SOMAIYA
VIDYAVIHAR UNIVERSITY

Nmap(Network Mapper)

Submitted By

Qusai Sakerwala

16010122231

Himanshu Garg

16010122238

Ayush Nayak

16010122243

Mourvi Joshi

16010122279

Guide

Zaheed Shaikh

Department of Computer Engineering

Contents:

Introduction……………………………………………………………………………..	iii
Features/Characteristics…………………………………………………………………	iv
Methodology………………………………………………………………………...….	v
Results…………………………………………………………………………………..	v
Conclusion………………………………………………………………………………	xiv
References …………………………………………………………………………...	xiv

Introduction

Nmap (Network Mapper) stands as a quintessential tool in the arsenal of network administrators and cybersecurity professionals due to its extensive capabilities in network exploration and security auditing. Originally created by Gordon Lyon (Fyodor) in 1997, Nmap was designed to provide a comprehensive and efficient means of scanning large and complex networks to gather critical information. Today, it has evolved into a widely utilized open-source utility that helps individuals and organizations enhance their security posture by detecting vulnerabilities, unauthorized devices, and potential points of attack.

At its core, Nmap is used to discover devices connected to a network, map out the network topology, and uncover key details about the devices, such as their IP addresses, open ports, running services, and even operating system types. These capabilities allow network administrators to maintain control over their infrastructure, while also giving security experts a tool to identify weak spots that malicious actors could exploit. Nmap's utility is not confined to basic network discovery; it is also extensively used for security assessments, vulnerability scanning, and penetration testing.

What sets Nmap apart is its flexibility. Whether performing simple ping sweeps or advanced penetration testing, Nmap can adapt to various scanning needs through its diverse set of features, such as OS fingerprinting, service version detection, and customizable scriptable functionality. This adaptability has made Nmap a go-to tool for security professionals engaged in ethical hacking and cybersecurity assessments, as it offers a deep level of insight into a system's security posture without requiring proprietary or expensive solutions.

The ongoing development of Nmap by an active open-source community ensures that it remains a cutting-edge tool, constantly evolving to address new security challenges. With Nmap, cybersecurity experts can proactively uncover network flaws, monitor for new vulnerabilities, and conduct thorough assessments, making it an indispensable resource in the world of network security and penetration testing. Its widespread use across industries underscores the essential role it plays in safeguarding digital infrastructures against emerging threats and ensuring network resilience.

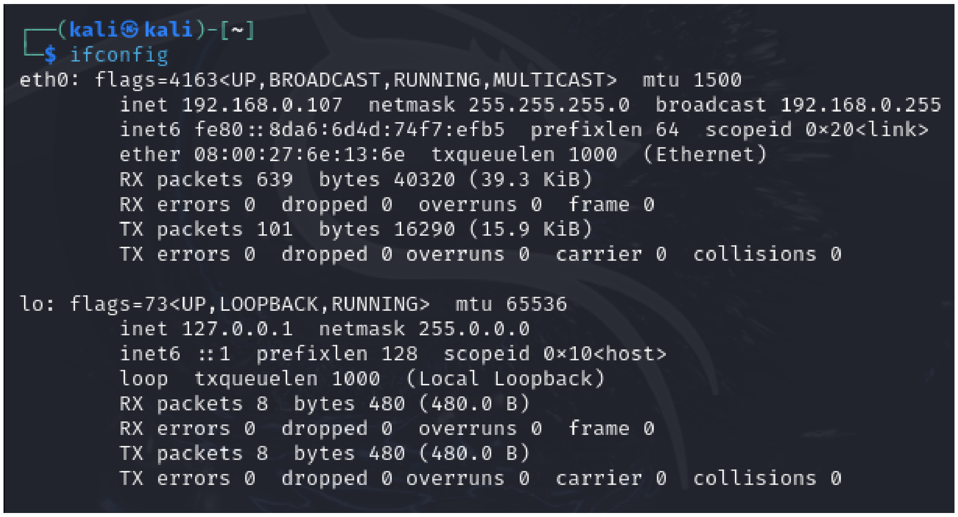
Features/Characteristics

1. **Host Discovery**: Nmap efficiently identifies active devices on a network by sending ICMP (ping) requests or using other methods to determine which systems are live. This is a fundamental first step in network analysis, especially when managing large networks or performing penetration tests.
2. **Port Scanning**: One of the core functions of Nmap is its ability to detect open ports on a device. These ports are crucial points of communication, and discovering which ones are open helps security professionals assess the potential entry points for attackers. Nmap supports various scanning techniques to perform thorough port scans, including TCP, UDP, and SCTP scanning.
3. **Service and Version Detection**: Nmap goes beyond simple port scanning by identifying the specific services running on open ports and their versions. This is particularly useful for identifying outdated or vulnerable software, enabling security experts to address potential risks by updating or patching the services accordingly.
4. **OS Detection**: Using TCP/IP fingerprinting, Nmap can determine the operating system running on a target device. This feature allows security professionals to tailor their scans based on the operating system, as different OSes have varying vulnerabilities. OS detection provides valuable insights into the system's architecture and its susceptibility to specific attacks.
5. **Security Auditing**: Nmap is widely used for security auditing purposes, where it helps to identify vulnerabilities within a network, devices, and applications. This is crucial for spotting misconfigurations, identifying unauthorized access points, or testing the strength of firewall rules to ensure they are properly configured to protect the network from malicious threats.
6. **Stealth Scanning**: Nmap offers several scanning methods designed to perform stealth scans, such as SYN scanning (also known as half-open scanning) or FIN scanning. These techniques are employed to avoid detection by firewalls and intrusion detection systems (IDS), allowing penetration testers to conduct more discreet assessments.
7. **Nmap Scripting Engine (NSE)**: One of Nmap’s most powerful features, the Nmap Scripting Engine, allows users to write custom scripts or utilize a collection of pre-built scripts for a variety of purposes. These include vulnerability detection, service discovery, network monitoring, and even exploit testing. NSE enhances Nmap's capabilities, enabling automation of tasks that would otherwise be time-consuming.
8. **Zenmap (GUI for Nmap)**: Zenmap is a graphical user interface (GUI) for Nmap, providing an intuitive and user-friendly interface that makes network scanning more accessible. Zenmap allows users to visually map out their network, generate reports, and save scan results in a format that’s easy to understand and analyze, making it a helpful tool for both beginners and advanced users.

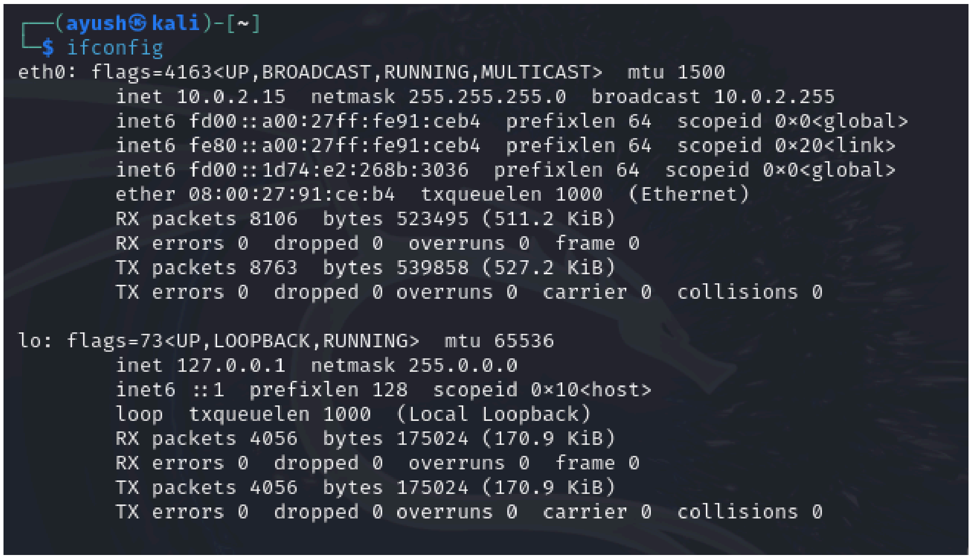
Methodology and Results

To perform network scanning using Nmap, we utilized various commands to analyze different aspects of network security. Below are the methodologies followed in our assignment:

1. **Checking Network Configuration:**
   - ○ Command: **`ifconfig`**
   - ○ Purpose: Displays network interface details including IP address and subnet mask.

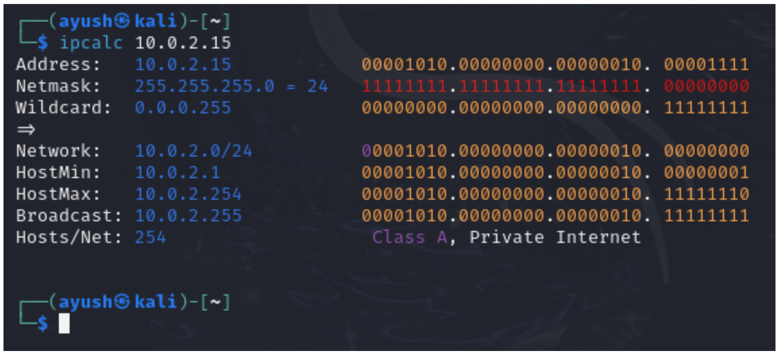


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.107  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::8da6:6d4d:74f7:efb5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)
        RX packets 639  bytes 40320 (39.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 101  bytes 16290 (15.9 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
```

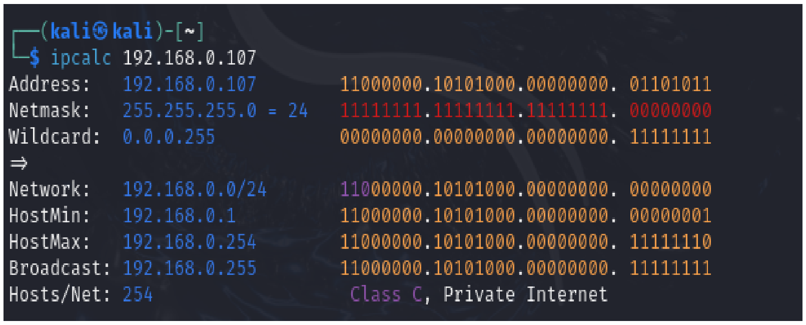


```
┌──(ayush㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd00::a00:27ff:fe91:ceb4  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe91:ceb4  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::1d74:e2:268b:3036  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:91:ce:b4  txqueuelen 1000  (Ethernet)
        RX packets 8106  bytes 523495 (511.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8763  bytes 539858 (527.2 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 4056  bytes 175024 (170.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4056  bytes 175024 (170.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. **IP Address Calculation:**
   - Command: **`ipcalc <IP Address>`**
   - Purpose: Calculates and displays network-related information such as netmask,
   - broadcast, and host range.

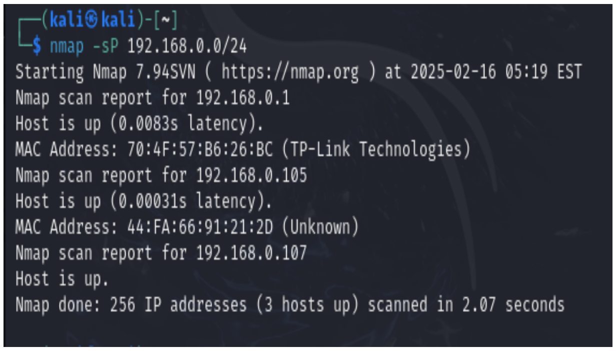


```
┌──(ayush㉿kali)-[~]
└─$ ipcalc 10.0.2.15
Address:   10.0.2.15            00001010.00000000.00000010. 00001111
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   10.0.2.0/24          00001010.00000000.00000010. 00000000
HostMin:   10.0.2.1             00001010.00000000.00000010. 00000001
HostMax:   10.0.2.254           00001010.00000000.00000010. 11111110
Broadcast: 10.0.2.255           00001010.00000000.00000010. 11111111
Hosts/Net: 254                   Class A, Private Internet


┌──(ayush㉿kali)-[~]
└─$ █
```

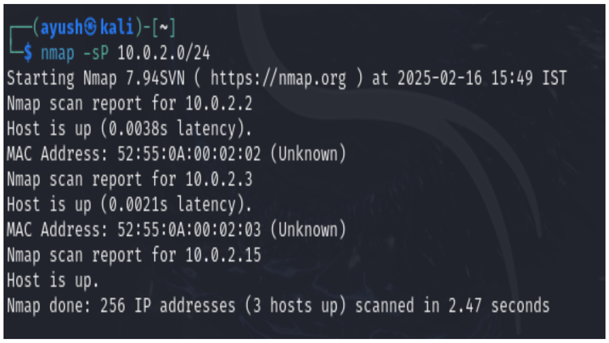


```
┌──(kali㉿kali)-[~]
└─$ ipcalc 192.168.0.107
Address:   192.168.0.107        11000000.10101000.00000000. 01101011
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.0.0/24       11000000.10101000.00000000. 00000000
HostMin:   192.168.0.1          11000000.10101000.00000000. 00000001
HostMax:   192.168.0.254        11000000.10101000.00000000. 11111110
Broadcast: 192.168.0.255        11000000.10101000.00000000. 11111111
Hosts/Net: 254                   Class C, Private Internet
```

3. **Scanning Live Hosts on a Network:**
   - Command: **`nmap -sP <Network IP>`**
   - Purpose: Identifies active devices on a subnet.

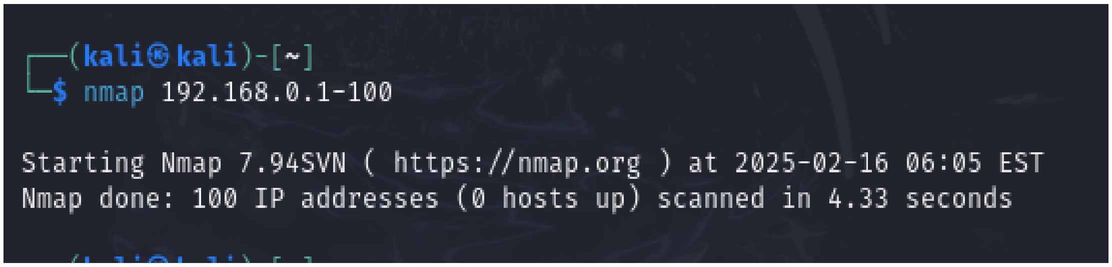


```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 05:19 EST
Nmap scan report for 192.168.0.1
Host is up (0.0083s latency).
MAC Address: 70:4F:57:B6:26:BC (TP-Link Technologies)
Nmap scan report for 192.168.0.105
Host is up (0.00031s latency).
MAC Address: 44:FA:66:91:21:2D (Unknown)
Nmap scan report for 192.168.0.107
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.07 seconds
```



```
┌──(ayush㉿kali)-[~]
└─$ nmap -sP 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 15:49 IST
Nmap scan report for 10.0.2.2
Host is up (0.0038s latency).
MAC Address: 52:55:0A:00:02:02 (Unknown)
Nmap scan report for 10.0.2.3
Host is up (0.0021s latency).
MAC Address: 52:55:0A:00:02:03 (Unknown)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.47 seconds
```

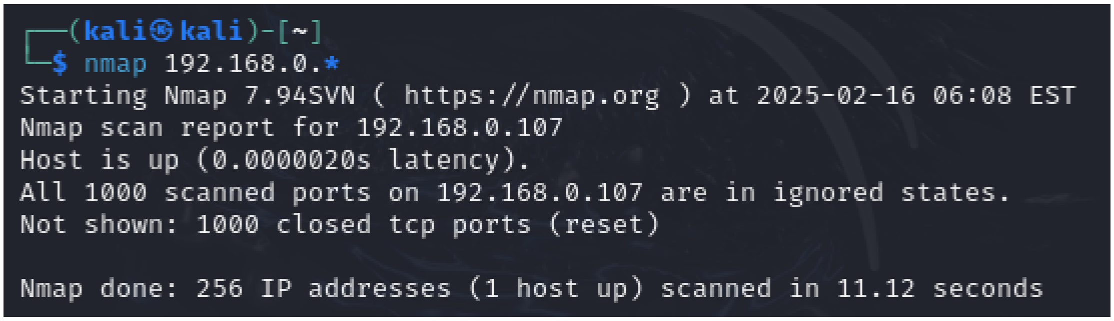
4. **Scanning a Range of IP Addresses:**
   - Command: **`nmap <start-IP>-<end-IP>`**
   - Purpose: Scans a specified range of IP addresses



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.0.1-100

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 06:05 EST
Nmap done: 100 IP addresses (0 hosts up) scanned in 4.33 seconds
```

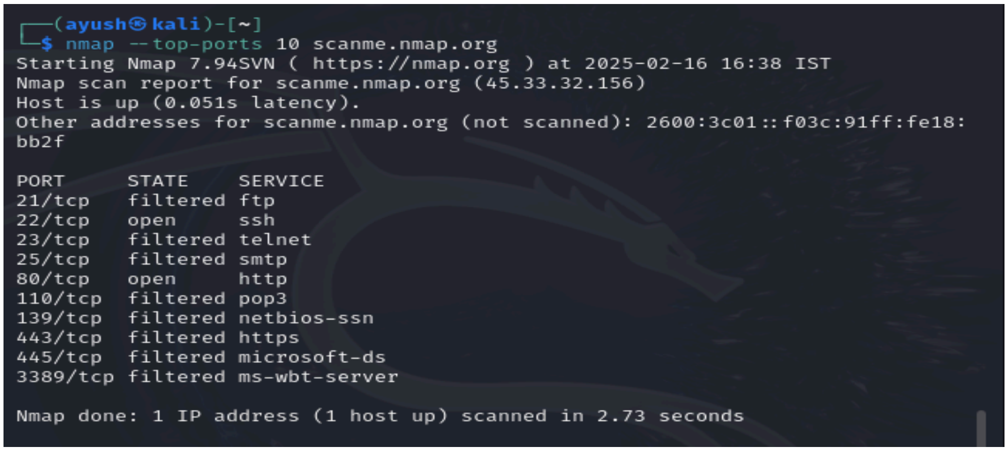
.

5. **Scanning an Entire Subnet:**
   - Command: **`nmap <subnet>`**
   - Purpose: Scans all devices within a subnet.



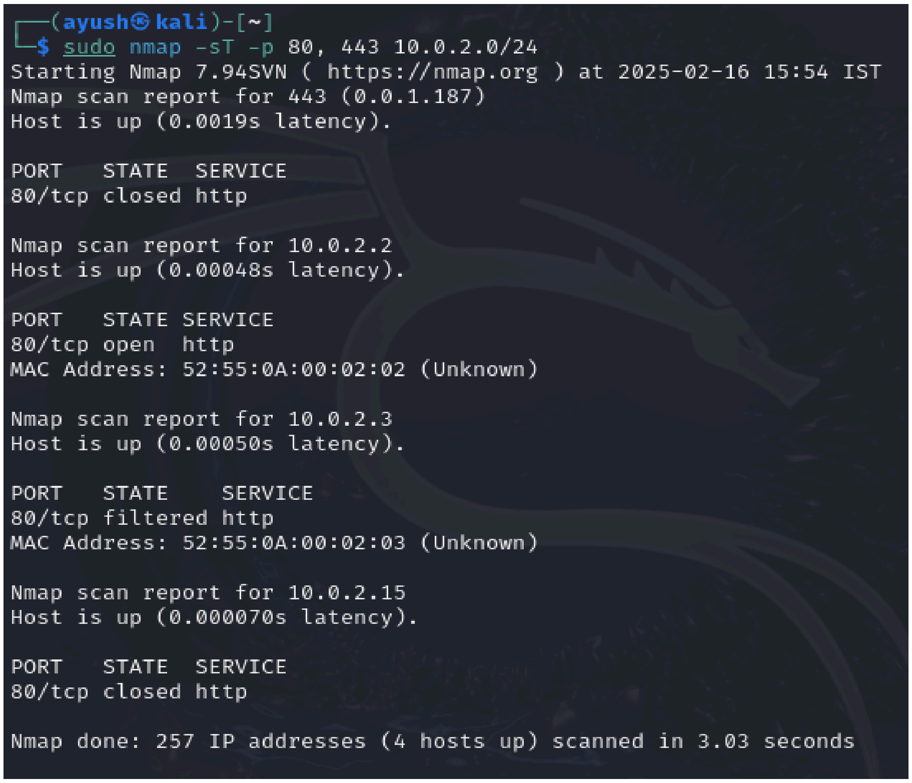
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.0.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 06:08 EST
Nmap scan report for 192.168.0.107
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.0.107 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (1 host up) scanned in 11.12 seconds
```

6. **Scanning the Top N Most Common Ports:**
   - Command: **`nmap --top-ports 10 scanme.nmap.org`**
   - Purpose: Scans the top 10 most commonly used ports.

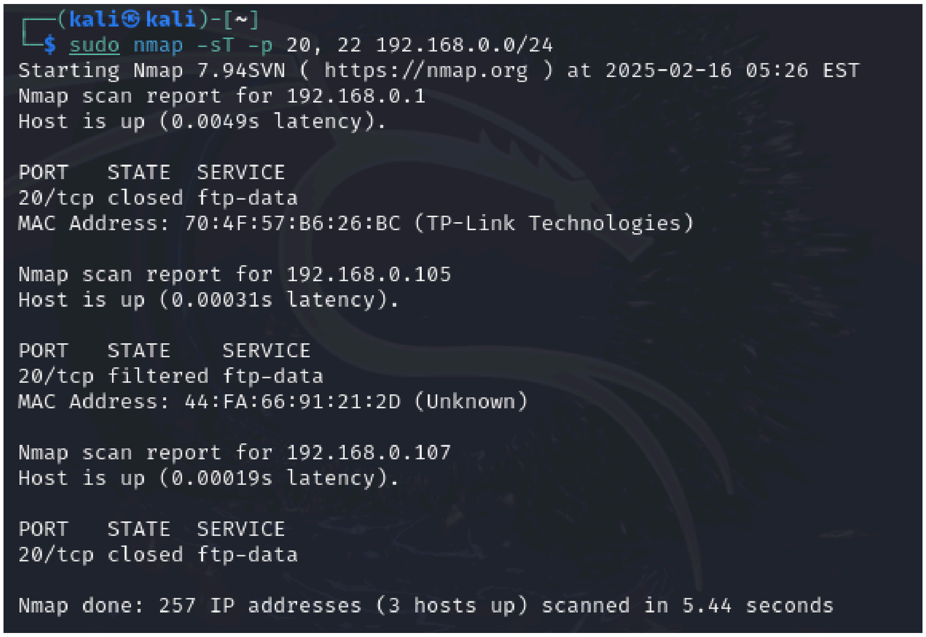


```
┌──(ayush㉿kali)-[~]
└─$ nmap --top-ports 10 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 16:38 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.051s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   open     http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.73 seconds
```

7. **Scanning Specific Ports Using Different Scan Methods:**
    - Command: `sudo nmap` **`-sT -p 80,443 <Network IP>`** (TCP Connect Scan)
    - Command: `sudo nmap` **`-sS -p 80,443 <Network IP>`** (Stealth Scan)
    - Purpose: Checks whether specific ports (e.g., 80, 443) are open.

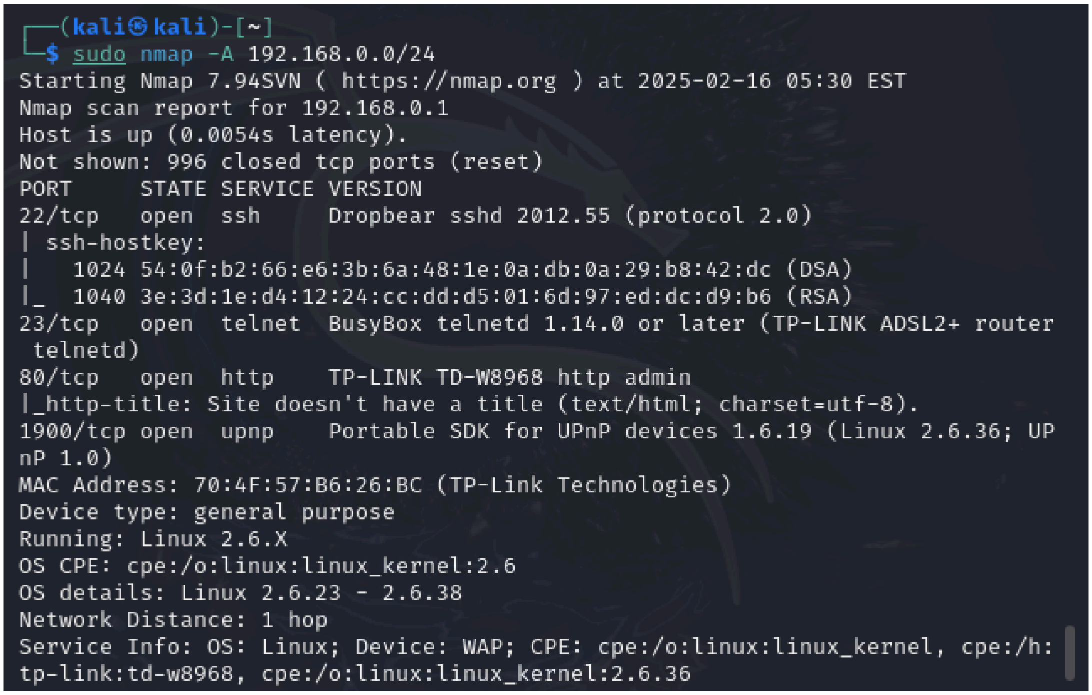


```
┌──(ayush㉿kali)-[~]
└─$ sudo nmap -sT -p 80, 443 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 15:54 IST
Nmap scan report for 443 (0.0.1.187)
Host is up (0.0019s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 10.0.2.2
Host is up (0.00048s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.00050s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.000070s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 257 IP addresses (4 hosts up) scanned in 3.03 seconds
```



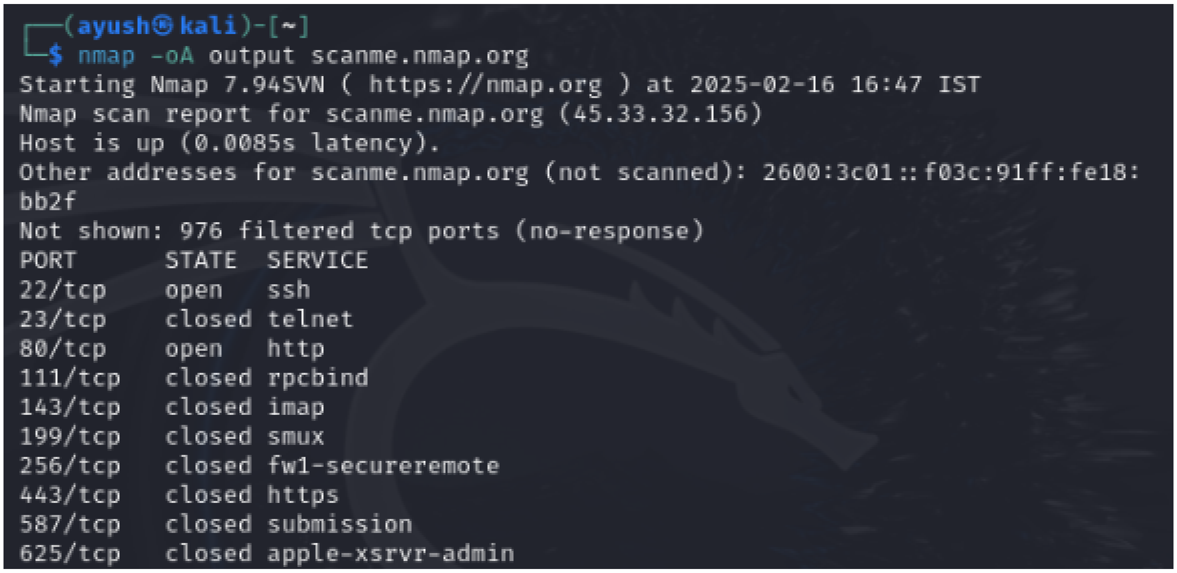
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -p 20, 22 192.168.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 05:26 EST
Nmap scan report for 192.168.0.1
Host is up (0.0049s latency).

PORT   STATE  SERVICE
20/tcp closed ftp-data
MAC Address: 70:4F:57:B6:26:BC (TP-Link Technologies)

Nmap scan report for 192.168.0.105
Host is up (0.00031s latency).

PORT   STATE    SERVICE
20/tcp filtered ftp-data
MAC Address: 44:FA:66:91:21:2D (Unknown)

Nmap scan report for 192.168.0.107
Host is up (0.00019s latency).

PORT   STATE  SERVICE
20/tcp closed ftp-data

Nmap done: 257 IP addresses (3 hosts up) scanned in 5.44 seconds
```

8. **Aggressive Scan for Detailed Information:**
   - Command: nmap **`-A <IP Address>`**
   - Purpose: Performs a comprehensive scan, including OS detection, version detection, and script scanning.

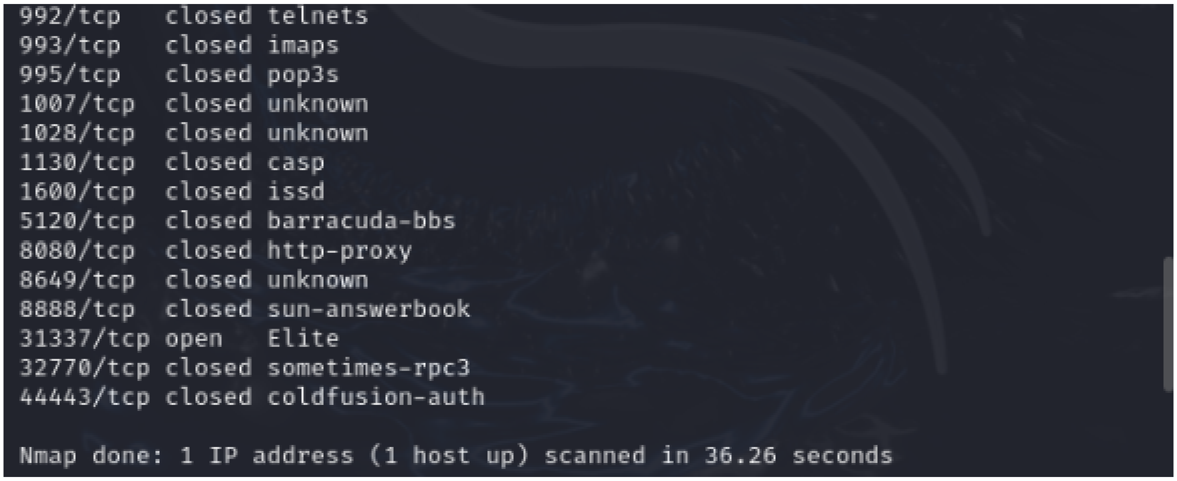


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 05:30 EST
Nmap scan report for 192.168.0.1
Host is up (0.0054s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     Dropbear sshd 2012.55 (protocol 2.0)
| ssh-hostkey:
|   1024 54:0f:b2:66:e6:3b:6a:48:1e:0a:db:0a:29:b8:42:dc (DSA)
|_  1040 3e:3d:1e:d4:12:24:cc:dd:d5:01:6d:97:ed:dc:d9:b6 (RSA)
23/tcp   open  telnet  BusyBox telnetd 1.14.0 or later (TP-LINK ADSL2+ router
 telnetd)
80/tcp   open  http    TP-LINK TD-W8968 http admin
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
1900/tcp open  upnp    Portable SDK for UPnP devices 1.6.19 (Linux 2.6.36; UP
nP 1.0)
MAC Address: 70:4F:57:B6:26:BC (TP-Link Technologies)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.23 - 2.6.38
Network Distance: 1 hop
Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel, cpe:/h:
tp-link:td-w8968, cpe:/o:linux:linux_kernel:2.6.36
```

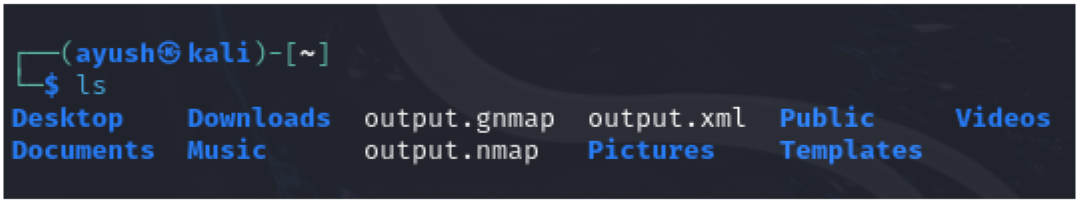
9. **Saving Scan Output:**
    - Command: nmap **`-oA output scanme.nmap.org`**
    - Purpose: Saves scan results in different formats for further analysis.



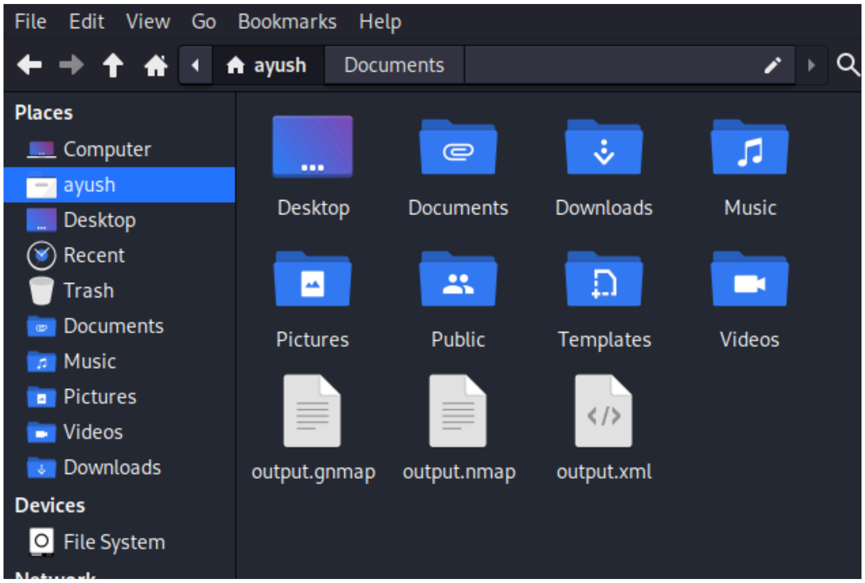
```
┌──(ayush㉿kali)-[~]
└─$ nmap -oA output scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 16:47 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0085s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 976 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
23/tcp    closed telnet
80/tcp    open   http
111/tcp   closed rpcbind
143/tcp   closed imap
199/tcp   closed smux
256/tcp   closed fw1-secureremote
443/tcp   closed https
587/tcp   closed submission
625/tcp   closed apple-xsrvr-admin
```

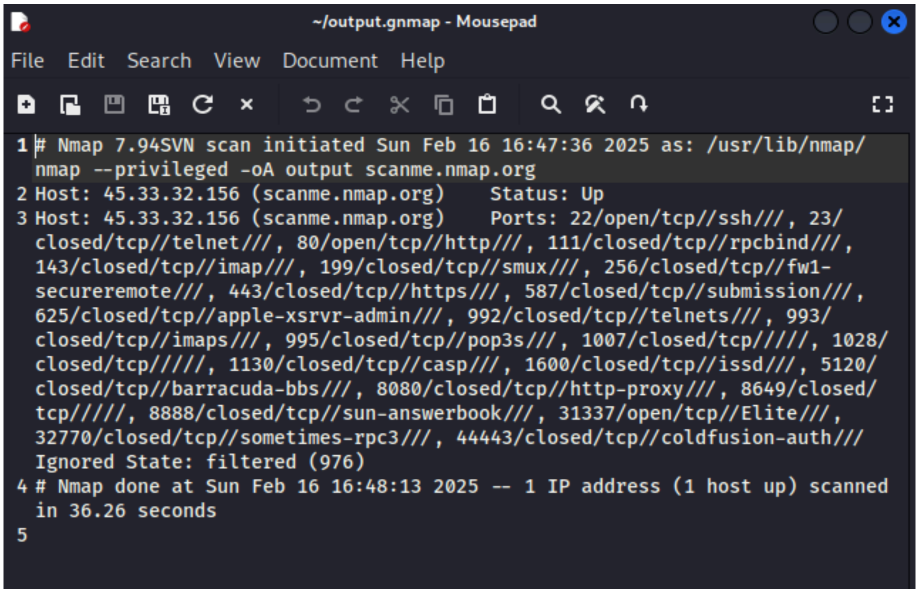


```
992/tcp   closed telnets
993/tcp   closed imaps
995/tcp   closed pop3s
1007/tcp  closed unknown
1028/tcp  closed unknown
1130/tcp  closed casp
1600/tcp  closed issd
5120/tcp  closed barracuda-bbs
8080/tcp  closed http-proxy
8649/tcp  closed unknown
8888/tcp  closed sun-answerbook
31337/tcp open   Elite
32770/tcp closed sometimes-rpc3
44443/tcp closed coldfusion-auth

Nmap done: 1 IP address (1 host up) scanned in 36.26 seconds
```

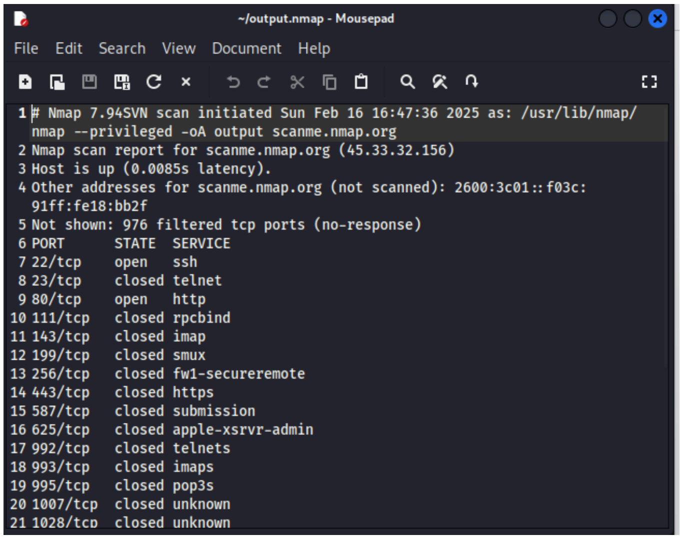


```
┌──(ayush㉿kali)-[~]
└─$ ls
Desktop    Downloads  output.gnmap  output.xml  Public     Videos
Documents  Music      output.nmap   Pictures    Templates
```





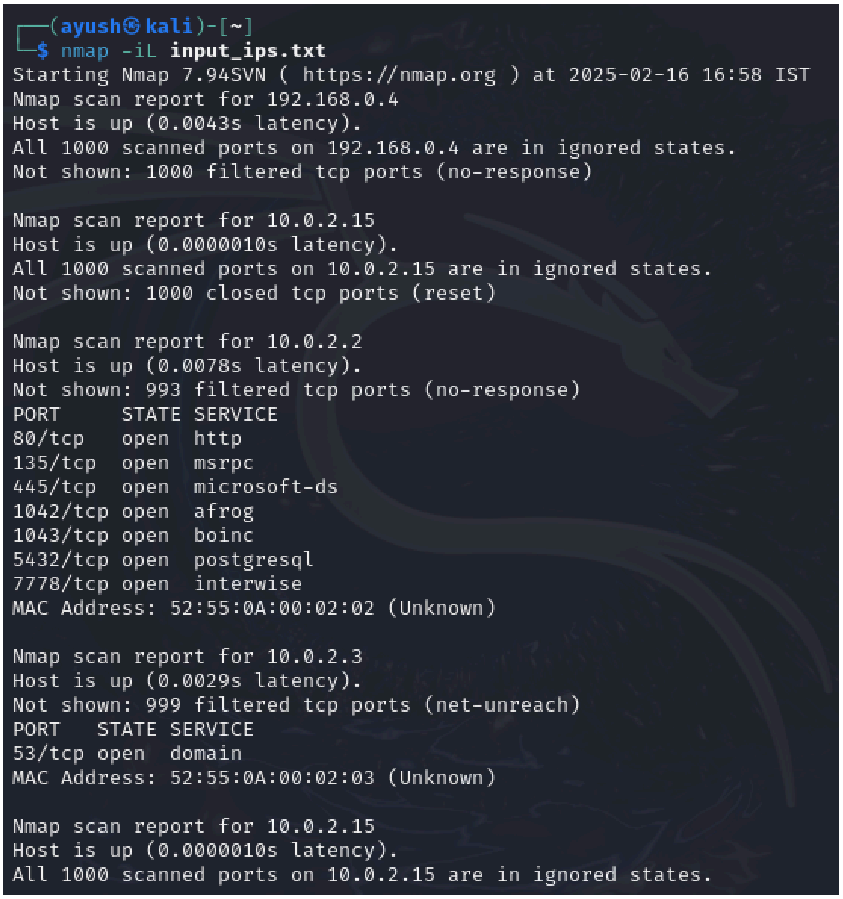
```
# Nmap 7.94SVN scan initiated Sun Feb 16 16:47:36 2025 as: /usr/lib/nmap/
nmap --privileged -oA output scanme.nmap.org
Host: 45.33.32.156 (scanme.nmap.org)    Status: Up
Host: 45.33.32.156 (scanme.nmap.org)    Ports: 22/open/tcp//ssh///, 23/
closed/tcp//telnet///, 80/open/tcp//http///, 111/closed/tcp//rpcbind///,
143/closed/tcp//imap///, 199/closed/tcp//smux///, 256/closed/tcp//fw1-
securemote///, 443/closed/tcp//https///, 587/closed/tcp//submission///,
625/closed/tcp//apple-xsrvr-admin///, 992/closed/tcp//telnets///, 993/
closed/tcp//imaps///, 995/closed/tcp//pop3s///, 1007/closed/tcp/////, 1028/
closed/tcp/////, 1130/closed/tcp//casp///, 1600/closed/tcp//issd///, 5120/
closed/tcp//barracuda-bbs///, 8080/closed/tcp//http-proxy///, 8649/closed/
tcp/////, 8888/closed/tcp//sun-answerbook///, 31337/open/tcp//Elite///,
32770/closed/tcp//sometimes-rpc3///, 44443/closed/tcp//coldfusion-auth///
Ignored State: filtered (976)
# Nmap done at Sun Feb 16 16:48:13 2025 -- 1 IP address (1 host up) scanned
in 36.26 seconds
```



```
# Nmap 7.94SVN scan initiated Sun Feb 16 16:47:36 2025 as: /usr/lib/nmap/
nmap --privileged -oA output scanme.nmap.org
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0085s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:
91ff:fe18:bb2f
Not shown: 976 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
23/tcp    closed telnet
80/tcp    open   http
111/tcp   closed rpcbind
143/tcp   closed imap
199/tcp   closed smux
256/tcp   closed fw1-secureremote
443/tcp   closed https
587/tcp   closed submission
625/tcp   closed apple-xsrvr-admin
992/tcp   closed telnets
993/tcp   closed imaps
995/tcp   closed pop3s
1007/tcp  closed unknown
1028/tcp  closed unknown
```

10. **Scanning Multiple Targets from a File:**

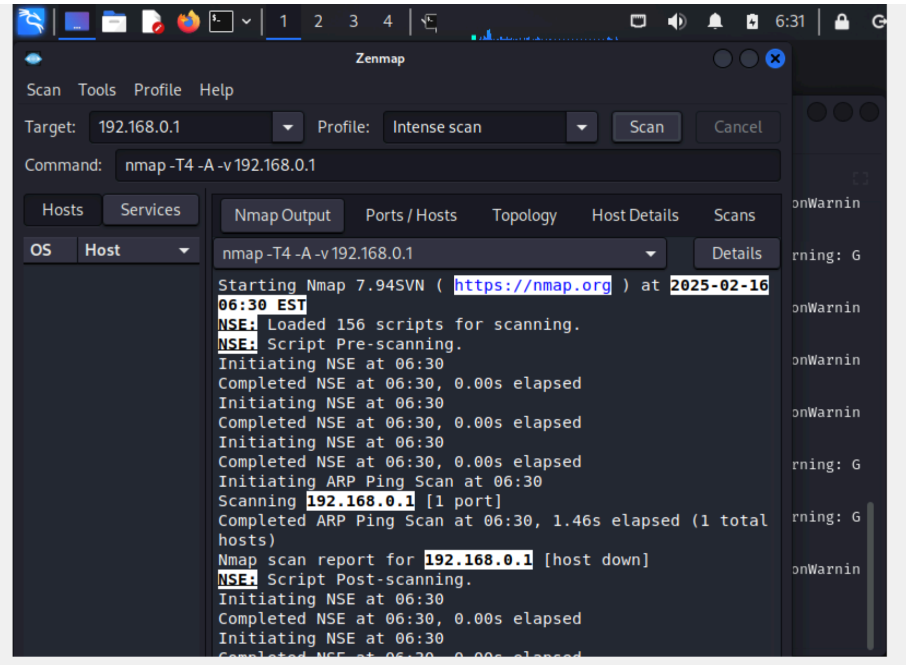
- Command: **`nmap -iL input_ips.txt`**
- Purpose: Reads target IPs from a file and performs scanning.



```
┌──(ayush㉿kali)-[~]
└─$ nmap -iL input_ips.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 16:58 IST
Nmap scan report for 192.168.0.4
Host is up (0.0043s latency).
All 1000 scanned ports on 192.168.0.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for 10.0.2.2
Host is up (0.0078s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1042/tcp open  afrog
1043/tcp open  boinc
5432/tcp open  postgresql
7778/tcp open  interwise
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.0029s latency).
Not shown: 999 filtered tcp ports (net-unreach)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
```

11. **Using Zenmap (GUI for Nmap):**

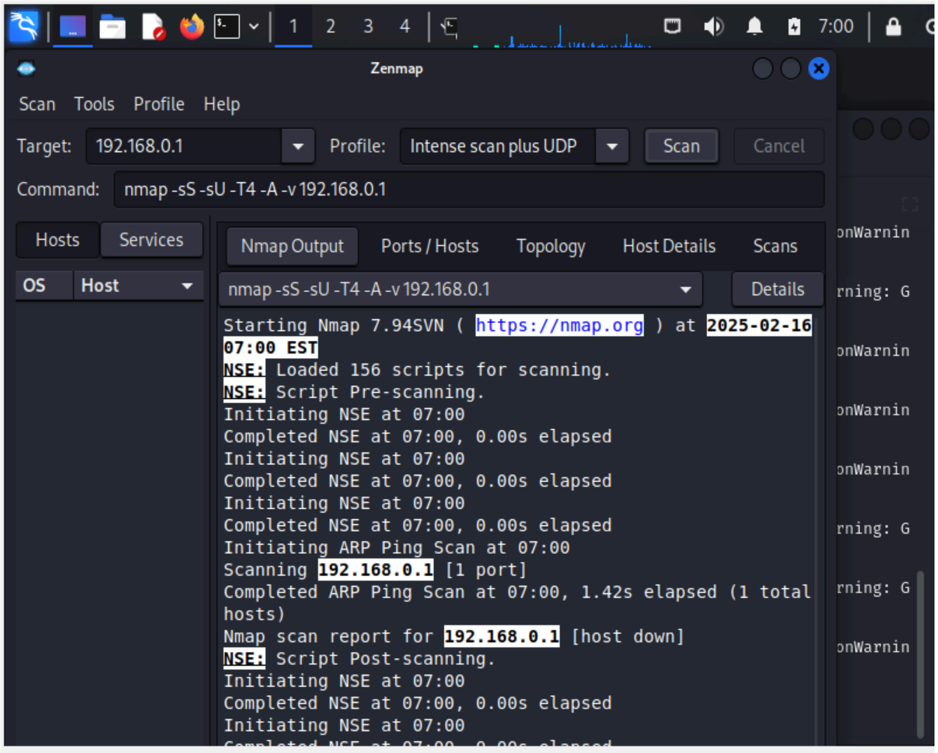
- Purpose: Provides a user-friendly interface for performing and visualizing scans.



Target: 192.168.0.1 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.1

```
nmap -T4 -A -v 192.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16
06:30 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:30
Completed NSE at 06:30, 0.00s elapsed
Initiating NSE at 06:30
Completed NSE at 06:30, 0.00s elapsed
Initiating NSE at 06:30
Completed NSE at 06:30, 0.00s elapsed
Initiating ARP Ping Scan at 06:30
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 06:30, 1.46s elapsed (1 total
hosts)
Nmap scan report for 192.168.0.1 [host down]
NSE: Script Post-scanning.
Initiating NSE at 06:30
Completed NSE at 06:30, 0.00s elapsed
Initiating NSE at 06:30
Completed NSE at 06:30, 0.00s elapsed
```



Target: 192.168.0.1 Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v 192.168.0.1

```
nmap -sS -sU -T4 -A -v 192.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16
07:00 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:00
Completed NSE at 07:00, 0.00s elapsed
Initiating NSE at 07:00
Completed NSE at 07:00, 0.00s elapsed
Initiating NSE at 07:00
Completed NSE at 07:00, 0.00s elapsed
Initiating ARP Ping Scan at 07:00
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 07:00, 1.42s elapsed (1 total
hosts)
Nmap scan report for 192.168.0.1 [host down]
NSE: Script Post-scanning.
Initiating NSE at 07:00
Completed NSE at 07:00, 0.00s elapsed
Initiating NSE at 07:00
Completed NSE at 07:00, 0.00s elapsed
```

Conclusion

Nmap is a powerful and essential tool for network security analysis, penetration testing, and cybersecurity research. Its ability to perform host discovery, port scanning, service identification, and OS detection makes it invaluable for security professionals. Our study demonstrated the efficiency of Nmap in identifying vulnerabilities and assessing network configurations. The use of advanced scanning techniques, including stealth and aggressive scans, further emphasized its versatility in cybersecurity assessments. With its continuous updates and scripting capabilities, Nmap remains a crucial tool in modern network security.

References

1. FreeCodeCamp - What is Nmap and How to Use It
2. Official Nmap Website