LOVELY PROFESSIONAL UNIVERSITY

NAME- D. L. P SUPRIYA

REG. NO.: 11902522

ROLL NO.: 38

INT301

CA- 3

Q) Suppose you are an ethical hacker and you are asked to perform a scan on your simulated network. Your task is to identify:

a) Live hosts

b) Services running on live hosts

c) Banner grabbing

d) OS fingerprinting

e) Conducting performance scans based on your current network bandwidth.

Use any open-source software to generate a report on the same.

-> I have used nmap tool for the given question.

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing.

Nmap allows you to scan your network and discover not only everything connected to it, but also a wide variety of information about whats connected, what services each host is operating and so on.

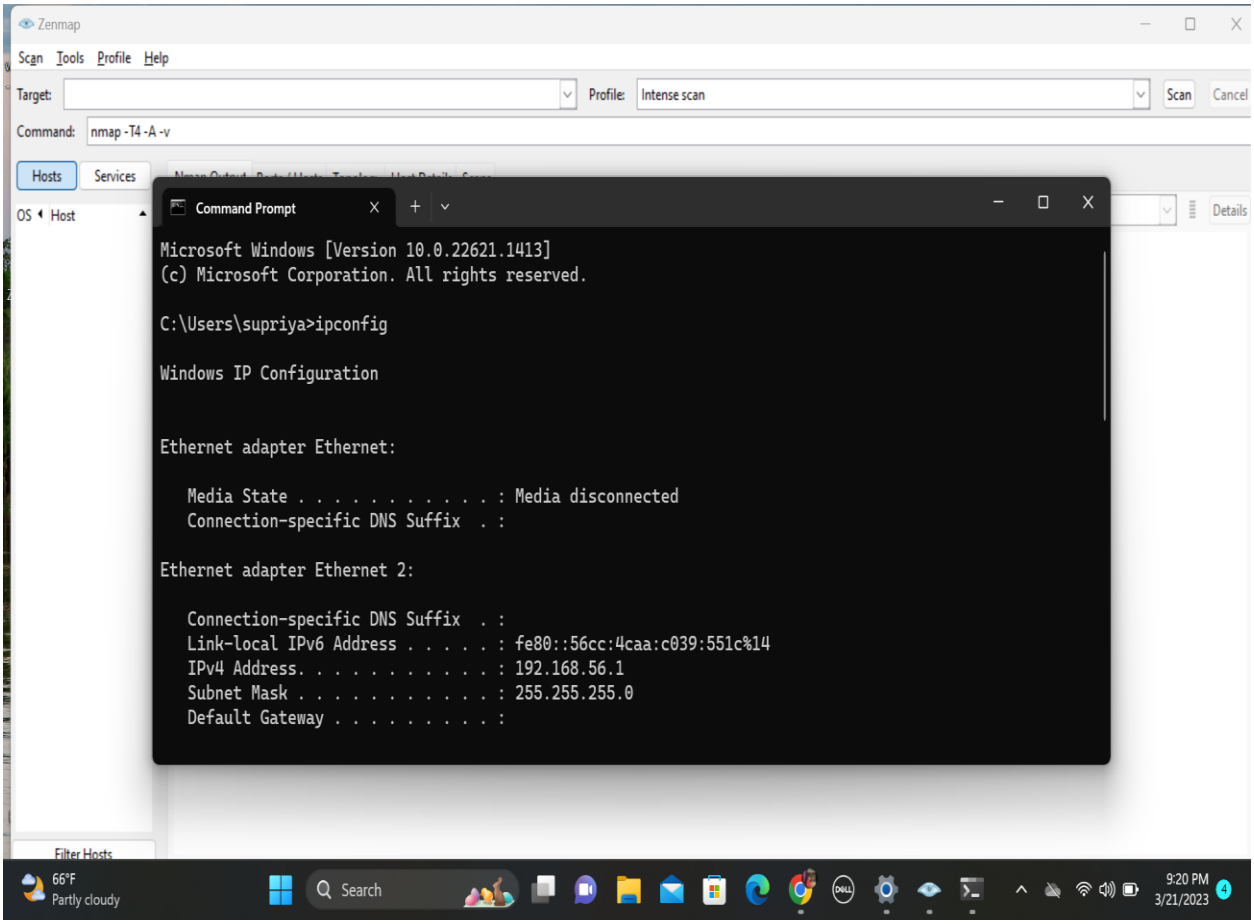
Nmap can be used by hackers to gain access to uncontrolled ports on the network that may lead to providing access to the system.

Github link: https://github.com/supriyad20/CA3/tree/main

Step- 1

Install the nmap tool, after the installation process completes, open the command prompt and run the command “ipconfig” to know the ip address.

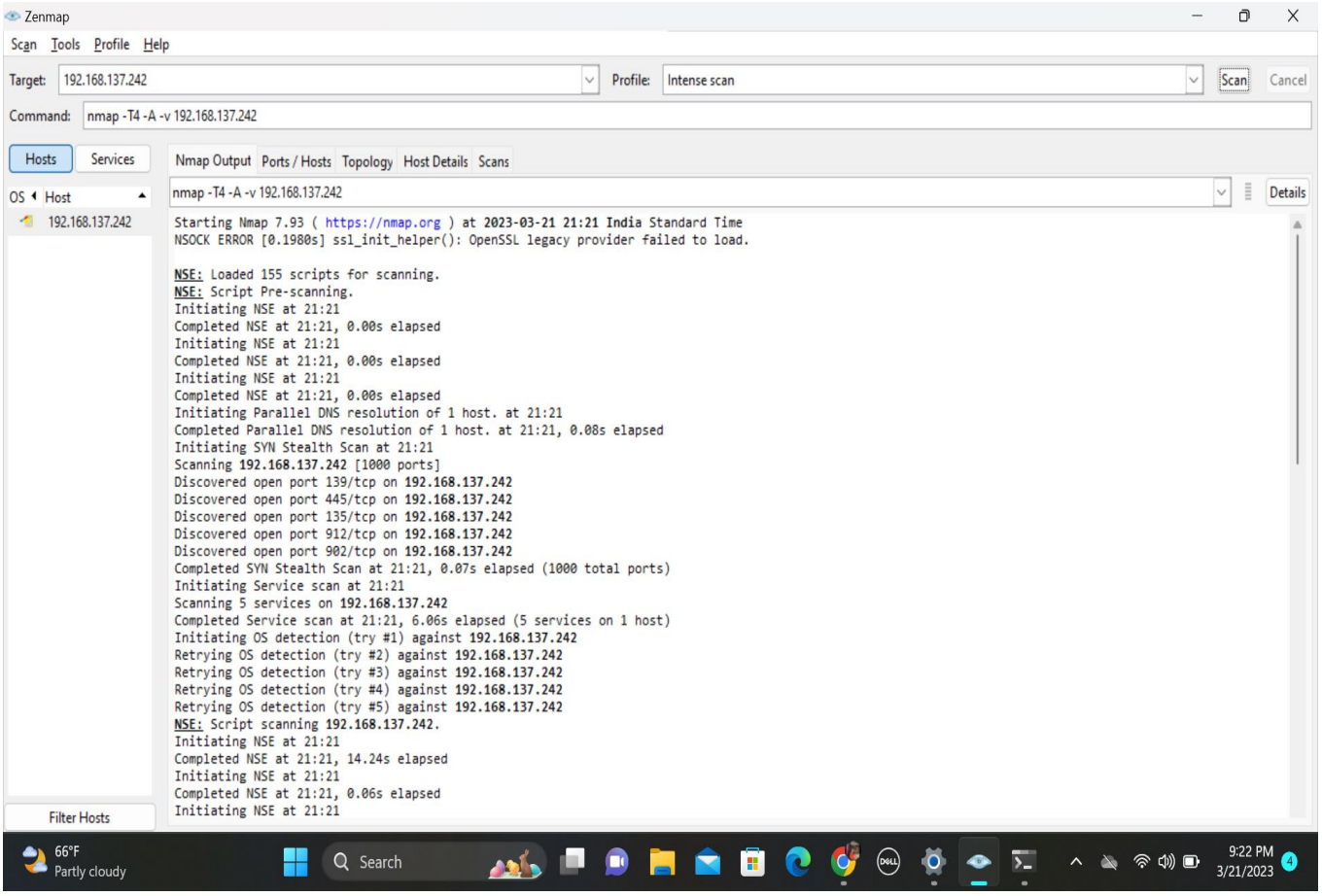
IP address- 192.168.137.242



Step- 2

In the nmap tool, in “target” enter the IP address and run the network scan.

In “profile” select the type of scan to use.

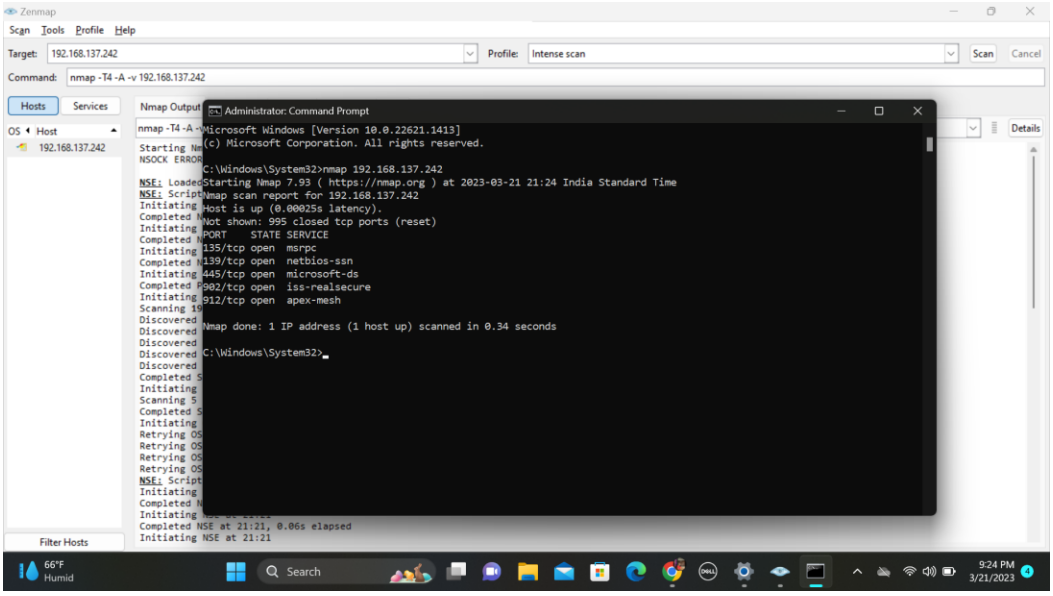


Step- 3

Now run the command prompt as administrator.

And enter the command nmap 192.168.137.242 (IP address) and run it.

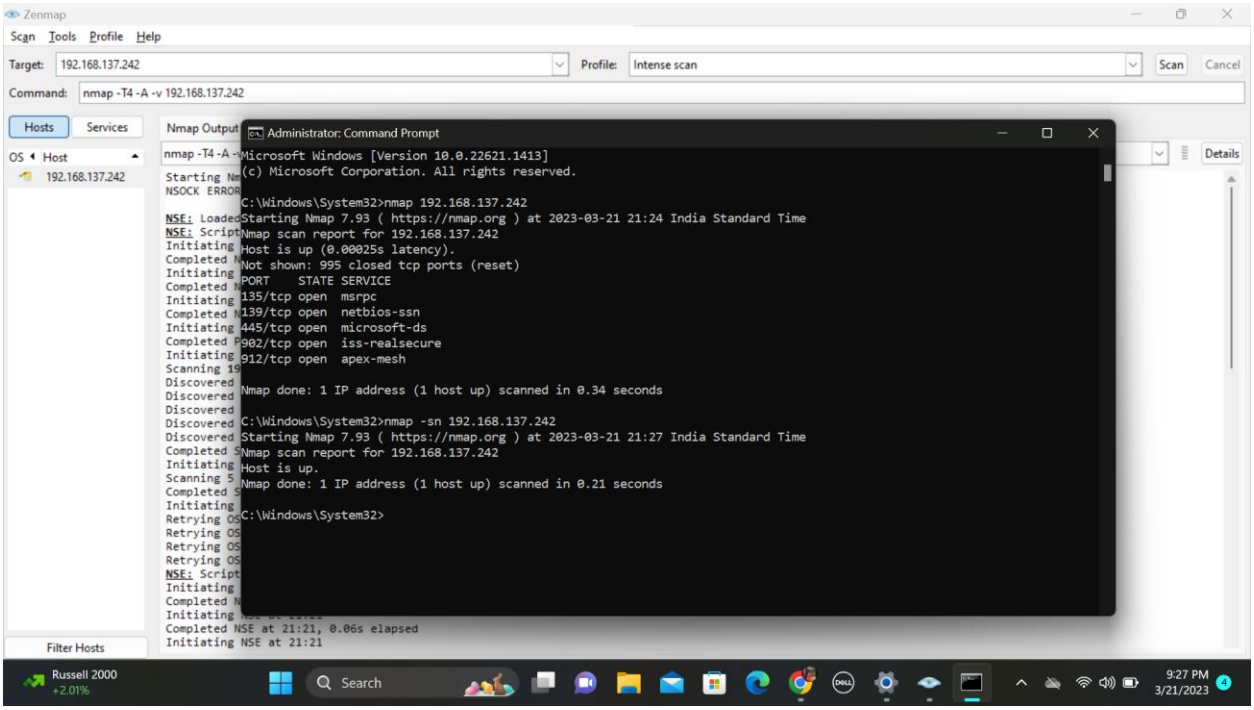
This command will show all the open ports.



a) Live hosts.

Command used: nmap -sn <IP range>

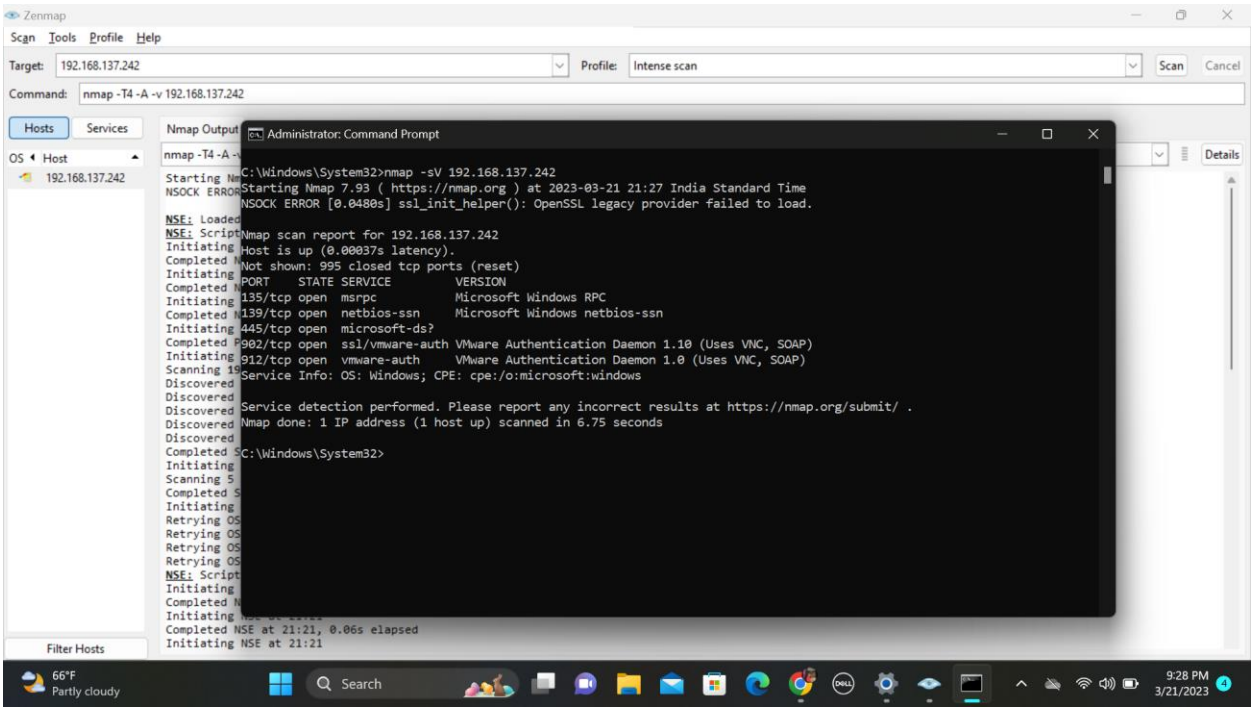
This command will use the -sn option to perform a "ping scan" on the specified IP range, which will identify all the live hosts on the network.



b) Services running on live hosts.

Command used: nmap -sV <IP range>

This command will use the -sV option to perform version detection on the identified services, which will determine the software and version numbers running on all the open ports.



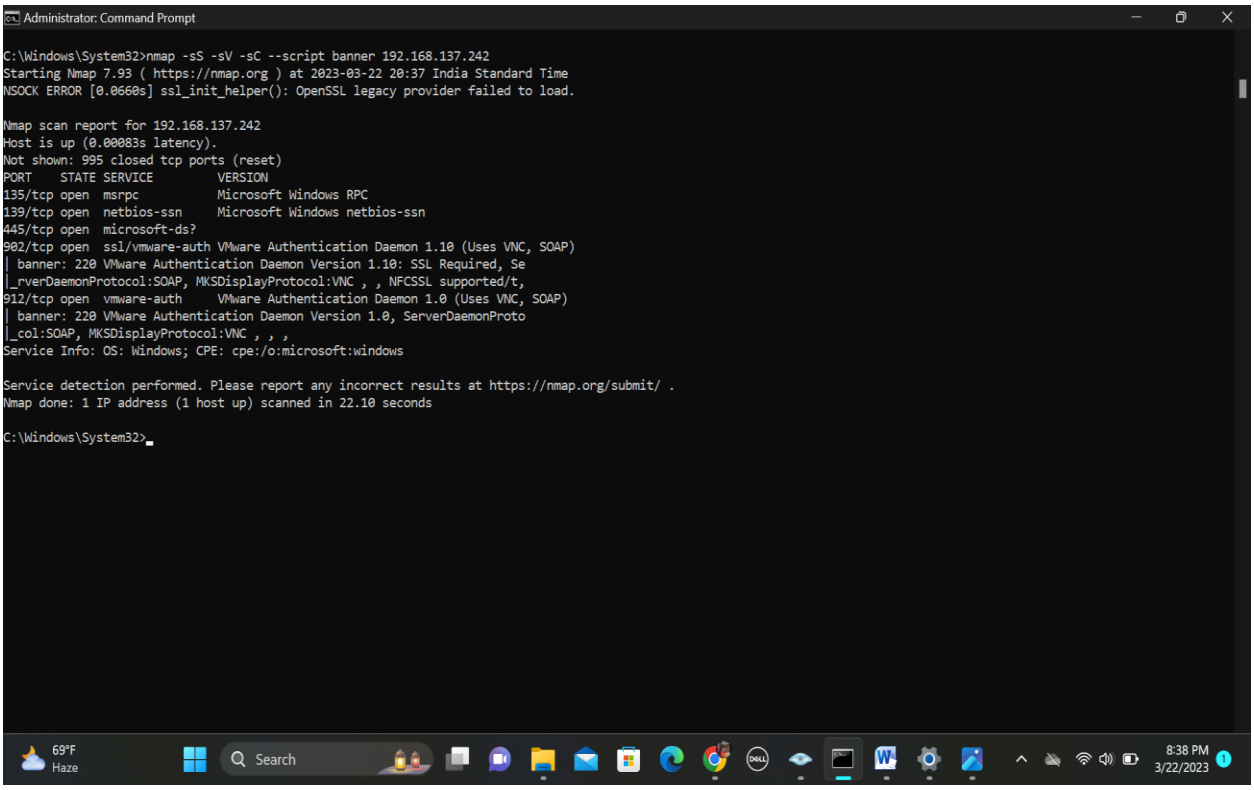
c) Banner grabbing.

Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.

Command used: nmap -sS -sV -sC --script banner <IP range>

This command will use the -sS option to perform a "TCP SYN scan," the -sV option to perform version detection, and the -sC option to enable Nmap's default script scanning. The --script

banner option will then tell Nmap to run the "banner" script, which will retrieve banner information from the identified services.

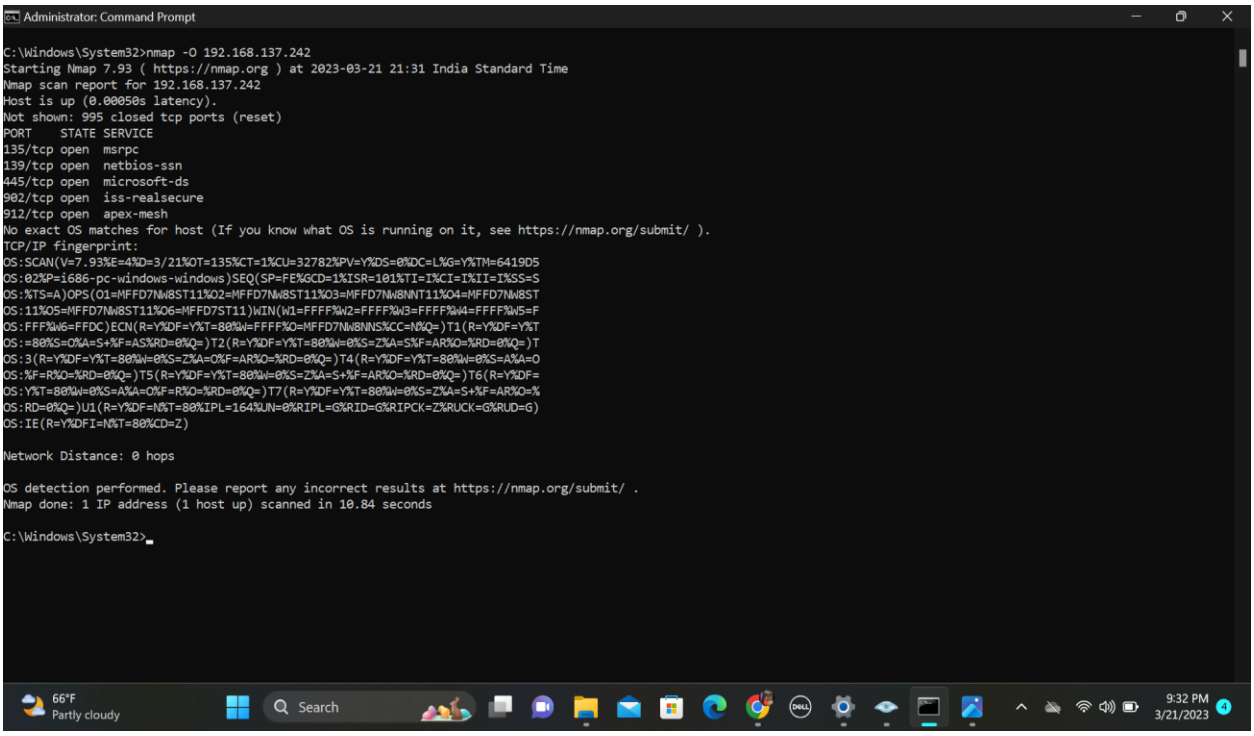


d) OS fingerprinting.

The term OS fingerprinting in Ethical Hacking refers to any method used to determine what operating system is running on a remote computer.

<u>Command used</u>: nmap -O <IP range>

This command will use the -O option to perform OS detection on the specified IP range, which will attempt to identify the operating system running on each of the live hosts.



```
Administrator: Command Prompt

C:\Windows\System32>nmap -O 192.168.137.242
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 21:31 India Standard Time
Nmap scan report for 192.168.137.242
Host is up (0.00050s 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
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=7.93%E=4%D=3/21%OT=135%CT=1%CU=32782%PV=Y%DS=0%DC=L%G=Y%TM=6419D5
OS:02%P=i686-pc-windows-windows)SEQ(SP=FE%GCD=1%ISR=101%TI=I%CI=I%II=I%SS=S
OS:%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST
OS:11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=F
OS:FFF%W6=FFDC)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T
OS:=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T
OS:3(R=Y%DF=Y%T=80%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
OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
OS:Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=N%T=80%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 10.84 seconds

C:\Windows\System32>
```

e) Conducting performance scans based on your current network bandwidth.

<u>Command used</u>: nmap -T4 -A -v <IP range>
This command will use the -T4 option to set the timing template to "aggressive", the -A option to enable OS detection, version detection, script scanning, and traceroute, and the -v option to enable verbose output. This scan will provide information on the performance of the network based on the current bandwidth.

Here, aggressive mode of the template speeds scans up by making the assumption that you are on a reasonably fast and reliable network.

Administrator: Command Prompt

```
C:\Windows\System32>nmap -T4 -A -v 192.168.137.242
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 21:44 India Standard Time
NSOCK ERROR [0.2000s] ssl_init_helper(): OpenSSL legacy provider failed to load.

NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 21:44
Completed Parallel DNS resolution of 1 host. at 21:44, 0.08s elapsed
Initiating SYN Stealth Scan at 21:44
Scanning 192.168.137.242 [1000 ports]
Discovered open port 445/tcp on 192.168.137.242
Discovered open port 135/tcp on 192.168.137.242
Discovered open port 139/tcp on 192.168.137.242
Discovered open port 912/tcp on 192.168.137.242
Discovered open port 902/tcp on 192.168.137.242
Completed SYN Stealth Scan at 21:44, 0.09s elapsed (1000 total ports)
Initiating Service scan at 21:44
Scanning 5 services on 192.168.137.242
Completed Service scan at 21:44, 6.03s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 192.168.137.242
NSE: Script scanning 192.168.137.242.
Initiating NSE at 21:44
Completed NSE at 21:44, 14.18s elapsed
Initiating NSE at 21:44
Completed NSE at 21:44, 0.07s elapsed
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Nmap scan report for 192.168.137.242
Host is up (0.00078s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE         VERSION
135/tcp open  msrpc           Microsoft Windows RPC
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
```

66°F Partly cloudy | Search | 9:44 PM 3/21/2023

Administrator: Command Prompt

```
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-03-21T16:14:14
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 22.27 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2043 (86.920KB)

C:\Windows\System32>_
```

66°F Partly cloudy | Search | 9:44 PM 3/21/2023

To save the results into a text file:

Command used:

nmap -sn -sS -sV -sC -O -T4 -A -v -oA scan_results <IP range>