Aim: Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan, udp port scan, etc.

Theory:

Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It helps network administrators manage service upgrade schedules, monitor host or service uptime, and detect security risks.

Key Functions of Nmap:

1. **Open Port Scanning:** This helps you find out which ports on a device are open and accepting connections. For example, the command `nmap -p 1-200`

`192.168.47.59` scans ports 1 to 200 on the IP address `192.168.47.59`.

2. **OS Fingerprinting:** OS fingerprinting is a technique used to identify the operating system of a remote device by analyzing its network behavior. Nmap performs this through two methods: active fingerprinting, which sends specially crafted packets to the target and examines the responses, and passive fingerprinting, which observes existing network traffic to infer the OS without sending any probes.For example, using the command `nmap -O 192.168.47.59` allows you to identify the operating system of

the specified IP address.

3. **Ping Scan:** This is used to check which devices in a network are active and reachable. The command `nmap -sn 192.168.47.0/24` sends pings to all devices in that subnet to see which ones respond.

4. **TCP Port Scan:** This identifies open TCP ports and the services running on them. The command `nmap -sT 192.168.47.59` performs a TCP scan.

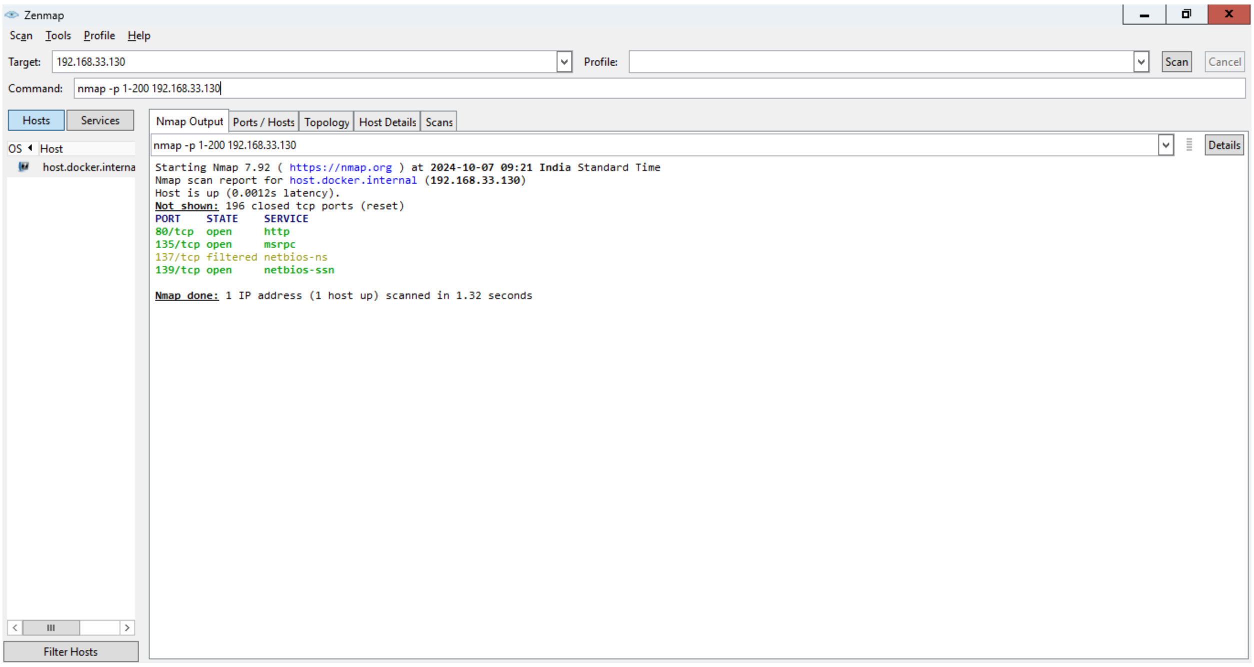
5. **UDP Port Scan:** Nmap can also scan for open UDP ports, which is more complex because UDP doesn't establish connections like TCP. You can use `nmap -sU -p 1-200 192.168.47.59` for this.

Always ensure you have permission to scan the networks or devices you are targeting. Scanning without permission can lead to legal issues.

Nmap Commands:

For port scanning between 1 to 200

ex.nmap -p 1-200 192.168.33.130



Target: 192.168.33.130

Command: nmap -p 1-200 192.168.33.130

```
nmap -p 1-200 192.168.33.130
```

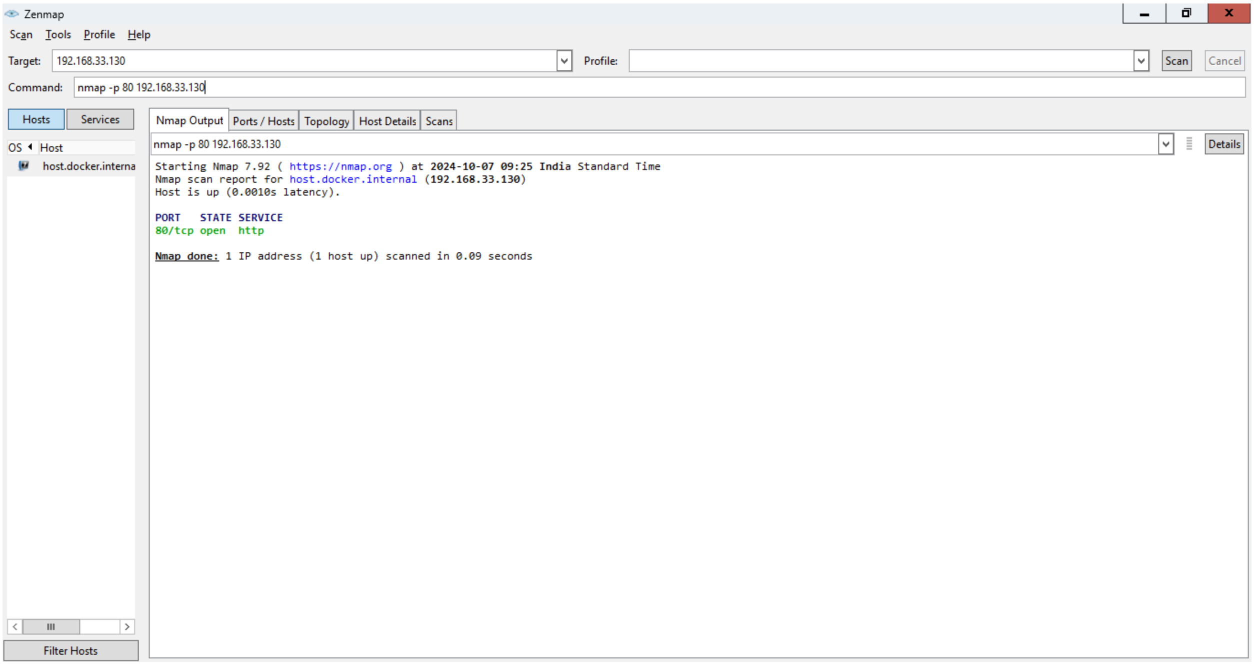
```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:21 India Standard Time
Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.0012s latency).
Not shown: 196 closed tcp ports (reset)
PORT    STATE    SERVICE
80/tcp  open     http
135/tcp open     msrpc
137/tcp filtered netbios-ns
139/tcp open     netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

Type your own ip address in Target as shown above

Type command nmap -p 1-200 <ip_address> to see ports that are open

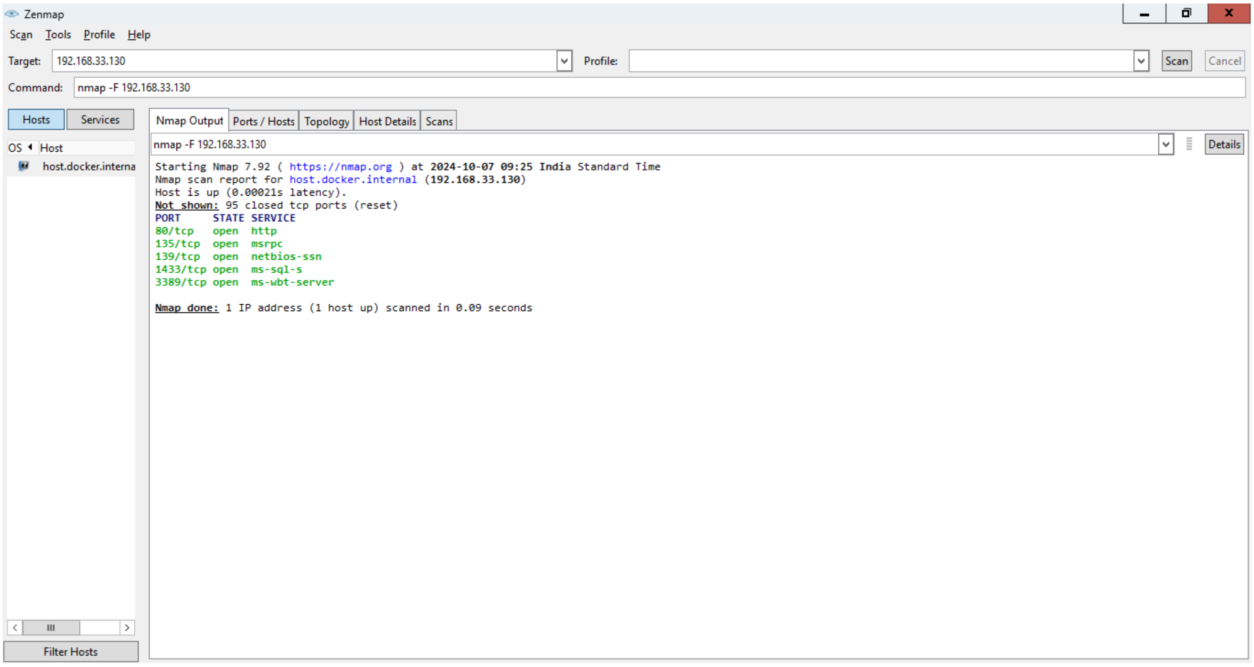
Ex. nmap -p 1-200 192.168.33.130

nmap -p 80 192.168.33.130



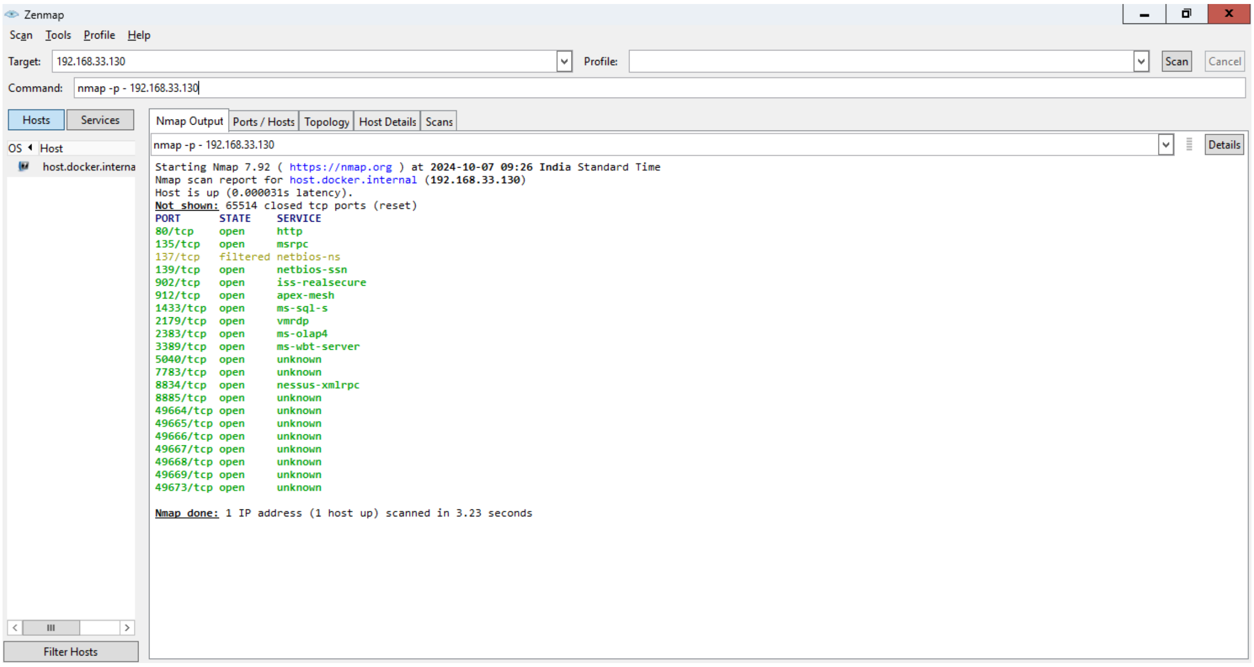
```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:25 India Standard Time
Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.0010s latency).

PORT   STATE SERVICE
80/tcp open  http

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

nmap -F 192.168.33.130



```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:25 India Standard Time
Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.00021s latency).
Not shown: 95 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server

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

nmap -p - 192.168.33.130

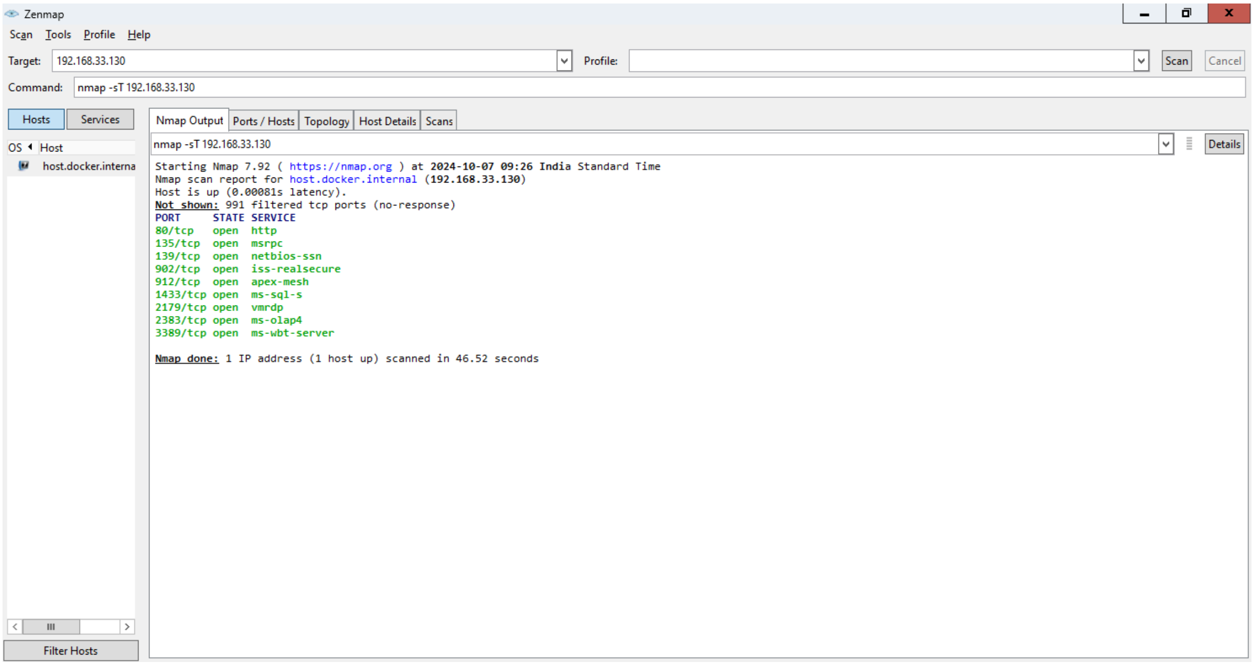


Target: 192.168.33.130

Command: nmap -p - 192.168.33.130

```
nmap -p - 192.168.33.130
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:26 India Standard Time
Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.000031s latency).
Not shown: 65514 closed tcp ports (reset)
PORT      STATE    SERVICE
80/tcp    open     http
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1433/tcp  open     ms-sql-s
2179/tcp  open     vmrdp
2383/tcp  open     ms-olap4
3389/tcp  open     ms-wbt-server
5040/tcp  open     unknown
7783/tcp  open     unknown
8834/tcp  open     nessus-xmlrpc
8885/tcp  open     unknown
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49669/tcp open     unknown
49673/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 3.23 seconds
```

nmap -sT 192.168.33.130

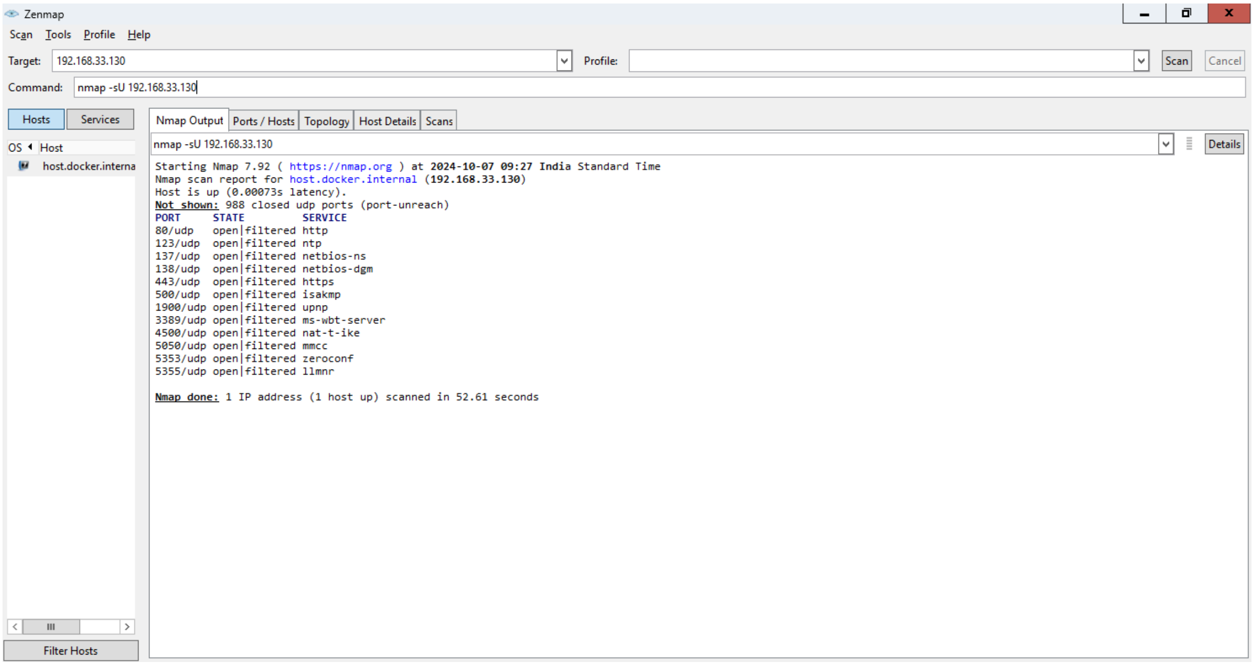


Target: 192.168.33.130

Command: nmap -sT 192.168.33.130

```
nmap -sT 192.168.33.130
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:26 India Standard Time
Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.00081s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1433/tcp open  ms-sql-s
2179/tcp open  vmrdp
2383/tcp open  ms-olap4
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 46.52 seconds
```

nmap -sU 192.168.33.130

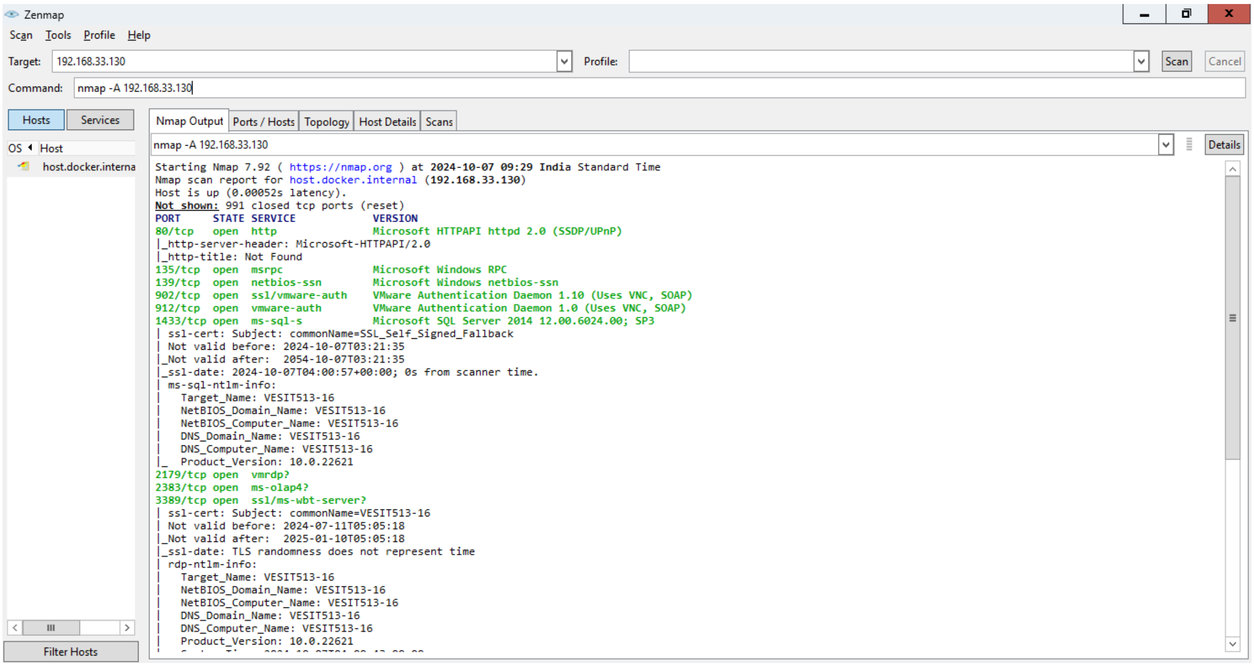


Target: 192.168.33.130

Command: nmap -sU 192.168.33.130

```
nmap -sU 192.168.33.130
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:27 India Standard Time
Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.00073s latency).
Not shown: 988 closed udp ports (port-unreach)
PORT     STATE         SERVICE
80/udp   open|filtered http
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
443/udp  open|filtered https
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
3389/udp open|filtered ms-wbt-server
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 52.61 seconds
```

nmap -A 192.168.33.130

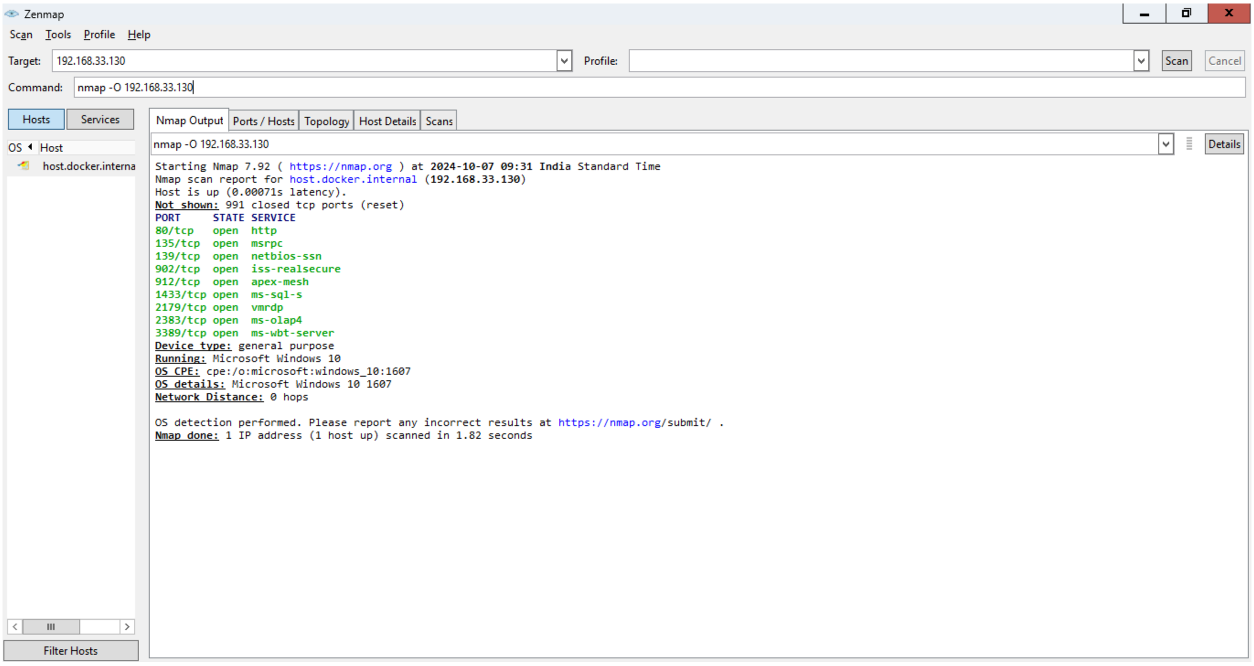


Target: 192.168.33.130

Command: nmap -A 192.168.33.130

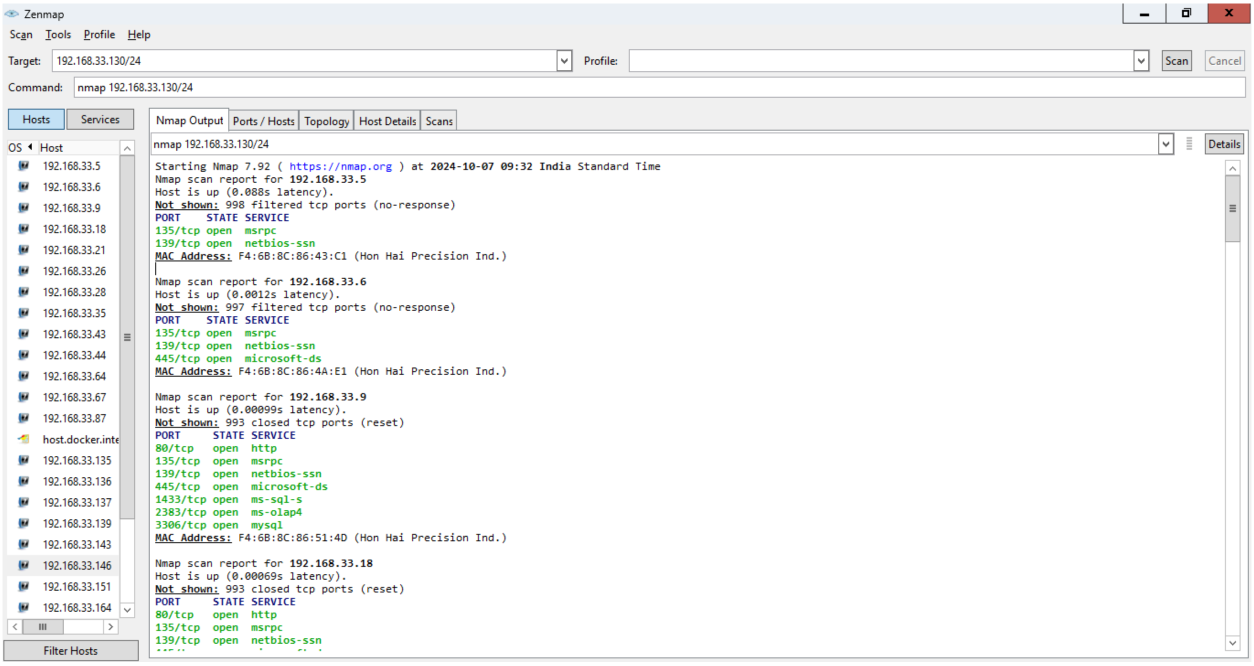
```
nmap -A 192.168.33.130
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:29 India Standard Time
Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.00052s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE            VERSION
80/tcp   open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
902/tcp  open  ssl/vmware-auth    VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth        VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1433/tcp open  ms-sql-s           Microsoft SQL Server 2014 12.00.6024.00; SP3
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-10-07T03:21:35
|_Not valid after:  2054-10-07T03:21:35
|_ssl-date: 2024-10-07T04:00:57+00:00; 0s from scanner time.
| ms-sql-ntlm-info:
|   Target_Name: VESIT513-16
|   NetBIOS_Domain_Name: VESIT513-16
|   NetBIOS_Computer_Name: VESIT513-16
|   DNS_Domain_Name: VESIT513-16
|   DNS_Computer_Name: VESIT513-16
|_  Product_Version: 10.0.22621
2179/tcp open  vmrdp?
2383/tcp open  ms-olap4?
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=VESIT513-16
| Not valid before: 2024-07-11T05:05:18
|_Not valid after:  2025-01-10T05:05:18
|_ssl-date: TLS randomness does not represent time
| rdp-ntlm-info:
|   Target_Name: VESIT513-16
|   NetBIOS_Domain_Name: VESIT513-16
|   NetBIOS_Computer_Name: VESIT513-16
|   DNS_Domain_Name: VESIT513-16
|   DNS_Computer_Name: VESIT513-16
|   Product_Version: 10.0.22621
```

For OS fingerprinting
nmap -O 192.168.33.130



```
nmap -O 192.168.33.130
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:31 India Standard Time
Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.00071s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1433/tcp open  ms-sql-s
2179/tcp open  vmrdp
2383/tcp open  ms-olap4
3389/tcp open  ms-wbt-server
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
```

For subnet scan
Nmap 192.168.33.130/24

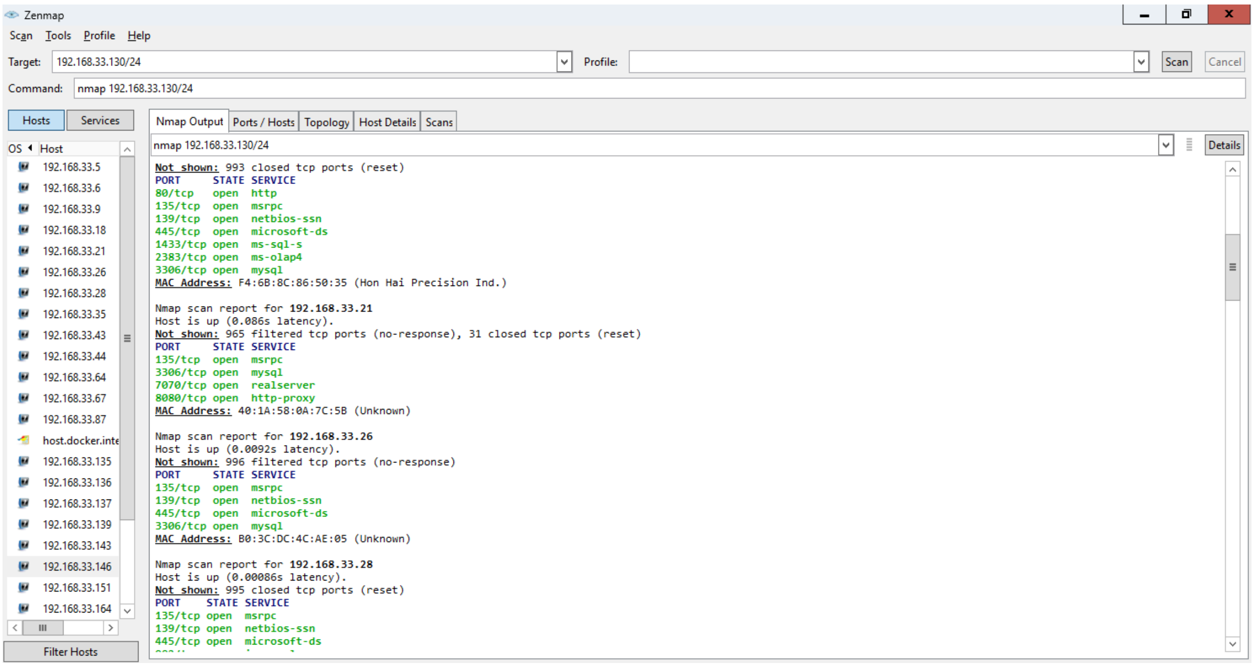


Target: 192.168.33.130/24
Profile:
Command: nmap 192.168.33.130/24

```
192.168.33.5
192.168.33.6
192.168.33.9
192.168.33.18
192.168.33.21
192.168.33.26
192.168.33.28
192.168.33.35
192.168.33.43
192.168.33.44
192.168.33.64
192.168.33.67
192.168.33.87
host.docker.inte
192.168.33.135
192.168.33.136
192.168.33.137
192.168.33.139
192.168.33.143
192.168.33.146
192.168.33.151
192.168.33.164
```

nmap 192.168.33.130/24

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-07 09:32 India Standard Time
Nmap scan report for 192.168.33.5
Host is up (0.088s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
MAC Address: F4:6B:8C:86:43:C1 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.6
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: F4:6B:8C:86:4A:E1 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.9
Host is up (0.00099s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
2383/tcp open  ms-olap4
3306/tcp open  mysql
MAC Address: F4:6B:8C:86:51:4D (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.18
Host is up (0.00069s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
```

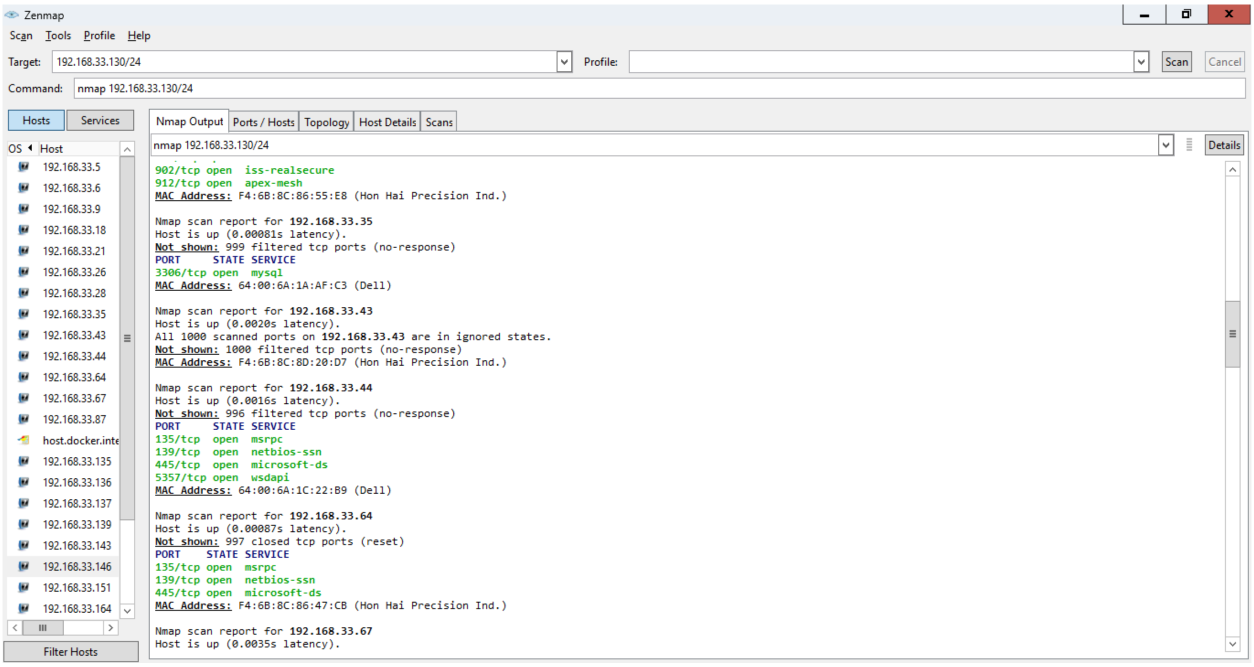


Target: 192.168.33.130/24
Profile:
Command: nmap 192.168.33.130/24

```
192.168.33.5
192.168.33.6
192.168.33.9
192.168.33.18
192.168.33.21
192.168.33.26
192.168.33.28
192.168.33.35
192.168.33.43
192.168.33.44
192.168.33.64
192.168.33.67
192.168.33.87
host.docker.inte
192.168.33.135
192.168.33.136
192.168.33.137
192.168.33.139
192.168.33.143
192.168.33.146
192.168.33.151
192.168.33.164
```

nmap 192.168.33.130/24

```
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
2383/tcp open  ms-olap4
3306/tcp open  mysql
MAC Address: F4:6B:8C:86:50:35 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.21
Host is up (0.086s latency).
Not shown: 965 filtered tcp ports (no-response), 31 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
3306/tcp open  mysql
7070/tcp open  realserver
8080/tcp open  http-proxy
MAC Address: 40:1A:58:0A:7C:5B (Unknown)

Nmap scan report for 192.168.33.26
Host is up (0.0092s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: B0:3C:DC:4C:AE:05 (Unknown)

Nmap scan report for 192.168.33.28
Host is up (0.00086s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

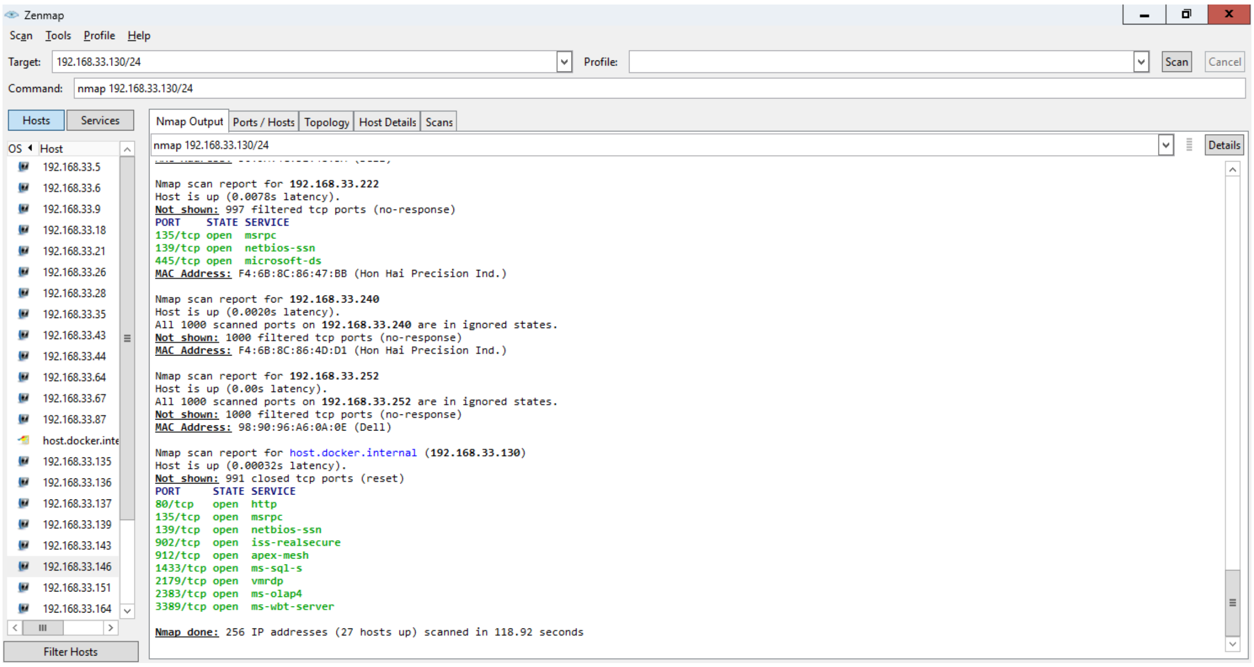


Target: 192.168.33.130/24

Command: nmap 192.168.33.130/24

```
OS Host
192.168.33.5
192.168.33.6
192.168.33.9
192.168.33.18
192.168.33.21
192.168.33.26
192.168.33.28
192.168.33.35
192.168.33.43
192.168.33.44
192.168.33.64
192.168.33.67
192.168.33.87
host.docker.inte
192.168.33.135
192.168.33.136
192.168.33.137
192.168.33.139
192.168.33.143
192.168.33.146
192.168.33.151
192.168.33.164
```

```
nmap 192.168.33.130/24
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: F4:6B:8C:86:55:E8 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.35
Host is up (0.00081s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 64:00:6A:1A:AF:C3 (Dell)

Nmap scan report for 192.168.33.43
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.33.43 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F4:6B:8C:8D:20:D7 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.44
Host is up (0.0016s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 64:00:6A:1C:22:B9 (Dell)

Nmap scan report for 192.168.33.64
Host is up (0.00087s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: F4:6B:8C:86:47:CB (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.67
Host is up (0.0035s latency).
```



Target: 192.168.33.130/24

Command: nmap 192.168.33.130/24

```
OS Host
192.168.33.5
192.168.33.6
192.168.33.9
192.168.33.18
192.168.33.21
192.168.33.26
192.168.33.28
192.168.33.35
192.168.33.43
192.168.33.44
192.168.33.64
192.168.33.67
192.168.33.87
host.docker.inte
192.168.33.135
192.168.33.136
192.168.33.137
192.168.33.139
192.168.33.143
192.168.33.146
192.168.33.151
192.168.33.164
```

```
nmap 192.168.33.130/24

Nmap scan report for 192.168.33.222
Host is up (0.0078s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: F4:6B:8C:86:47:BB (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.240
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.33.240 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F4:6B:8C:86:4D:D1 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.33.252
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.33.252 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 98:90:96:A6:0A:0E (Dell)

Nmap scan report for host.docker.internal (192.168.33.130)
Host is up (0.00032s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1433/tcp open  ms-sql-s
2179/tcp open  vmrdp
2383/tcp open  ms-olap4
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (27 hosts up) scanned in 118.92 seconds
```