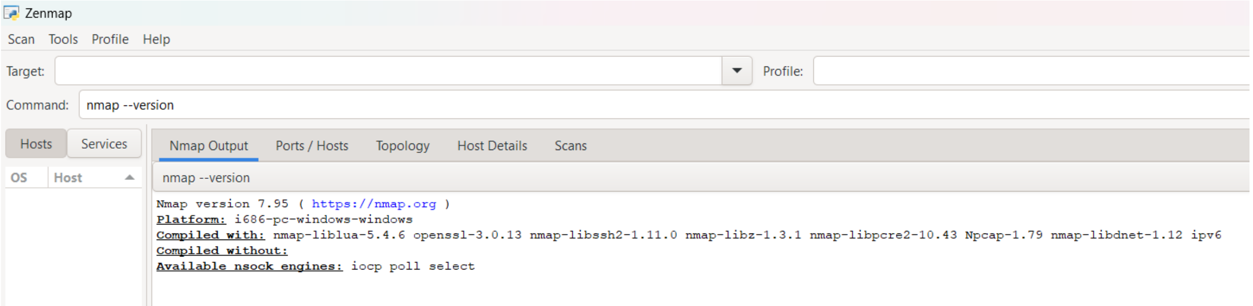
PRACTICAL – 3

AIM: Labs for Network scanning and Enumeration

1. Display the NMAP version.



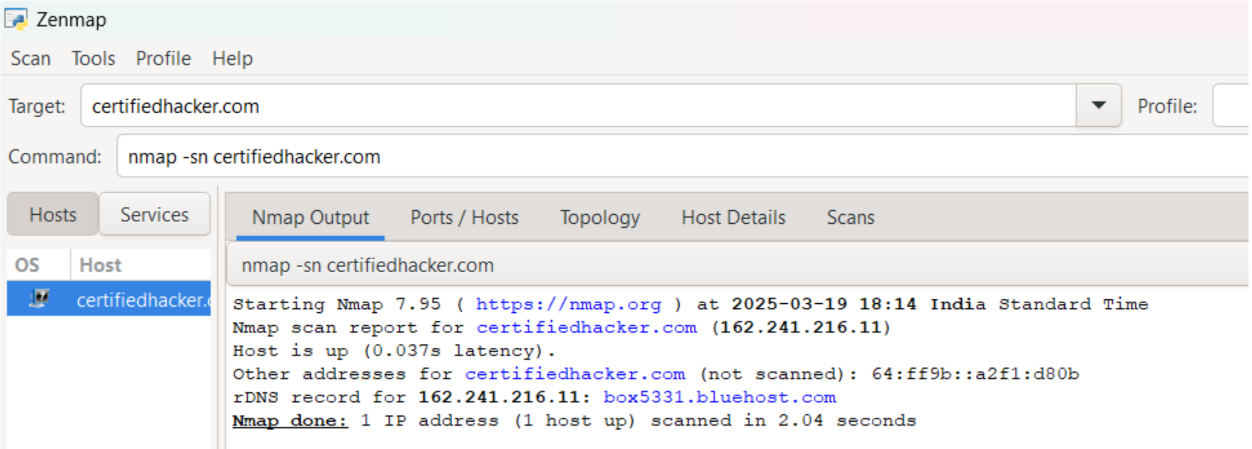
Target:

Profile:

Command: nmap --version

```
nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.6 openssl-3.0.13 nmap-libssh2-1.11.0 nmap-libz-1.3.1 nmap-libpcre2-10.43 Npcap-1.79 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select
```

2. Host Discovery or ping sweep scan (-sn) or (-sP).

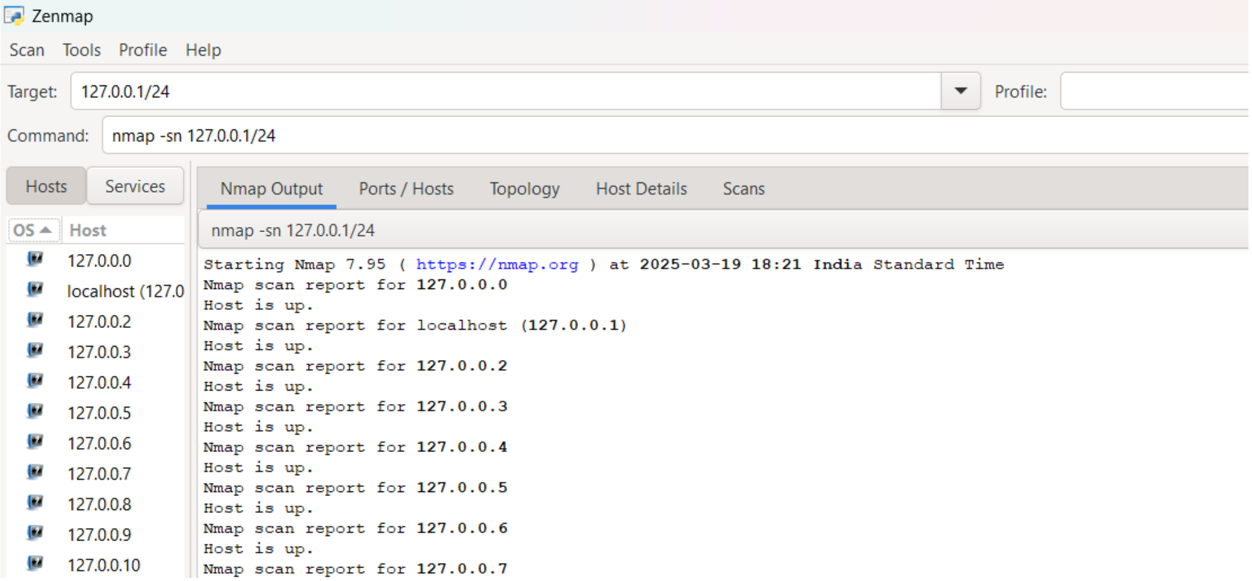


Target: certifiedhacker.com

Profile:

Command: nmap -sn certifiedhacker.com

```
nmap -sn certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:14 India Standard Time
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.037s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```



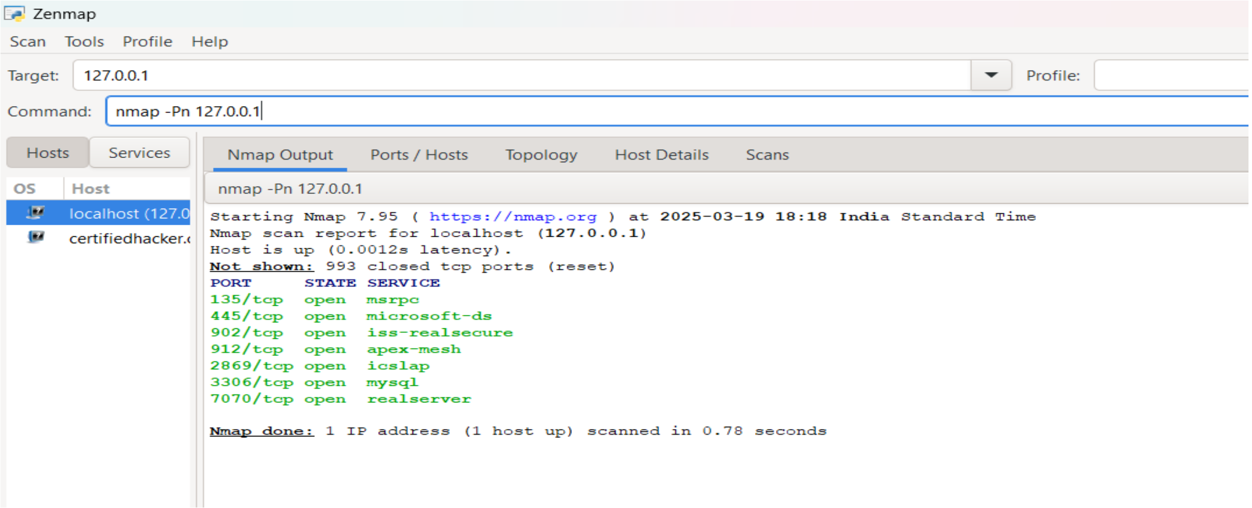
Target: 127.0.0.1/24

Profile:

Command: nmap -sn 127.0.0.1/24

```
nmap -sn 127.0.0.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:21 India Standard Time
Nmap scan report for 127.0.0.0
Host is up.
Nmap scan report for localhost (127.0.0.1)
Host is up.
Nmap scan report for 127.0.0.2
Host is up.
Nmap scan report for 127.0.0.3
Host is up.
Nmap scan report for 127.0.0.4
Host is up.
Nmap scan report for 127.0.0.5
Host is up.
Nmap scan report for 127.0.0.6
Host is up.
Nmap scan report for 127.0.0.7
```

3. No ping scan (-Pn).



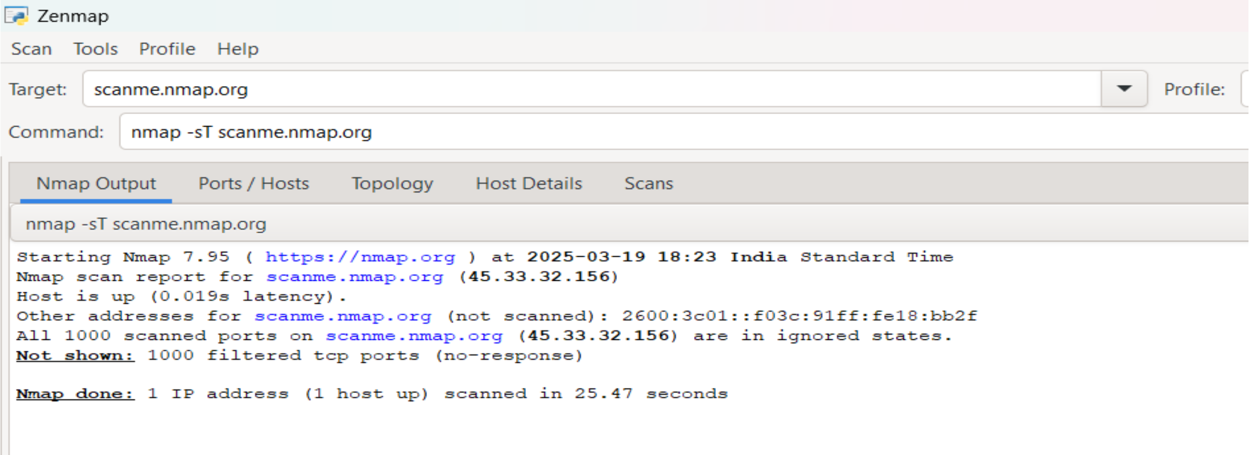
Target: 127.0.0.1

Command: nmap -Pn 127.0.0.1

nmap -Pn 127.0.0.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:18 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0012s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

4. TCP connect scan (Full scan) (-sT).

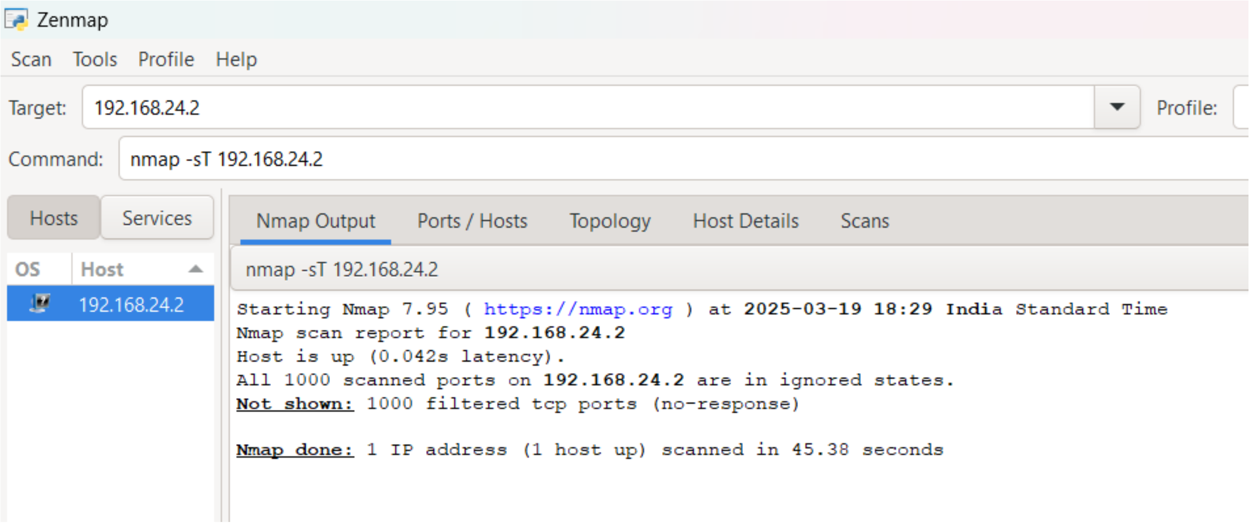


Target: scanme.nmap.org

Command: nmap -sT scanme.nmap.org

nmap -sT scanme.nmap.org

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:23 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.019s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 25.47 seconds
```



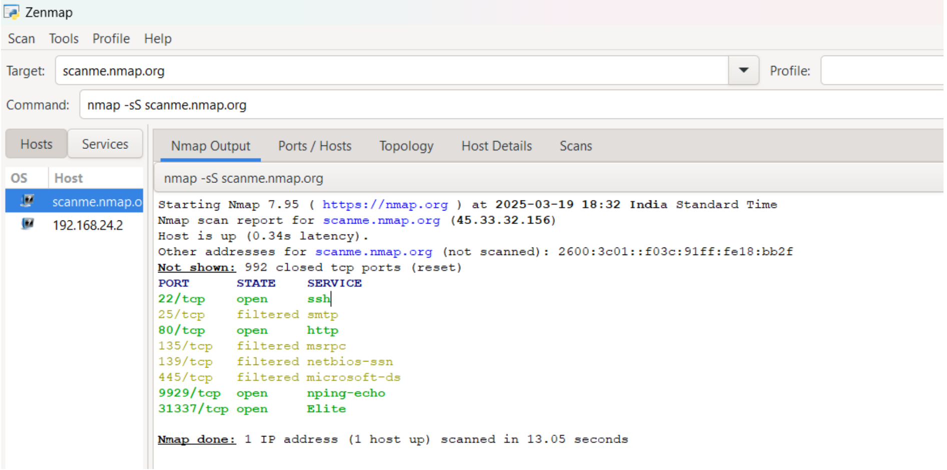
Target: 192.168.24.2

Command: nmap -sT 192.168.24.2

nmap -sT 192.168.24.2

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:29 India Standard Time
Nmap scan report for 192.168.24.2
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.24.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 45.38 seconds
```

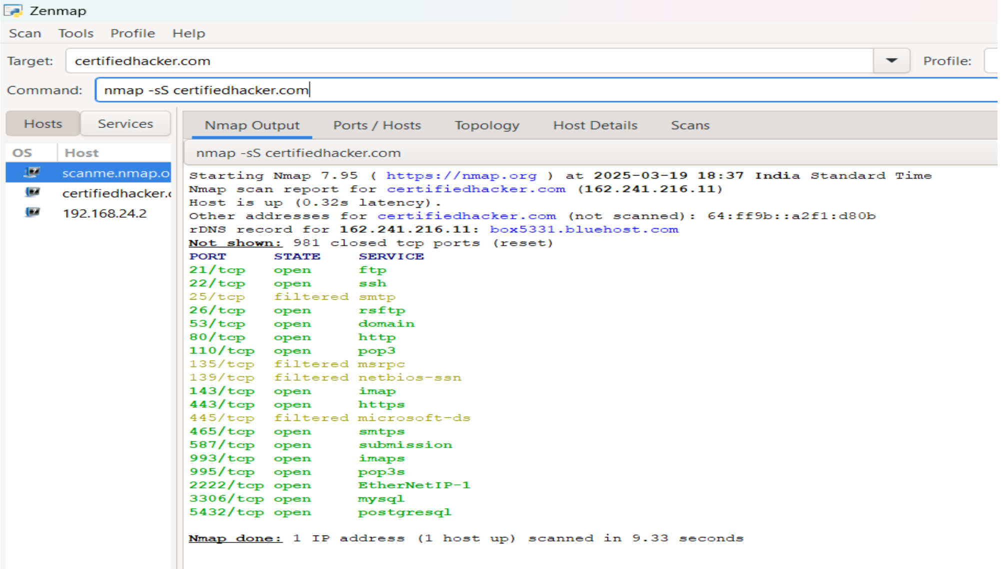
5. TCP SYN scan (“Half-open” or “Stealth” scans) (-sS).



Target: scanme.nmap.org

Command: nmap -sS scanme.nmap.org

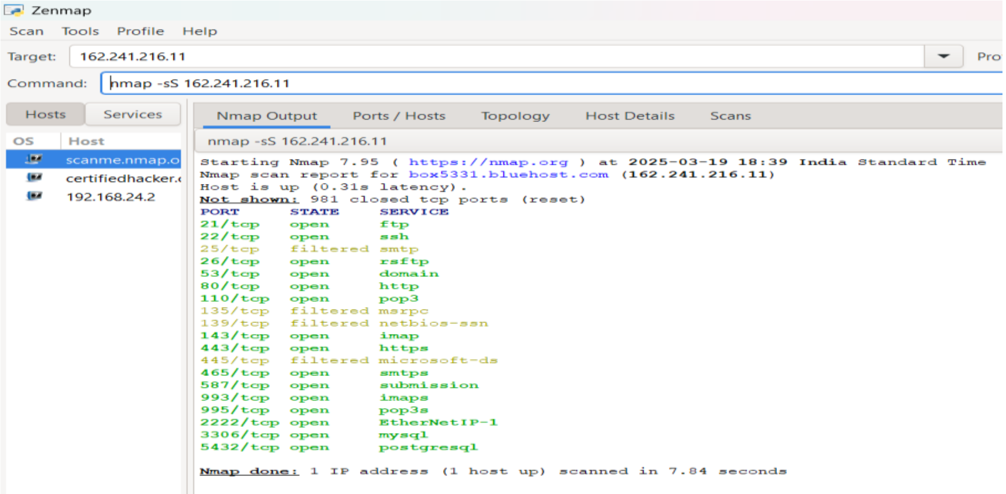
```
nmap -sS scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:32 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (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
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
```



Target: certifiedhacker.com

Command: nmap -sS certifiedhacker.com

```
nmap -sS certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:37 India Standard Time
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.32s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   filtered smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql
5432/tcp open     postgresql

Nmap done: 1 IP address (1 host up) scanned in 9.33 seconds
```



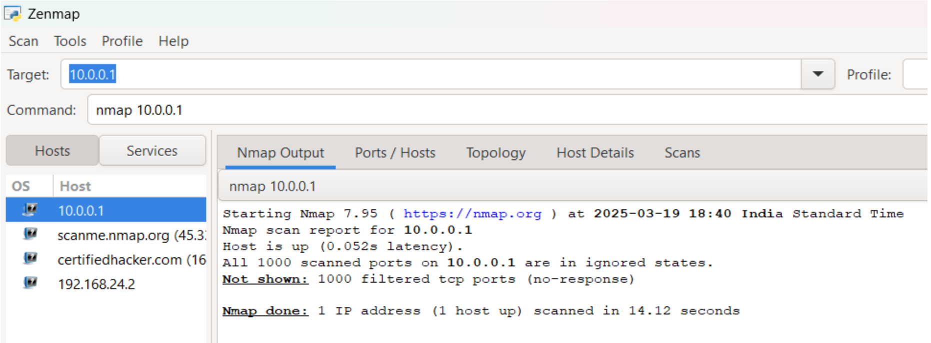
Target: 162.241.216.11

Command: nmap -sS 162.241.216.11

```
nmap -sS 162.241.216.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:39 India Standard Time
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.31s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   filtered smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql
5432/tcp open     postgresql

Nmap done: 1 IP address (1 host up) scanned in 7.84 seconds
```

6. IP address scan (Targets).

a. nmap 10.0.0.1

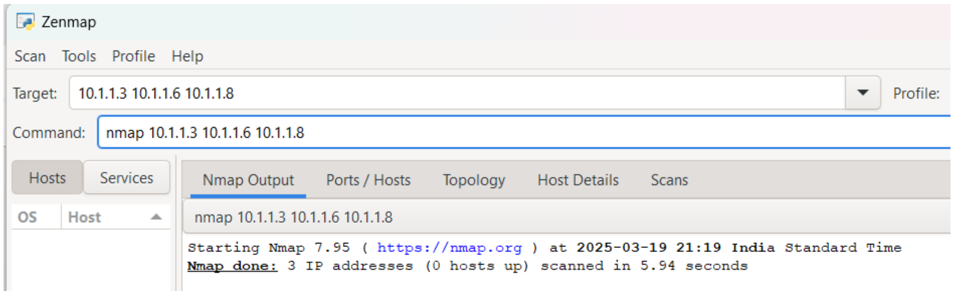


Target: 10.0.0.1

Command: nmap 10.0.0.1

```
nmap 10.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 18:40 India Standard Time
Nmap scan report for 10.0.0.1
Host is up (0.052s latency).
All 1000 scanned ports on 10.0.0.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 14.12 seconds
```

b. nmap 10.1.1.3 10.1.1.6 10.1.1.8

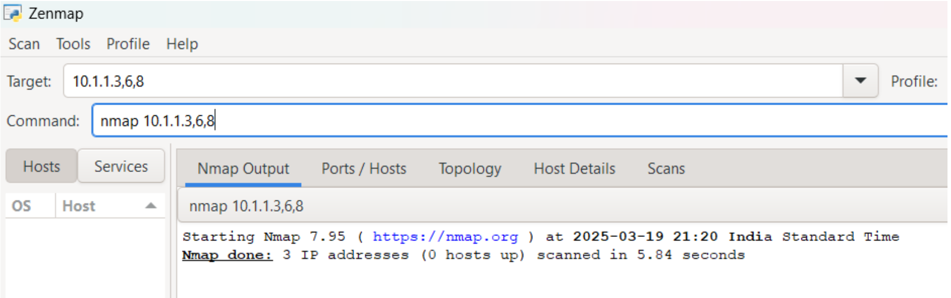


Target: 10.1.1.3 10.1.1.6 10.1.1.8

Command: nmap 10.1.1.3 10.1.1.6 10.1.1.8

```
nmap 10.1.1.3 10.1.1.6 10.1.1.8

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:19 India Standard Time
Nmap done: 3 IP addresses (0 hosts up) scanned in 5.94 seconds
```

c. nmap 10.1.1.3,6,8

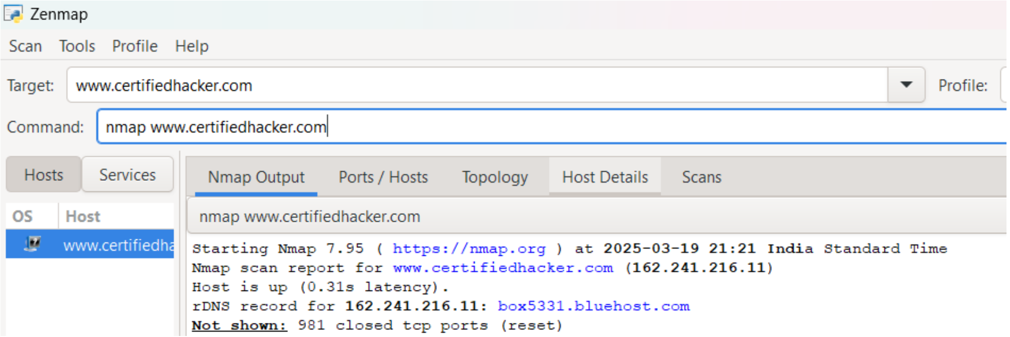


Target: 10.1.1.3,6,8

Command: nmap 10.1.1.3,6,8

```
nmap 10.1.1.3,6,8

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:20 India Standard Time
Nmap done: 3 IP addresses (0 hosts up) scanned in 5.84 seconds
```

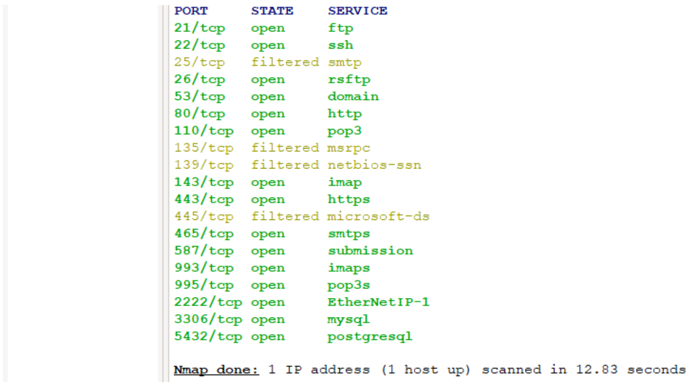
d. nmap www.certifiedhacker.com



Target: www.certifiedhacker.com

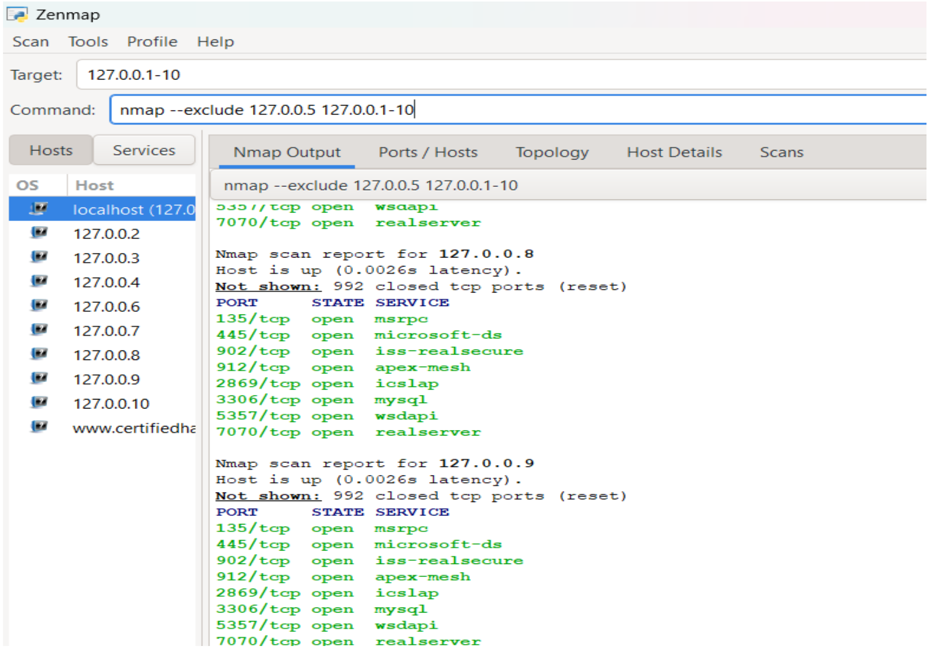
Command: nmap www.certifiedhacker.com

```
nmap www.certifiedhacker.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:21 India Standard Time
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.31s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
```



```
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   filtered smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql
5432/tcp open     postgresql

Nmap done: 1 IP address (1 host up) scanned in 12.83 seconds
```

e. nmap --exclude 127.0.0.5 127.0.0.1-10



Target: 127.0.0.1-10

Command: nmap --exclude 127.0.0.5 127.0.0.1-10

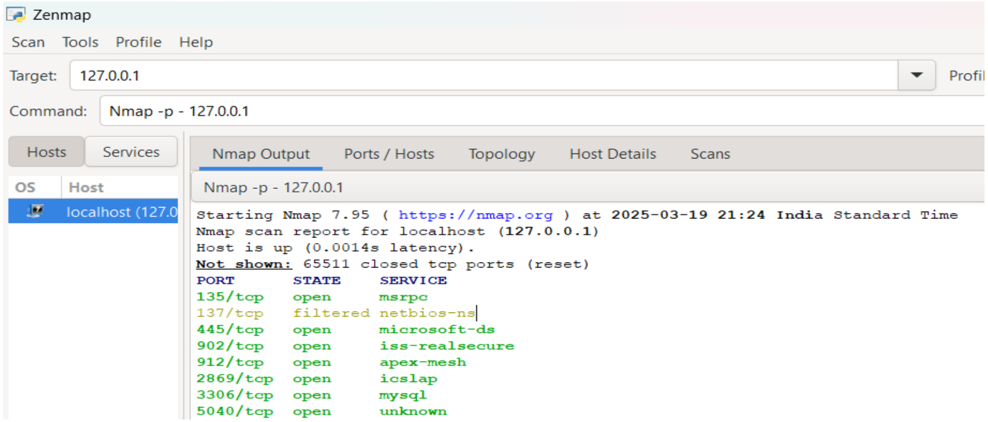
```
localhost (127.0
127.0.0.2
127.0.0.3
127.0.0.4
127.0.0.6
127.0.0.7
127.0.0.8
127.0.0.9
127.0.0.10
www.certifiedha
```

nmap --exclude 127.0.0.5 127.0.0.1-10

```
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap scan report for 127.0.0.8
Host is up (0.0026s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap scan report for 127.0.0.9
Host is up (0.0026s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
5357/tcp open  wsdapi
7070/tcp open  realserver
```

7. Scan the specified port or port range.

a. Nmap -p- 127.0.0.1

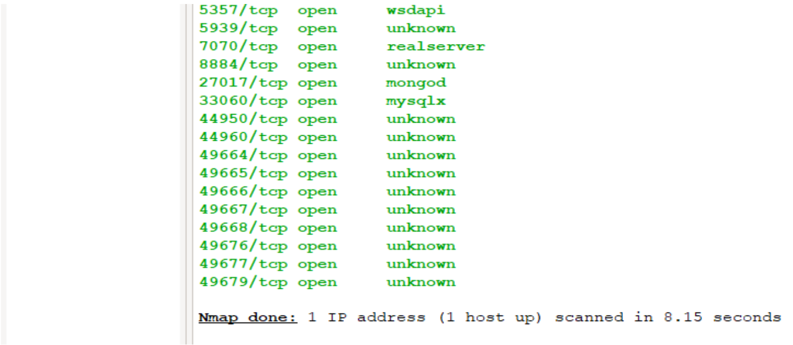


Target: 127.0.0.1

Command: Nmap -p - 127.0.0.1

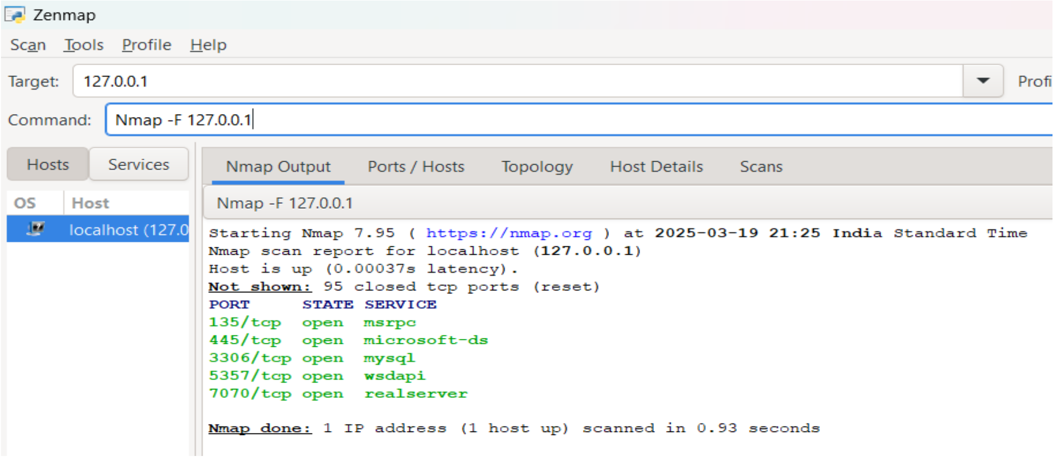
Nmap -p - 127.0.0.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:24 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0014s latency).
Not shown: 65511 closed tcp ports (reset)
PORT     STATE    SERVICE
135/tcp  open     msrpc
137/tcp  filtered netbios-ns
445/tcp  open     microsoft-ds
902/tcp  open     iss-realsecure
912/tcp  open     apex-mesh
2869/tcp open     icslap
3306/tcp open     mysql
5040/tcp open     unknown
```



```
5357/tcp  open     wsdapi
5939/tcp  open     unknown
7070/tcp  open     realserver
8884/tcp  open     unknown
27017/tcp open     mongod
33060/tcp open     mysqlx
44950/tcp open     unknown
44960/tcp open     unknown
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49676/tcp open     unknown
49677/tcp open     unknown
49679/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 8.15 seconds
```

b. Nmap -F 127.0.0.1

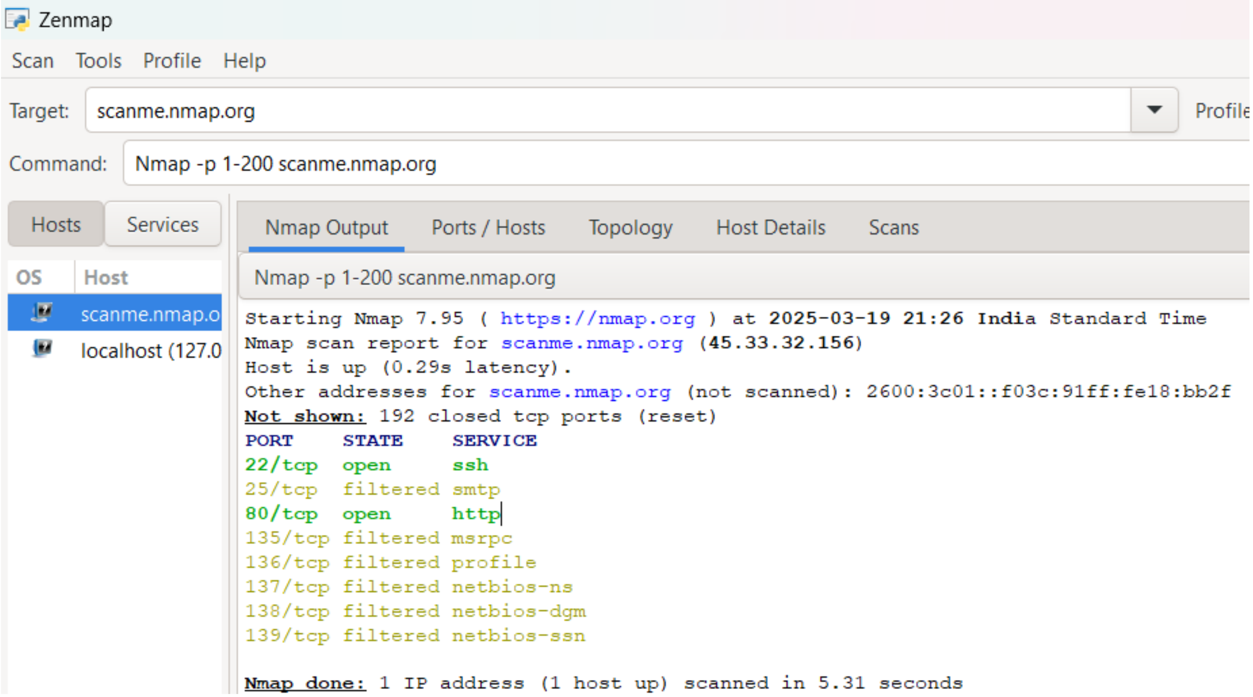


Target: 127.0.0.1

Command: Nmap -F 127.0.0.1

```
Nmap -F 127.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:25 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00037s latency).
Not shown: 95 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.93 seconds
```

c. Nmap -p 1-200 scanme.nmap.org

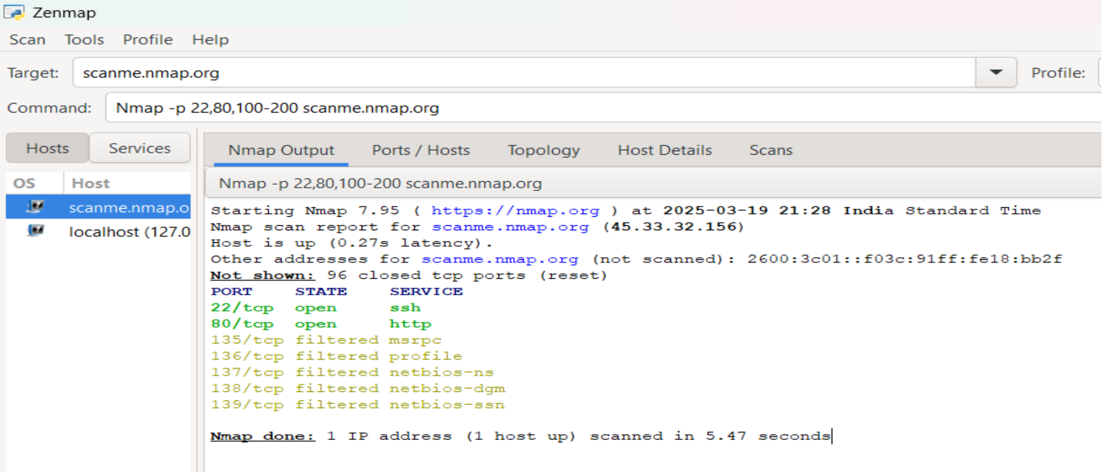


Target: scanme.nmap.org

Command: Nmap -p 1-200 scanme.nmap.org

```
Nmap -p 1-200 scanme.nmap.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:26 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 192 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   open     ssh
25/tcp   filtered smtp
80/tcp   open     http
135/tcp  filtered msrpc
136/tcp  filtered profile
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds
```

d. Nmap -p 22,80,100-200 scanme.nmap.org

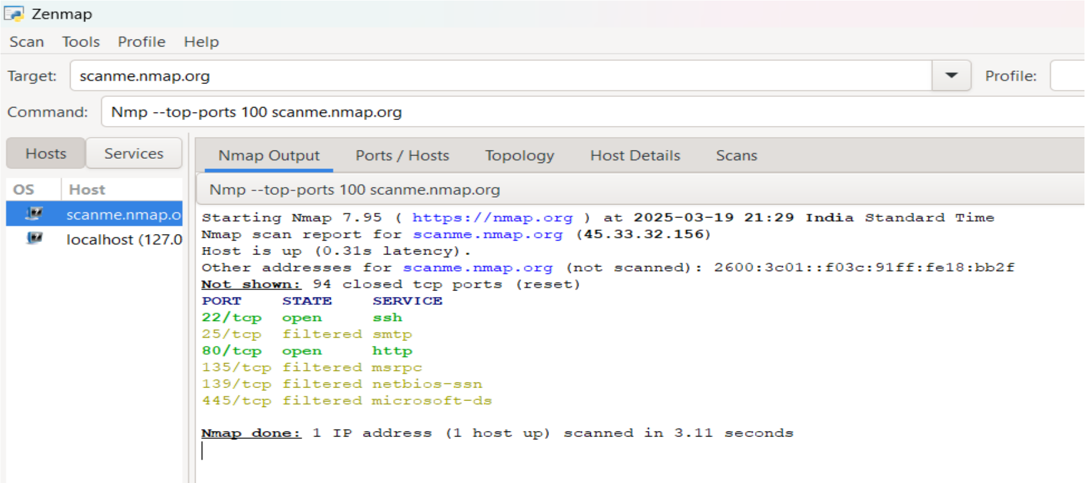


Target: scanme.nmap.org

Command: Nmap -p 22,80,100-200 scanme.nmap.org

```
Nmap -p 22,80,100-200 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:28 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 96 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  open     ssh
80/tcp  open     http
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds
```

e. Nmp --top-ports 100 scanme.nmap.org

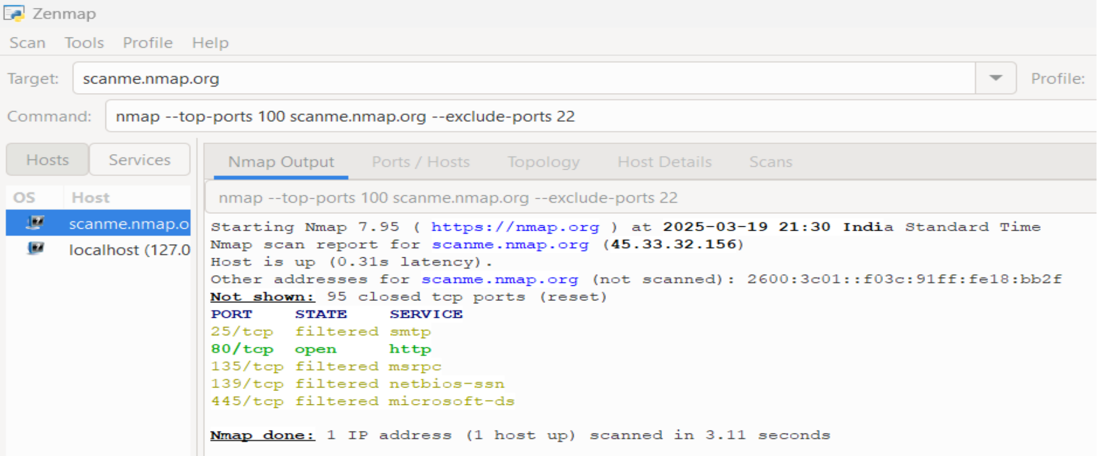


Target: scanme.nmap.org

Command: Nmp --top-ports 100 scanme.nmap.org

```
Nmp --top-ports 100 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:29 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 94 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

Nmap done: 1 IP address (1 host up) scanned in 3.11 seconds
```

f. nmap --top-ports 100 scanme.nmap.org --exclude-ports 22

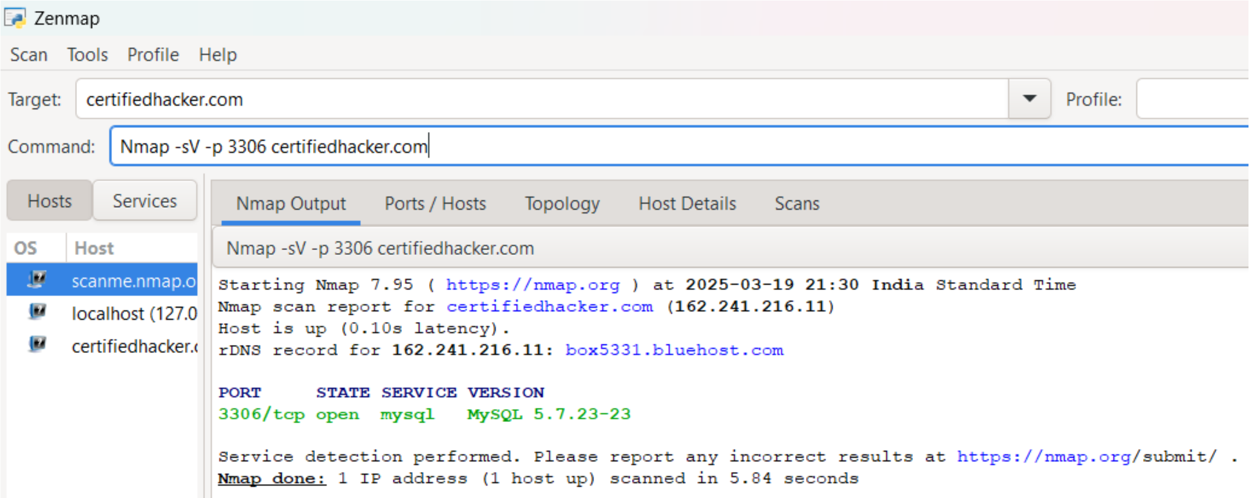


Target: scanme.nmap.org

Command: nmap --top-ports 100 scanme.nmap.org --exclude-ports 22

```
nmap --top-ports 100 scanme.nmap.org --exclude-ports 22
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:30 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 95 closed tcp ports (reset)
PORT    STATE    SERVICE
25/tcp  filtered smtp
80/tcp  open     http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 3.11 seconds
```

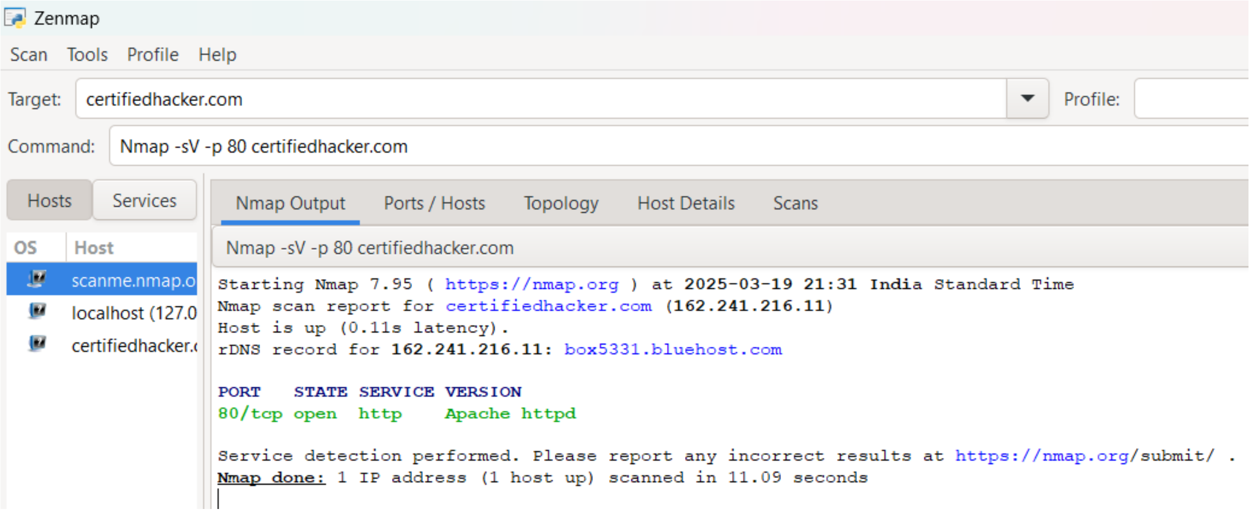
8. Determine the Service/Version information from open port (-sV).



Target: certifiedhacker.com

Command: Nmap -sV -p 3306 certifiedhacker.com

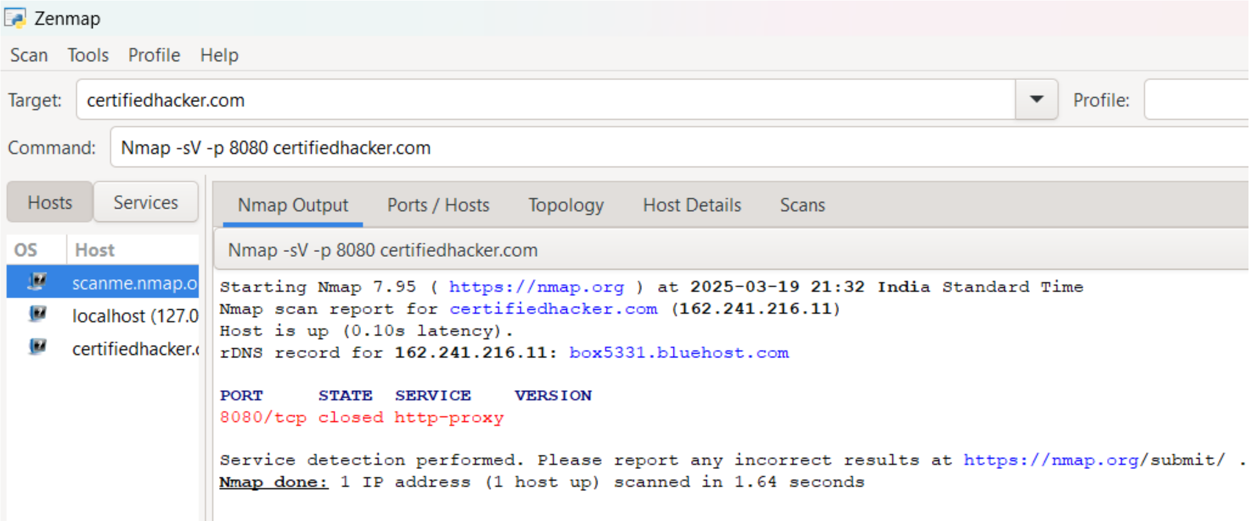
```
Nmap -sV -p 3306 certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:30 India Standard Time
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.10s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.7.23-23

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds
```



Target: certifiedhacker.com

Command: Nmap -sV -p 80 certifiedhacker.com

```
Nmap -sV -p 80 certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:31 India Standard Time
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.11s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.09 seconds
```

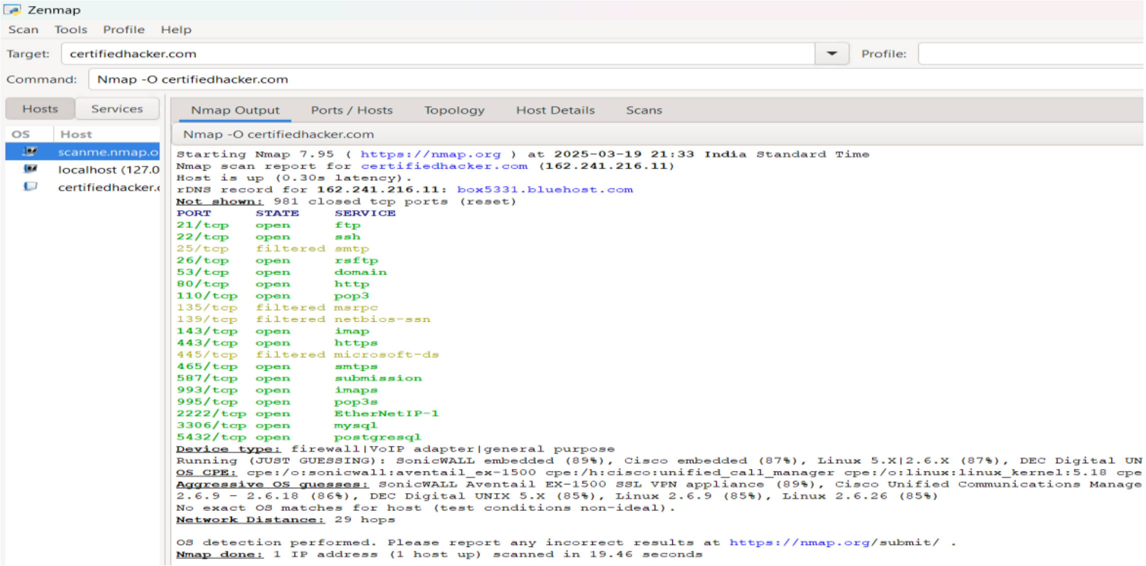


Target: certifiedhacker.com

Command: Nmap -sV -p 8080 certifiedhacker.com

```
Nmap -sV -p 8080 certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:32 India Standard Time
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.10s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT     STATE  SERVICE    VERSION
8080/tcp closed http-proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
```

9. Detect the Operating System of Target System (-O).

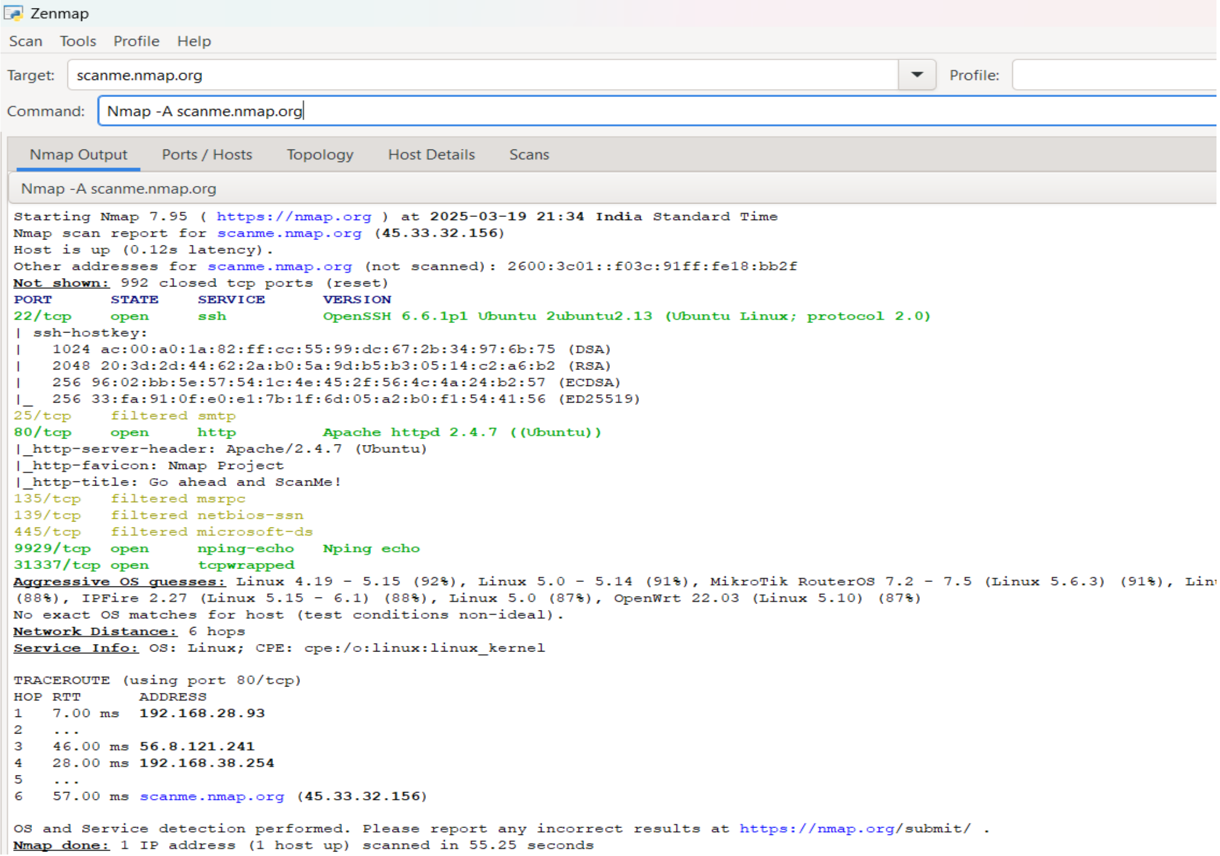


Target: certifiedhacker.com

Command: Nmap -O certifiedhacker.com

```
Nmap -O certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:33 India Standard Time
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.30s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    filtered smtp
26/tcp    open     rsftp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
445/tcp   filtered microsoft-ds
465/tcp   open     smtps
587/tcp   open     submission
993/tcp   open     imaps
995/tcp   open     pop3s
2222/tcp open      EtherNetIP-1
3306/tcp open      mysql
5432/tcp open      postgresql
Device type: firewall|VoIP adapter|general purpose
Running (JUST GUESSING): SonicWALL embedded (89%), Cisco embedded (87%), Linux 5.X|2.6.X (87%), DEC Digital UN
OS CPE: cpe:/o:sonicwall:aventail_ex-1500 cpe:/h:cisco:unified_call_manager cpe:/o:linux:linux_kernel:5.18 cpe
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (89%), Cisco Unified Communications Manage
2.6.9 - 2.6.18 (86%), DEC Digital UNIX 5.X (85%), Linux 2.6.9 (85%), Linux 2.6.26 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 29 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.46 seconds
```

10. Enable OS detection, version detection, script scanning, and traceroute (Aggressive scan) (-A).

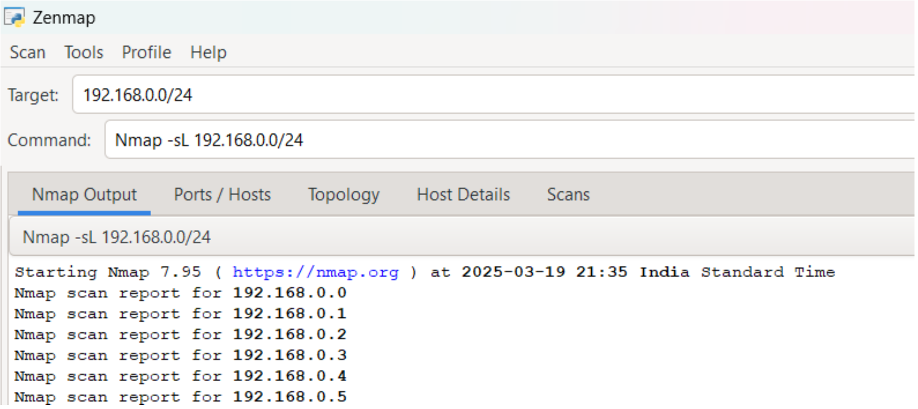


Target: scanme.nmap.org

Command: Nmap -A scanme.nmap.org

```
Nmap -A scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:34 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 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    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-favicon: Nmap Project
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 4.19 - 5.15 (92%), Linux 5.0 - 5.14 (91%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (91%), Lin
(88%), IPFire 2.27 (Linux 5.15 - 6.1) (88%), Linux 5.0 (87%), OpenWrt 22.03 (Linux 5.10) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 6 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   7.00 ms  192.168.28.93
2   ...
3   46.00 ms 56.8.121.241
4   28.00 ms 192.168.38.254
5   ...
6   57.00 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 55.25 seconds
```

11. List Scan (-sL) (Host Discovery).



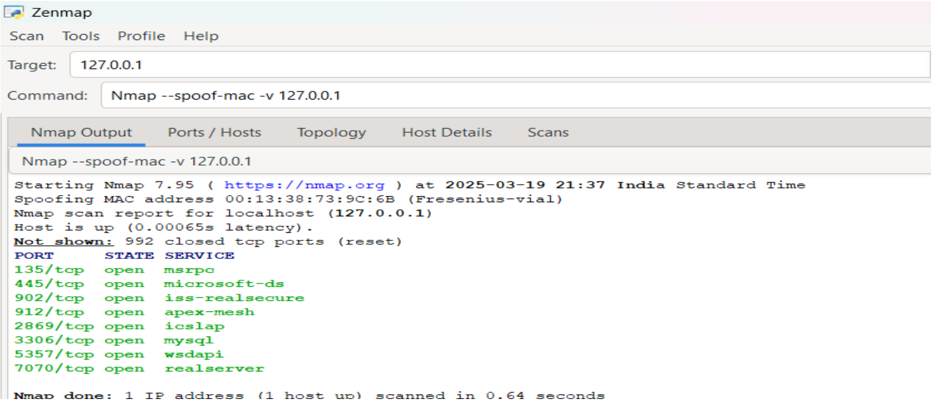
Target: 192.168.0.0/24

Command: Nmap -sL 192.168.0.0/24

Nmap -sL 192.168.0.0/24

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:35 India Standard Time
Nmap scan report for 192.168.0.0
Nmap scan report for 192.168.0.1
Nmap scan report for 192.168.0.2
Nmap scan report for 192.168.0.3
Nmap scan report for 192.168.0.4
Nmap scan report for 192.168.0.5
```

12. Verbose mode scan (-v) / (-vv) / (-vvv).

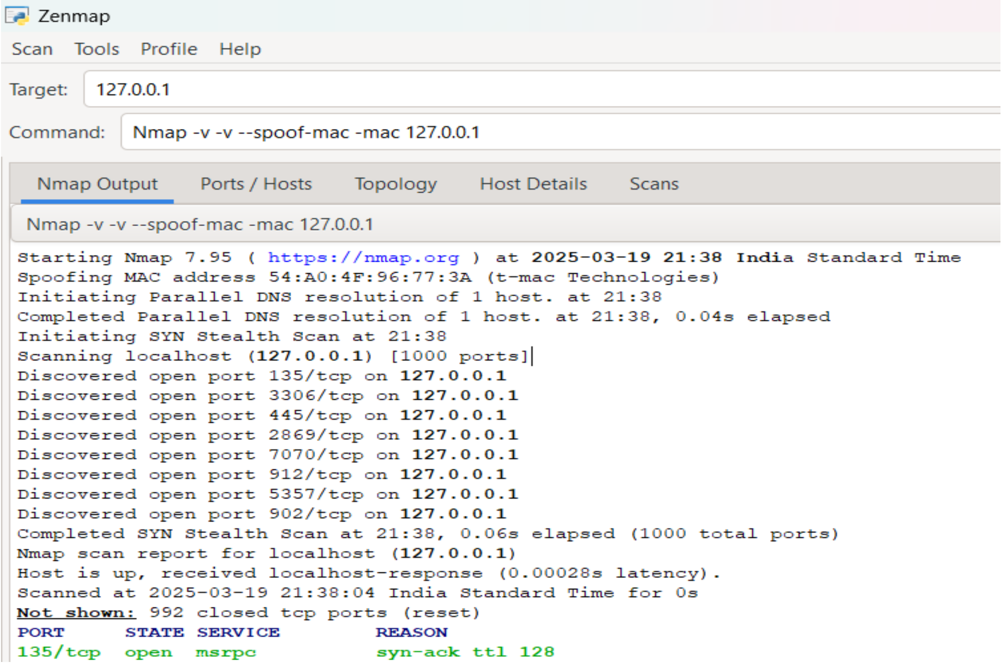


Target: 127.0.0.1

Command: Nmap --spoof-mac -v 127.0.0.1

Nmap --spoof-mac -v 127.0.0.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:37 India Standard Time
Spoofing MAC address 00:13:38:73:9C:6B (Fresenius-vial)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00065s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
```

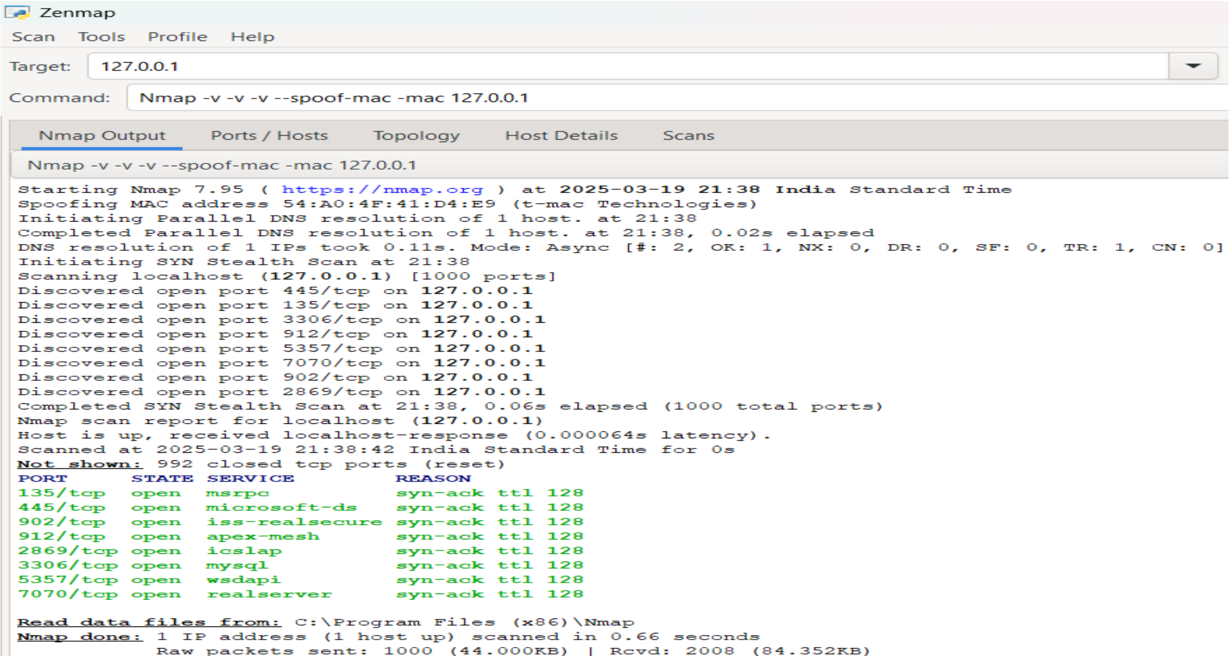


Target: 127.0.0.1

Command: Nmap -v -v --spoof-mac -mac 127.0.0.1

Nmap -v -v --spoof-mac -mac 127.0.0.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:38 India Standard Time
Spoofing MAC address 54:A0:4F:96:77:3A (t-mac Technologies)
Initiating Parallel DNS resolution of 1 host. at 21:38
Completed Parallel DNS resolution of 1 host. at 21:38, 0.04s elapsed
Initiating SYN Stealth Scan at 21:38
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 2869/tcp on 127.0.0.1
Discovered open port 7070/tcp on 127.0.0.1
Discovered open port 912/tcp on 127.0.0.1
Discovered open port 5357/tcp on 127.0.0.1
Discovered open port 902/tcp on 127.0.0.1
Completed SYN Stealth Scan at 21:38, 0.06s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.00028s latency).
Scanned at 2025-03-19 21:38:04 India Standard Time for 0s
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE        REASON
135/tcp  open  msrpc          syn-ack ttl 128
```

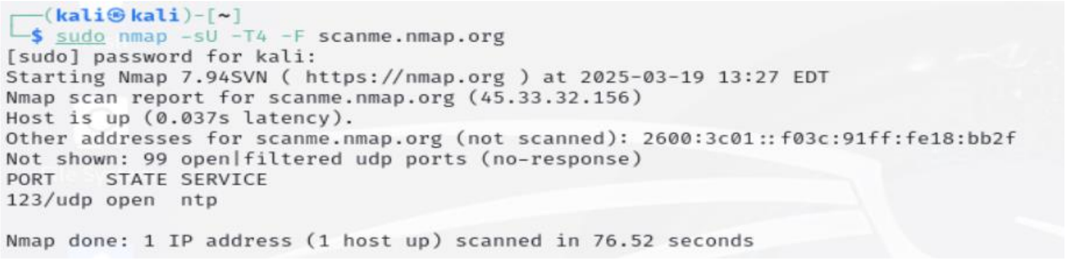


Target: 127.0.0.1

Command: Nmap -v -v -v --spoof-mac -mac 127.0.0.1

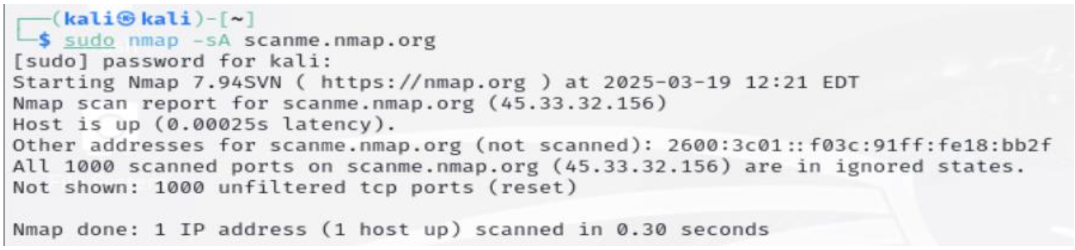
```
Nmap -v -v -v --spoof-mac -mac 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 21:38 India Standard Time
Spoofing MAC address 54:A0:4F:41:D4:E9 (t-mac Technologies)
Initiating Parallel DNS resolution of 1 host. at 21:38
Completed Parallel DNS resolution of 1 host. at 21:38, 0.02s elapsed
DNS resolution of 1 IPs took 0.11s. Mode: Async [#: 2, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 21:38
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 912/tcp on 127.0.0.1
Discovered open port 5357/tcp on 127.0.0.1
Discovered open port 7070/tcp on 127.0.0.1
Discovered open port 902/tcp on 127.0.0.1
Discovered open port 2869/tcp on 127.0.0.1
Completed SYN Stealth Scan at 21:38, 0.06s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.000064s latency).
Scanned at 2025-03-19 21:38:42 India Standard Time for 0s
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE        REASON
135/tcp  open  msrpc          syn-ack ttl 128
445/tcp  open  microsoft-ds   syn-ack ttl 128
902/tcp  open  iss-realsecure syn-ack ttl 128
912/tcp  open  apex-mesh      syn-ack ttl 128
2869/tcp open  icslap         syn-ack ttl 128
3306/tcp open  mysql          syn-ack ttl 128
5357/tcp open  wsdapi         syn-ack ttl 128
7070/tcp open  realserver     syn-ack ttl 128

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
           Raw packets sent: 1000 (44.000KB) | Rcvd: 2008 (84.352KB)
```

13. UDP scan (-sU)

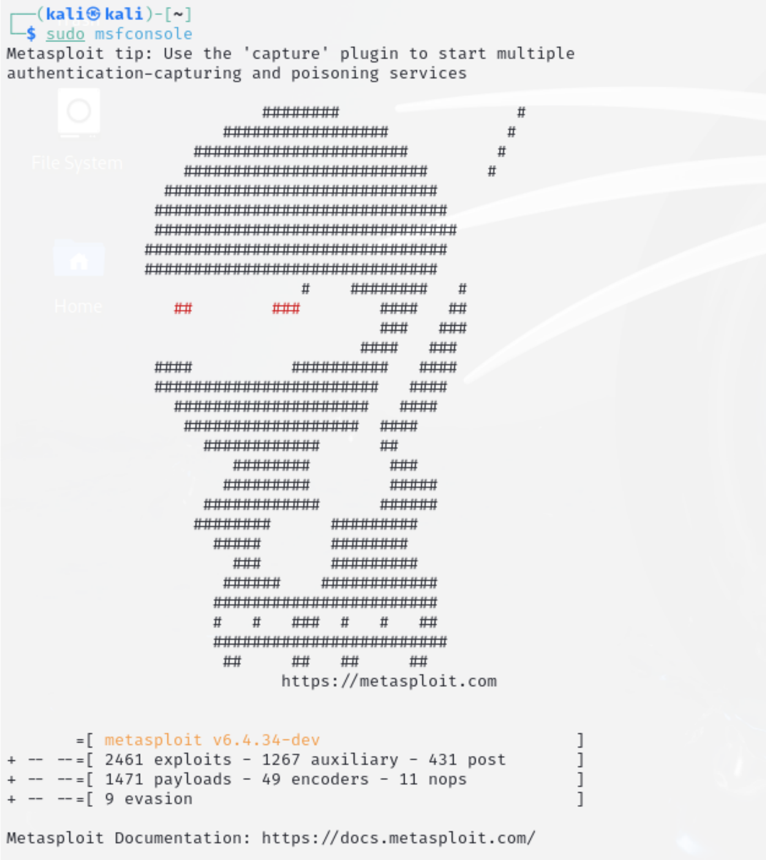


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -T4 -F scanme.nmap.org
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-19 13:27 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.037s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 99 open|filtered udp ports (no-response)
PORT    STATE SERVICE
123/udp open  ntp

Nmap done: 1 IP address (1 host up) scanned in 76.52 seconds
```

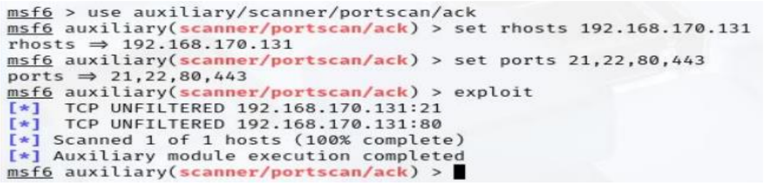
14. ACK scan (-sA)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA scanme.nmap.org
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-19 12:21 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00025s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

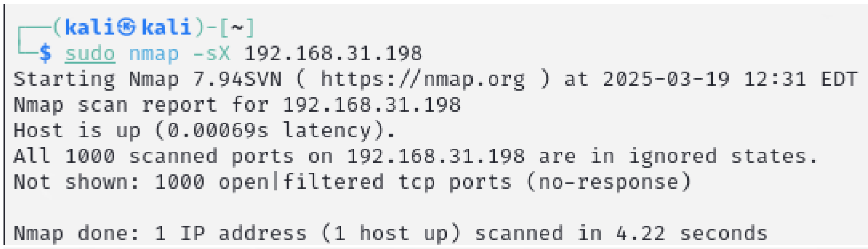


```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

                 ########                  #
             #################            #
          ######################         #
         #########################      #
       ############################
      ##############################
      ###############################
     ###############################
     ##############################
                     #    ########   #
        ##        ###        ####   ##
                             ###   ###
                           ####   ###
      ####          ##########   ####
      #######################   ####
        ####################   ####
         ##################  ####
           ############      ##
              ########        ###
             #########        #####
           ############      ######
          ########      #########
            #####       ########
              ###       #########
             ######    ############
            #######################
            #   #   ###  #   #   ##
            ########################
             ##     ##   ##     ##
                   https://metasploit.com


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

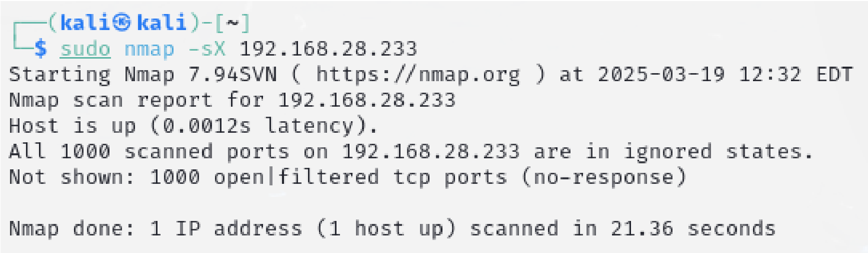


```
msf6 > use auxiliary/scanner/portscan/ack
msf6 auxiliary(scanner/portscan/ack) > set rhosts 192.168.170.131
rhosts => 192.168.170.131
msf6 auxiliary(scanner/portscan/ack) > set ports 21,22,80,443
ports => 21,22,80,443
msf6 auxiliary(scanner/portscan/ack) > exploit
[*]  TCP UNFILTERED 192.168.170.131:21
[*]  TCP UNFILTERED 192.168.170.131:80
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/ack) > █
```

15. XMAS Scan (-sX)

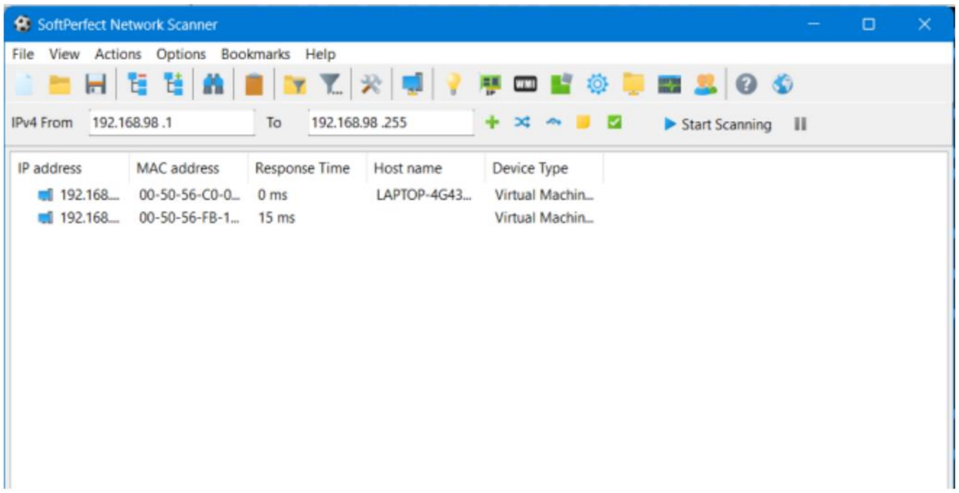


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX 192.168.31.198
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-19 12:31 EDT
Nmap scan report for 192.168.31.198
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.31.198 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX 192.168.28.233
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-19 12:32 EDT
Nmap scan report for 192.168.28.233
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.28.233 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.36 seconds
```

16. Enumeration using “SoftPerfect Network Scanner” Tool (Window based)


SoftPerfect Network Scanner
File View Actions Options Bookmarks Help
IPv4 From 192.168.98 .1 To 192.168.98 .255
Start Scanning

IP address	MAC address	Response Time	Host name	Device Type
192.168...	00-50-56-C0-0...	0 ms	LAPTOP-4G43...	Virtual Machin...
192.168...	00-50-56-FB-1...	15 ms		Virtual Machin...

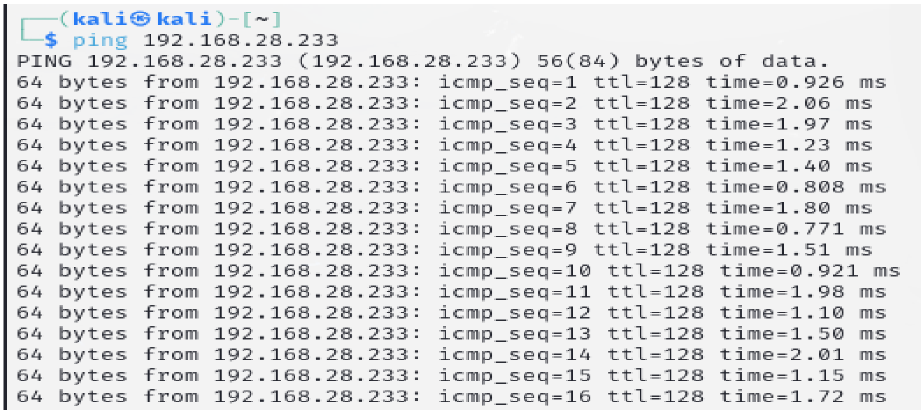
17. Perform banner grabbing using following tools:

Required machines are as follow:

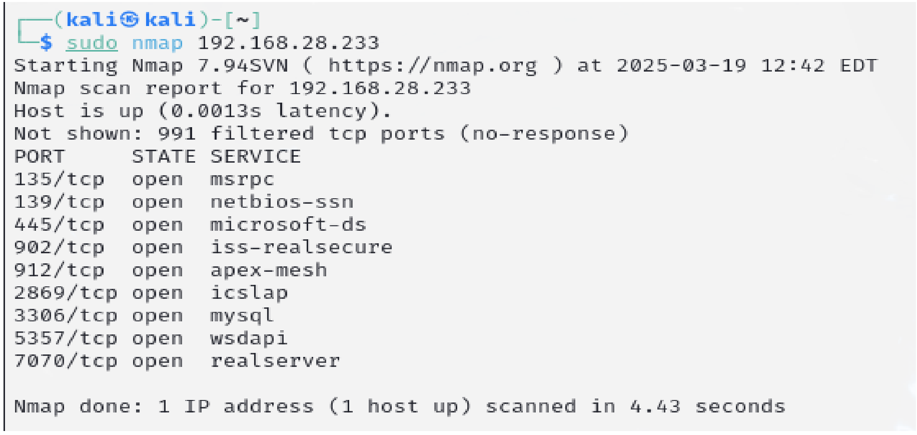
A. Kali linux (Attacker machine)

B. Metasploitable 2 (Target machine)

Check the connectivity between two machines:

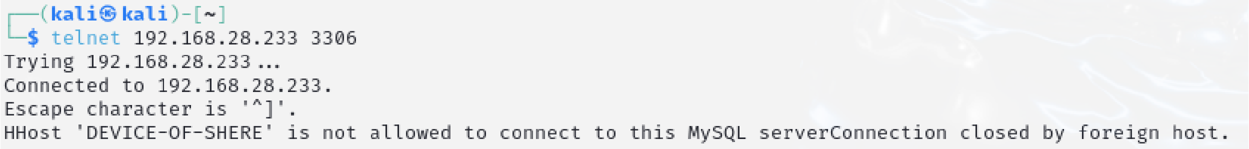


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.28.233
PING 192.168.28.233 (192.168.28.233) 56(84) bytes of data.
64 bytes from 192.168.28.233: icmp_seq=1 ttl=128 time=0.926 ms
64 bytes from 192.168.28.233: icmp_seq=2 ttl=128 time=2.06 ms
64 bytes from 192.168.28.233: icmp_seq=3 ttl=128 time=1.97 ms
64 bytes from 192.168.28.233: icmp_seq=4 ttl=128 time=1.23 ms
64 bytes from 192.168.28.233: icmp_seq=5 ttl=128 time=1.40 ms
64 bytes from 192.168.28.233: icmp_seq=6 ttl=128 time=0.808 ms
64 bytes from 192.168.28.233: icmp_seq=7 ttl=128 time=1.80 ms
64 bytes from 192.168.28.233: icmp_seq=8 ttl=128 time=0.771 ms
64 bytes from 192.168.28.233: icmp_seq=9 ttl=128 time=1.51 ms
64 bytes from 192.168.28.233: icmp_seq=10 ttl=128 time=0.921 ms
64 bytes from 192.168.28.233: icmp_seq=11 ttl=128 time=1.98 ms
64 bytes from 192.168.28.233: icmp_seq=12 ttl=128 time=1.10 ms
64 bytes from 192.168.28.233: icmp_seq=13 ttl=128 time=1.50 ms
64 bytes from 192.168.28.233: icmp_seq=14 ttl=128 time=2.01 ms
64 bytes from 192.168.28.233: icmp_seq=15 ttl=128 time=1.15 ms
64 bytes from 192.168.28.233: icmp_seq=16 ttl=128 time=1.72 ms
```



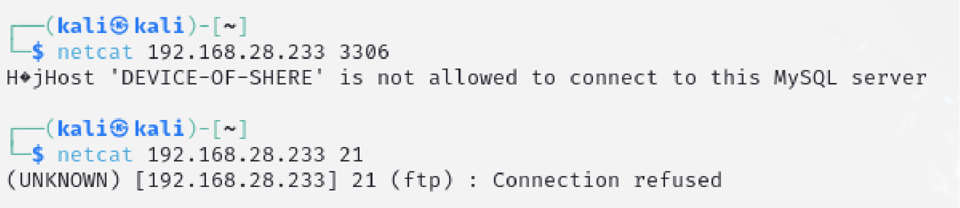
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.28.233
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-19 12:42 EDT
Nmap scan report for 192.168.28.233
Host is up (0.0013s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 4.43 seconds
```

a. Telnet



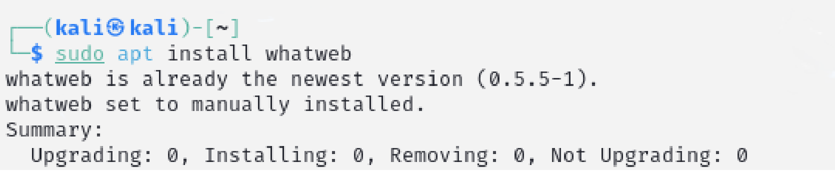
```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.28.233 3306
Trying 192.168.28.233...
Connected to 192.168.28.233.
Escape character is '^]'.
HHost 'DEVICE-OF-SHERE' is not allowed to connect to this MySQL serverConnection closed by foreign host.
```

b. Netcat

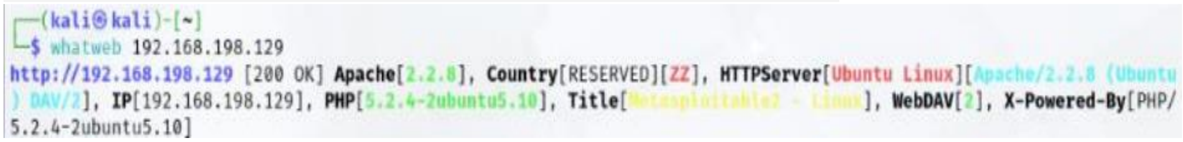


```
┌──(kali㉿kali)-[~]
└─$ netcat 192.168.28.233 3306
H◆jHost 'DEVICE-OF-SHERE' is not allowed to connect to this MySQL server

┌──(kali㉿kali)-[~]
└─$ netcat 192.168.28.233 21
(UNKNOWN) [192.168.28.233] 21 (ftp) : Connection refused
```

c. WhatWeb

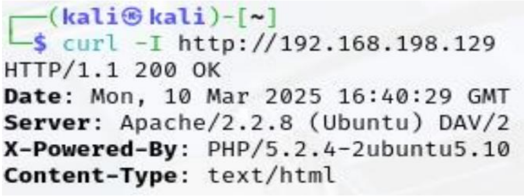


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install whatweb
whatweb is already the newest version (0.5.5-1).
whatweb set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```



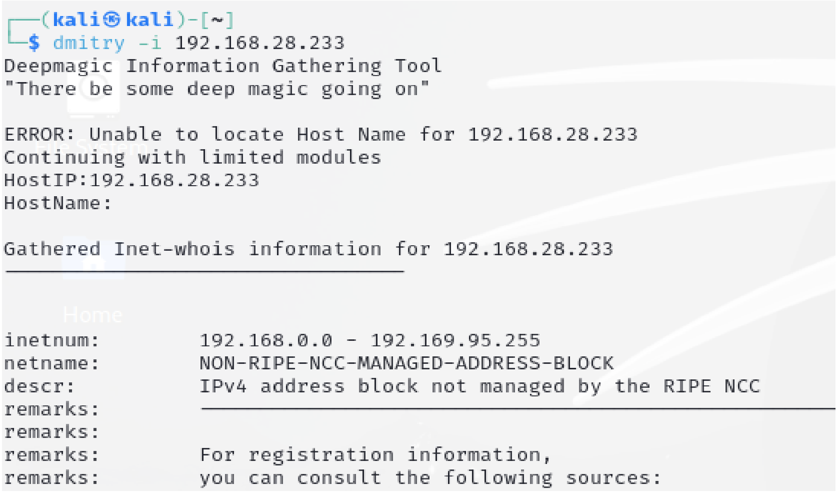
```
┌──(kali㉿kali)-[~]
└─$ whatweb 192.168.198.129
http://192.168.198.129 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu
) DAV/2], IP[192.168.198.129], PHP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/
5.2.4-2ubuntu5.10]
```

d. Curl



```
┌──(kali㉿kali)-[~]
└─$ curl -I http://192.168.198.129
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 16:40:29 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

e. Dmtriy



```
┌──(kali㉿kali)-[~]
└─$ dmitry -i 192.168.28.233
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.28.233
Continuing with limited modules
HostIP:192.168.28.233
HostName:

Gathered Inet-whois information for 192.168.28.233
─────────────────────────────────


inetnum:        192.168.0.0 - 192.169.95.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ────────────────────────────────────────────────────
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
```