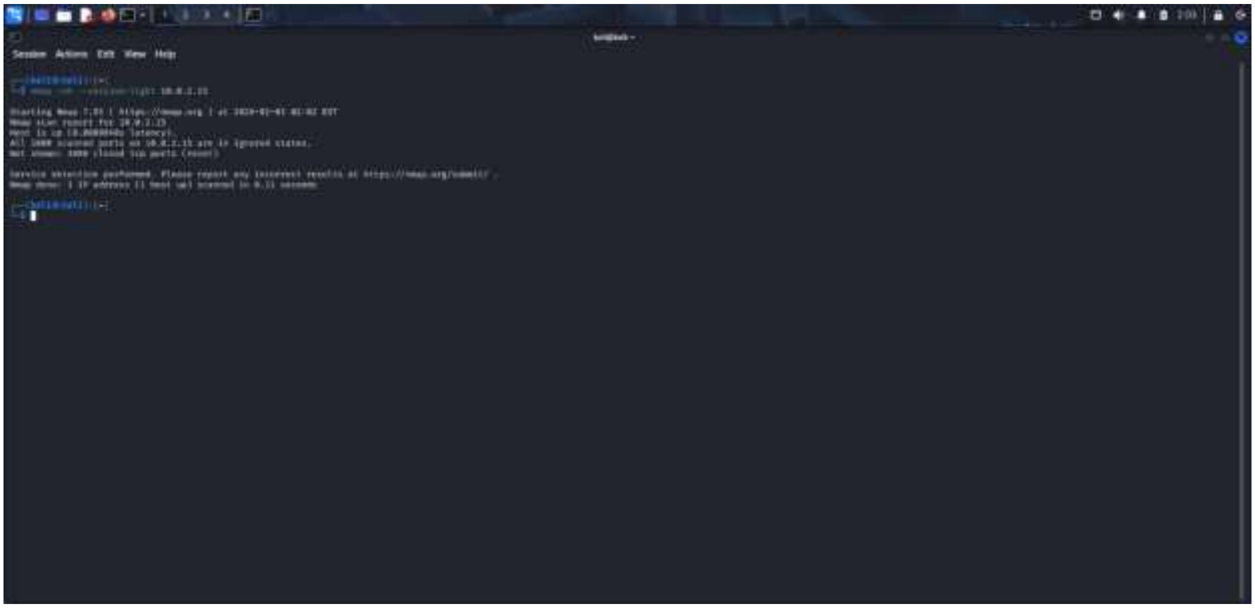


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible]s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Detects running services and their version numbers.

Light Version Detection

Command Used:
nmap -sV --version-light 10.85.57.71

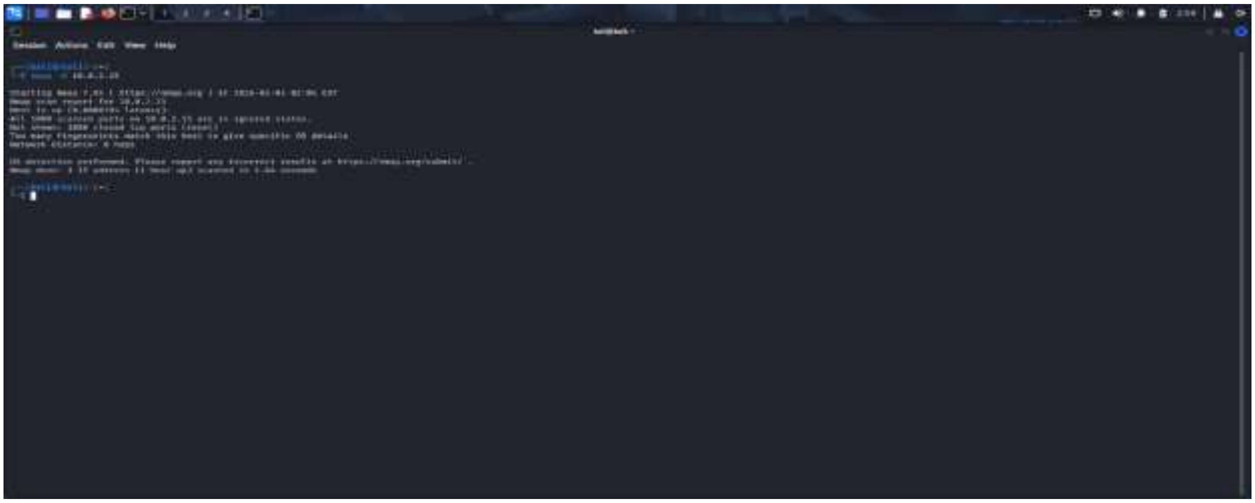


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --version-light 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up (0.000094s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Performs faster service detection using fewer probes.

OS Detection

Command Used:
nmap -O 10.85.57.71

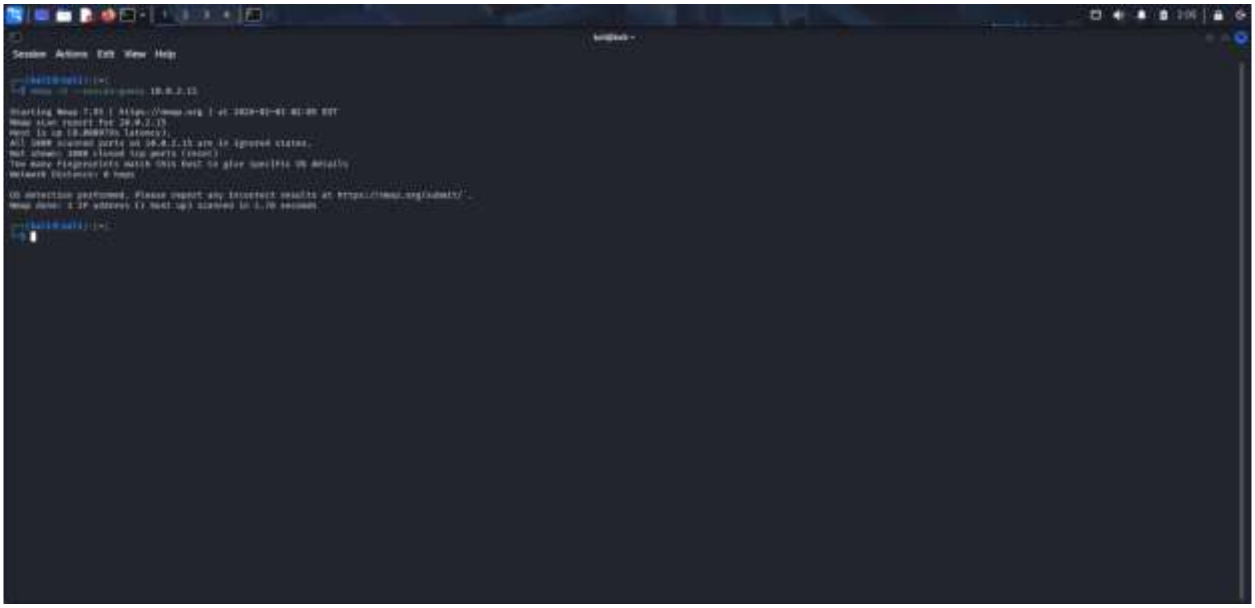


```
┌──(kali㉿kali)-[~]
└─$ nmap -O 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up (0.000070s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Identifies the operating system of the target machine.

Aggressive OS Detection

Command Used:
nmap -O --osscan-guess 10.85.57.71

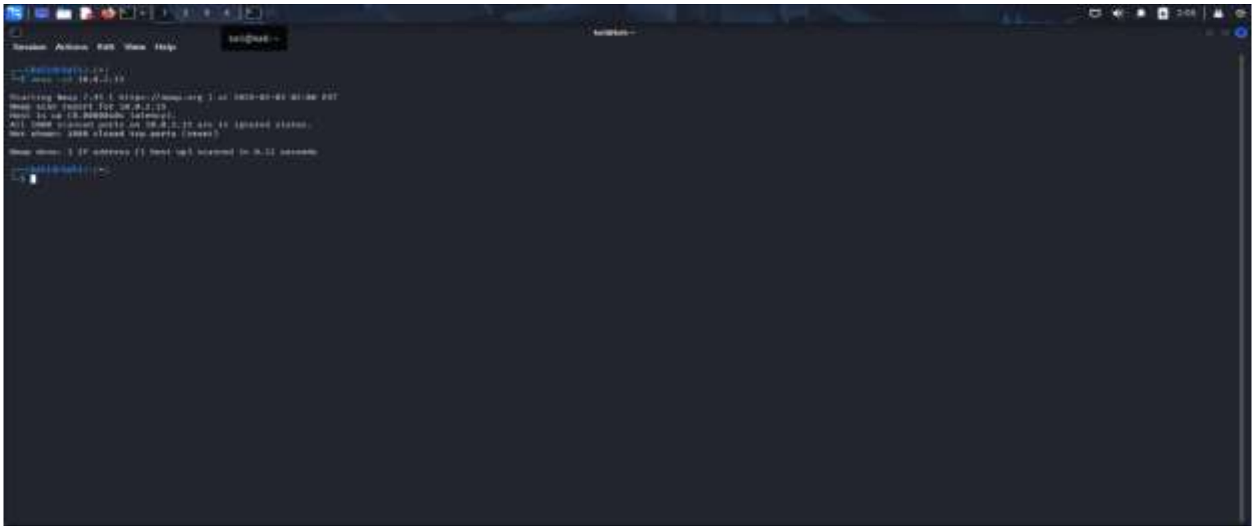


```
┌──(kali㉿kali)-[~]
└─$ nmap -O --osscan-guess 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible] latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds

┌──(kali㉿kali)-[~]
└─$
```

Explanation:
Aggressively guesses the operating system when detection is difficult.

Stealth Scan (SYN)

Command Used:
nmap -sS 10.85.57.71

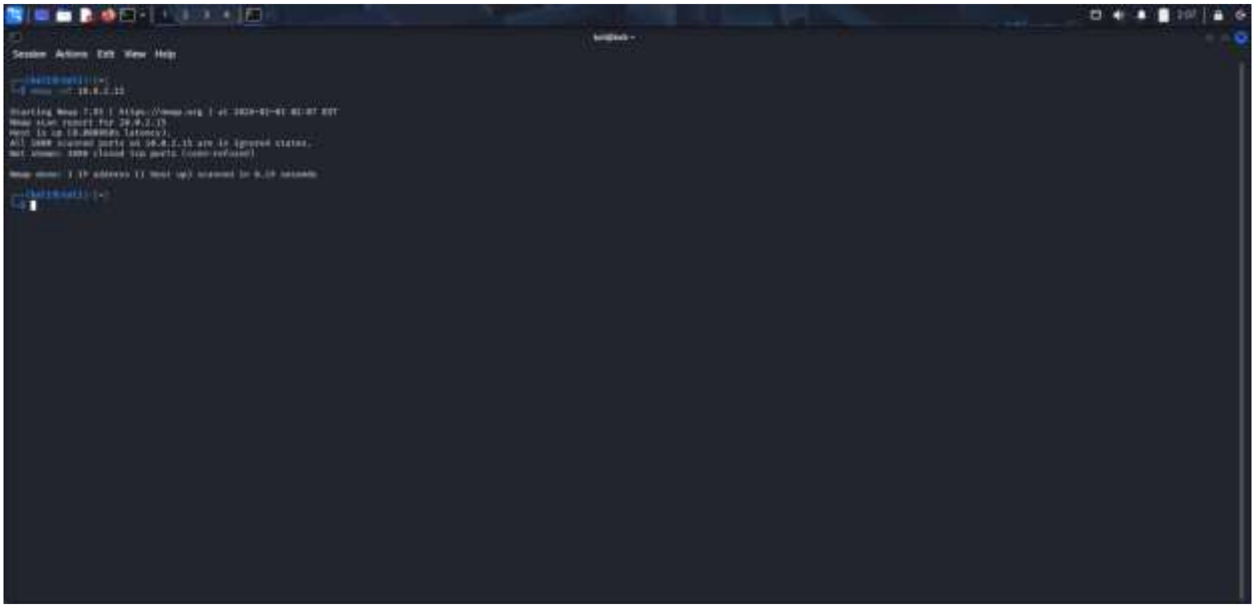


```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible] latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

┌──(kali㉿kali)-[~]
└─$
```

Explanation:
Performs a stealthy SYN scan to reduce detection.

TCP Connect Scan

Command Used:
nmap -sT 10.85.57.71

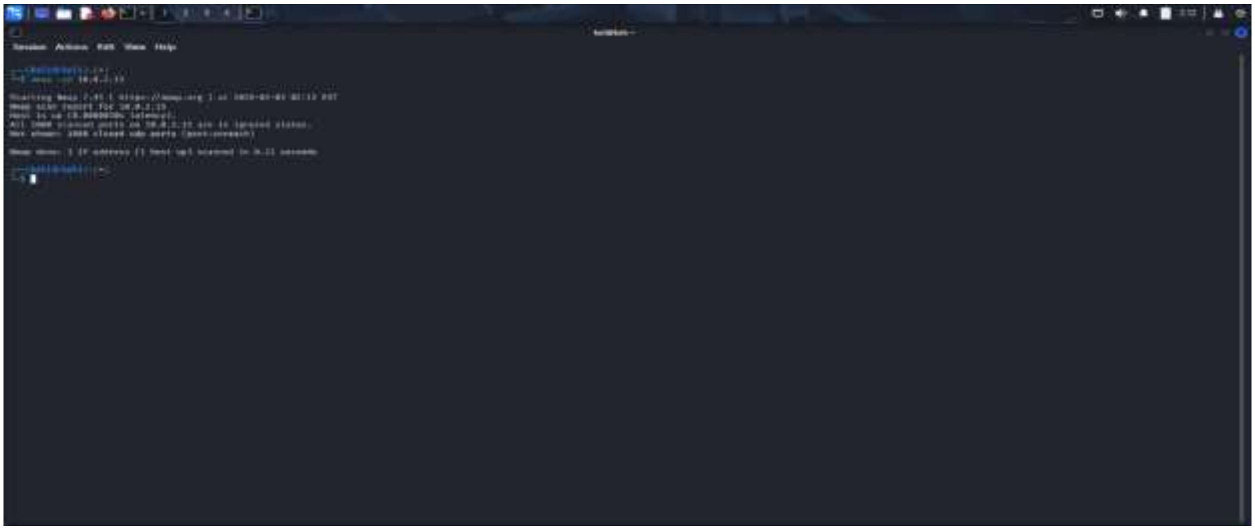


```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 02:07 EST
Nmap scan report for 10.0.2.15
Host is up (0.000050s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Uses full TCP connections to scan ports.

UDP Scan

Command Used:
nmap -sU 10.85.57.71

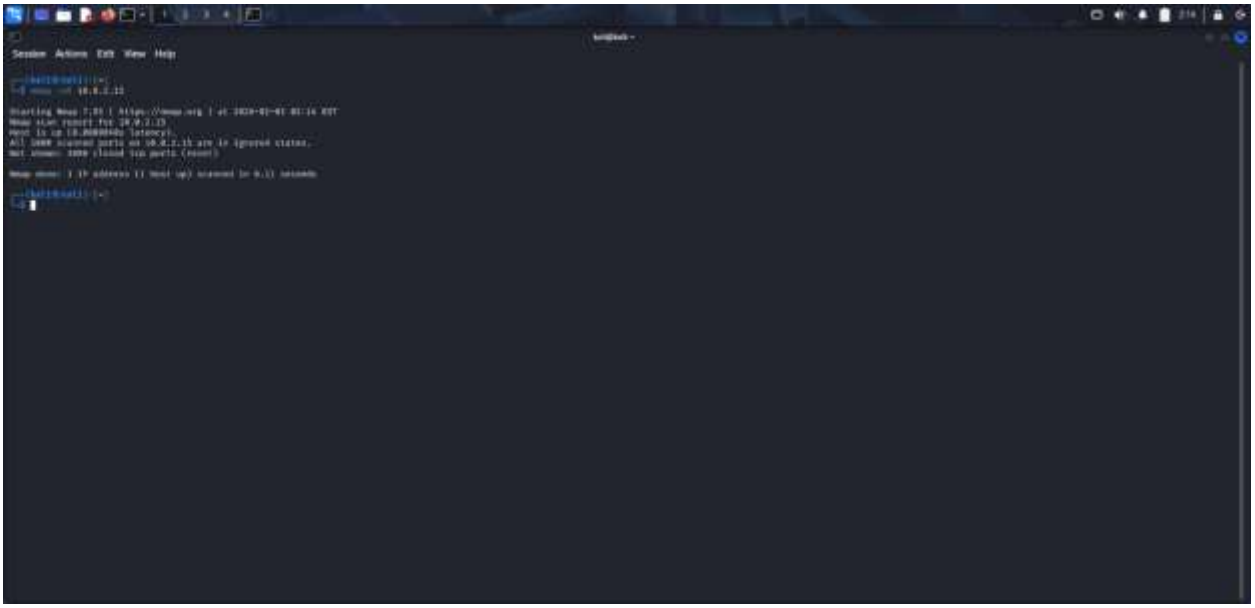


```
┌──(kali㉿kali)-[~]
└─$ nmap -sU 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 02:13 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Scans UDP ports to identify UDP-based services.

FIN Scan

Command Used:
nmap -sF 10.85.57.71

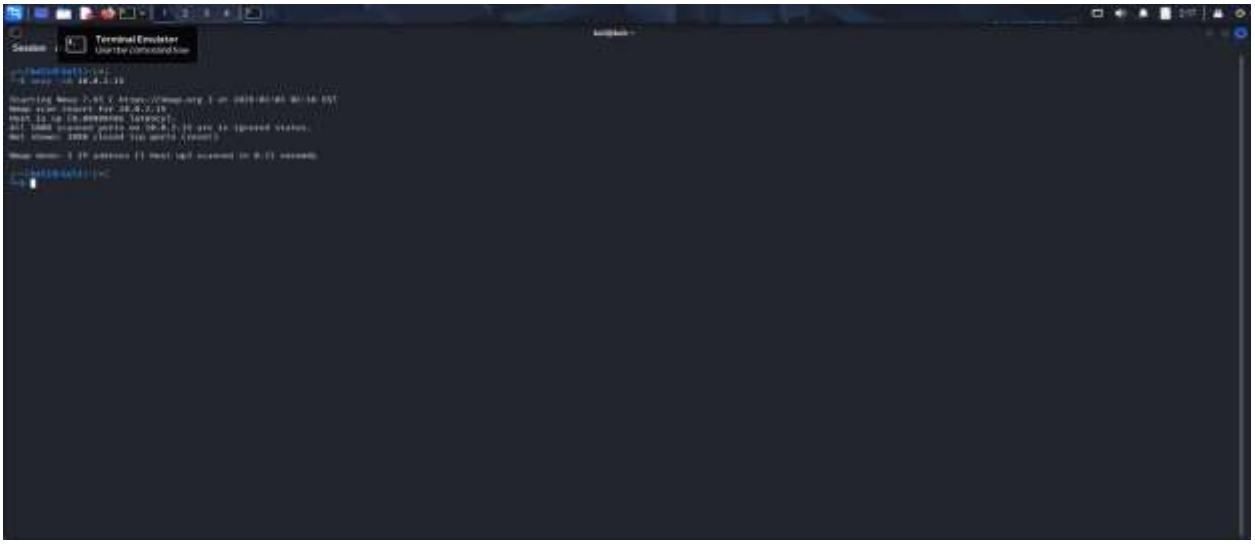


```
┌──(kali㉿kali)-[~]
└─$ nmap -sF 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:16 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Uses FIN packets to bypass some firewall rules.

NULL Scan

Command Used:
nmap -sN 10.85.57.71

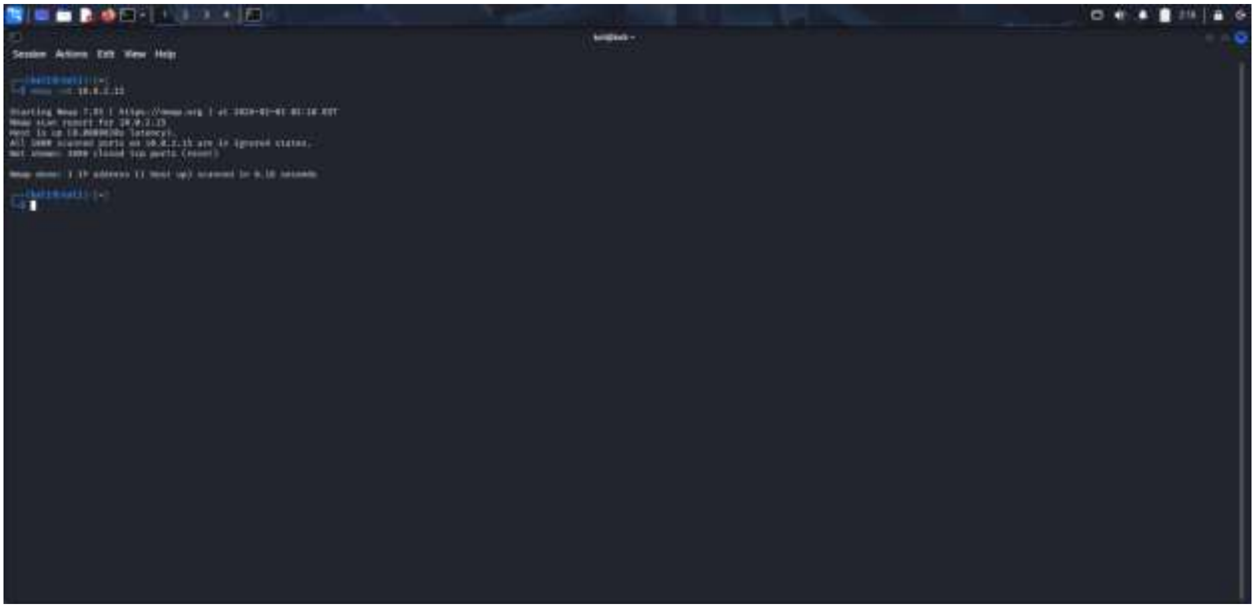


```
┌──(kali㉿kali)-[~]
└─$ nmap -sN 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 01:16 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Sends packets with no TCP flags set.

Xmas Scan

Command Used:
nmap -sX 10.85.57.71

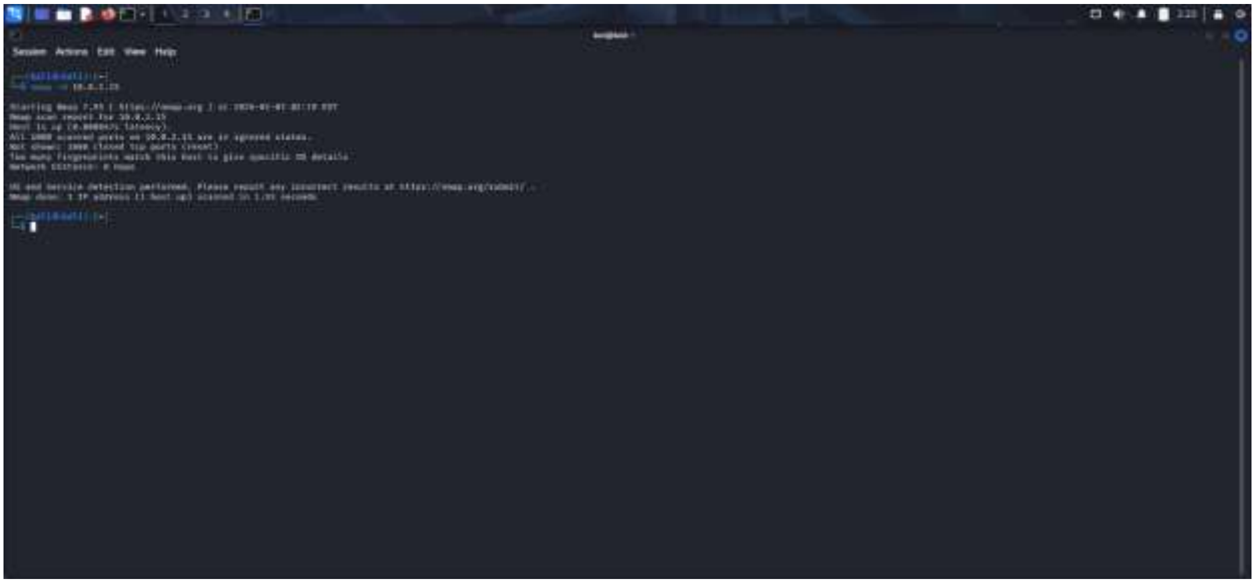


```
┌──(kali㉿kali)-[~]
└─$ nmap -sX 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible] latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$ 
```

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

Aggressive Scan

Command Used:
nmap -A 10.85.57.71

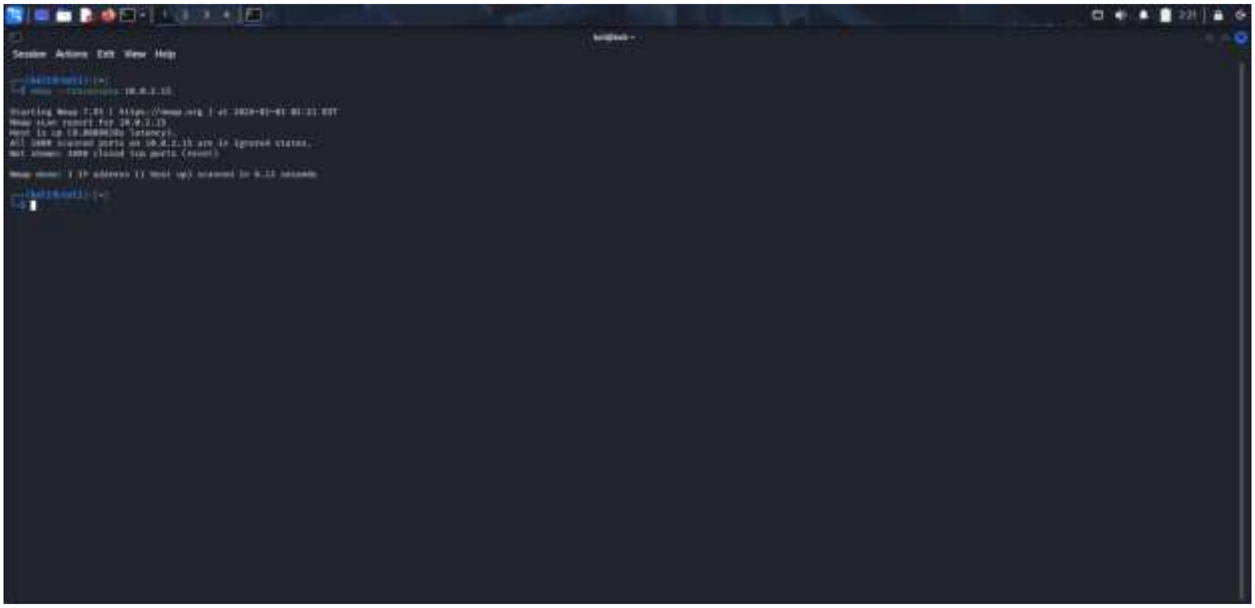


```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible] latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

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

┌──(kali㉿kali)-[~]
└─$ 
```

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

Traceroute

Command Used:
nmap --traceroute 10.85.57.71

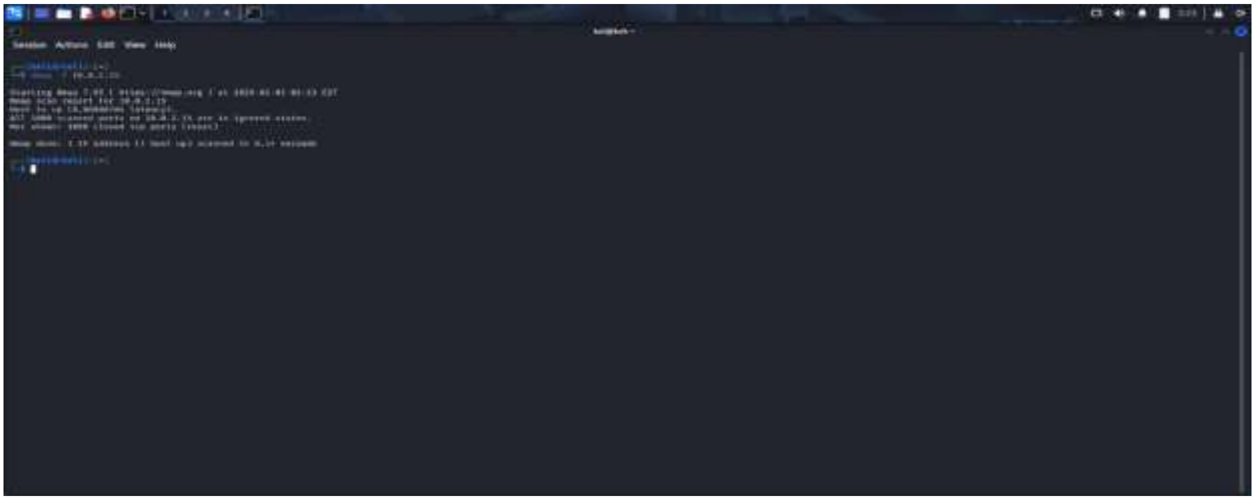


```
┌──(kali㉿kali)-[~]
└─$ nmap --traceroute 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible]s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Displays the network path between scanner and target.

Fragment Packet Scan

Command Used:
nmap -f 10.85.57.71

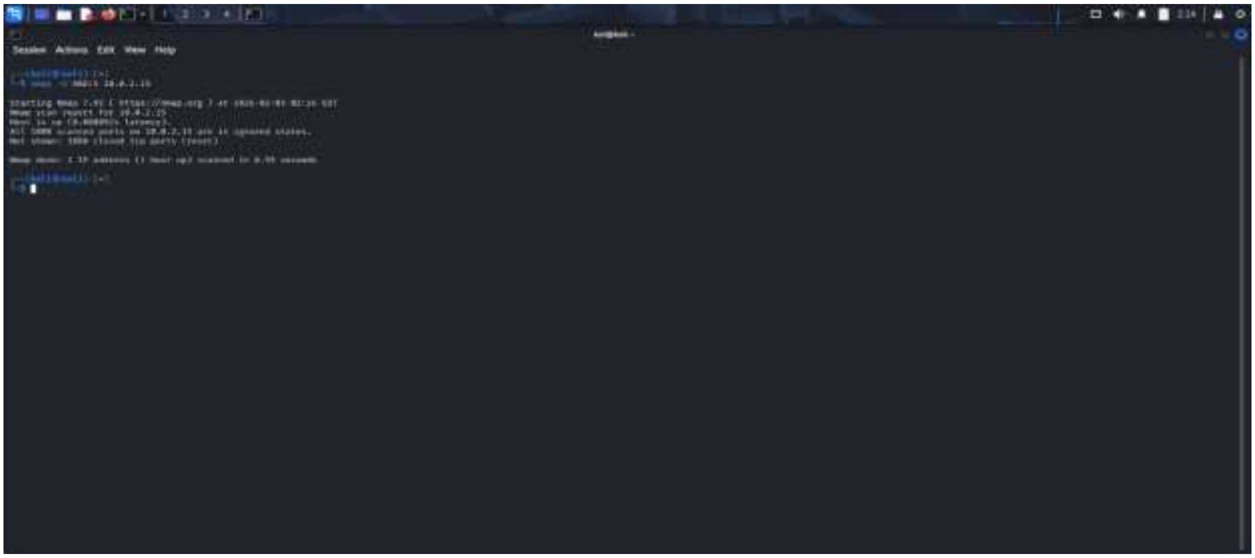


```
┌──(kali㉿kali)-[~]
└─$ nmap -f 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible]s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Fragments packets to evade firewall inspection.

Decoy Scan

Command Used:
nmap -D RND:5 10.85.57.71

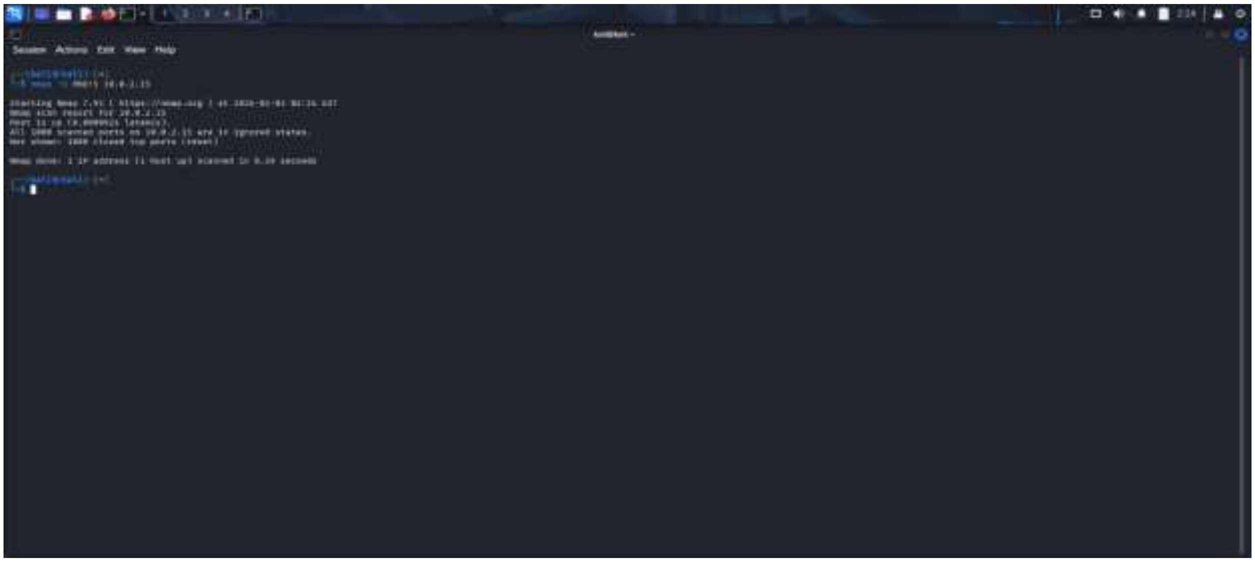


```
[illegible]
└─$ nmap [illegible] 10.0.2.15

Starting Nmap 7.9[illegible] ( https://nmap.org ) at 2026-0[illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible] latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

[illegible]
└─$
```

Explanation:
Uses decoy IP addresses to hide the real scanning source.

Spoof MAC Address

Command Used:
nmap --spoof-mac random 10.85.57.71

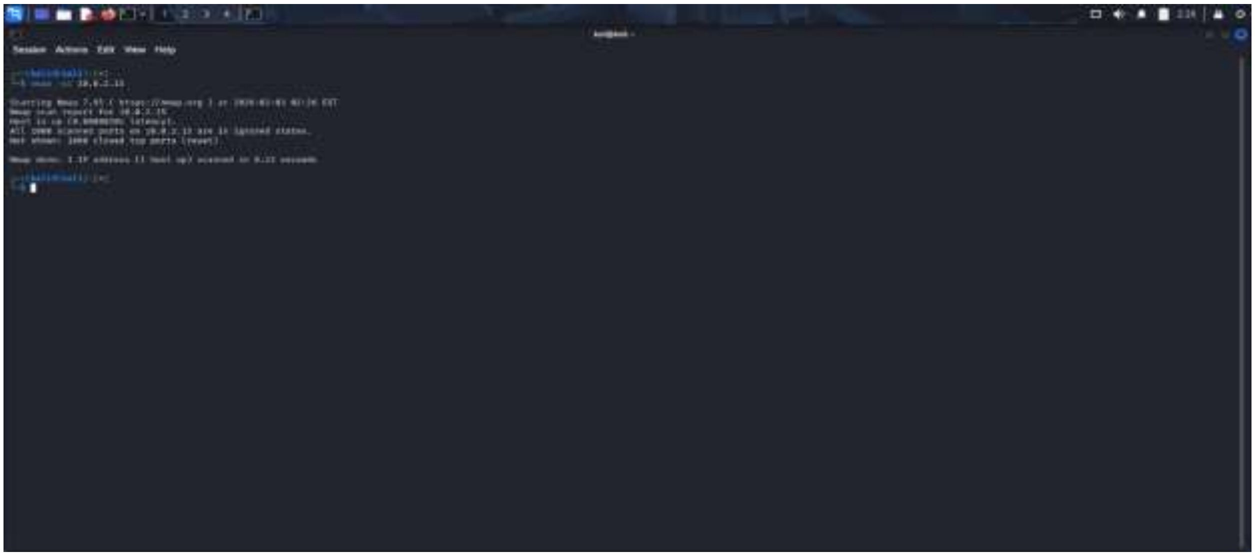


```
[illegible]
└─$ nmap [illegible] 10.0.2.15

Starting Nmap 7.9[illegible] ( https://nmap.org ) at 2026-0[illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible] latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

[illegible]
└─$
```

Explanation:
Changes the MAC address of the scanning system.

Default Script Scan

Command Used:
nmap -sC 10.85.57.71

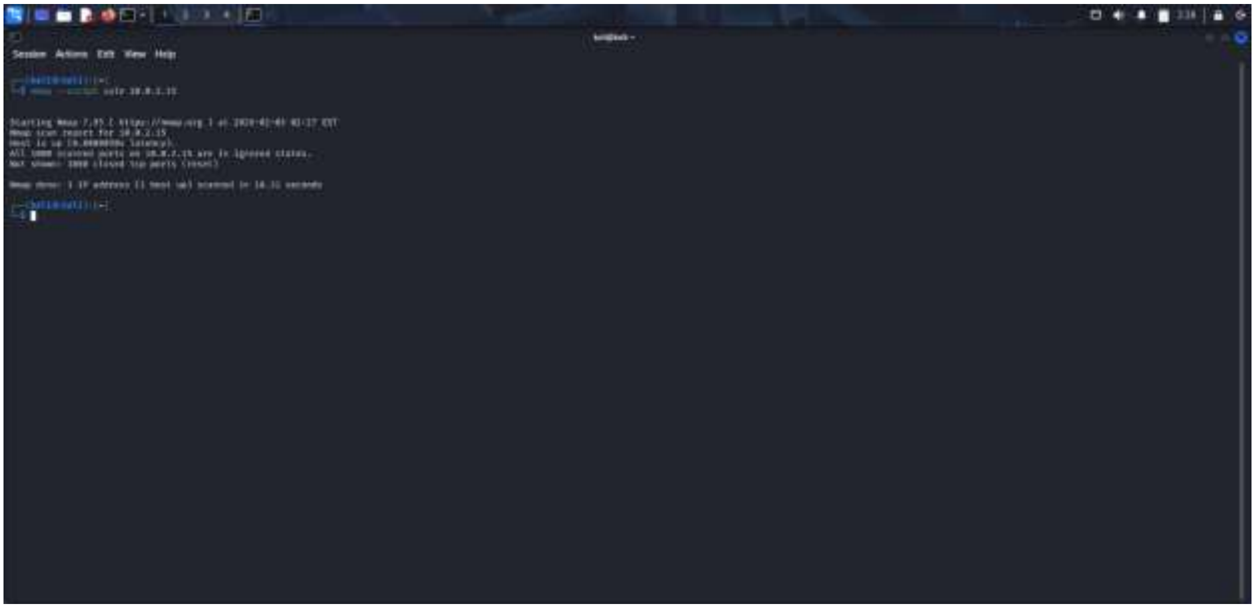


```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible]s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$
```

Explanation:
Runs default Nmap scripts for basic security checks.

Vulnerability Scan

Command Used:
nmap --script vuln 10.85.57.71

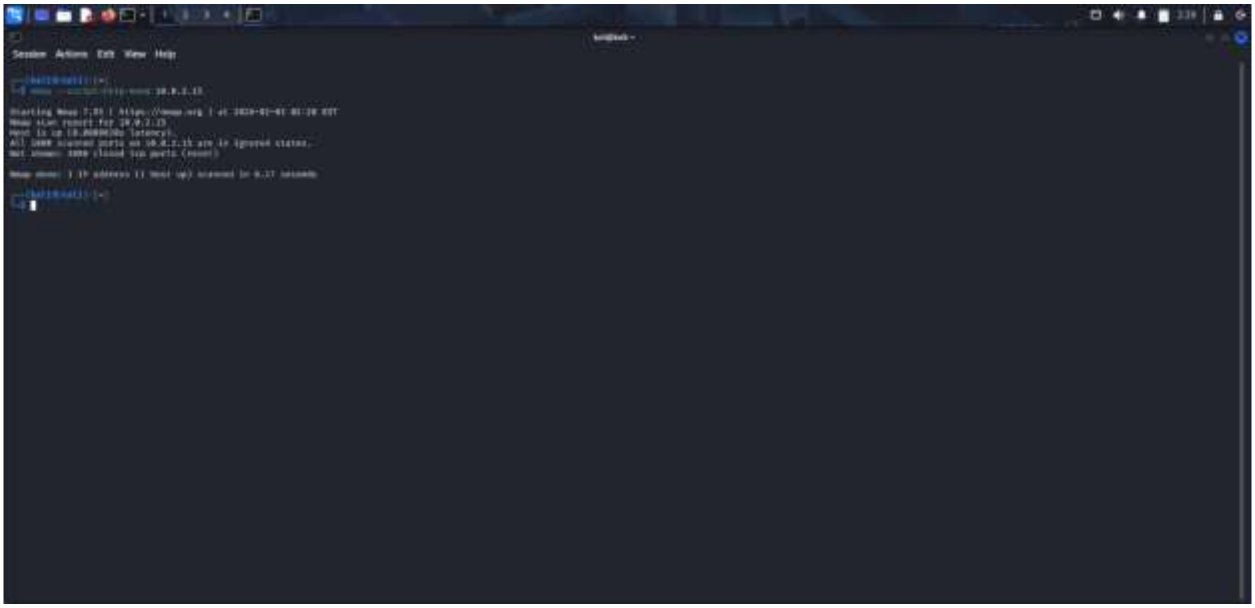


```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up ([illegible]s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$
```

Explanation:
Scans the target for known vulnerabilities.

Specific Script Scan

Command Used:
nmap --script http-title 10.85.57.71

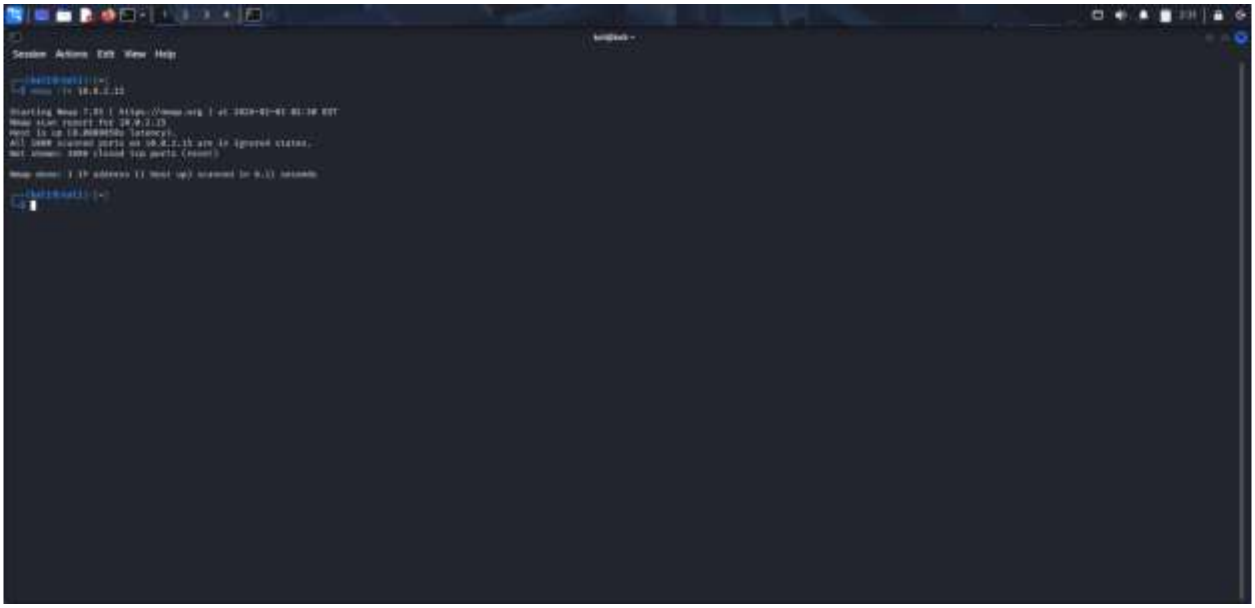


```
┌──(kali㉿kali)-[~]
└─$ nmap --script [illegible] 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at 2024-02-01 01:28 EST
Nmap scan report for 10.0.2.15
Host is up (0.000063s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Runs a specific Nmap script on the target.

Faster Timing Scan

Command Used:
nmap -T4 10.85.57.71



```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 10.0.2.15

Starting Nmap 7.9[illegible] ( https://nmap.org ) at [illegible] EST
Nmap scan report for 10.0.2.15
Host is up (0.000065s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Explanation:
Increases scanning speed using aggressive timing.

---

4. SCAN RESULTS

The scans produced valuable information about the target system.

4.1 Host Status

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

4.2 Open Ports Identified

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

4.3 Services Detected

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

4.4 Operating System

- 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