# Experiment No. 10

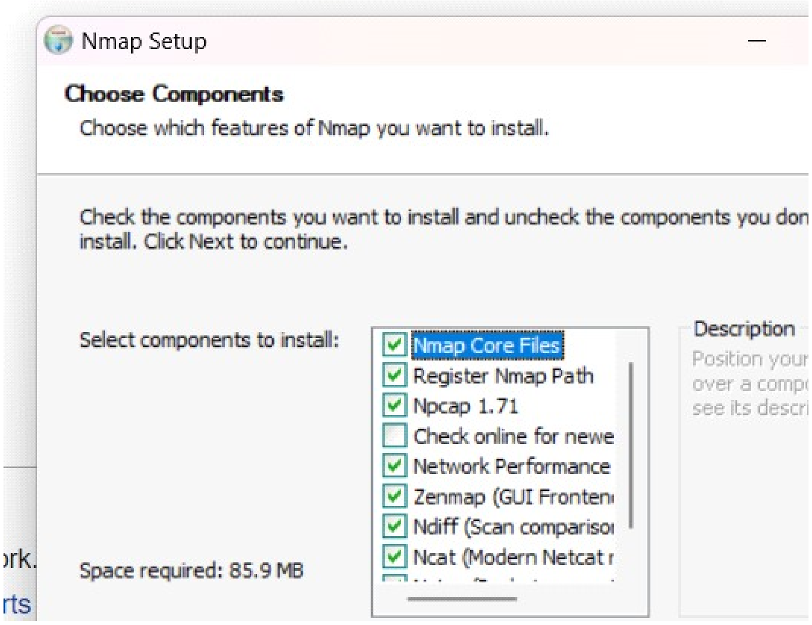
**Aim：** To install and implement NMAP.

**NMAP：** Nmap (**Network Mapper**) is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

**INSTALLATION OF NMAP :**

- Run the installer and click next :



Nmap Setup

**Choose Components**

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don
install. Click Next to continue.

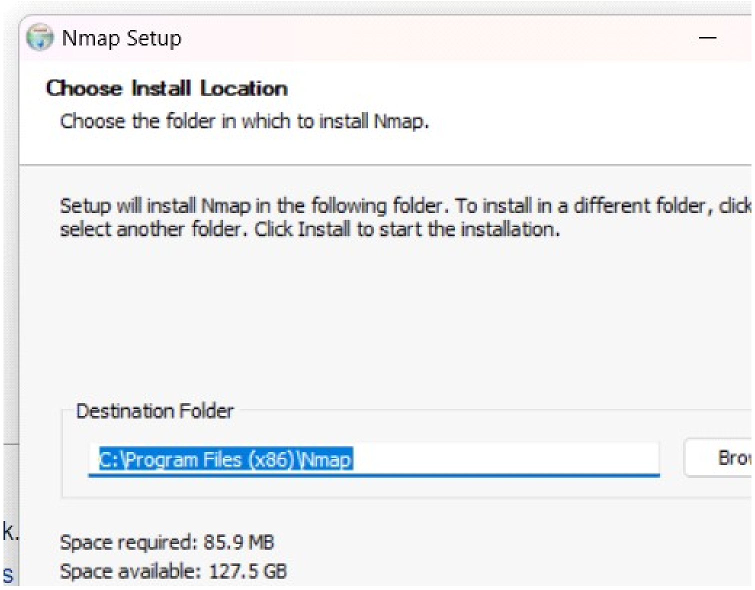
Select components to install:

☑ Nmap Core Files
☑ Register Nmap Path
☑ Npcap 1.71
☐ Check online for newe
☑ Network Performance
☑ Zenmap (GUI Fronten
☑ Ndiff (Scan compariso
☑ Ncat (Modern Netcat r

Description

Position your
over a compo
see its descri

Space required: 85.9 MB

- 

  Nmap Setup

  **Choose Install Location**

  Choose the folder in which to install Nmap.

  Setup will install Nmap in the following folder. To install in a different folder, click
  select another folder. Click Install to start the installation.

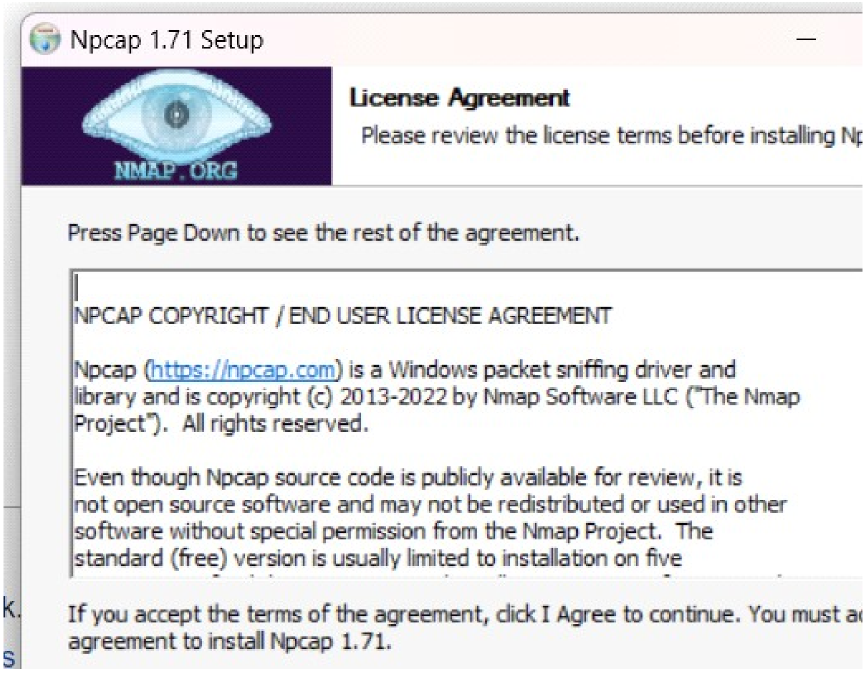
  Destination Folder

  C:\Program Files (x86)\Nmap

  Space required: 85.9 MB
  Space available: 127.5 GB

  Click on install :

- **Click on I Agree** :



Npcap 1.71 Setup

**License Agreement**

Please review the license terms before installing Np

Press Page Down to see the rest of the agreement.

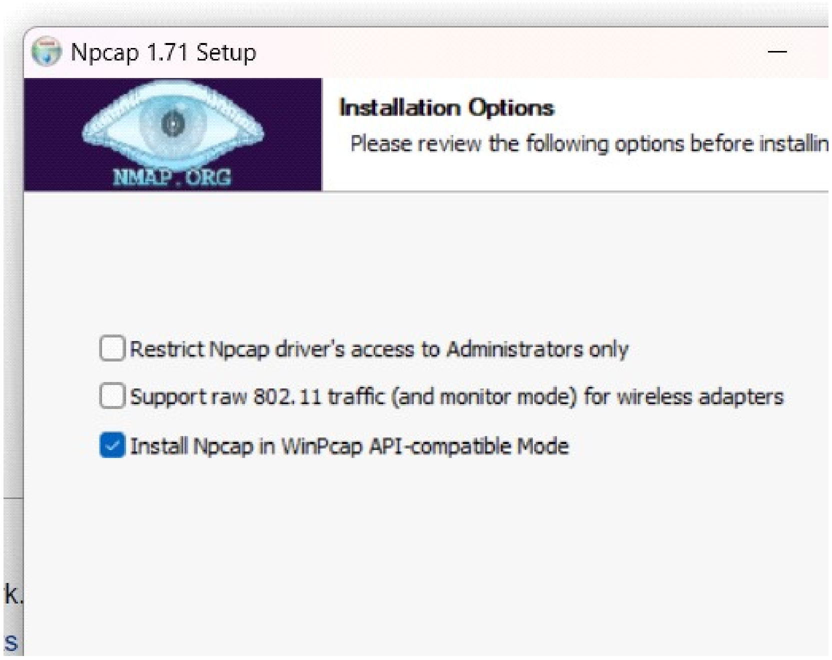
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

Npcap (https://npcap.com) is a Windows packet sniffing driver and library and is copyright (c) 2013-2022 by Nmap Software LLC ("The Nmap Project"). All rights reserved.

Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed or used in other software without special permission from the Nmap Project. The standard (free) version is usually limited to installation on five

If you accept the terms of the agreement, click I Agree to continue. You must ac
agreement to install Npcap 1.71.

- **Click on Install :**



Npcap 1.71 Setup

**Installation Options**

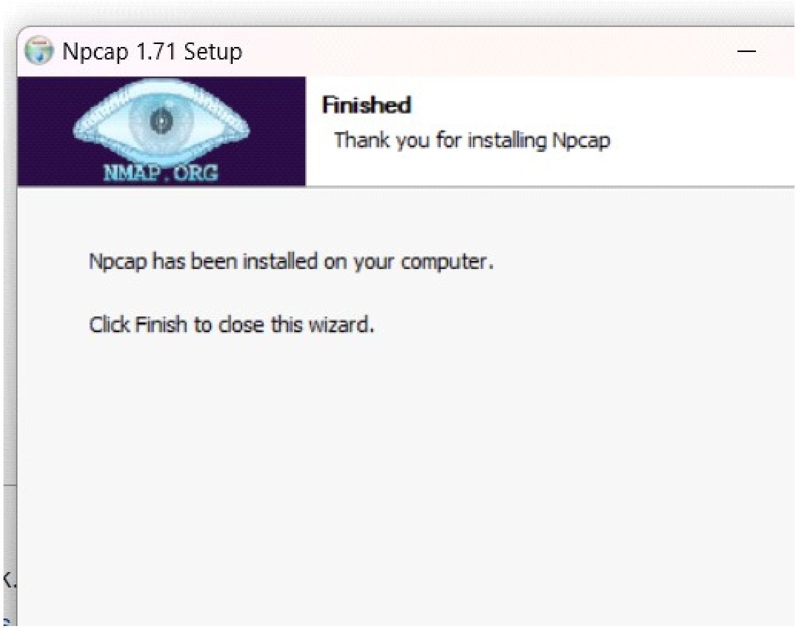
Please review the following options before installin

□ Restrict Npcap driver's access to Administrators only

□ Support raw 802.11 traffic (and monitor mode) for wireless adapters

☑ Install Npcap in WinPcap API-compatible Mode

- Click on Finish :



Npcap 1.71 Setup

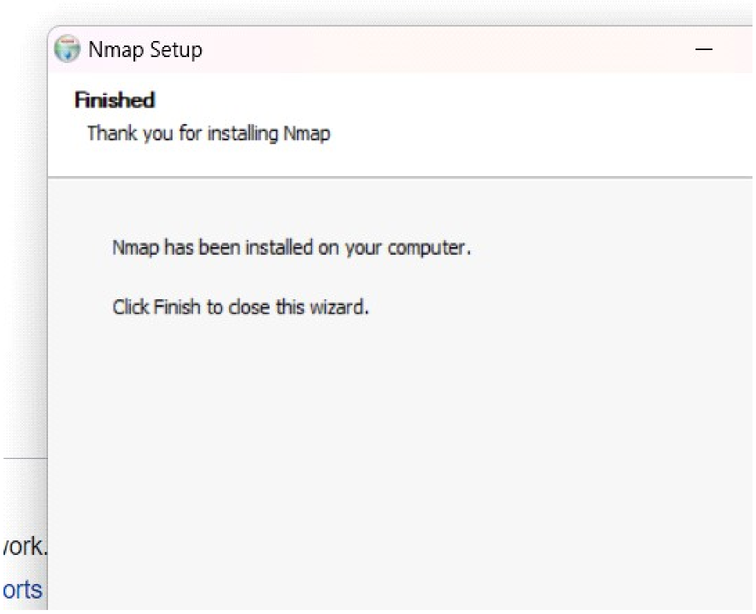
**Finished**

Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.

- **Click on Finish :**



Nmap Setup

**Finished**

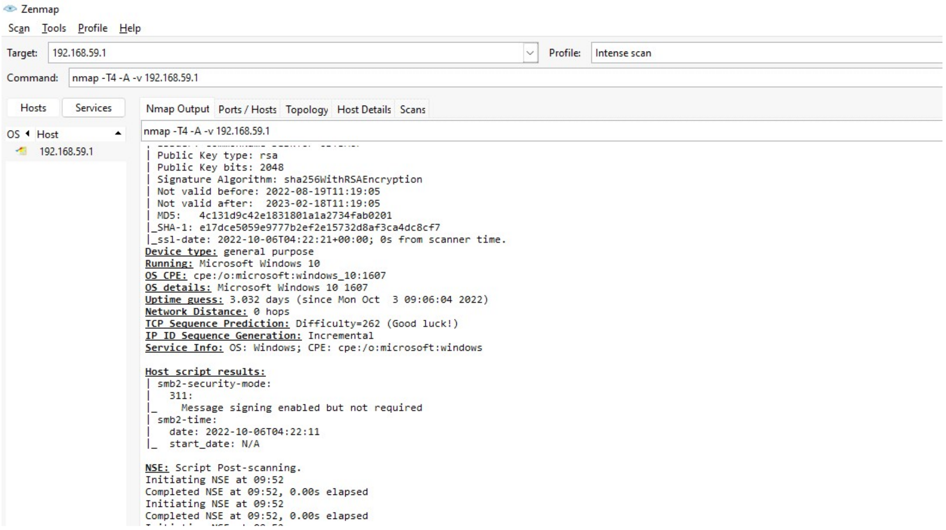
Thank you for installing Nmap

Nmap has been installed on your computer.

Click Finish to close this wizard.

- **IMPLEMENTATION OF NMAP** :

1. nmap-T4-A-v (ip address):



Target: 192.168.59.1

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.59.1

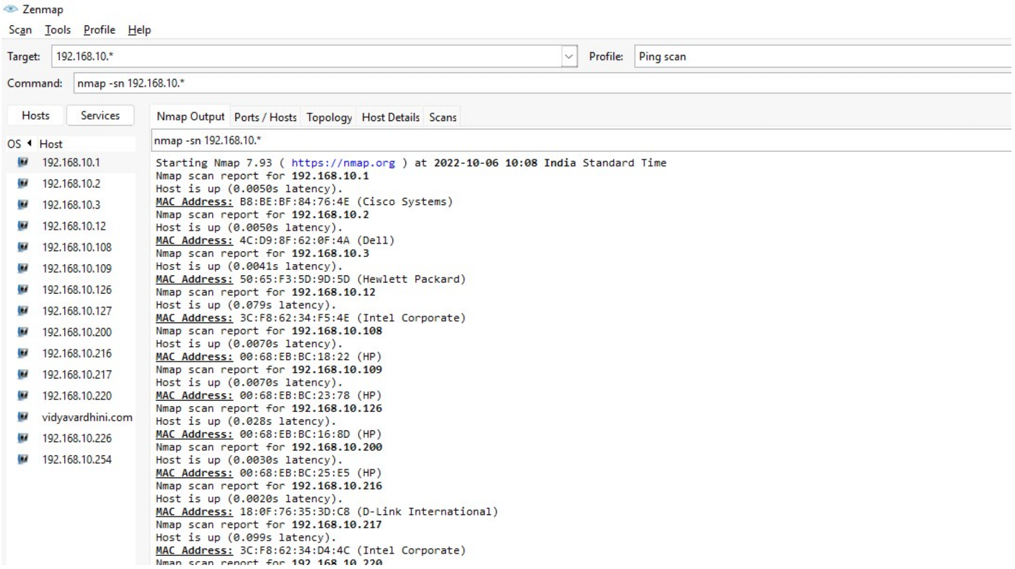
192.168.59.1

```
nmap -T4 -A -v 192.168.59.1
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-19T11:19:05
| Not valid after:  2023-02-18T11:19:05
| MD5:   4c131d9c42e1831801a1a2734fab0201
|_SHA-1: e17dce5059e9777b2ef2e15732d8af3ca4dc8cf7
|_ssl-date: 2022-10-06T04:22:21+00:00; 0s from scanner time.
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Uptime guess: 3.032 days (since Mon Oct  3 09:06:04 2022)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-06T04:22:11
|_  start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 09:52
Completed NSE at 09:52, 0.00s elapsed
Initiating NSE at 09:52
Completed NSE at 09:52, 0.00s elapsed
```

1. nmap -sn (ip address):



Target: 192.168.10.*

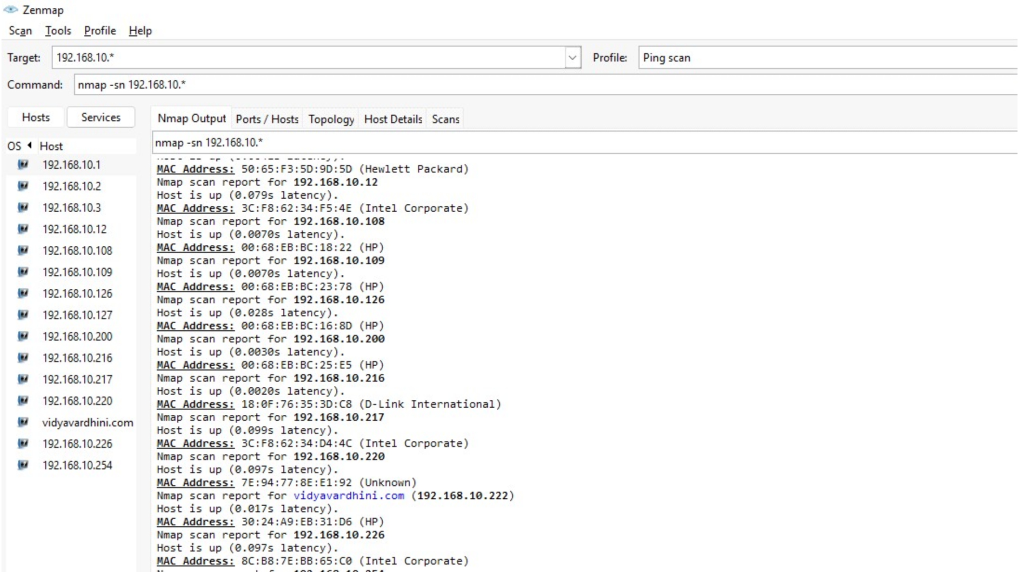
Profile: Ping scan

Command: nmap -sn 192.168.10.*

192.168.10.1
192.168.10.2
192.168.10.3
192.168.10.12
192.168.10.108
192.168.10.109
192.168.10.126
192.168.10.127
192.168.10.200
192.168.10.216
192.168.10.217
192.168.10.220
vidyavardhini.com
192.168.10.226
192.168.10.254

nmap -sn 192.168.10.*

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-06 10:08 India Standard Time
Nmap scan report for 192.168.10.1
Host is up (0.0050s latency).
MAC Address: B8:BE:BF:84:76:4E (Cisco Systems)
Nmap scan report for 192.168.10.2
Host is up (0.0050s latency).
MAC Address: 4C:D9:8F:62:0F:4A (Dell)
Nmap scan report for 192.168.10.3
Host is up (0.0041s latency).
MAC Address: 50:65:F3:5D:9D:5D (Hewlett Packard)
Nmap scan report for 192.168.10.12
Host is up (0.079s latency).
MAC Address: 3C:F8:62:34:F5:4E (Intel Corporate)
Nmap scan report for 192.168.10.108
Host is up (0.0070s latency).
MAC Address: 00:68:EB:BC:18:22 (HP)
Nmap scan report for 192.168.10.109
Host is up (0.0070s latency).
MAC Address: 00:68:EB:BC:23:78 (HP)
Nmap scan report for 192.168.10.126
Host is up (0.028s latency).
MAC Address: 00:68:EB:BC:16:8D (HP)
Nmap scan report for 192.168.10.200
Host is up (0.0030s latency).
MAC Address: 00:68:EB:BC:25:E5 (HP)
Nmap scan report for 192.168.10.216
Host is up (0.0020s latency).
MAC Address: 18:0F:76:35:3D:C8 (D-Link International)
Nmap scan report for 192.168.10.217
Host is up (0.099s latency).
MAC Address: 3C:F8:62:34:D4:4C (Intel Corporate)
Nmap scan report for 192.168.10.220
```



Target: 192.168.10.*

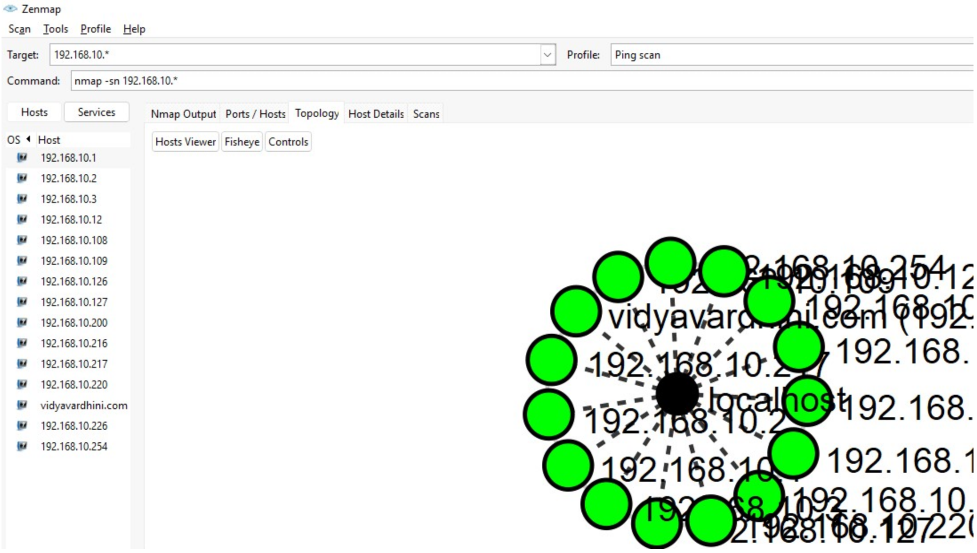
Profile: Ping scan

Command: nmap -sn 192.168.10.*

192.168.10.1
192.168.10.2
192.168.10.3
192.168.10.12
192.168.10.108
192.168.10.109
192.168.10.126
192.168.10.127
192.168.10.200
192.168.10.216
192.168.10.217
192.168.10.220
vidyavardhini.com
192.168.10.226
192.168.10.254

nmap -sn 192.168.10.*

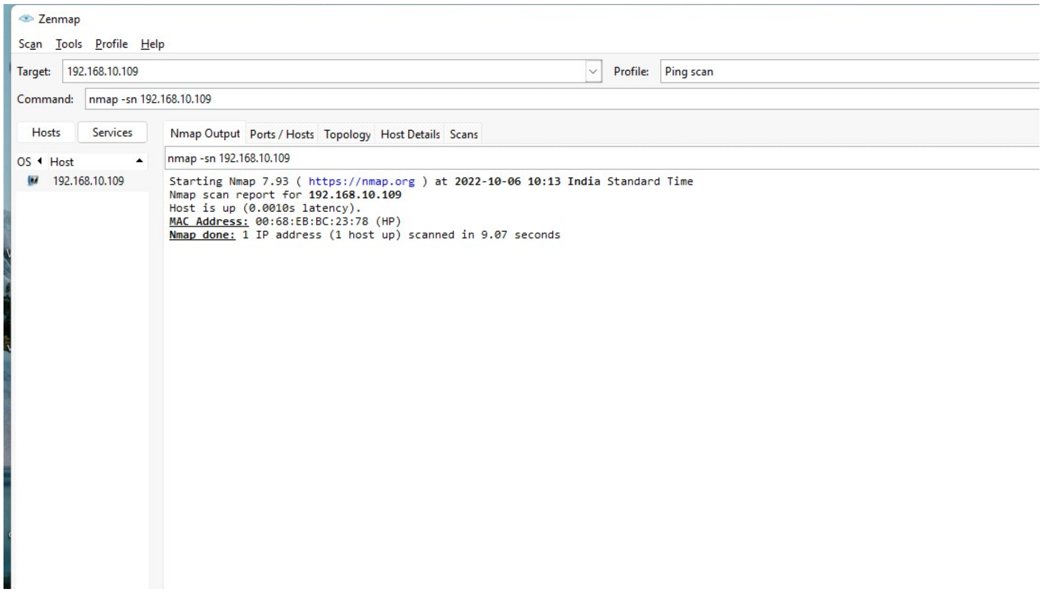
```
MAC Address: 50:65:F3:5D:9D:5D (Hewlett Packard)
Nmap scan report for 192.168.10.12
Host is up (0.079s latency).
MAC Address: 3C:F8:62:34:F5:4E (Intel Corporate)
Nmap scan report for 192.168.10.108
Host is up (0.0070s latency).
MAC Address: 00:68:EB:BC:18:22 (HP)
Nmap scan report for 192.168.10.109
Host is up (0.0070s latency).
MAC Address: 00:68:EB:BC:23:78 (HP)
Nmap scan report for 192.168.10.126
Host is up (0.028s latency).
MAC Address: 00:68:EB:BC:16:8D (HP)
Nmap scan report for 192.168.10.200
Host is up (0.0030s latency).
MAC Address: 00:68:EB:BC:25:E5 (HP)
Nmap scan report for 192.168.10.216
Host is up (0.0020s latency).
MAC Address: 18:0F:76:35:3D:C8 (D-Link International)
Nmap scan report for 192.168.10.217
Host is up (0.099s latency).
MAC Address: 3C:F8:62:34:D4:4C (Intel Corporate)
Nmap scan report for 192.168.10.220
Host is up (0.097s latency).
MAC Address: 7E:94:77:8E:E1:92 (Unknown)
Nmap scan report for vidyavardhini.com (192.168.10.222)
Host is up (0.017s latency).
MAC Address: 30:24:A9:EB:31:D6 (HP)
Nmap scan report for 192.168.10.226
Host is up (0.097s latency).
MAC Address: 8C:B8:7E:BB:65:C0 (Intel Corporate)
```


Zenmap
Scan Tools Profile Help
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
OS Host
localhost
vidyavardhini.com

Target: 192.168.10.*
Profile: Ping scan
Command: nmap -sn 192.168.10.*

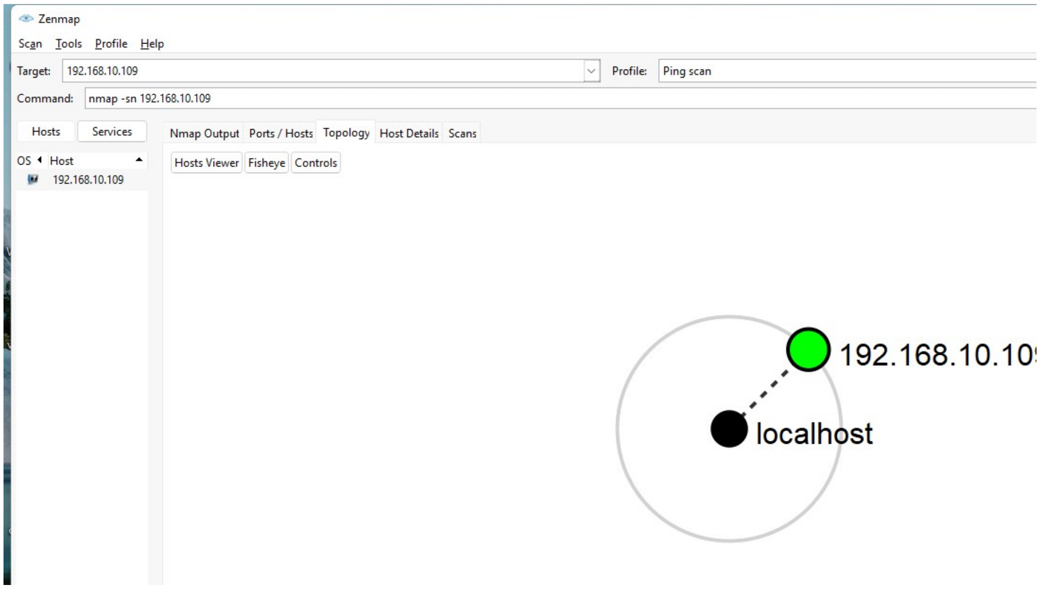
```
192.168.10.1
192.168.10.2
192.168.10.3
192.168.10.12
192.168.10.108
192.168.10.109
192.168.10.126
192.168.10.127
192.168.10.200
192.168.10.216
192.168.10.217
192.168.10.220
vidyavardhini.com
192.168.10.226
192.168.10.254
```

1. nmap -sn (reciever’s ip address) :



Target: 192.168.10.109
Profile: Ping scan
Command: nmap -sn 192.168.10.109

```
nmap -sn 192.168.10.109
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-06 10:13 India Standard Time
Nmap scan report for 192.168.10.109
Host is up (0.0010s latency).
MAC Address: 00:68:EB:BC:23:78 (HP)
Nmap done: 1 IP address (1 host up) scanned in 9.07 seconds
```


Zenmap
Scan Tools Profile Help
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
OS Host
192.168.10.10
localhost

Target: 192.168.10.109

Profile: Ping scan

Command: nmap -sn 192.168.10.109

192.168.10.109

- **Conclusion :**

Nmap is clearly the “Swiss Army Knife” of networking, thanks to its inventory of versatile commands. It lets you quickly scan and discover essential information about your network, hosts, ports, firewalls, and operating systems. Nmap has numerous settings, flags, and preferences that help system administrators analyze a network in detail.

Q1.

Q2.