Name : Manjyot Wadhwa
Div : D15C Batch : C Roll
No : 74

CNS Experiment 09

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:

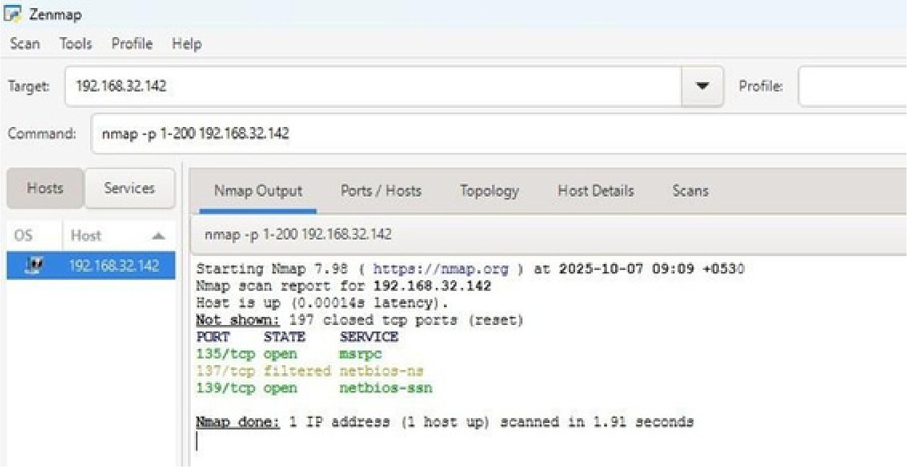
Nmap Commands

For port scanning between 1 to 200

Scan Open Port Range

Ex. nmap -p 1-200 192.168.32.142

Used to scan ports 1 to 200 on a target to identify which ones are open.
It helps in checking the availability of network services running within a specific range.



Target: 192.168.32.142

Command: nmap -p 1-200 192.168.32.142

```
nmap -p 1-200 192.168.32.142

Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-07 09:09 +0530
Nmap scan report for 192.168.32.142
Host is up (0.00014s 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
```

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

Scans a single specified port (in this case, port 902) on the target system.

It’s useful when you want to verify if a specific service or application is accessible.

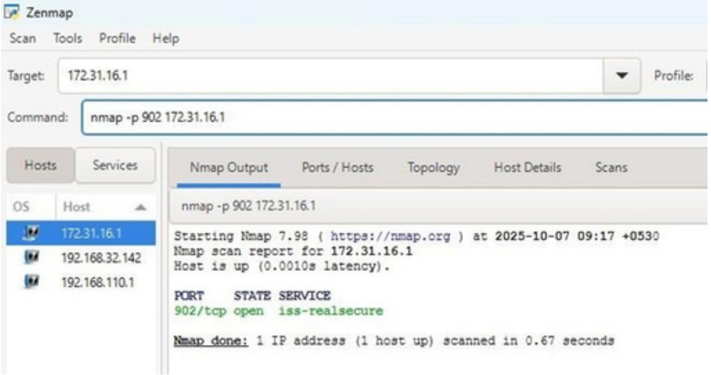
Ex. **Single Port**

Nmap -p 902

172.31.16.1

Scans one specific port on the target to check if that service is open, closed, or filtered.

Useful for quickly verifying a single service (e.g., SSH on port 22) without scanning other ports.



Target: 172.31.16.1

Command: nmap -p 902 172.31.16.1

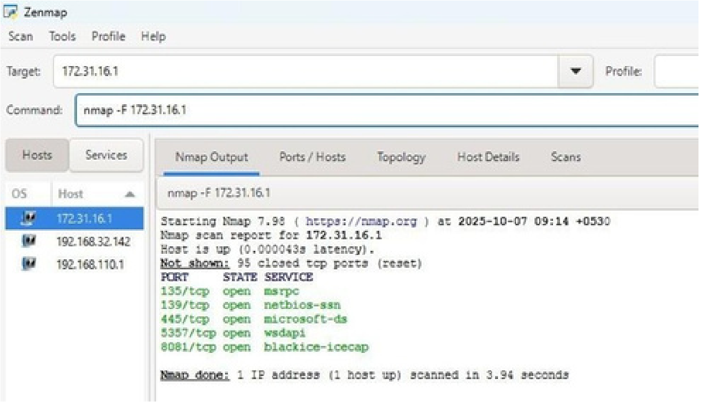
```
nmap -p 902 172.31.16.1
```

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-07 09:17 +0530
Nmap scan report for 172.31.16.1
Host is up (0.0010s latency).

PORT    STATE SERVICE
902/tcp open  iss-realsecure

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

Fast Scan

Nmap-F 172.31.16.

Performs a quick scan using only the most common 100 ports instead of all 65,535.
This saves time and provides a quick overview of major open services.



Target: 172.31.16.1

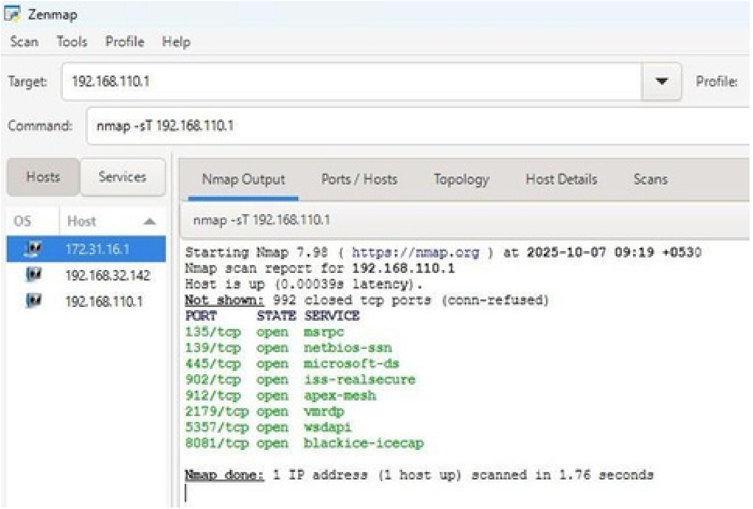
Command: nmap -F 172.31.16.1

```
nmap -F 172.31.16.1
```

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-07 09:14 +0530
Nmap scan report for 172.31.16.1
Host is up (0.000043s 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
5357/tcp open  wsdapi
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 3.94 seconds
```

TP connect SCAN (uses OS connect(), reliable on Windows) nmap -sT 192.168.110.1

Uses the TCP connect() system call to establish a full connection with each port. It is reliable on all systems, especially Windows, but easier to detect by firewalls.



Target: 192.168.110.1

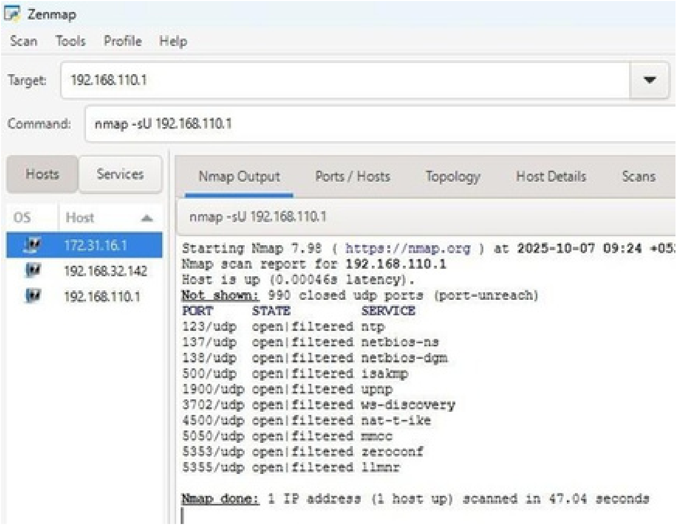
Command: nmap -sT 192.168.110.1

```
nmap -sT 192.168.110.1

Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-07 09:19 +0530
Nmap scan report for 192.168.110.1
Host is up (0.00039s latency).
Not shown: 992 closed tcp ports (conn-refused)
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
2179/tcp open  vmrdp
5357/tcp open  wsdapi
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
```

UDP Scan nmap sU 192.168.110.1

Scans UDP ports to detect services that use the UDP protocol.

Since UDP lacks connection acknowledgment, these scans are slower and less reliable.



Target: 192.168.110.1

Command: nmap -sU 192.168.110.1

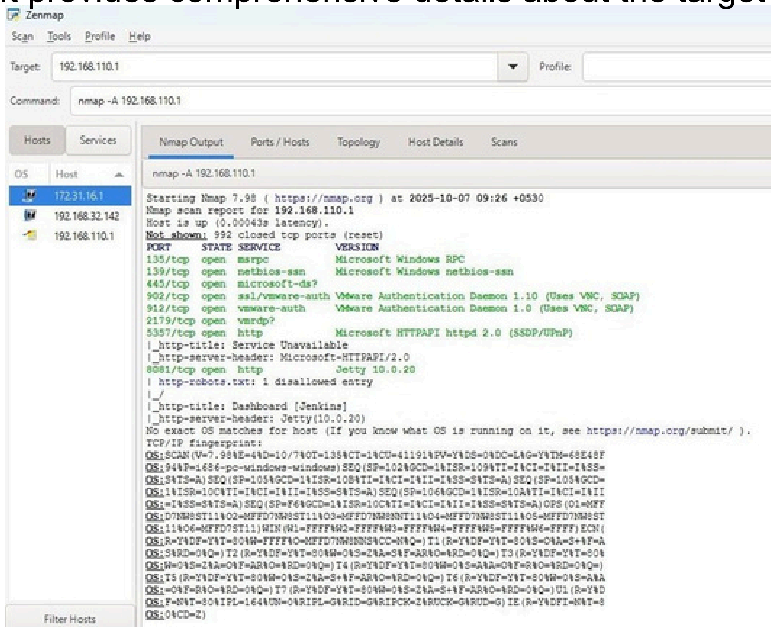
```
nmap -sU 192.168.110.1

Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-07 09:24 +05
Nmap scan report for 192.168.110.1
Host is up (0.00046s latency).
Not shown: 990 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
3702/udp open|filtered ws-discovery
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 47.04 seconds
```

Aggressive scan (OS detection + version + script + traceroute):

nmap-A 192.168.110.1

Performs OS detection, version detection, script scanning, and traceroute in one go.

It provides comprehensive details about the target system but is quite intrusive.



Target: 192.168.110.1

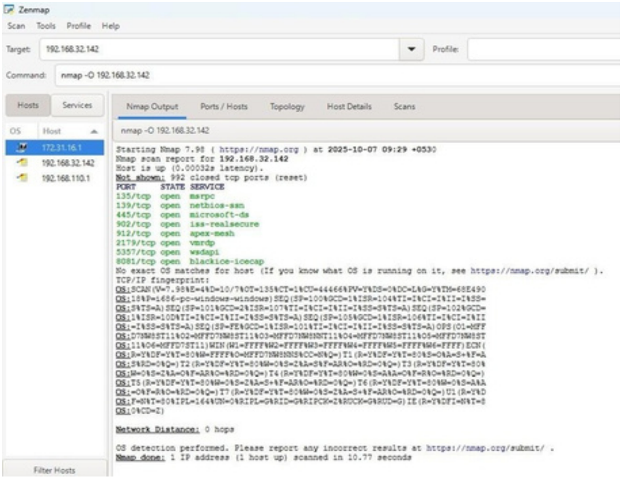
Command: nmap -A 192.168.110.1

```
nmap -A 192.168.110.1

Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-07 09:26 +0530
Nmap scan report for 192.168.110.1
Host is up (0.00043s latency).
Not shown: 992 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)
2179/tcp open  vmrdp?
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
8081/tcp open  http            Jetty 10.0.20
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Dashboard [Jenkins]
|_http-server-header: Jetty(10.0.20)
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=7.98%E=4%D=10/7%OT=135%CT=1%CU=41191%PV=Y%DS=0%DC=L%G=Y%TM=68E48F
OS:94%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=105%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=105%GCD=
OS:1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=1%ISR=10A%TI=I%CI=I%II
OS:=I%SS=S%TS=A)SEQ(SP=F6%GCD=1%ISR=10C%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)
```

For OS fingerprinting (Combines many checks — verbose and intrusive. Use only on permitted targets) nmap-O 192.168.32.142

Identifies theoperating system running onthe target by analyzingnetwork responses.

Useful for vulnerability assessment but should only be used on authorized systems



Target: 192.168.32.142

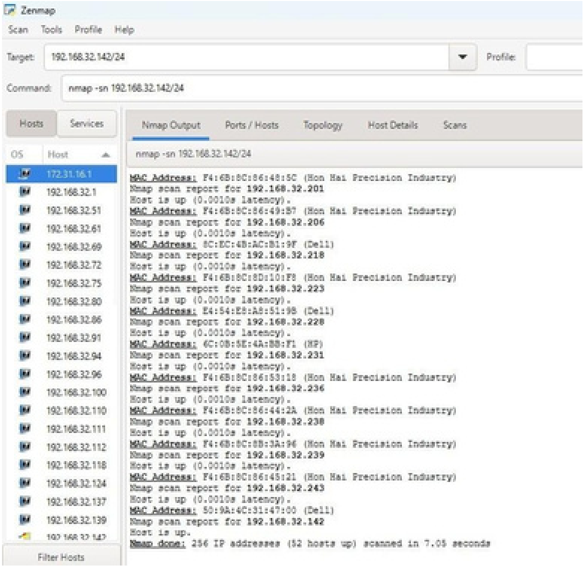
Command: nmap -O 192.168.32.142

```
nmap -O 192.168.32.142

Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-07 09:29 +0530
Nmap scan report for 192.168.32.142
Host is up (0.00032s latency).
Not shown: 992 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
2179/tcp open  vmrdp
5357/tcp open  wsdapi
8081/tcp open  blackice-icecap
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=7.98%E=4%D=10/7%OT=135%CT=1%CU=44466%PV=Y%DS=0%DC=L%G=Y%TM=68E490
OS:18%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=104%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=101%GCD=2%ISR=107%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=102%GCD=
OS:1%ISR=10D%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=105%GCD=1%ISR=106%TI=I%CI=I%II
OS:=I%SS=S%TS=A)SEQ(SP=FE%GCD=1%ISR=101%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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.77 seconds
```

Ping scan (host discovery; do not probe ports): nmap -sn 192.168.32.142/24

Performs host discovery without scanningports to checkwhichhostsareonline.

It’s a safe and fast way to map active devices in a network.

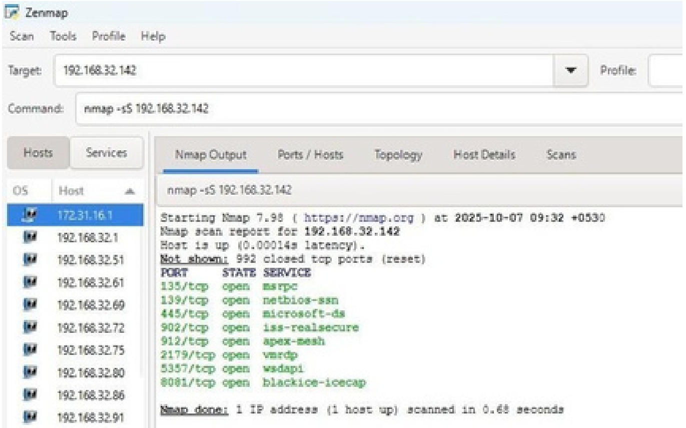


```
MAC Address: F4:6B:8C:86:48:5C (Hon Hai Precision Industry)
Nmap scan report for 192.168.32.201
Host is up (0.0010s latency).
MAC Address: F4:6B:8C:86:49:B7 (Hon Hai Precision Industry)
Nmap scan report for 192.168.32.206
Host is up (0.0010s latency).
MAC Address: 8C:EC:4B:AC:B1:9F (Dell)
Nmap scan report for 192.168.32.218
Host is up (0.0010s latency).
MAC Address: F4:6B:8C:8D:10:F8 (Hon Hai Precision Industry)
Nmap scan report for 192.168.32.223
Host is up (0.0010s latency).
MAC Address: E4:54:E8:A8:51:9B (Dell)
Nmap scan report for 192.168.32.228
Host is up (0.0010s latency).
MAC Address: 6C:0B:5E:4A:B8:F1 (HP)
Nmap scan report for 192.168.32.231
Host is up (0.0010s latency).
MAC Address: F4:6B:8C:86:53:18 (Hon Hai Precision Industry)
Nmap scan report for 192.168.32.236
Host is up (0.0010s latency).
MAC Address: F4:6B:8C:86:44:2A (Hon Hai Precision Industry)
Nmap scan report for 192.168.32.238
Host is up (0.0010s latency).
MAC Address: F4:6B:8C:8B:3A:96 (Hon Hai Precision Industry)
Nmap scan report for 192.168.32.239
Host is up (0.0010s latency).
MAC Address: F4:6B:8C:86:45:21 (Hon Hai Precision Industry)
Nmap scan report for 192.168.32.243
Host is up (0.0010s latency).
MAC Address: 50:9A:4C:31:47:00 (Dell)
Nmap scan report for 192.168.32.142
Host is up.
Nmap done: 256 IP addresses (52 hosts up) scanned in 7.05 seconds
```

SYN scan (stealth, requires Npcap and admin privileges; may be blocked on Windows):

Performs a stealth scanbysending SYNpacketsand notcompletingtheTCP handshake.

It’s faster and less detectable, ideal for security testing with admin privileges.



```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-07 09:32 +0530
Nmap scan report for 192.168.32.142
Host is up (0.00014s latency).
Not shown: 992 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
2179/tcp open  vmrdp
5357/tcp open  wsdapi
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

Conclusion :

Thus, the experiment was successfully carried out using Nmap to perform different types of network scans such as TCP, UDP, Ping, and OS fingerprinting. The practical helped us understand how to identify open ports, detect operating systems, and analyze the overall network security and vulnerabilities efficiently.