EXPERIMENT 9

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:

1. `nmap -p 80 192.168.1.100`
   - **Description: This command is used to scan a specific port (port 80 in this case) on the target host `192.168.1.100`.**
   - **Usage: It is typically used to check if a web server or service running on port 80 (HTTP) is open and accessible.**
   - **Example Scenario: Verifying if a web server is running on a specific machine.**
2. `nmap -F 192.168.1.100`
   - **Description: This command performs a fast scan on the target host `192.168.1.100`. It scans a limited number of well-known ports.**
   - **Usage: It is used for a quick overview of the services running on the most common ports.**
   - **Example Scenario: Quickly checking the status of commonly used ports on a host.**
3. `nmap -p - 192.168.1.100`
   - **Description: This command scans all 65535 ports on the target host `192.168.1.100`.**
   - **Usage: It is used when a comprehensive scan of all possible ports on a host is needed.**
   - **Example Scenario: Performing a thorough security assessment by checking every port on a host.**
4. `nmap -sT 192.168.1.100`
   - **Description: This command performs a TCP connect scan on the target host `192.168.1.100`.**
   - **Usage: It is used to determine which TCP ports are open by establishing a full connection (three-way handshake) with each port.**
   - **Example Scenario: Checking for open TCP ports in environments where SYN scans may not be allowed or supported.**
5. `nmap -sU 192.168.1.100`
   - **Description: This command performs a UDP scan on the target host `192.168.1.100`.**

- **Usage: It is used to determine which UDP ports are open and what services are running on them.**
- **Example Scenario: Identifying open UDP ports, such as DNS (port 53) or DHCP (port 67/68), on a host.**

6. `nmap -A 192.168.1.100`
   - **Description: This command performs an aggressive scan on the target host `192.168.1.100`. It includes OS detection, version detection, script scanning, and traceroute.**
   - **Usage: It is used for detailed information gathering about the target host.**
   - **Example Scenario: Conducting an in-depth analysis of a host to gather as much information as possible in one command.**

OS Fingerprinting

7. `nmap -O 192.168.1.100`
   - **Description: This command enables OS detection on the target host `192.168.1.100`.**
   - **Usage: It is used to identify the operating system running on the target host.**
   - **Example Scenario: Determining whether a host is running Windows, Linux, or another operating system for vulnerability assessment or inventory purposes.**

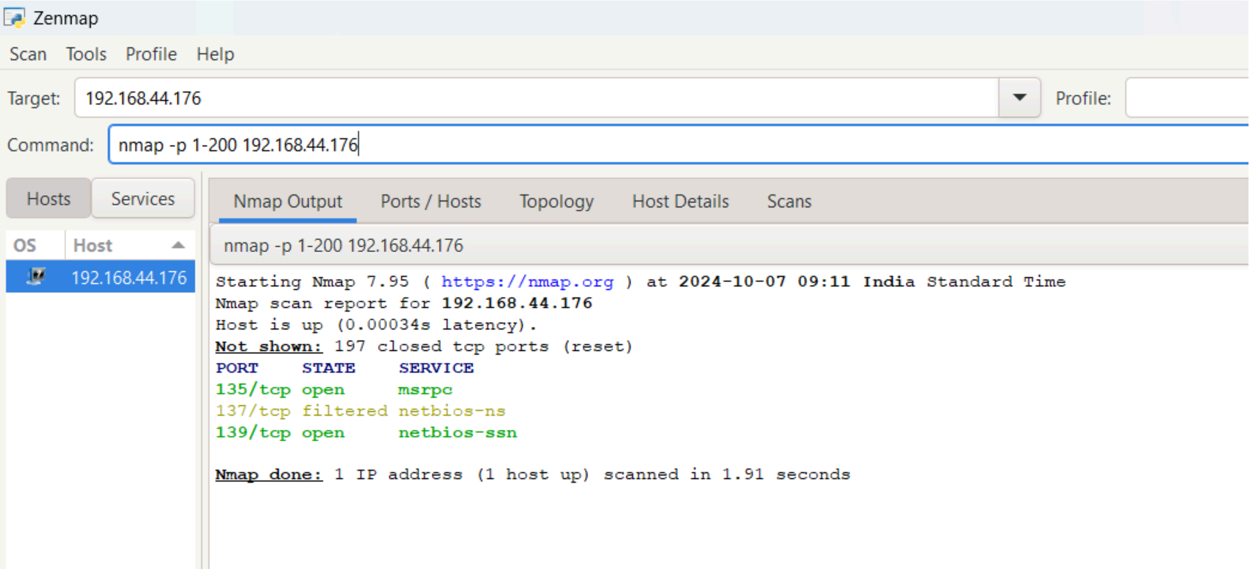
Subnet Scan

8. `nmap 192.168.1.100/24`
   - **Description: This command scans all hosts in the subnet `192.168.1.0/24`, which includes all IP addresses from `192.168.1.1` to `192.168.1.254`.**
   - **Usage: It is used to discover all active hosts and their open ports within a specified subnet.**
   - **Example Scenario: Conducting a network inventory or identifying all devices on a local network for security assessment.**

OUTPUT:

Nmap

nmap -p 1-200 192.168.44.176



Target: 192.168.44.176

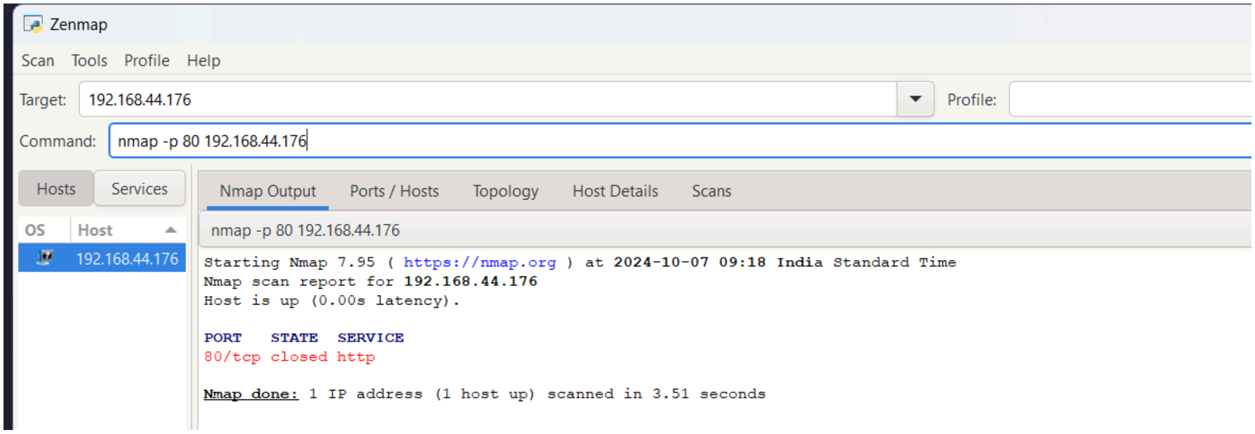
Profile:

Command: nmap -p 1-200 192.168.44.176

192.168.44.176

```
nmap -p 1-200 192.168.44.176
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:11 India Standard Time
Nmap scan report for 192.168.44.176
Host is up (0.00034s latency).
Not shown: 197 closed tcp ports (reset)
PORT    STATE    SERVICE
135/tcp open     msrpc
137/tcp filtered netbios-ns
139/tcp open     netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
```

nmap -p 80 192.168.44.176



Target: 192.168.44.176

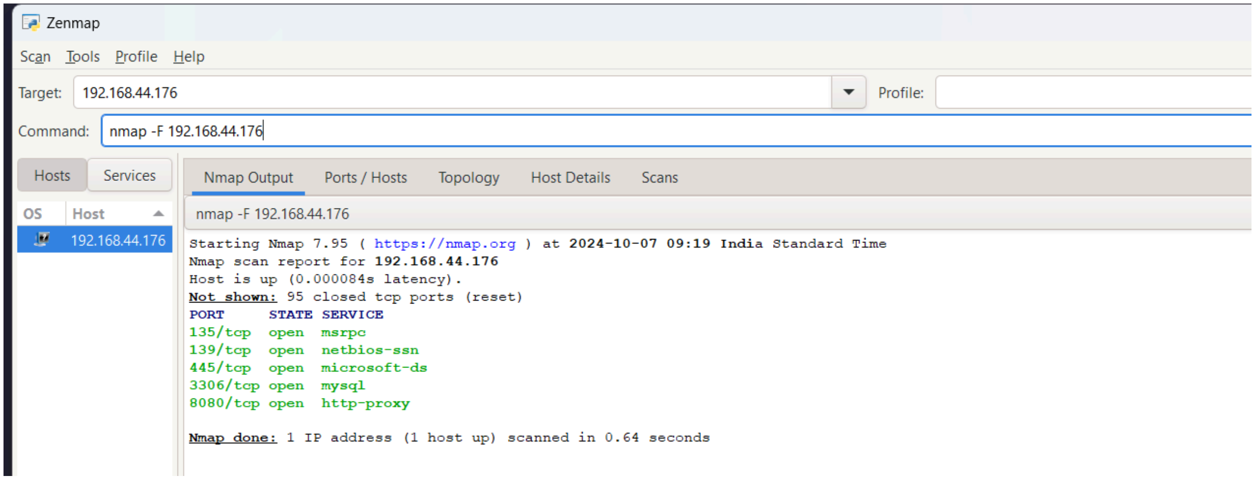
Profile:

Command: nmap -p 80 192.168.44.176

192.168.44.176

```
nmap -p 80 192.168.44.176
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:18 India Standard Time
Nmap scan report for 192.168.44.176
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 3.51 seconds
```

nmap -F 192.168.44.176



Target: 192.168.44.176

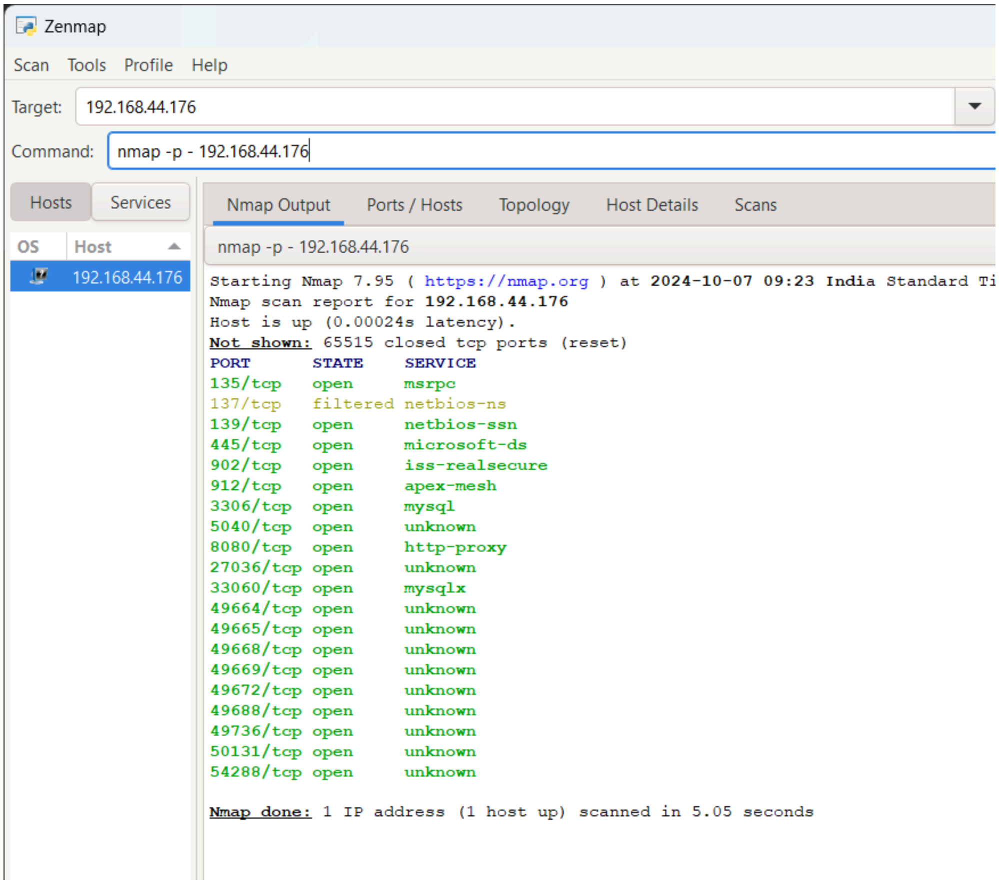
Profile:

Command: nmap -F 192.168.44.176

192.168.44.176

```
nmap -F 192.168.44.176
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:19 India Standard Time
Nmap scan report for 192.168.44.176
Host is up (0.000084s latency).
Not shown: 95 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
8080/tcp open  http-proxy

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

nmap -p- 192.168.1.100



Target: 192.168.44.176

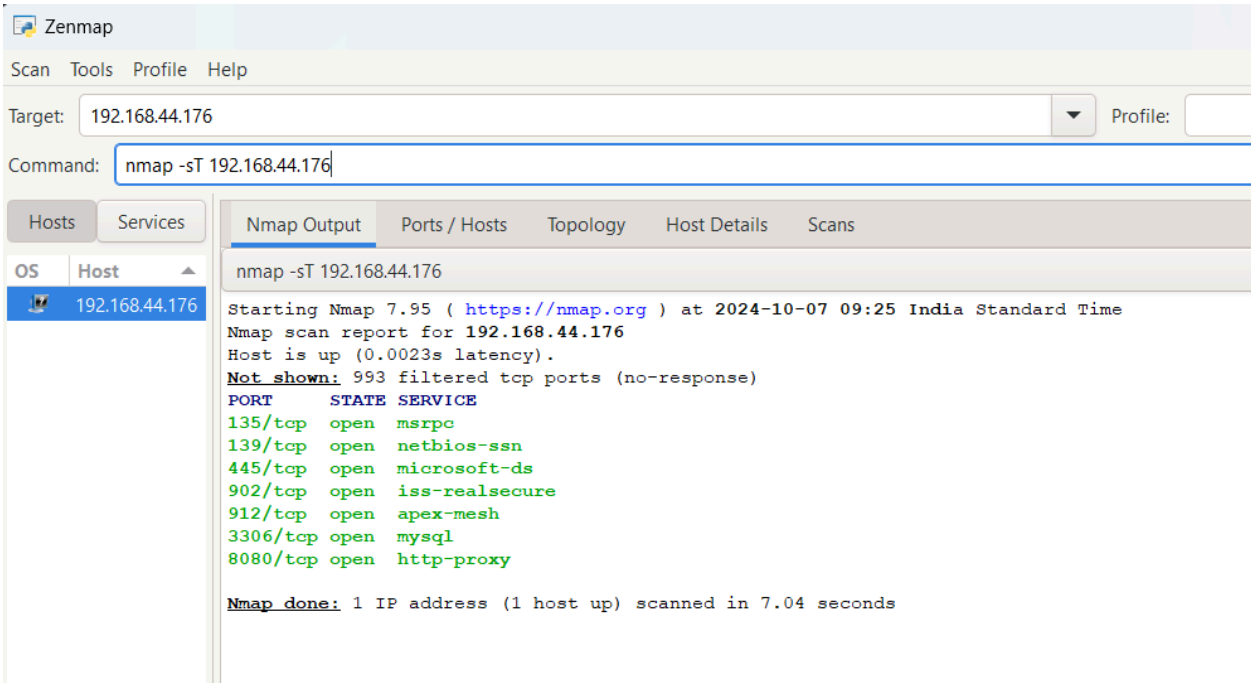
Command: nmap -p - 192.168.44.176

192.168.44.176

nmap -p - 192.168.44.176

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:23 India Standard Ti
Nmap scan report for 192.168.44.176
Host is up (0.00024s latency).
Not shown: 65515 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
3306/tcp  open     mysql
5040/tcp  open     unknown
8080/tcp  open     http-proxy
27036/tcp open     unknown
33060/tcp open     mysqlx
49664/tcp open     unknown
49665/tcp open     unknown
49668/tcp open     unknown
49669/tcp open     unknown
49672/tcp open     unknown
49688/tcp open     unknown
49736/tcp open     unknown
50131/tcp open     unknown
54288/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
```

nmap -sT 192.168.44.176



Target: 192.168.44.176

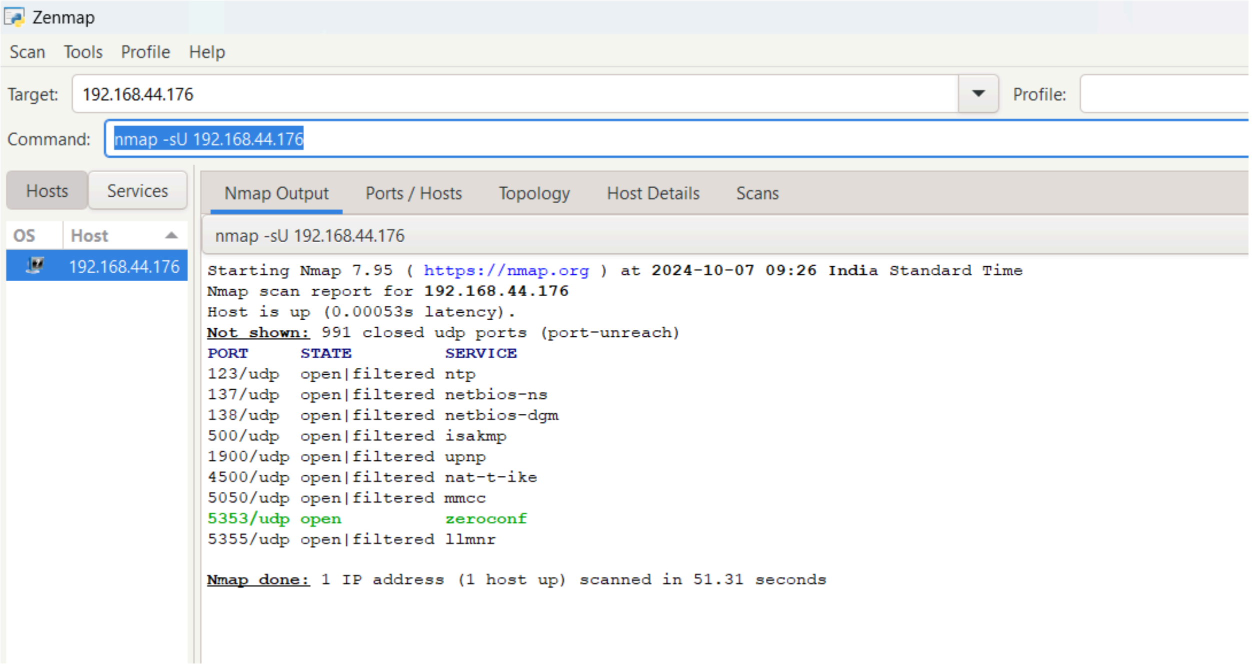
Command: nmap -sT 192.168.44.176

192.168.44.176

nmap -sT 192.168.44.176

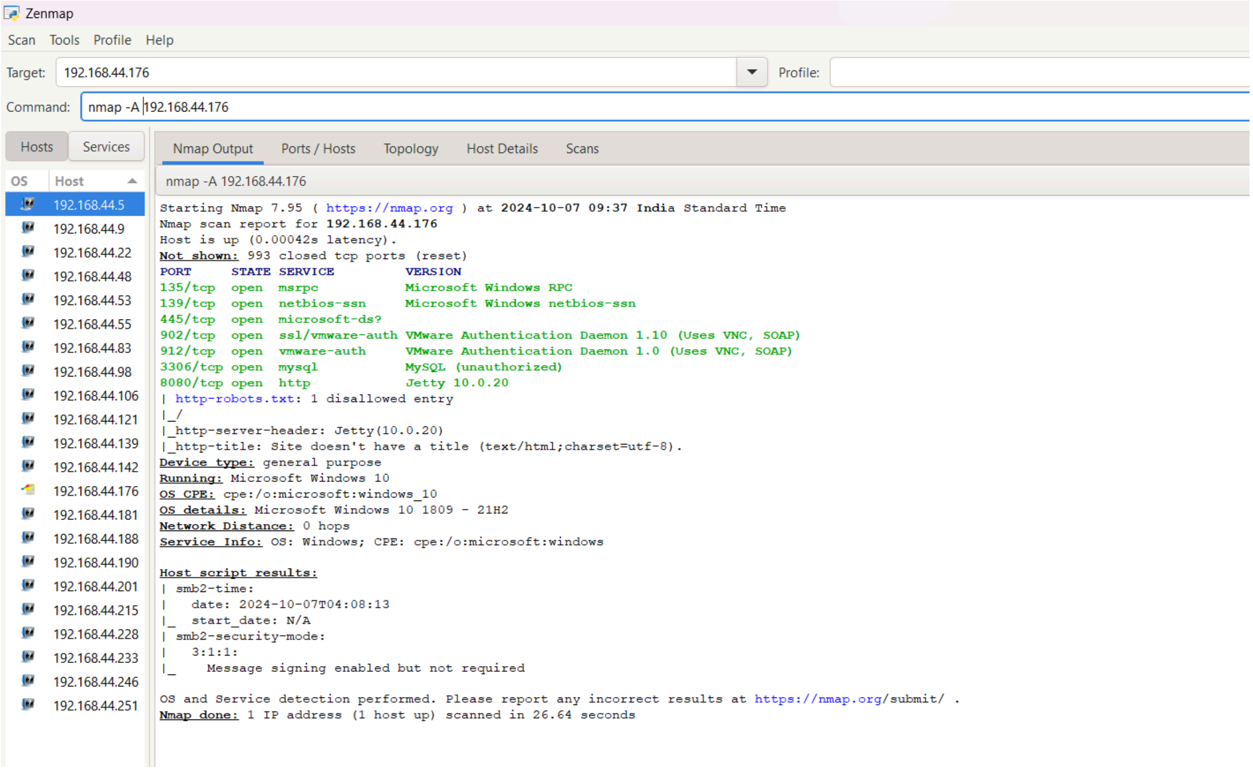
```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:25 India Standard Time
Nmap scan report for 192.168.44.176
Host is up (0.0023s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 7.04 seconds
```

nmap -sU 192.168.44.176



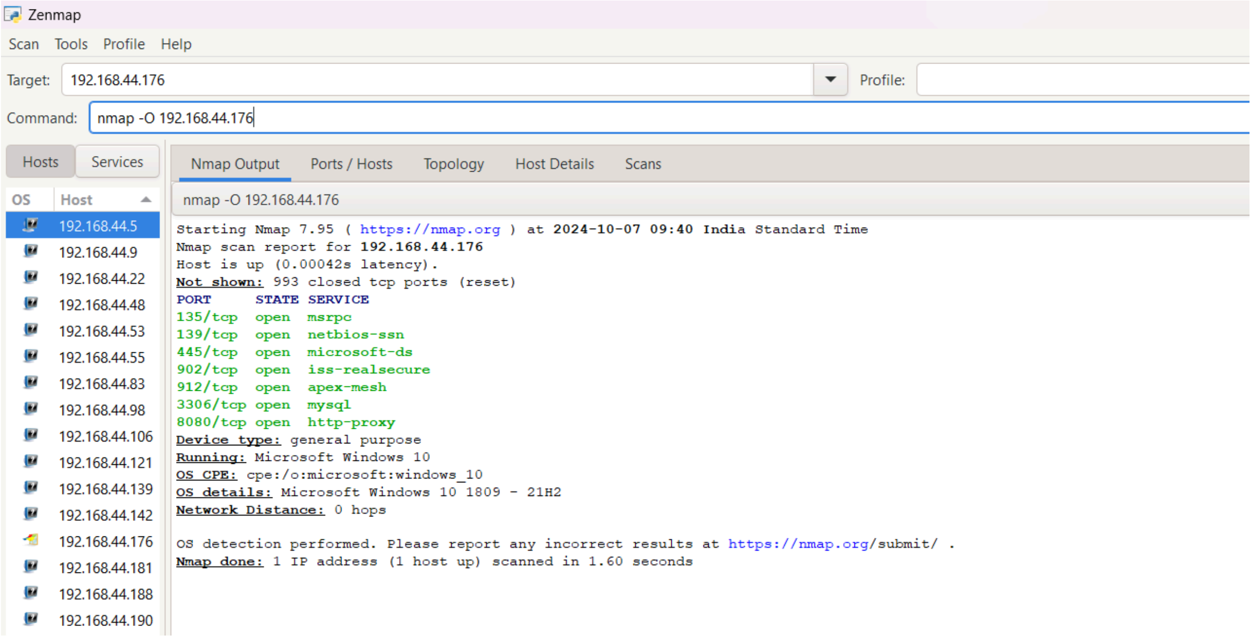
```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:26 India Standard Time
Nmap scan report for 192.168.44.176
Host is up (0.00053s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open          zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 51.31 seconds
```

nmap -A 192.168.44.176



```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:37 India Standard Time
Nmap scan report for 192.168.44.176
Host is up (0.00042s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE          VERSION
135/tcp  open  msrpc            Microsoft Windows RPC
139/tcp  open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
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)
3306/tcp open  mysql            MySQL (unauthorized)
8080/tcp open  http             Jetty 10.0.20
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(10.0.20)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-10-07T04:08:13
|_  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 26.64 seconds
```

nmap -O 192.168.44.176



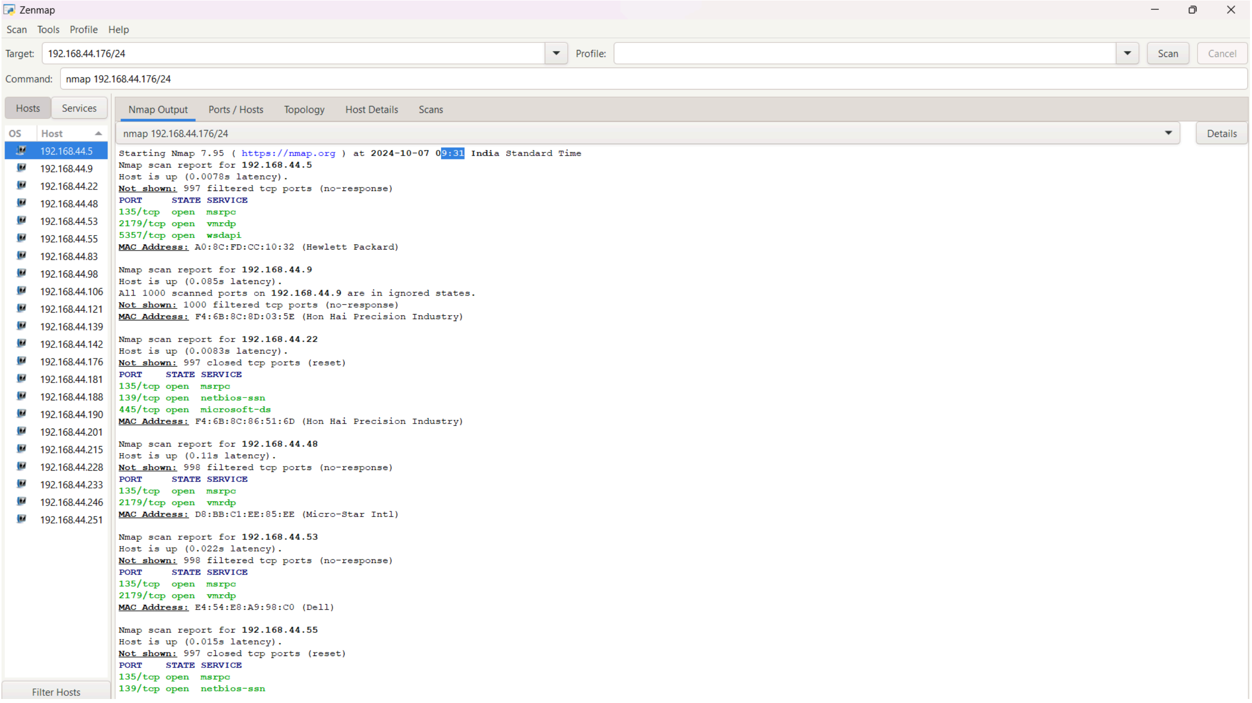
Target: 192.168.44.176

Command: nmap -O 192.168.44.176

nmap -O 192.168.44.176

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:40 India Standard Time
Nmap scan report for 192.168.44.176
Host is up (0.00042s latency).
Not shown: 993 closed tcp ports (reset)
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
3306/tcp open  mysql
8080/tcp open  http-proxy
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
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 1.60 seconds
```

nmap 192.168.44.176/24

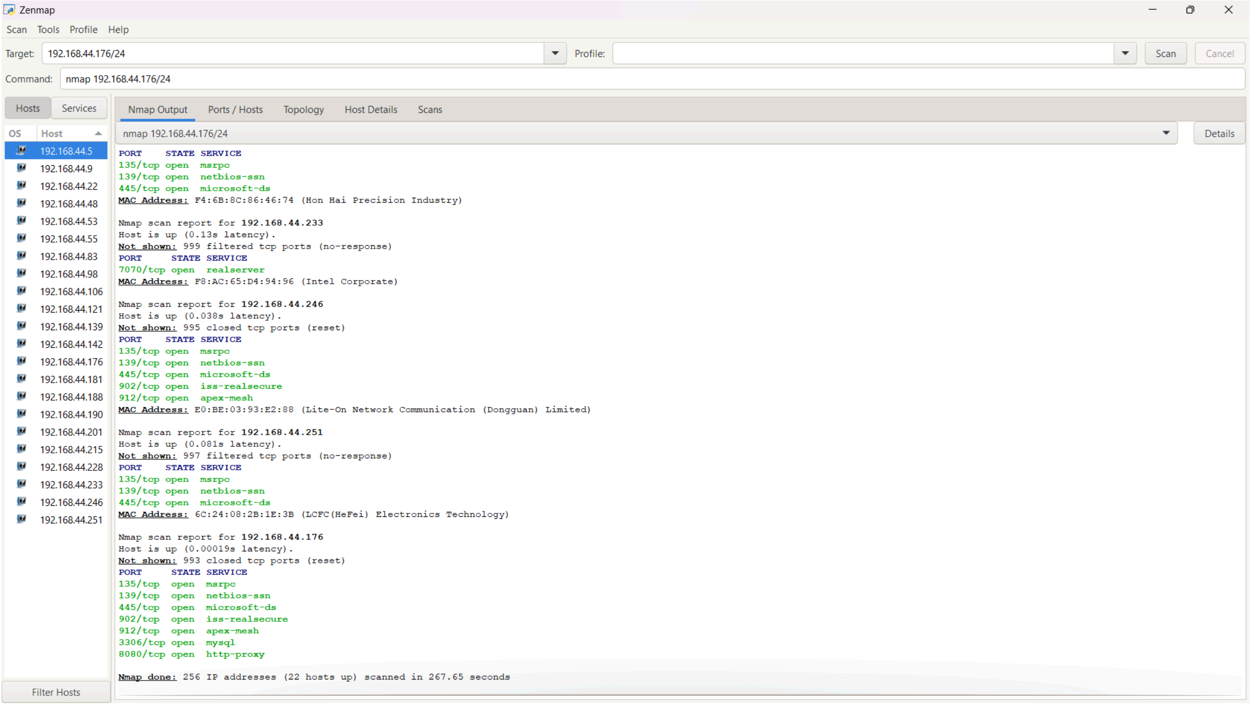


Target: 192.168.44.176/24

Command: nmap 192.168.44.176/24

nmap 192.168.44.176/24

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 09:31 India Standard Time
Nmap scan report for 192.168.44.5
Host is up (0.0078s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
5357/tcp open  wsdapi
MAC Address: A0:8C:FD:CC:10:32 (Hewlett Packard)

Nmap scan report for 192.168.44.9
Host is up (0.085s latency).
All 1000 scanned ports on 192.168.44.9 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F4:6B:8C:8D:03:5E (Hon Hai Precision Industry)

Nmap scan report for 192.168.44.22
Host is up (0.0083s 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:86:51:6D (Hon Hai Precision Industry)

Nmap scan report for 192.168.44.48
Host is up (0.11s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
MAC Address: D8:BB:C1:EE:85:EE (Micro-Star Intl)

Nmap scan report for 192.168.44.53
Host is up (0.022s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
MAC Address: E4:54:E8:A9:98:C0 (Dell)

Nmap scan report for 192.168.44.55
Host is up (0.015s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
```



Target: 192.168.44.176/24

Command: nmap 192.168.44.176/24

```
OS  Host
    192.168.44.5
    192.168.44.9
    192.168.44.22
    192.168.44.48
    192.168.44.53
    192.168.44.55
    192.168.44.83
    192.168.44.98
    192.168.44.106
    192.168.44.121
    192.168.44.139
    192.168.44.142
    192.168.44.176
    192.168.44.181
    192.168.44.188
    192.168.44.190
    192.168.44.201
    192.168.44.215
    192.168.44.228
    192.168.44.233
    192.168.44.246
    192.168.44.251
```

nmap 192.168.44.176/24

```
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: F4:6B:8C:86:46:74 (Hon Hai Precision Industry)

Nmap scan report for 192.168.44.233
Host is up (0.13s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: F8:AC:65:D4:94:96 (Intel Corporate)

Nmap scan report for 192.168.44.246
Host is up (0.038s 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
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: E0:BE:03:93:E2:88 (Lite-On Network Communication (Dongguan) Limited)

Nmap scan report for 192.168.44.251
Host is up (0.081s 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: 6C:24:08:2B:1E:3B (LCFC(HeFei) Electronics Technology)

Nmap scan report for 192.168.44.176
Host is up (0.00019s latency).
Not shown: 993 closed tcp ports (reset)
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
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 256 IP addresses (22 hosts up) scanned in 267.65 seconds
```