Vidyavardhini's College of Engineering and Technology, Vasai
Department of Computer Science & Engineering (Data Science)

EXPERIMENT 08

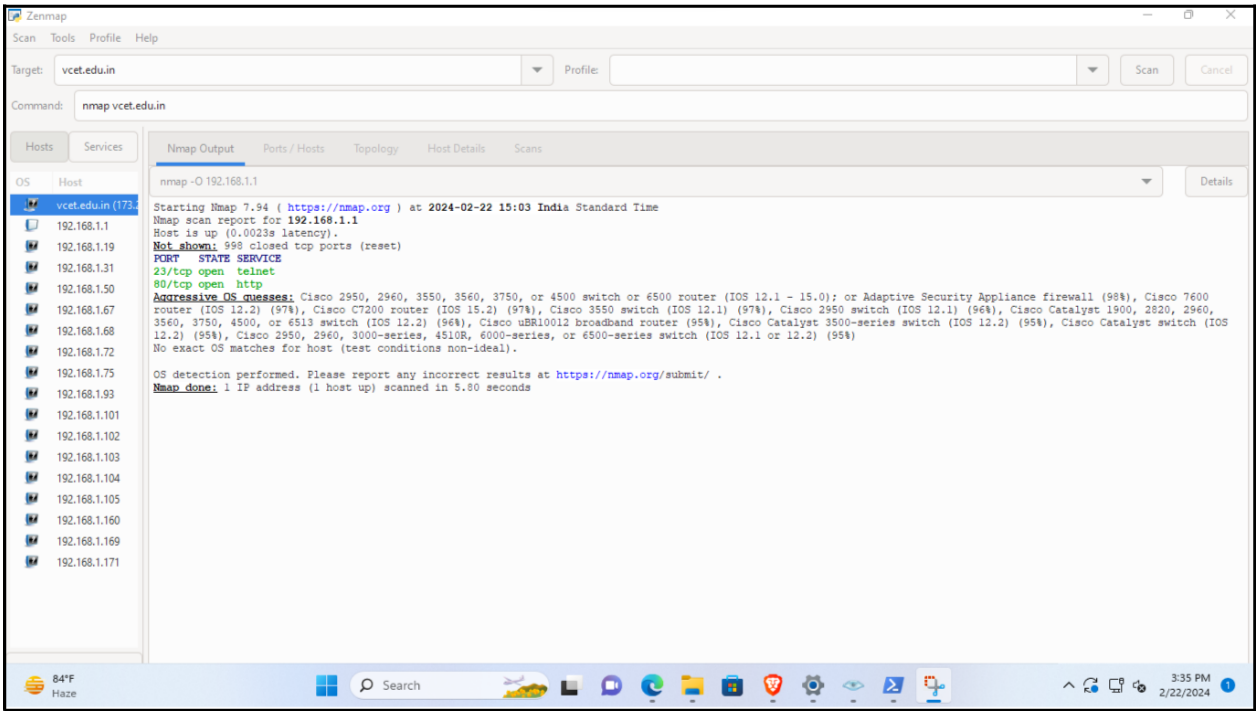
Aim:- Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, TCP port scan, UDP port scan, etc.

Theory:-

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap was named "Security Product of the Year" by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

In order to perform scan on a particular IP address, use the following command:
Command: nmap 192.168.1.1 -O



Target: vcet.edu.in

Profile:

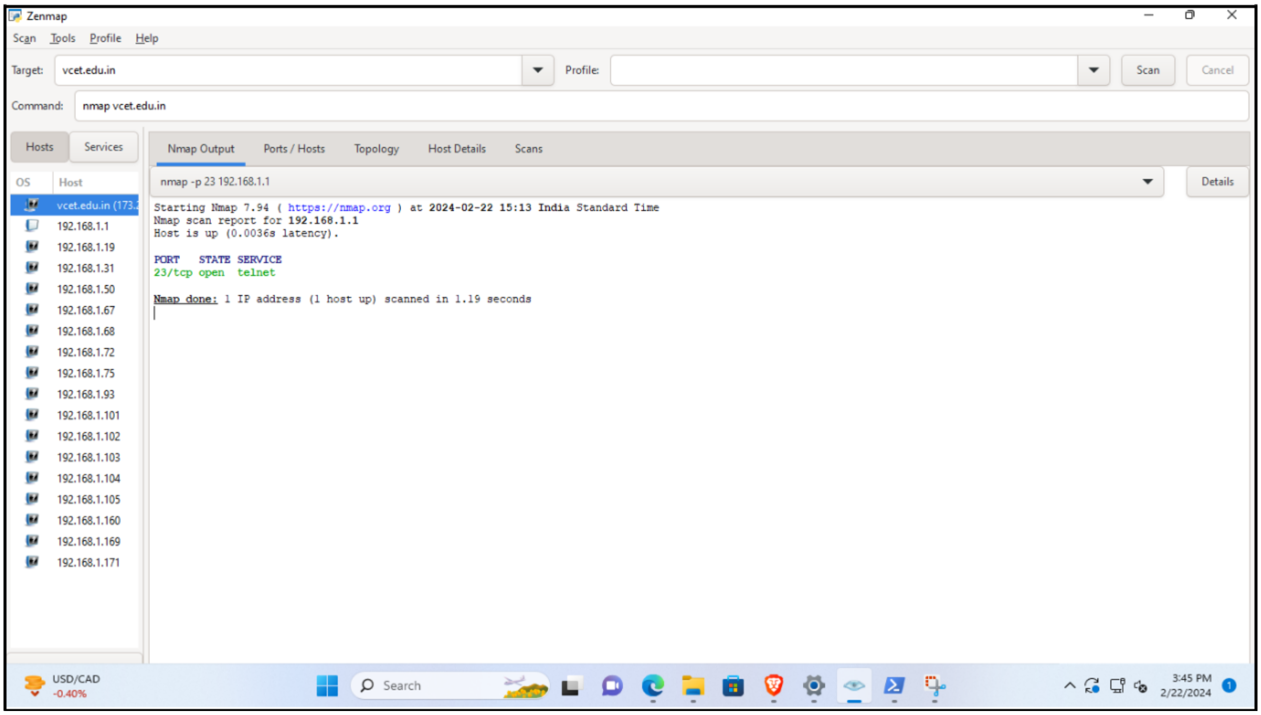
Command: nmap vcet.edu.in

nmap -O 192.168.1.1

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:03 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0023s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
Aggressive OS guesses: Cisco 2950, 2960, 3550, 3560, 3750, or 4500 switch or 6500 router (IOS 12.1 - 15.0); or Adaptive Security Appliance firewall (98%), Cisco 7600
router (IOS 12.2) (97%), Cisco C7200 router (IOS 15.2) (97%), Cisco 3550 switch (IOS 12.1) (97%), Cisco 2950 switch (IOS 12.1) (96%), Cisco Catalyst 1900, 2820, 2960,
3560, 3750, 4500, or 6513 switch (IOS 12.2) (96%), Cisco uBR10012 broadband router (95%), Cisco Catalyst 3500-series switch (IOS 12.2) (95%), Cisco Catalyst switch (IOS
12.2) (95%), Cisco 2950, 2960, 3000-series, 4510R, 6000-series, or 6500-series switch (IOS 12.1 or 12.2) (95%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.80 seconds
```

In order to scan a particular port, use the following command:

Command: nmap -p 23 192.168.1.1



Target: vcet.edu.in

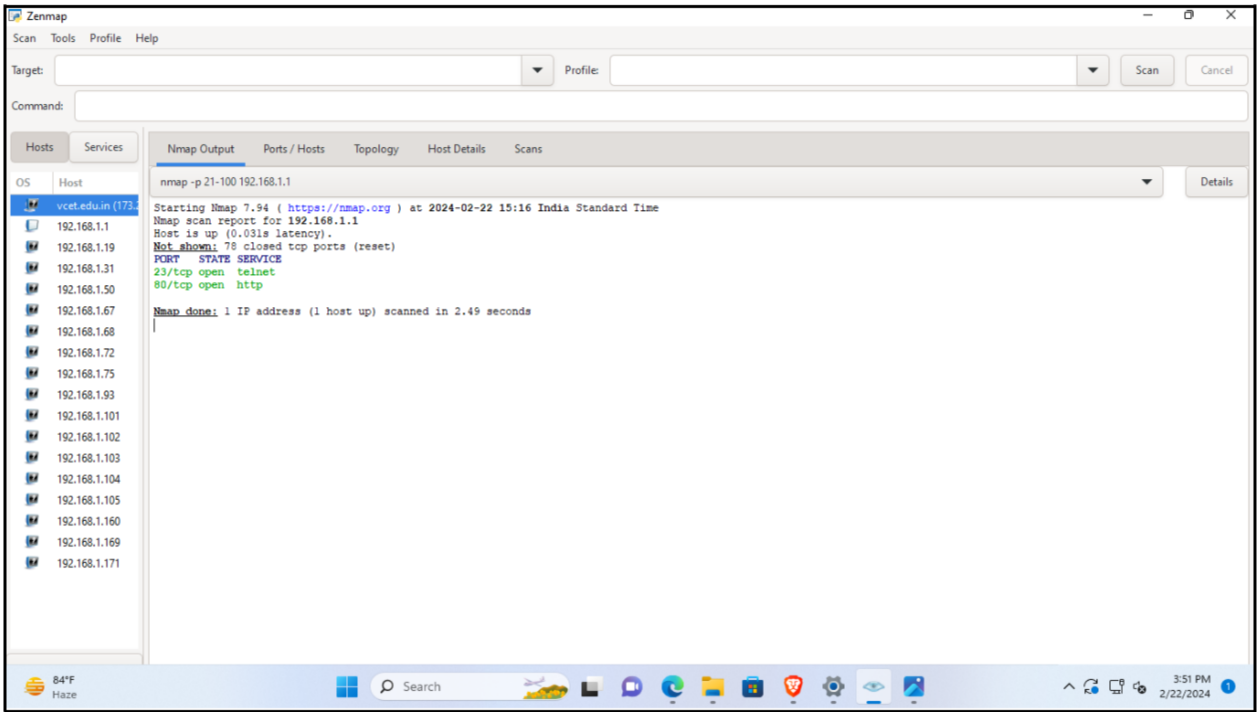
Profile:

Command: nmap vcet.edu.in

nmap -p 23 192.168.1.1

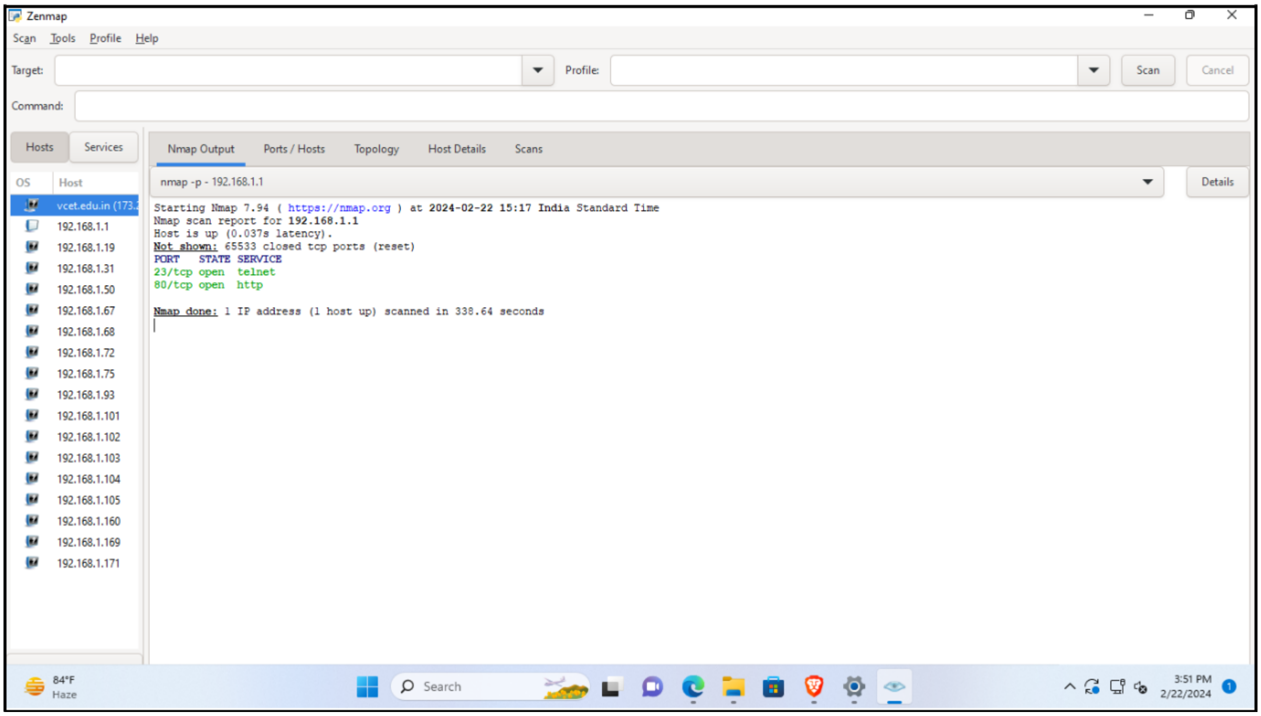
```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:13 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0036s latency).

PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
```

In order to scan range of IP, use the following command:
Command: nmap -p 21-100 192.168.1.1



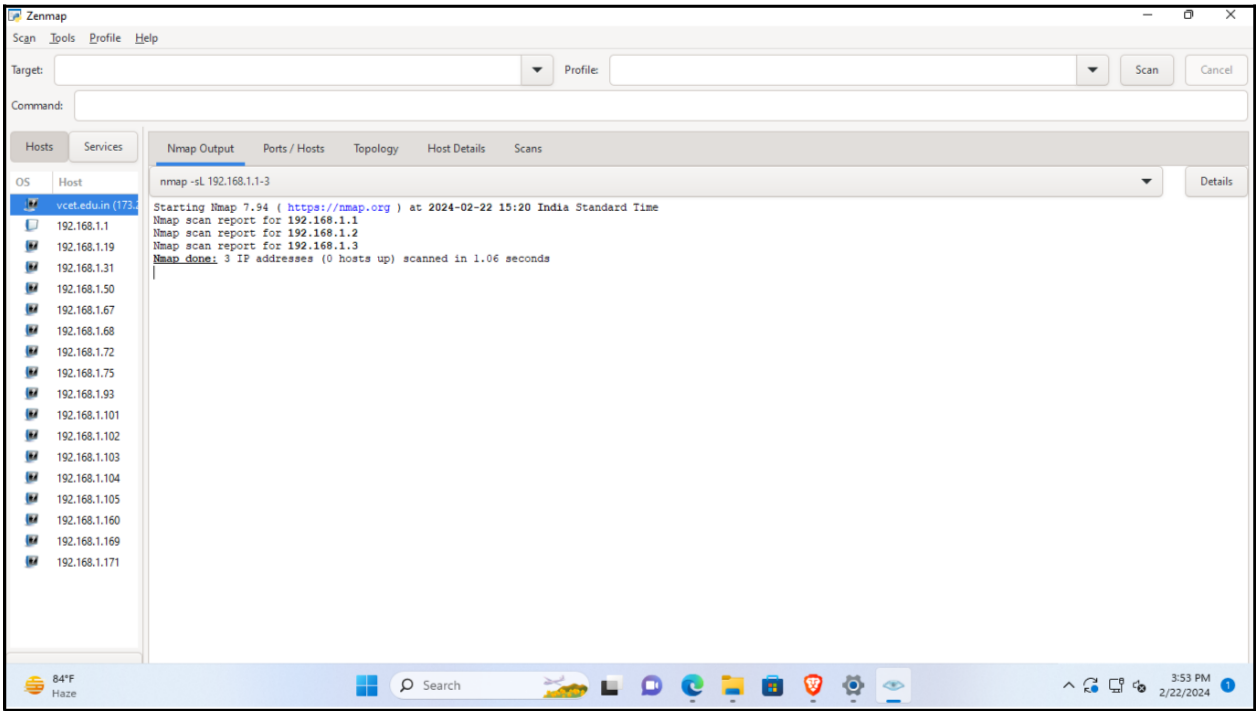
```
nmap -p 21-100 192.168.1.1

Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:16 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.031s latency).
Not shown: 78 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds
```

In order to scan available ports, use the following command:
Command: nmap 192.168.1.1 -p-



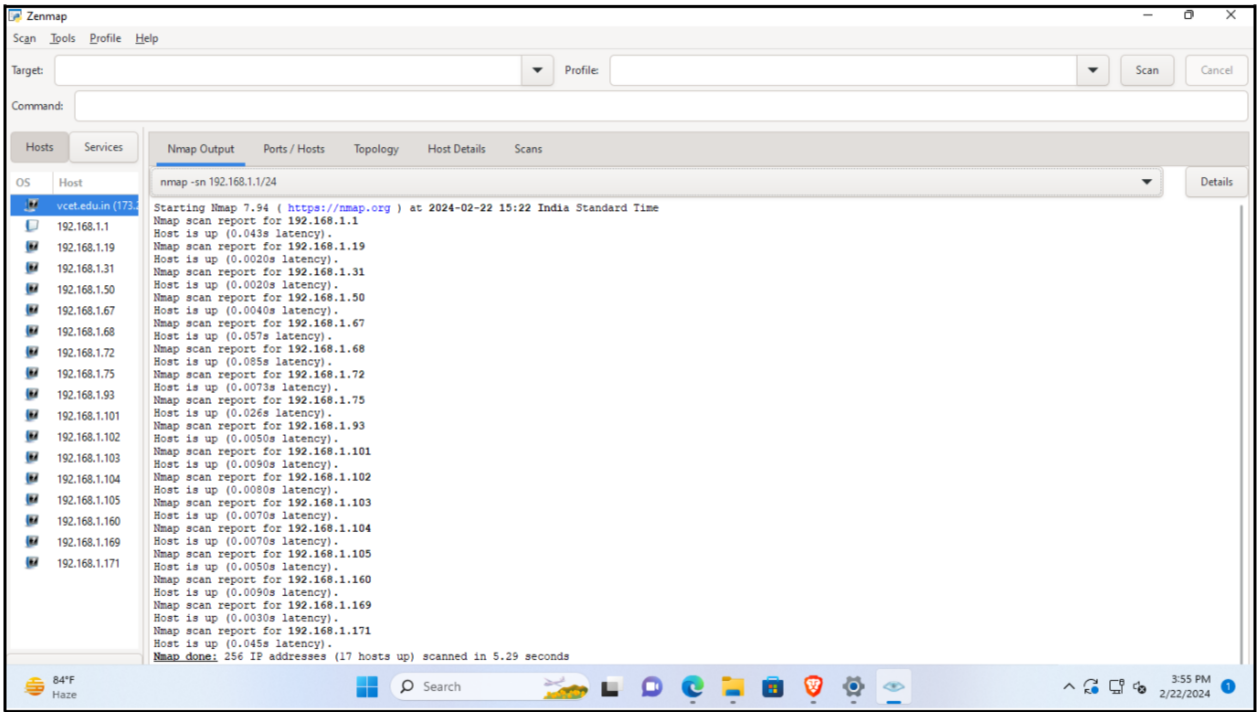
```
nmap -p - 192.168.1.1

Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:17 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.037s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 338.64 seconds
```

In order to List Scan from port 1-3, use the following command:
Command: nmap 192.168.1.1-3 -sL



```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:20 India Standard Time
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.2
Nmap scan report for 192.168.1.3
Nmap done: 3 IP addresses (0 hosts up) scanned in 1.06 seconds
```

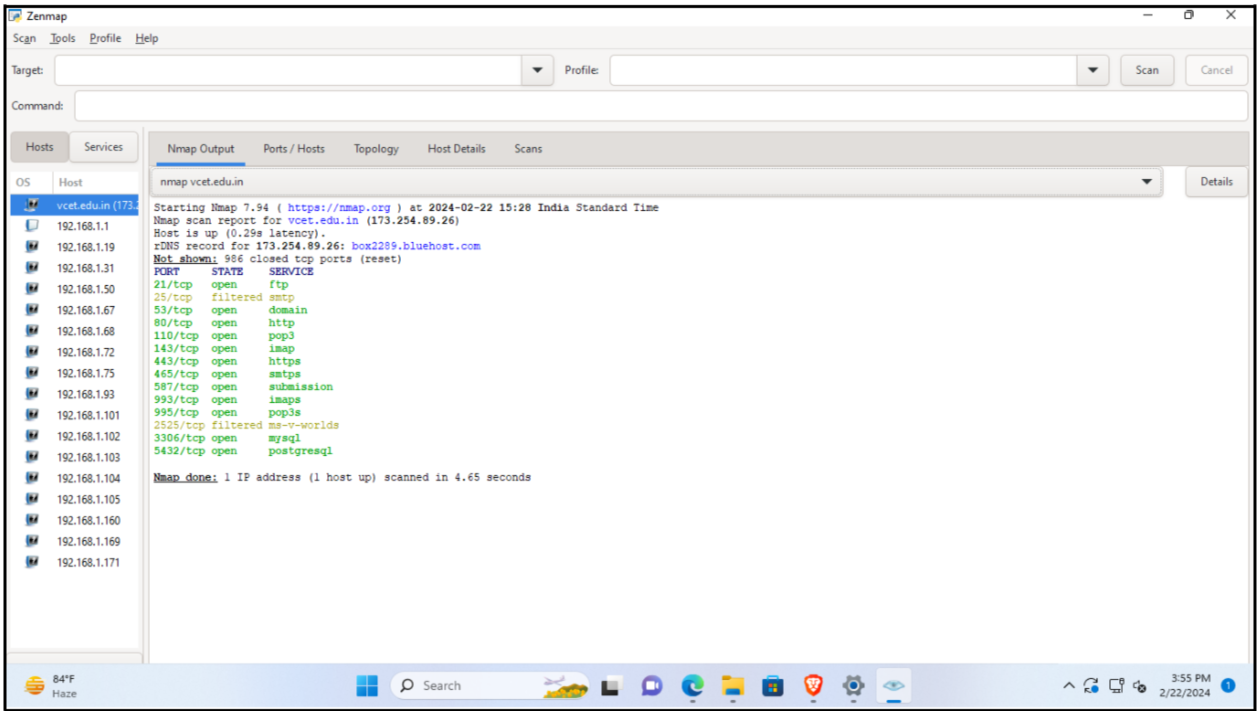
In order to disable port scan, use the following command:
Command: nmap 192.168.1.1/24 -sn



```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:22 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.043s latency).
Nmap scan report for 192.168.1.19
Host is up (0.0020s latency).
Nmap scan report for 192.168.1.31
Host is up (0.0020s latency).
Nmap scan report for 192.168.1.50
Host is up (0.0040s latency).
Nmap scan report for 192.168.1.67
Host is up (0.057s latency).
Nmap scan report for 192.168.1.68
Host is up (0.085s latency).
Nmap scan report for 192.168.1.72
Host is up (0.0073s latency).
Nmap scan report for 192.168.1.75
Host is up (0.026s latency).
Nmap scan report for 192.168.1.93
Host is up (0.0050s latency).
Nmap scan report for 192.168.1.101
Host is up (0.0090s latency).
Nmap scan report for 192.168.1.102
Host is up (0.0080s latency).
Nmap scan report for 192.168.1.103
Host is up (0.0070s latency).
Nmap scan report for 192.168.1.104
Host is up (0.0070s latency).
Nmap scan report for 192.168.1.105
Host is up (0.0050s latency).
Nmap scan report for 192.168.1.160
Host is up (0.0090s latency).
Nmap scan report for 192.168.1.169
Host is up (0.0030s latency).
Nmap scan report for 192.168.1.171
Host is up (0.045s latency).
Nmap done: 256 IP addresses (17 hosts up) scanned in 5.29 seconds
```

In order to disable Domain, use the following command:

Command: nmap vcet.edu.in



```
vcet.edu.in (173.2
192.168.1.1
192.168.1.19
192.168.1.31
192.168.1.50
192.168.1.67
192.168.1.68
192.168.1.72
192.168.1.75
192.168.1.93
192.168.1.101
192.168.1.102
192.168.1.103
192.168.1.104
192.168.1.105
192.168.1.160
192.168.1.169
192.168.1.171
```

nmap vcet.edu.in

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:28 India Standard Time
Nmap scan report for vcet.edu.in (173.254.89.26)
Host is up (0.29s latency).
rDNS record for 173.254.89.26: box2289.bluehost.com
Not shown: 986 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
25/tcp   filtered smtp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap
443/tcp  open     https
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2525/tcp filtered ms-v-worlds
3306/tcp open     mysql
5432/tcp open     postgresql

Nmap done: 1 IP address (1 host up) scanned in 4.65 seconds
```