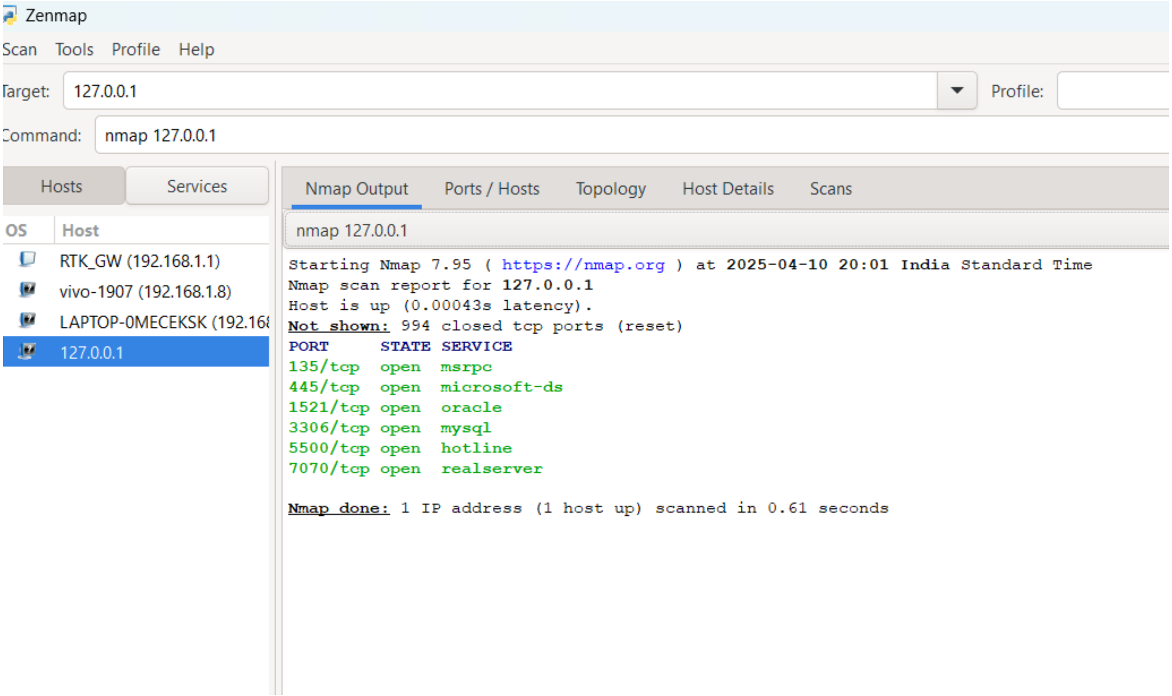
Basic Nmap Commands

1. Simple scan

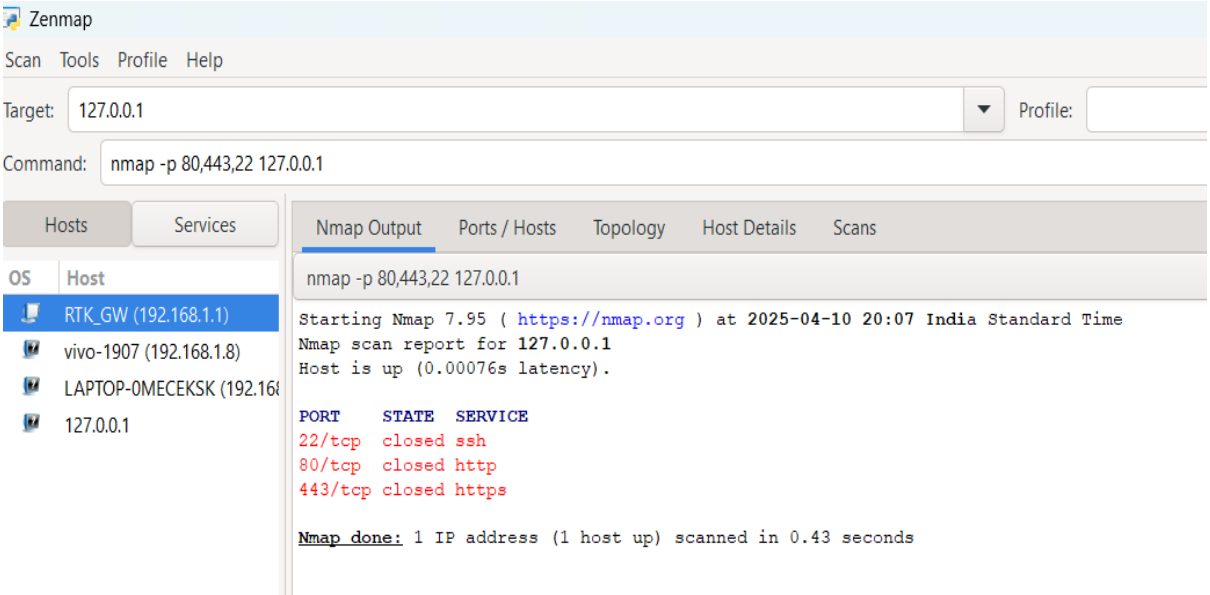


Target: 127.0.0.1

Command: nmap 127.0.0.1

```
nmap 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 20:01 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00043s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
5500/tcp open  hotline
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

2. Scan specific ports

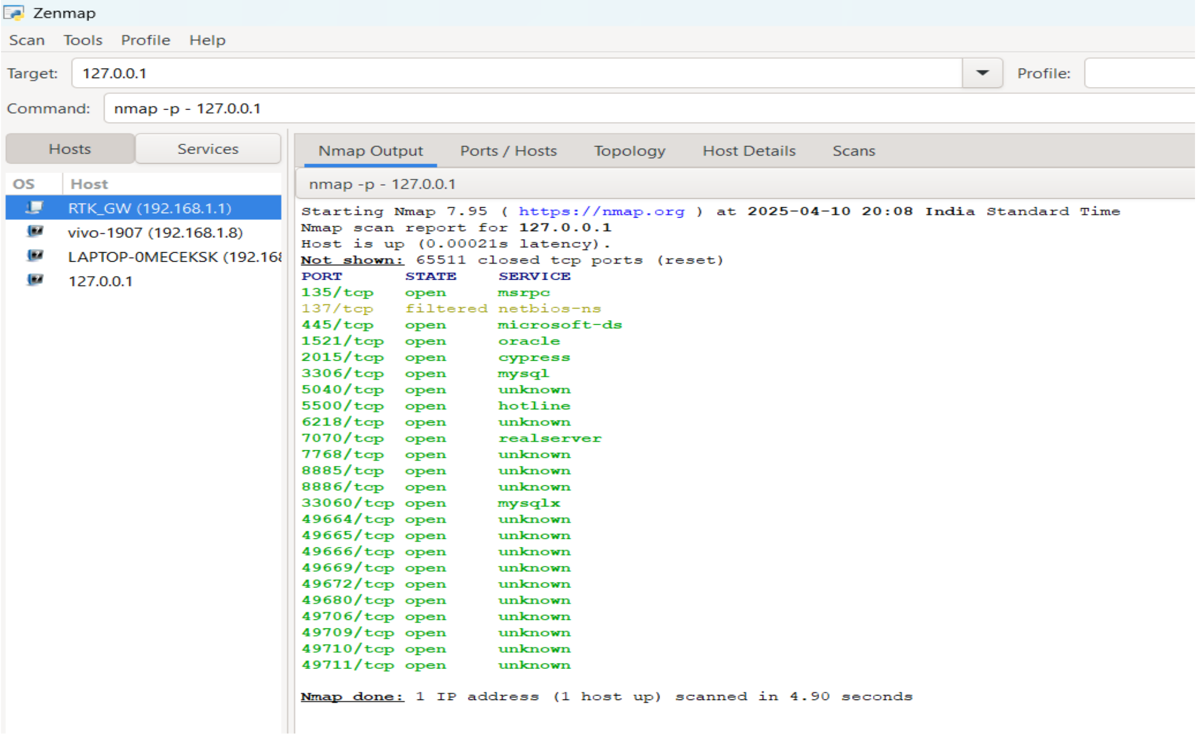


Target: 127.0.0.1

Command: nmap -p 80,443,22 127.0.0.1

```
nmap -p 80,443,22 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 20:07 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00076s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

3. Scan all ports



Target: 127.0.0.1

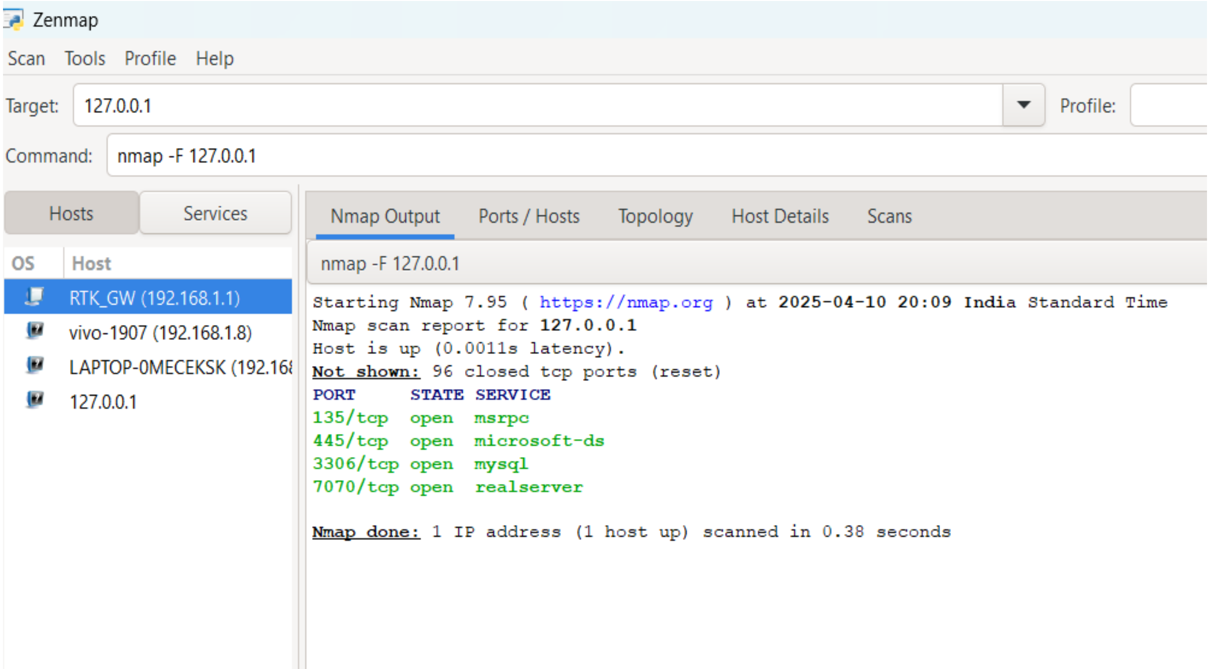
Command: nmap -p - 127.0.0.1

RTK_GW (192.168.1.1)
vivo-1907 (192.168.1.8)
LAPTOP-0MECEKSK (192.16
127.0.0.1

nmap -p - 127.0.0.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 20:08 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00021s 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
1521/tcp  open     oracle
2015/tcp  open     cypress
3306/tcp  open     mysql
5040/tcp  open     unknown
5500/tcp  open     hotline
6218/tcp  open     unknown
7070/tcp  open     realserver
7768/tcp  open     unknown
8885/tcp  open     unknown
8886/tcp  open     unknown
33060/tcp open     mysqlx
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49669/tcp open     unknown
49672/tcp open     unknown
49680/tcp open     unknown
49706/tcp open     unknown
49709/tcp open     unknown
49710/tcp open     unknown
49711/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 4.90 seconds
```

4. Fast Scan



Target: 127.0.0.1

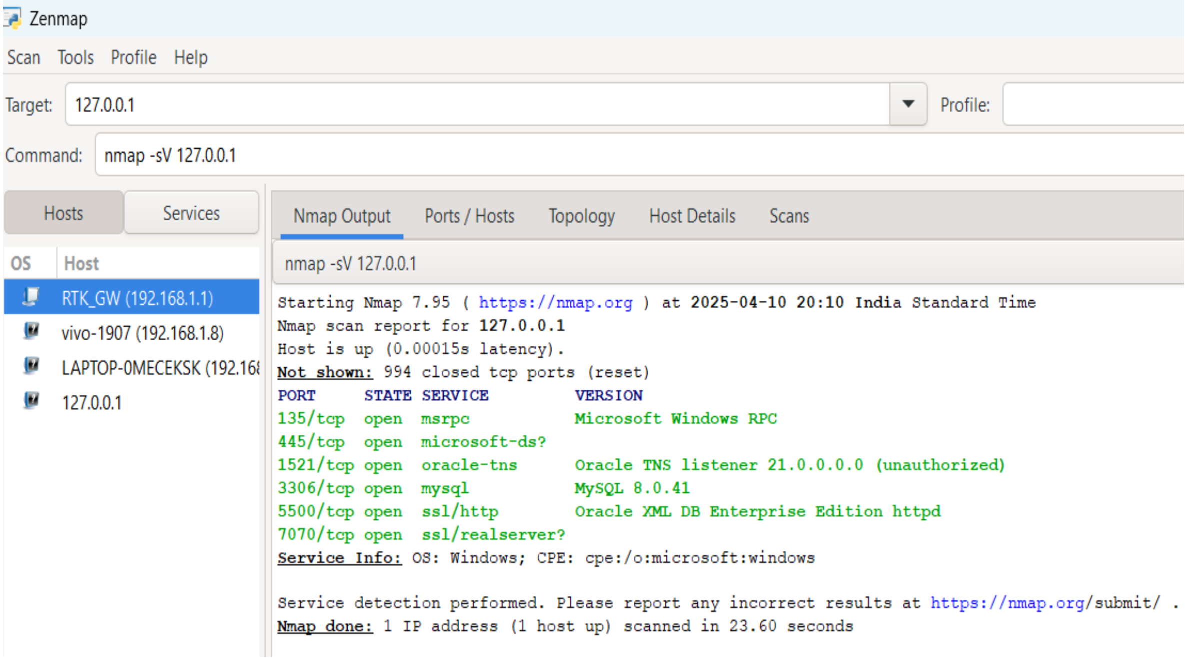
Command: nmap -F 127.0.0.1

RTK_GW (192.168.1.1)
vivo-1907 (192.168.1.8)
LAPTOP-0MECEKSK (192.16
127.0.0.1

nmap -F 127.0.0.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 20:09 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.0011s latency).
Not shown: 96 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

5. Service Version Detection



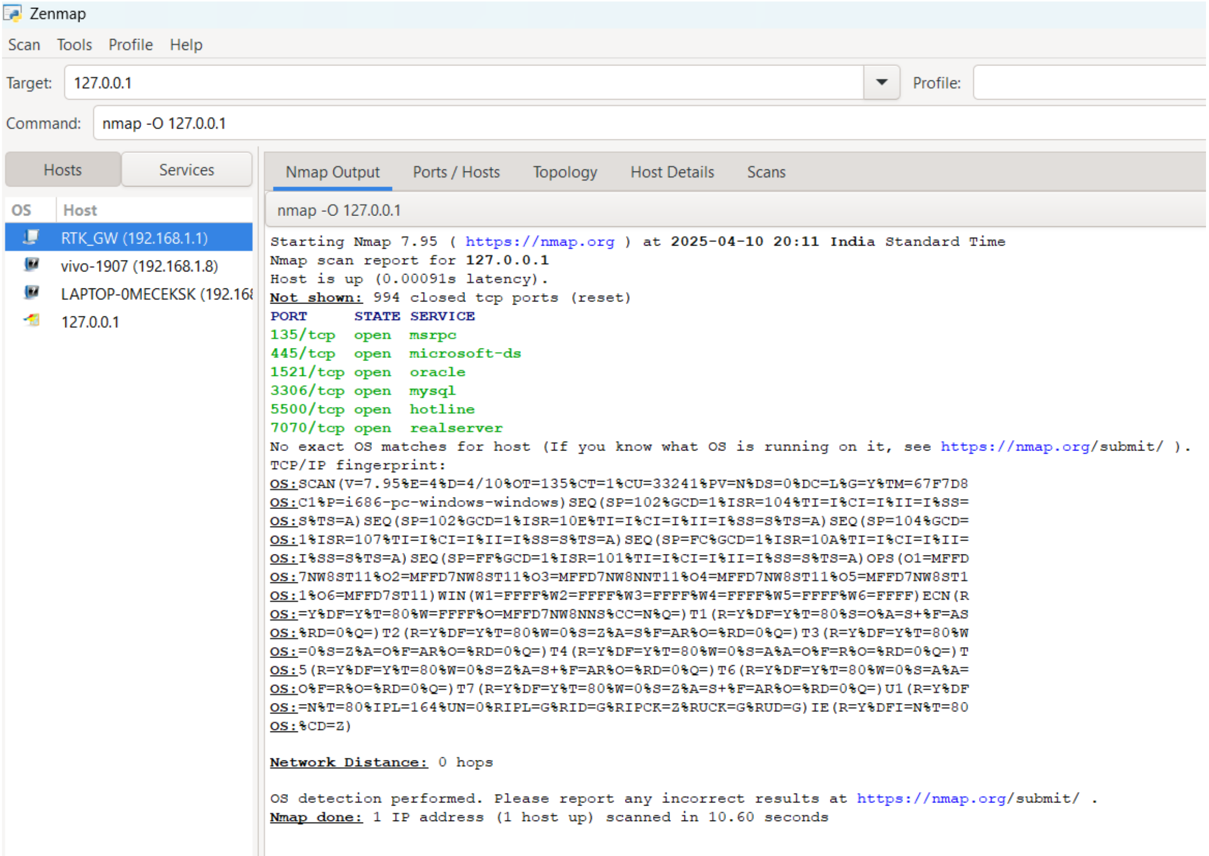
Target: 127.0.0.1 Profile:

Command: nmap -sV 127.0.0.1

nmap -sV 127.0.0.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 20:10 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00015s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
445/tcp  open  microsoft-ds?
1521/tcp open  oracle-tns      Oracle TNS listener 21.0.0.0.0 (unauthorized)
3306/tcp open  mysql           MySQL 8.0.41
5500/tcp open  ssl/http        Oracle XML DB Enterprise Edition httpd
7070/tcp open  ssl/realserver?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.60 seconds
```

6. OS Detection



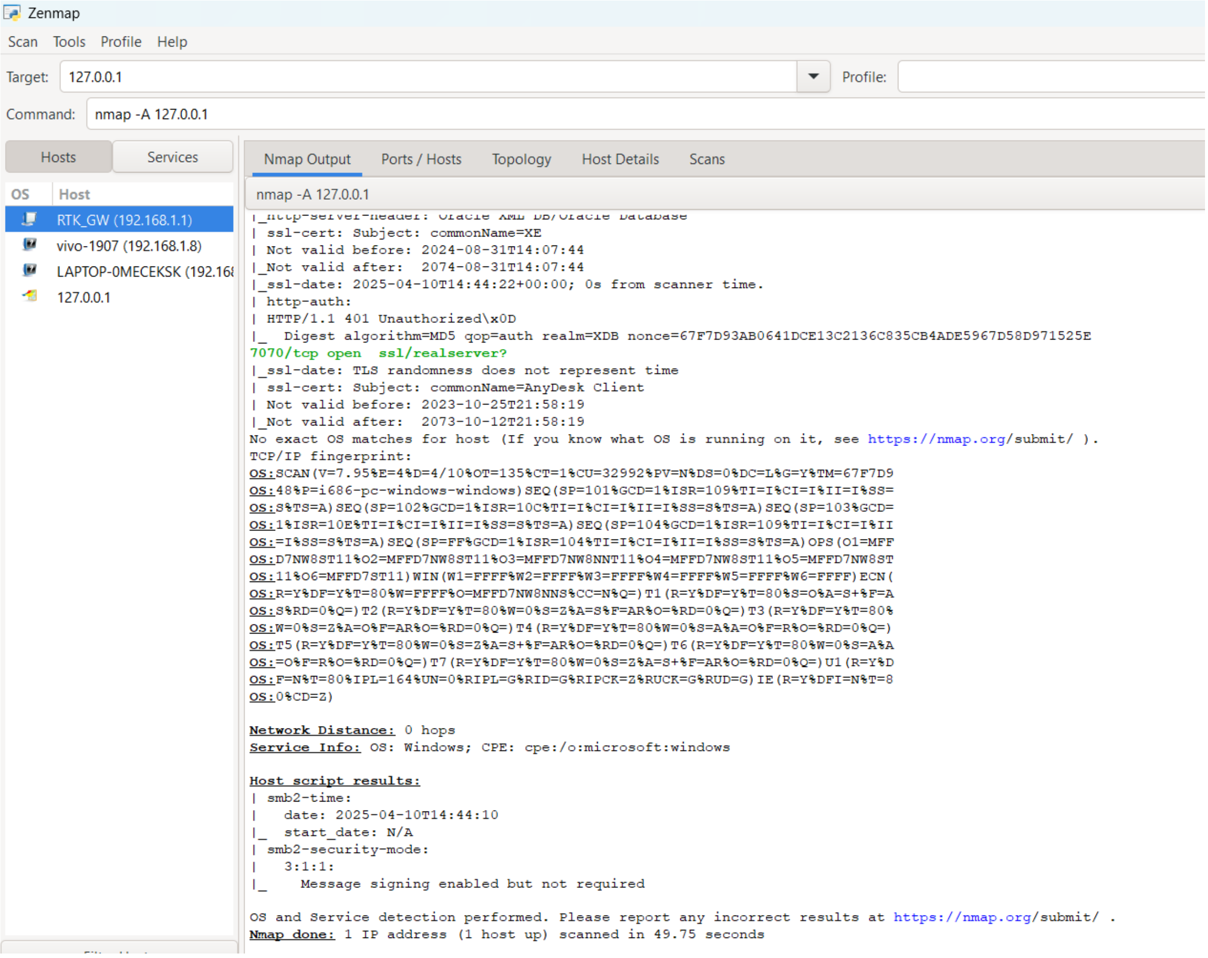
Target: 127.0.0.1 Profile:

Command: nmap -O 127.0.0.1

nmap -O 127.0.0.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 20:11 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00091s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
5500/tcp open  hotline
7070/tcp open  realserver
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=4/10%OT=135%CT=1%CU=33241%PV=N%DS=0%DC=L%G=Y%TM=67F7D8
OS:C1%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=104%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=102%GCD=1%ISR=10E%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=
OS:1%ISR=107%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=FC%GCD=1%ISR=10A%TI=I%CI=I%II=
OS:I%SS=S%TS=A)SEQ(SP=FF%GCD=1%ISR=101%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFFD
OS:7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST1
OS:1%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R
OS:=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W
OS:=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=
OS:O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80
OS:%CD=Z)

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 10.60 seconds
```

7. Aggressive Scan



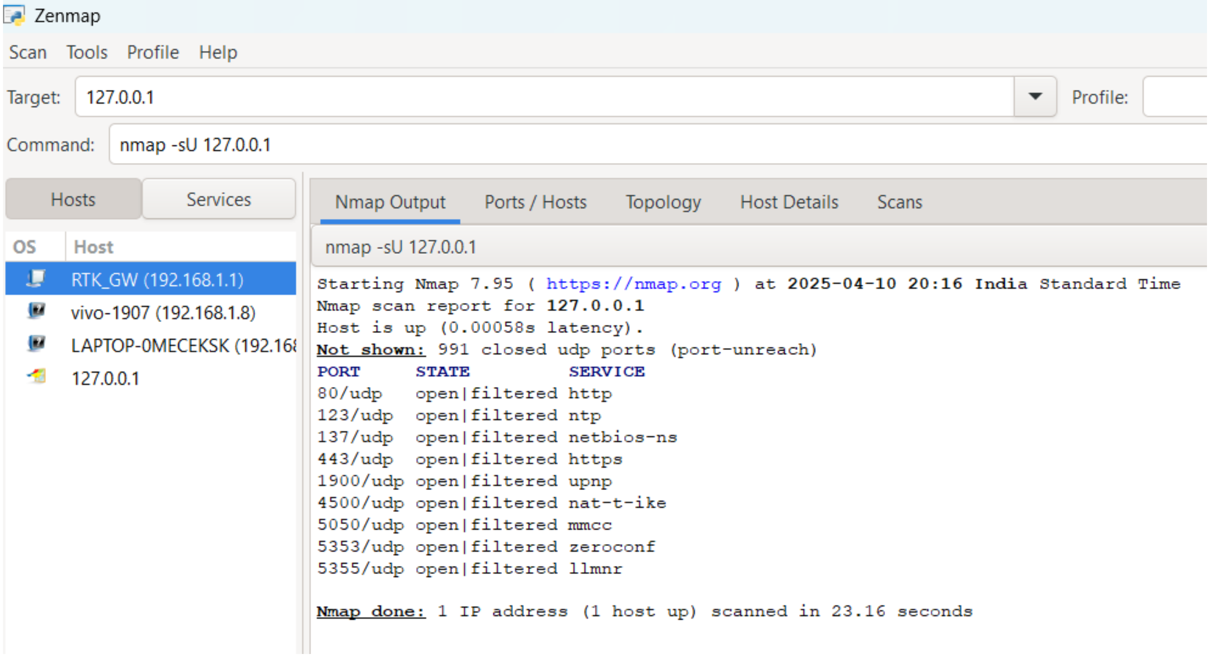
Target: 127.0.0.1

Command: nmap -A 127.0.0.1

nmap -A 127.0.0.1

```
|_http-server-header: Oracle XML DB/Oracle Database
| ssl-cert: Subject: commonName=XE
| Not valid before: 2024-08-31T14:07:44
|_Not valid after:  2074-08-31T14:07:44
|_ssl-date: 2025-04-10T14:44:22+00:00; 0s from scanner time.
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Digest algorithm=MD5 qop=auth realm=XDB nonce=67F7D93AB0641DCE13C2136C835CB4ADE5967D58D971525E
7070/tcp open  ssl/realserver?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2023-10-25T21:58:19
|_Not valid after:  2073-10-12T21:58:19
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=4/10%OT=135%CT=1%CU=32992%PV=N%DS=0%DC=L%G=Y%TM=67F7D9
OS:48%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=102%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=103%GCD=
OS:1%ISR=10E%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II
OS:=I%SS=S%TS=A)SEQ(SP=FF%GCD=1%ISR=104%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFF
OS:D7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST
OS:11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(
OS:R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%
OS:W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
OS:T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A
OS:=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D
OS:F=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=8
OS:0%CD=Z)

Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-04-10T14:44:10
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

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 49.75 seconds
```

8. UDP Scan



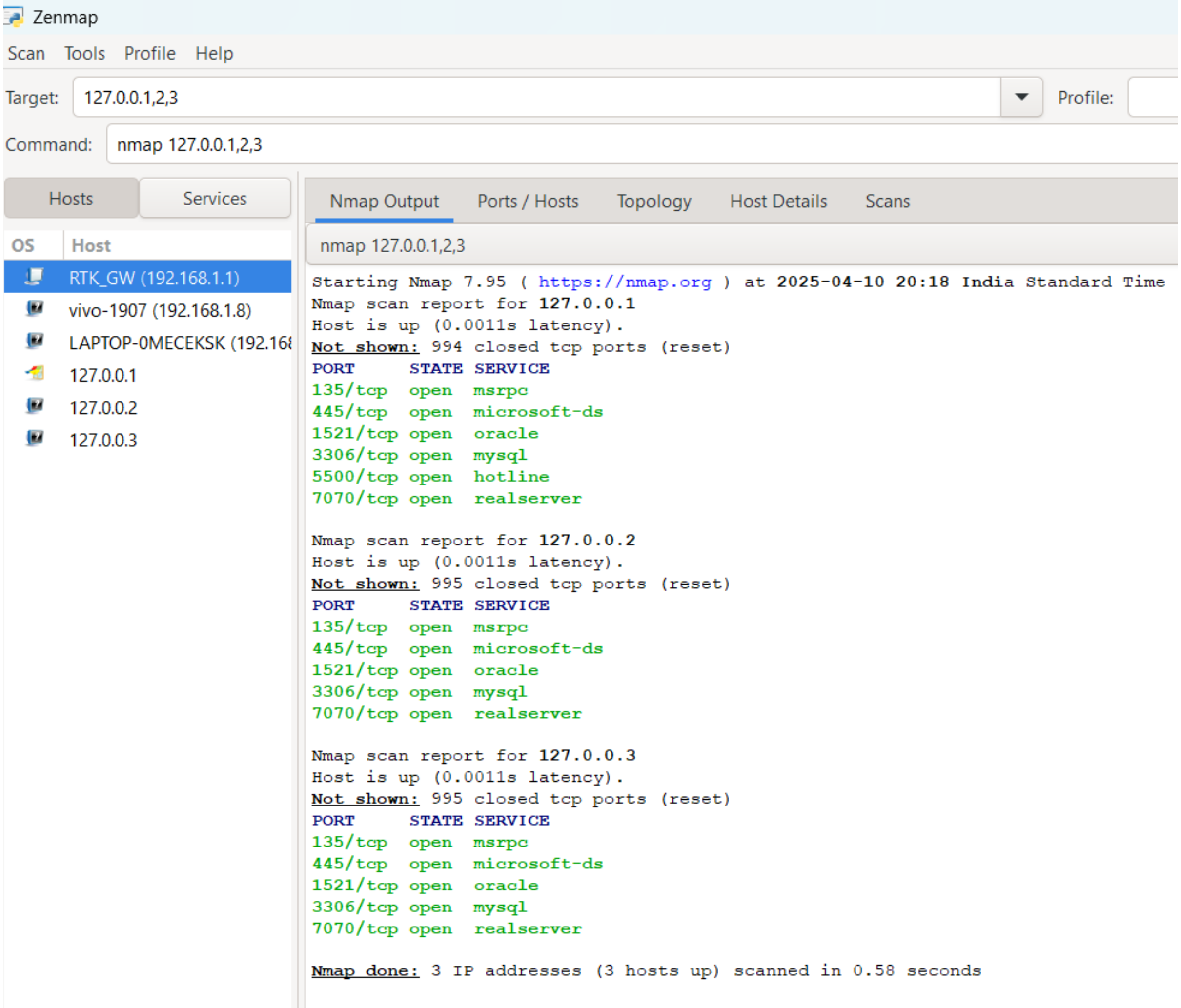
Target: 127.0.0.1

Command: nmap -sU 127.0.0.1

nmap -sU 127.0.0.1

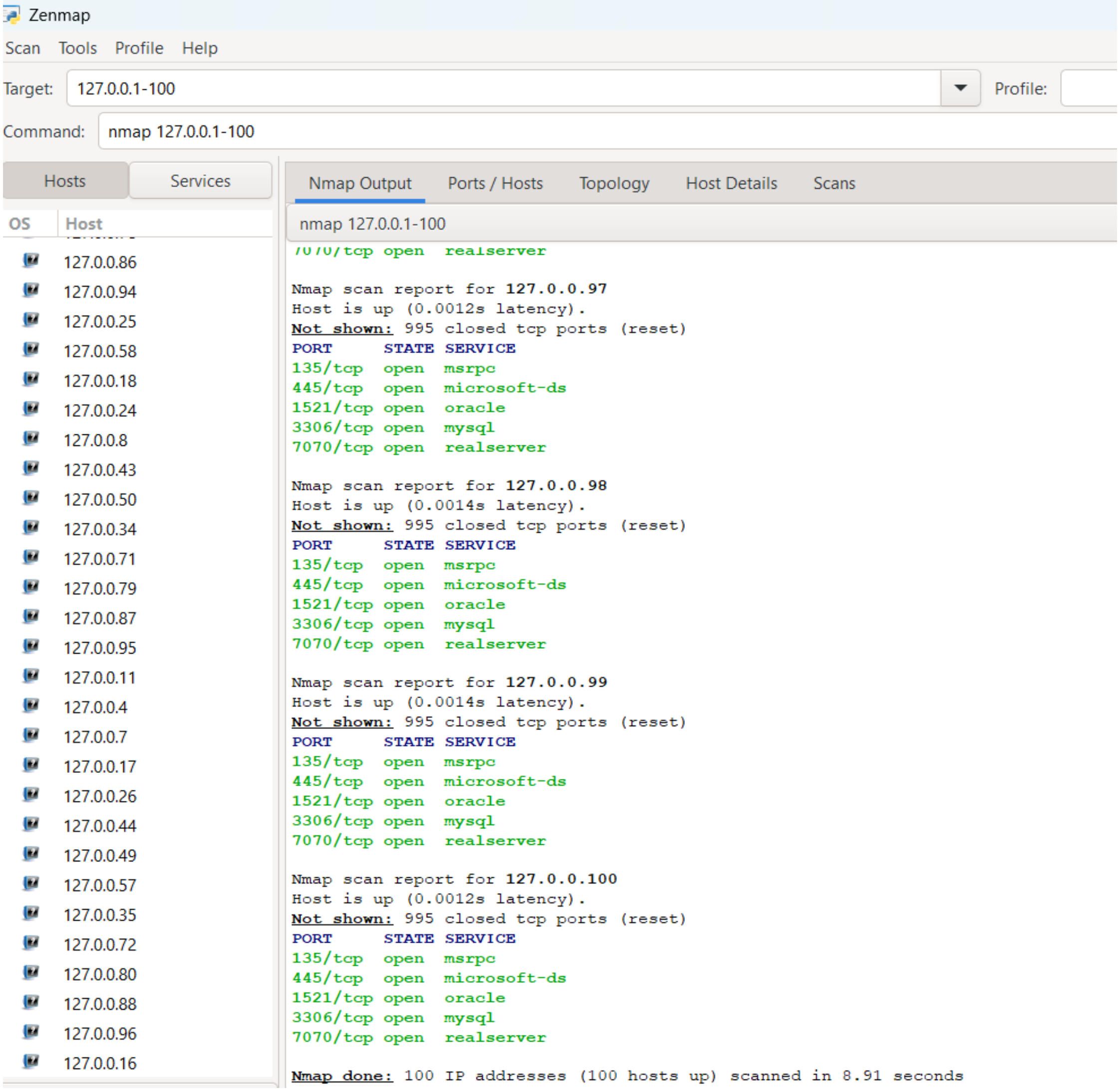
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 20:16 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00058s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT     STATE         SERVICE
80/udp   open|filtered http
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
443/udp  open|filtered https
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 23.16 seconds
```

9. Scan multiple hosts



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 20:18 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.0011s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
5500/tcp open  hotline
7070/tcp open  realserver

Nmap scan report for 127.0.0.2
Host is up (0.0011s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap scan report for 127.0.0.3
Host is up (0.0011s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 3 IP addresses (3 hosts up) scanned in 0.58 seconds
```

10. Scan a range



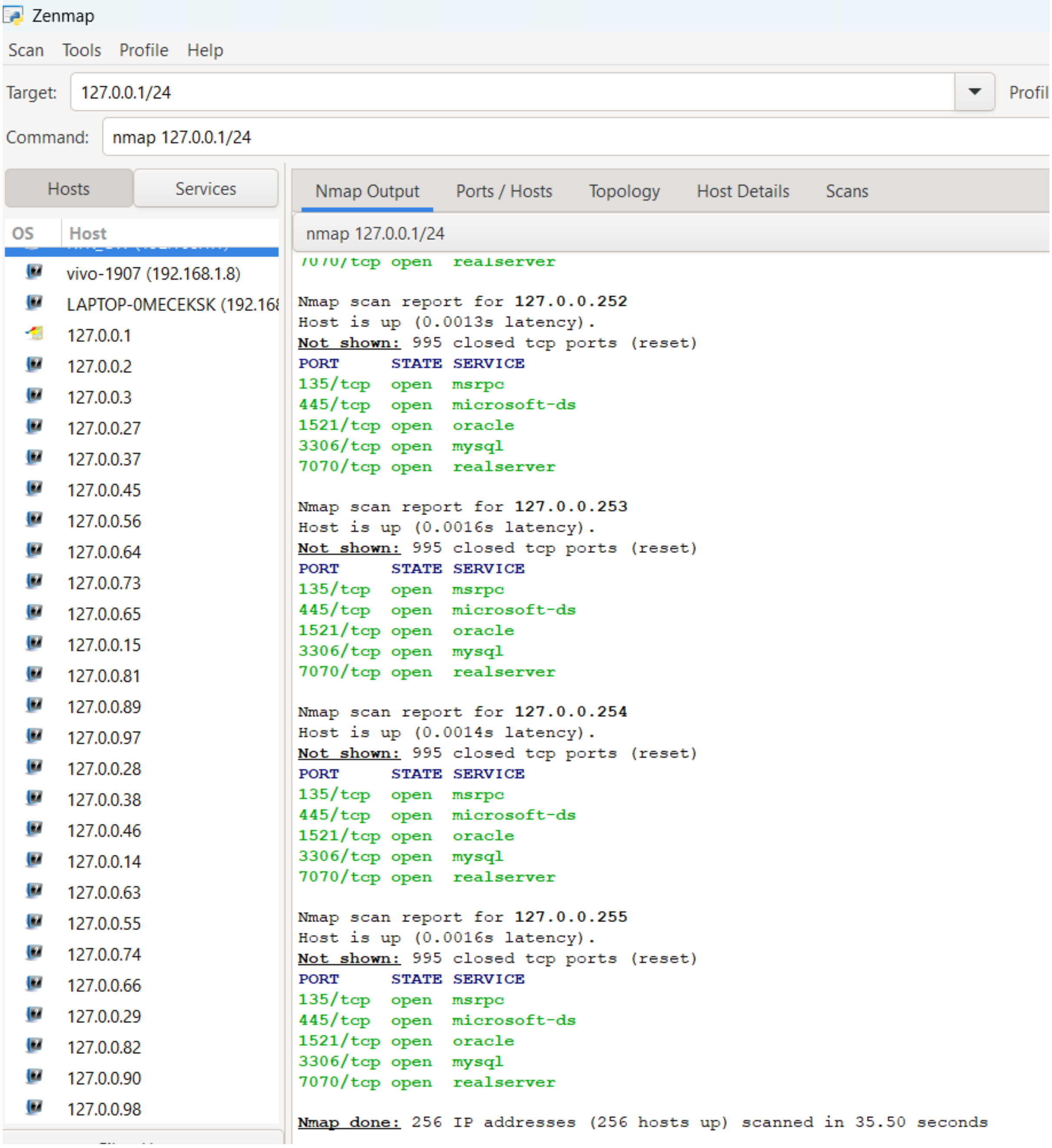
Target: 127.0.0.1-100

Command: nmap 127.0.0.1-100

nmap 127.0.0.1-100

```
7070/tcp open  realserver

Nmap scan report for 127.0.0.97
Host is up (0.0012s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap scan report for 127.0.0.98
Host is up (0.0014s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap scan report for 127.0.0.99
Host is up (0.0014s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap scan report for 127.0.0.100
Host is up (0.0012s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 100 IP addresses (100 hosts up) scanned in 8.91 seconds
```

11. Scan a subnet



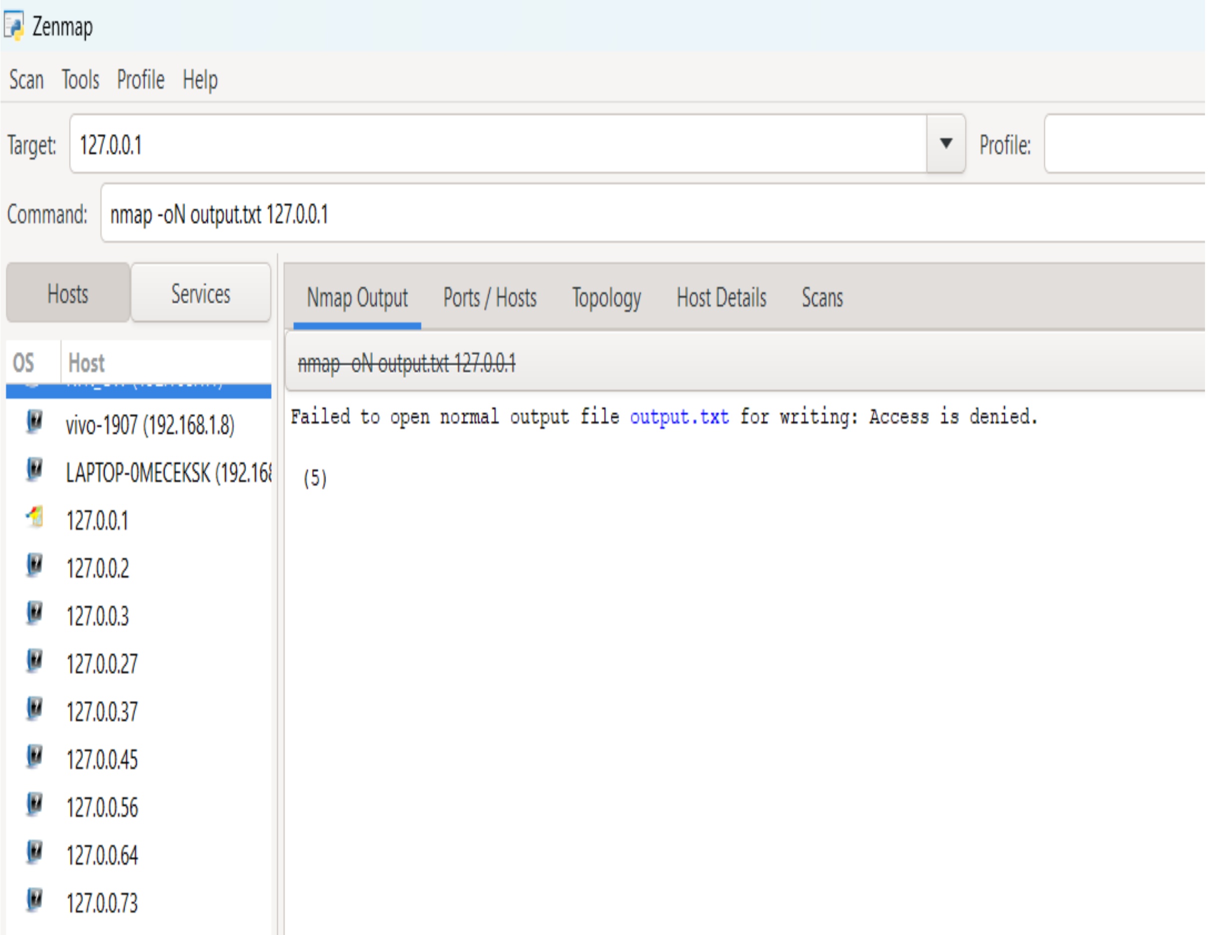
Target: 127.0.0.1/24

Command: nmap 127.0.0.1/24

nmap 127.0.0.1/24

```
7070/tcp open  realserver

Nmap scan report for 127.0.0.252
Host is up (0.0013s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap scan report for 127.0.0.253
Host is up (0.0016s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap scan report for 127.0.0.254
Host is up (0.0014s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap scan report for 127.0.0.255
Host is up (0.0016s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 256 IP addresses (256 hosts up) scanned in 35.50 seconds
```

12. Save Result to file



Target: 127.0.0.1

Profile:

Command: nmap -oN output.txt 127.0.0.1

~~nmap -oN output.txt 127.0.0.1~~

```
Failed to open normal output file output.txt for writing: Access is denied.
 (5)
```

e