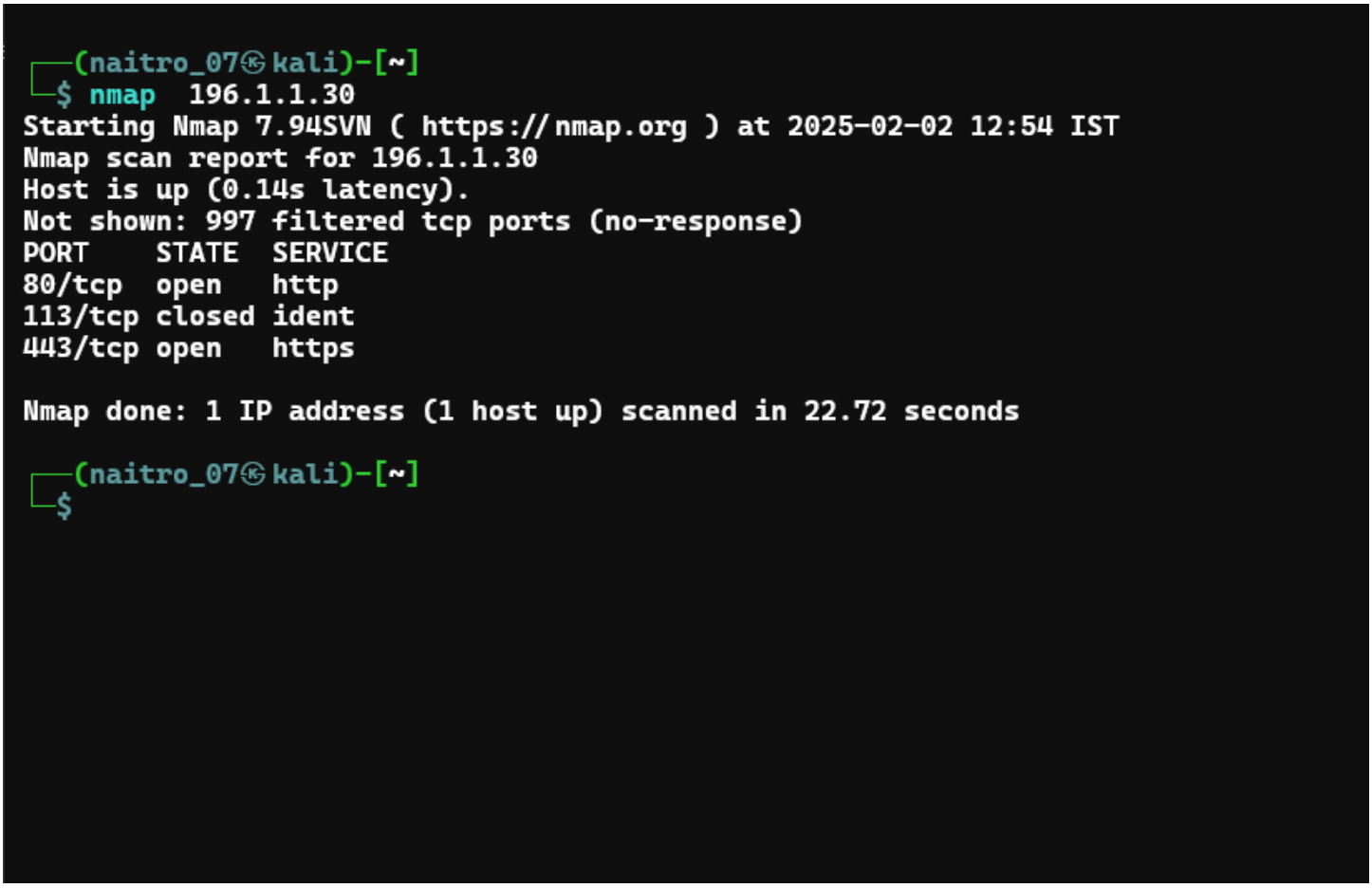
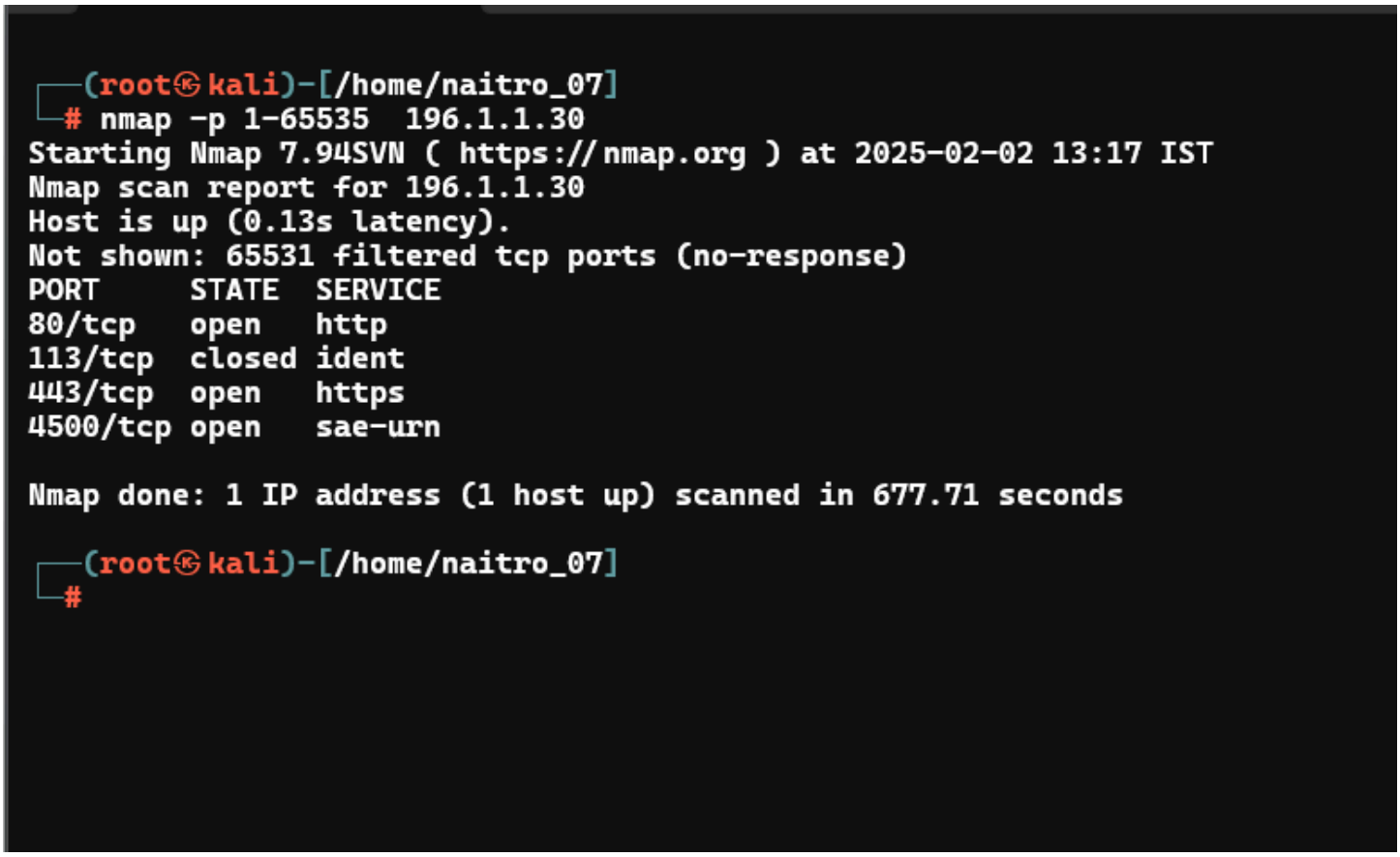
1. Basic Nmap Scan against IP or host



2. Scan specific ports or scan entire port ranges on a local or remote server. nmap -p 1-65535 localhost



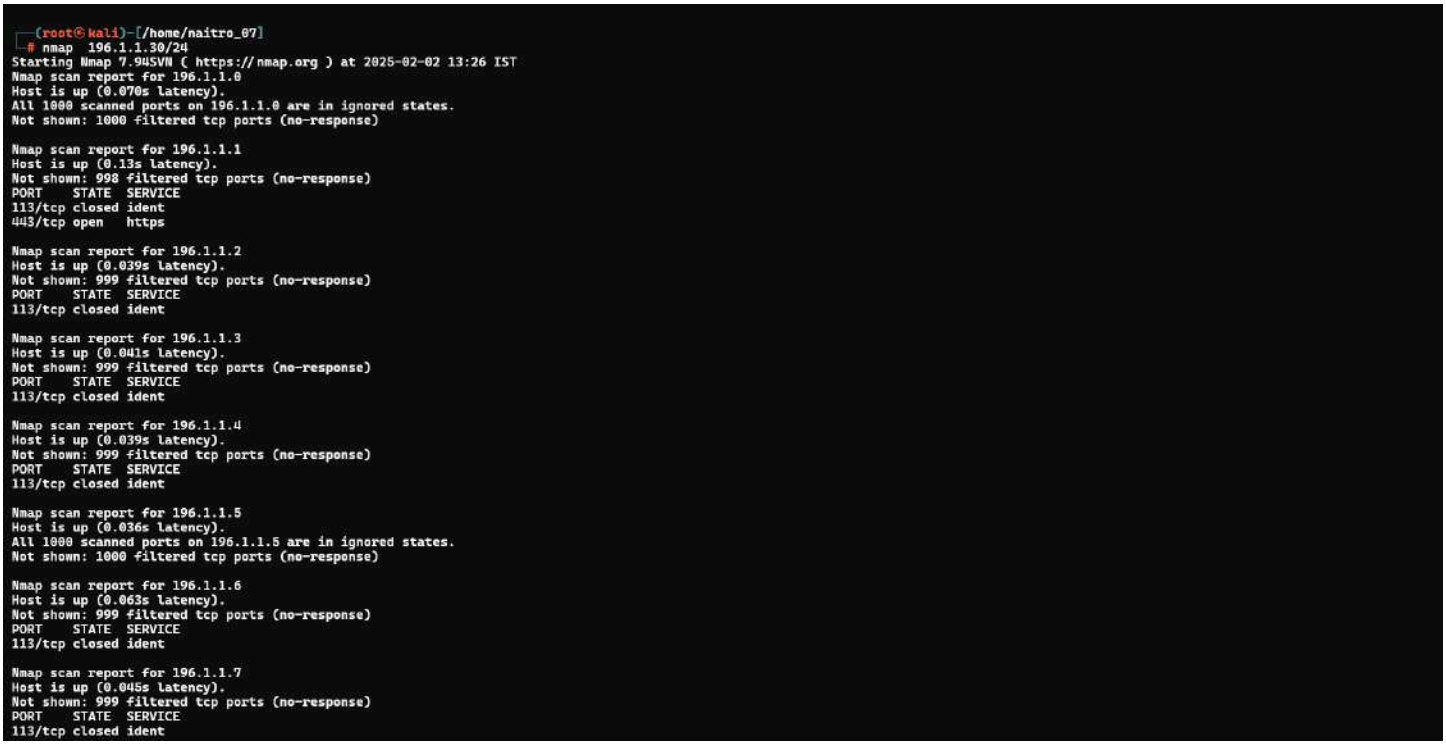
3. Nmap is able to scan all possible ports, but it can also scan specific ports

```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap -p 80,443  196.1.1.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 13:17 IST
Nmap scan report for 196.1.1.30
Host is up (0.097s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds

┌──(root㉿kali)-[/home/naitro_07]
└─#
```

4. Scan multiple IP addresses

```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap  196.1.1.30,35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 13:20 IST
Nmap scan report for 196.1.1.30
Host is up (0.058s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp open   https

Nmap scan report for 196.1.1.35
Host is up (0.069s latency).
All 1000 scanned ports on 196.1.1.35 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 2 IP addresses (2 hosts up) scanned in 21.08 seconds

┌──(root㉿kali)-[/home/naitro_07]
└─#
```

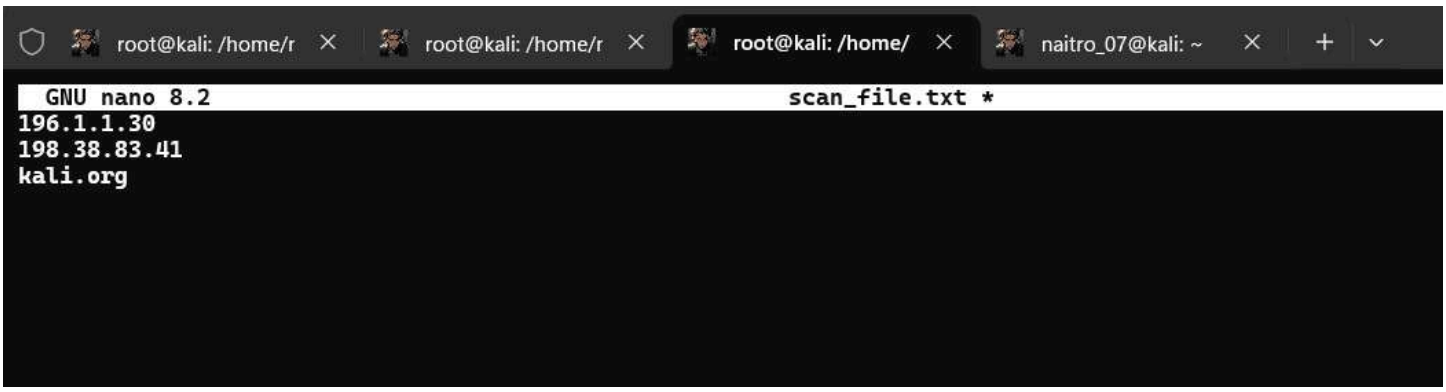
5. Scan IP ranges



6. Scan the most popular ports

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 13:28 IST
Nmap scan report for 196.1.1.30
Host is up (0.11s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   open     http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds

┌──(root㉿kali)-[/home/naitro_07]
└─#
```

7. Scan hosts and IP addresses reading from a text file



```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap -iL scan_file.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 13:40 IST
Nmap scan report for 196.1.1.30
Host is up (0.10s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp open   https

Nmap scan report for 599974-QamarRayees.securehostdns.com (198.38.83.41)
Host is up (0.10s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
8443/tcp open  https-alt

Nmap scan report for kali.org (104.18.4.159)
Host is up (0.095s latency).
Other addresses for kali.org (not scanned): 104.18.5.159 2606:4700:90c0:747e:a64:5be:cfc8:4636
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 3 IP addresses (3 hosts up) scanned in 23.73 seconds

┌──(root㉿kali)-[/home/naitro_07]
└─#
```

8. Save your Nmap scan results to a file

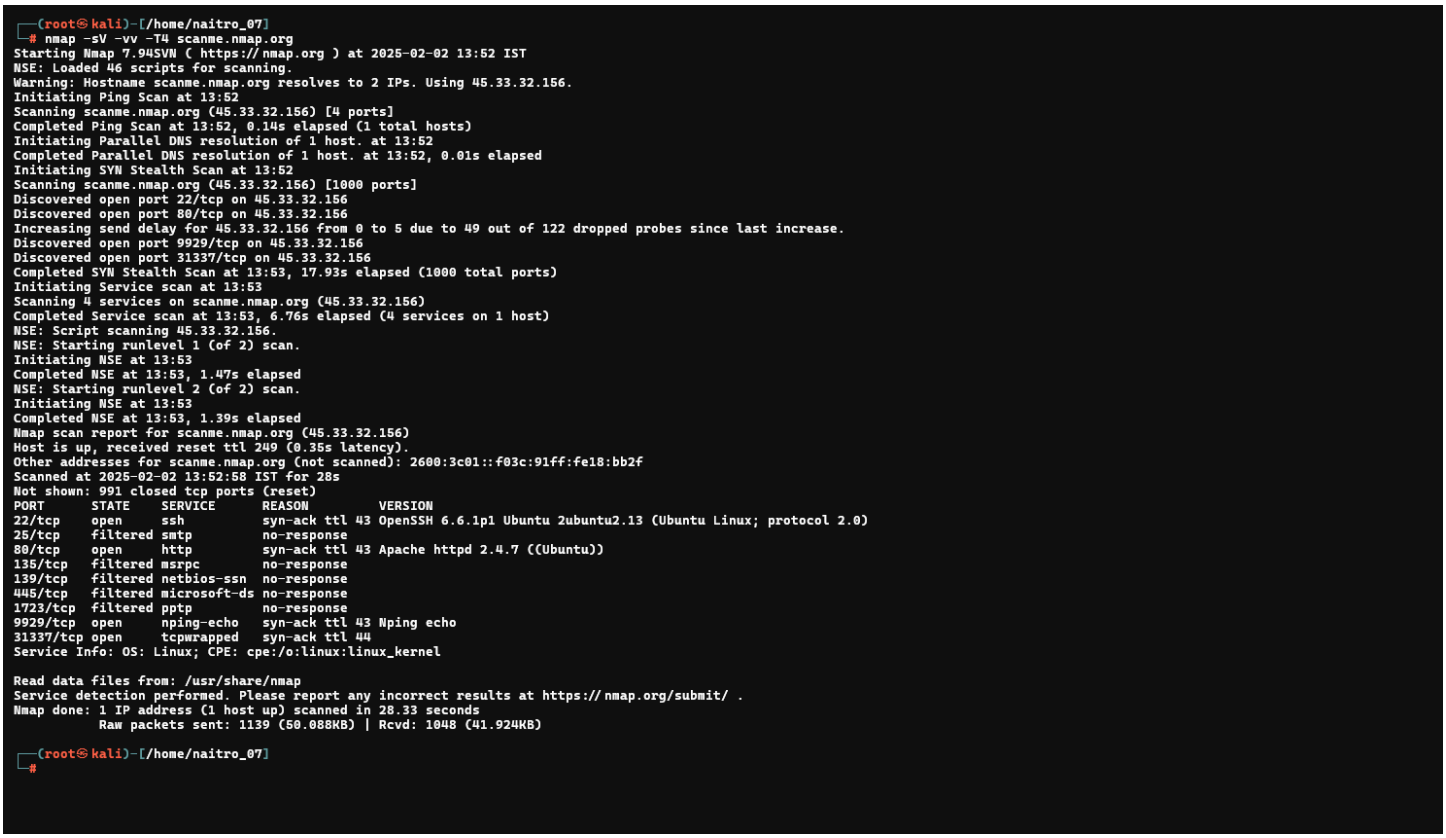
```
┌──(naitro_07㉿kali)-[~]
└─$ nmap -oN output.txt scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 13:45 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    filtered http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  filtered pptp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 42.17 seconds

┌──(naitro_07㉿kali)-[~]
└─$
```

```
  GNU nano 8.2                                        output.txt
# Nmap 7.94SVN scan initiated Sun Feb  2 13:45:03 2025 as: /usr/lib/nmap/nmap --privileged -oN output.txt scanme.nmap.o>
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    filtered http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  filtered pptp
9929/tcp  open     nping-echo
31337/tcp open     Elite

# Nmap done at Sun Feb  2 13:45:45 2025 -- 1 IP address (1 host up) scanned in 42.17 seconds

                                [ Read 17 lines ]
^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

9. Scan + OS and service detection with fast execution

```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 13:45 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    filtered http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  filtered pptp
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
OS fingerprint not ideal because: Host distance (27 network hops) is greater than five
No OS matches for host
Network Distance: 7 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.66 ms  NAITRO-07.mshome.net (172.21.208.1)
2   14.31 ms jiofiber.local.html (192.168.31.1)
3   14.35 ms 192.0.0.1
4   76.38 ms 192.0.0.1
5   77.04 ms 192.0.0.1
6   76.38 ms 192.0.0.1
7   72.96 ms scanme.nmap.org (45.33.32.156)

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 49.21 seconds

┌──(root㉿kali)-[/home/naitro_07]
└─#
```

10. Detect service/daemon versions



```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap -sV -vv -T4 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 13:52 IST
NSE: Loaded 46 scripts for scanning.
Warning: Hostname scanme.nmap.org resolves to 2 IPs. Using 45.33.32.156.
Initiating Ping Scan at 13:52
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 13:52, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:52
Completed Parallel DNS resolution of 1 host. at 13:52, 0.01s elapsed
Initiating SYN Stealth Scan at 13:52
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 49 out of 122 dropped probes since last increase.
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed SYN Stealth Scan at 13:53, 17.93s elapsed (1000 total ports)
Initiating Service scan at 13:53
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 13:53, 6.76s elapsed (4 services on 1 host)
NSE: Script scanning 45.33.32.156.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:53
Completed NSE at 13:53, 1.47s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 13:53
Completed NSE at 13:53, 1.39s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 249 (0.35s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Scanned at 2025-02-02 13:52:58 IST for 28s
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE      REASON         VERSION
22/tcp    open     ssh          syn-ack ttl 43 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp         no-response
80/tcp    open     http         syn-ack ttl 43 Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc        no-response
139/tcp   filtered netbios-ssn  no-response
445/tcp   filtered microsoft-ds no-response
1723/tcp  filtered pptp         no-response
9929/tcp  open     nping-echo   syn-ack ttl 43 Nping echo
31337/tcp open     tcpwrapped   syn-ack ttl 44
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.33 seconds
           Raw packets sent: 1139 (50.088KB) | Rcvd: 1048 (41.924KB)

┌──(root㉿kali)-[/home/naitro_07]
└─#
```

11. Scan using TCP or UDP protocols

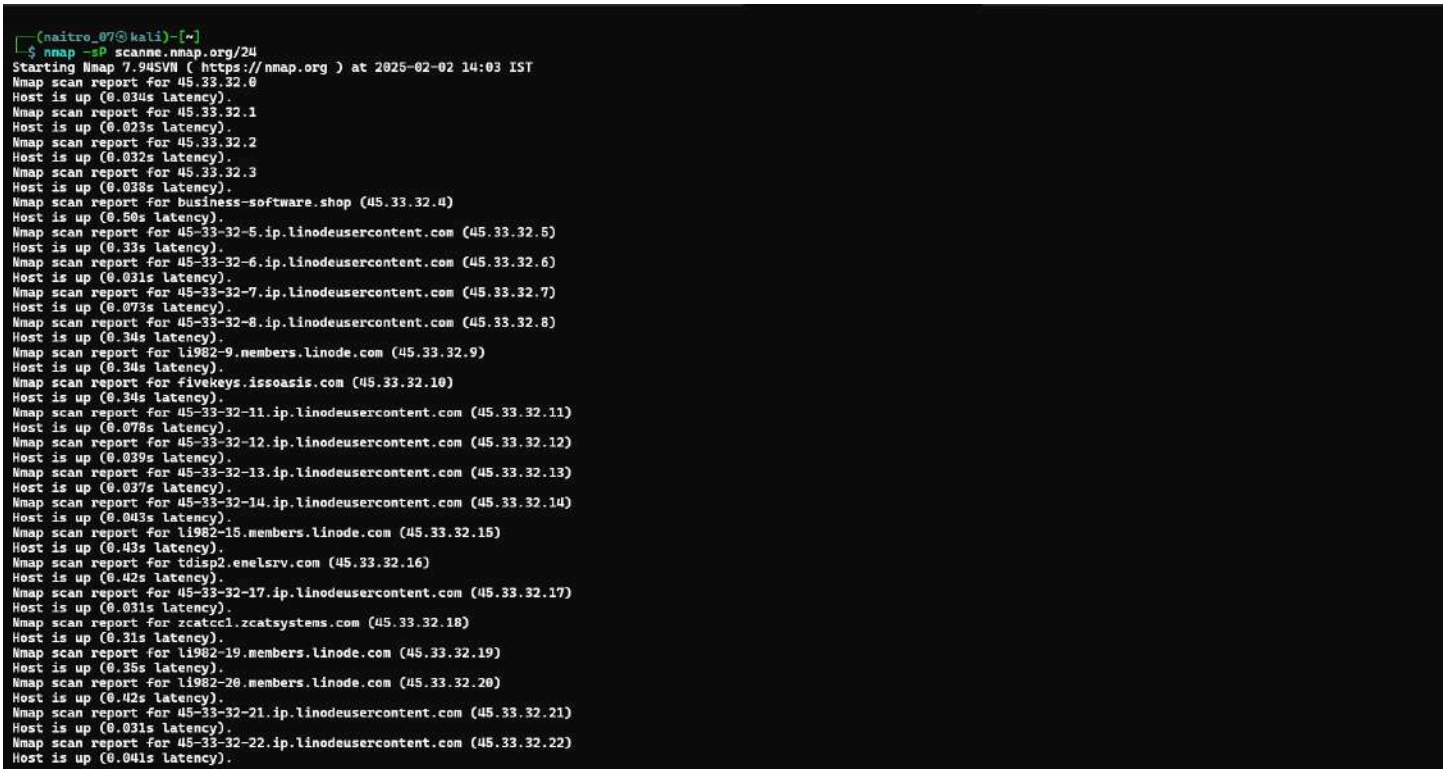
TCP

```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap -sT -T4 -vv scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 14:01 IST
Warning: Hostname scanme.nmap.org resolves to 2 IPs. Using 45.33.32.156.
Initiating Ping Scan at 14:01
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 14:01, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:01
Completed Parallel DNS resolution of 1 host. at 14:01, 0.00s elapsed
Initiating Connect Scan at 14:01
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 14:01, 32.01s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 249 (0.33s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Scanned at 2025-02-02 14:01:17 IST for 32s
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE    SERVICE      REASON
22/tcp    open     ssh          syn-ack
25/tcp    filtered smtp         no-response
80/tcp    open     http         syn-ack
135/tcp   filtered msrpc        no-response
139/tcp   filtered netbios-ssn  no-response
445/tcp   filtered microsoft-ds no-response
1723/tcp  filtered pptp         no-response
9929/tcp  open     nping-echo   syn-ack
31337/tcp open     Elite        syn-ack

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 32.20 seconds
           Raw packets sent: 4 (152B) | Rcvd: 1 (40B)

┌──(root㉿kali)-[/home/naitro_07]
└─#
```

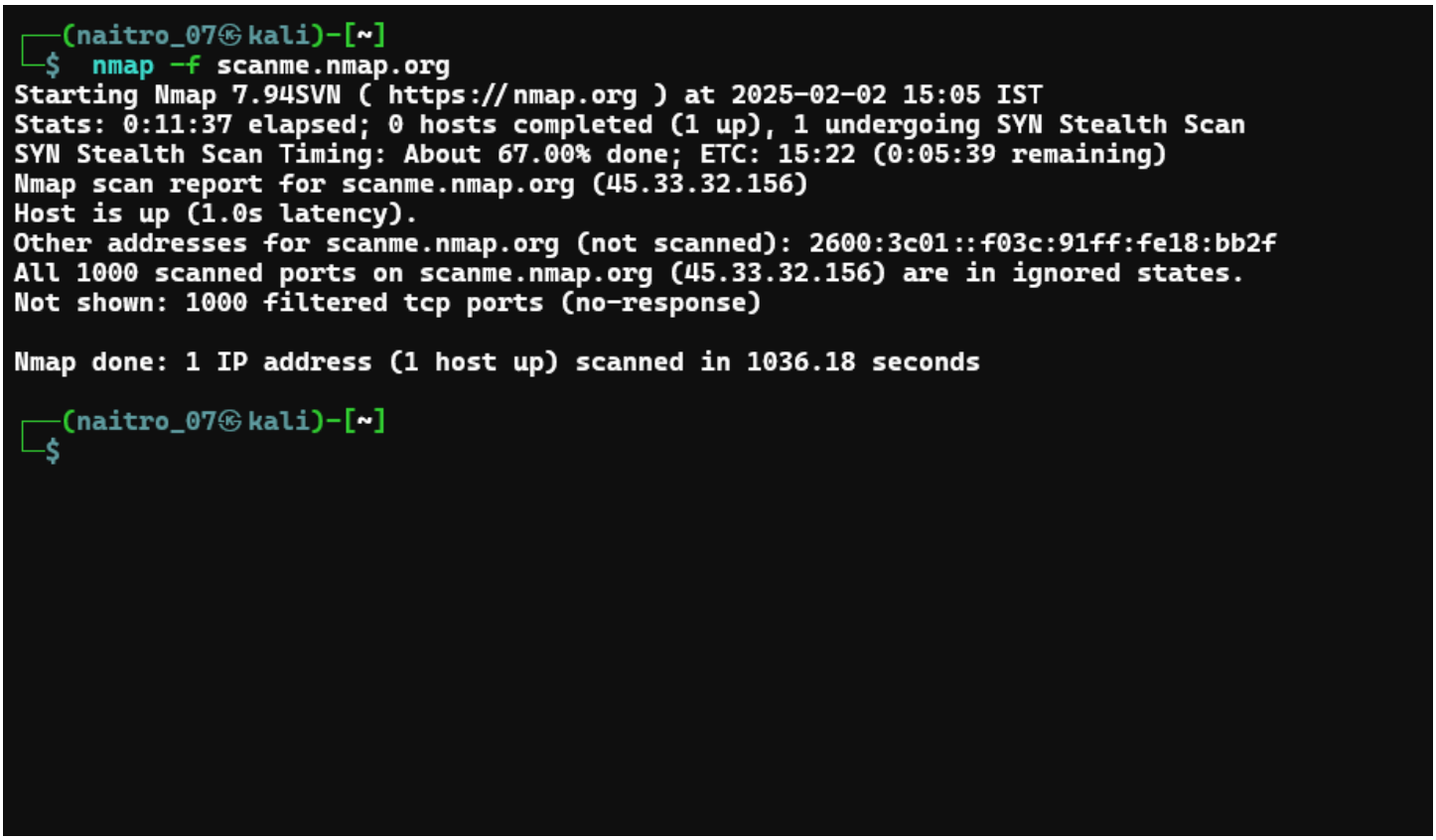
UDP

```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap -sU --top-ports 20 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 15:39 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
123/udp   open          ntp
135/udp   open|filtered msrpc
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   open|filtered netbios-ssn
161/udp   closed        snmp
162/udp   open|filtered snmptrap
445/udp   open|filtered microsoft-ds
500/udp   closed        isakmp
514/udp   open|filtered syslog
520/udp   closed        route
631/udp   open|filtered ipp
1434/udp  open|filtered ms-sql-m
1900/udp  closed        upnp
4500/udp  open|filtered nat-t-ike
49152/udp closed        unknown

Nmap done: 1 IP address (1 host up) scanned in 16.02 seconds
```

12. Finding multiple live hosts in the network



Bypassing firewall using fragmentation



To set a specific MTU (Maximum Transmission Unit) size:

```
┌──(naitro_07㉿kali)-[~]
└─$ nmap --mtu 24 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 15:32 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.36s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    filtered http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  filtered pptp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 35.30 seconds

┌──(naitro_07㉿kali)-[~]
└─$
```

Stealthy Scan to Avoid Firewall Detection

```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap -sS scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 15:06 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.36s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 990 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  filtered pptp
3261/tcp  filtered winshadow
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 79.84 seconds

┌──(root㉿kali)-[/home/naitro_07]
└─#
```

Using Nmap Script Engine (NSE)

```
┌──(root㉿kali)-[/home/naitro_07]
└─# nmap --script vuln scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 15:06 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.36s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=scanme.nmap.org
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://scanme.nmap.org:80/
|     Form id: nst-head-search
|     Form action: /search/
|
|     Path: http://scanme.nmap.org:80/
|     Form id: nst-foot-search
|_    Form action: /search/
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  filtered pptp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 405.79 seconds
```

DNS Enumeration

A. Discover Hosts and Services Using DNS

```
┌──(naitro_07㉿kali)-[~]
└─$ nmap --script=broadcast-dns-service-discovery scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 15:07 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.32s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  filtered pptp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 44.96 seconds

┌──(naitro_07㉿kali)-[~]
└─$
```

B. Brute Force DNS Subdomains

```
┌──(naitro_07㉿kali)-[~]
└─$ nmap -T4 -p 53 --script dns-brute scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 15:12 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT   STATE  SERVICE
53/tcp closed domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     chat.nmap.org - 45.33.32.156
|     chat.nmap.org - 2600:3c01::f03c:91ff:fe18:bb2f
|     *A: 50.116.1.184
|_    *AAAA: 2600:3c01:e000:3e6::6d4e:7061

Nmap done: 1 IP address (1 host up) scanned in 50.59 seconds

┌──(naitro_07㉿kali)-[~]
└─$
```