Real Time Cyber Threat Detection and Mitigation Practical Manual

Co-funded by the European Union

Chikitsak Samuha's

Sir Sitaram and Lady Shantabai Patkar College of Arts and Science

and V.P. Varde College of Commerce and Economics

Chapter 1. Advanced Network Security

Lab1: Create a basic network monitoring environment for real-time threat detection using NMAP and ZENMAP.

1. NMAP

Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing. It allows to Discover Hosts, Port Scanning, Service Detection, Operating System Detection, Network Inventory. Nmap is widely used by network administrators and security professionals for monitoring network security and conducting vulnerability assessments.

Task 1: Installation of Nmap on Ubuntu

1. What command should you run to update the package list on Ubuntu?
2. What command do you use to install Nmap?
3. How can you verify that Nmap has been installed successfully?

Task 2: Network Scanning

4. 4. What command will you use to scan the network and identify which servers and devices are up and running in the subnet 192.168.1.0/24?
5. 5. Any types of Nmap scans that you are aware of?

Step 1: installation of Nmap on Ubuntu

command → sudo apt update

```
root@comp413:~# sudo apt update
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1854 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [300 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13.3 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2451 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [422 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [584 B]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [910 kB]
```

command → sudo apt install nmap

```
root@comp413:~# sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 134 not upgraded.
Need to get 6113 kB of archives.
After this operation, 26.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/main amd64 libblas3 amd64 3.10.0-2ubuntu1 [228 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 liblinear4 amd64 2.3.0+dfsg-5 [41.4 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/main amd64 liblua5.3-0 amd64 5.3.6-1build1 [140 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
```

command → nmap --version

```
root@comp413:~# nmap --version
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-3.0.2 nmap-libs
```

Step 2: Scan a network and find out which servers and devices are up and running:

command → nmap 192.168.1.0/24

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.22000.856]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nmap 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-14 10:55 India Standard Time
Nmap scan report for 192.168.1.10
Host is up (0.019s latency).
Not shown: 976 closed tcp ports (reset)
PORT     STATE    SERVICE
100/tcp  open     newacct
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
1025/tcp open     NFS-or-IIS
1026/tcp open     LSA-or-nterm
1027/tcp open     IIS
1028/tcp open     unknown
1029/tcp open     ms-lsa
1030/tcp open     iad1
1067/tcp open     instl_boots
1073/tcp open     bridgecontrol
1533/tcp filtered virtual-places
1801/tcp open     msmq
2103/tcp open     zephyr-clt
2105/tcp open     eklogin
2107/tcp open     msmq-mgmt
2222/tcp open     EtherNetIP-1
3389/tcp open     ms-wbt-server
3814/tcp filtered neto-dcs
5357/tcp open     wsdapi
5985/tcp open     wsman
7070/tcp open     realserver
8080/tcp open     http-proxy
MAC Address: 30:9C:23:74:6D:C2 (Micro-Star Intl)

Nmap scan report for 192.168.1.20
Host is up (0.011s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE    SERVICE
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
443/tcp   open     https
```

Administrator: Command Prompt

```
Nmap scan report for 192.168.1.21
Host is up (0.017s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
1029/tcp  filtered ms-lsa
1455/tcp  filtered esl-lm
2222/tcp  open     EtherNetIP-1
4998/tcp  filtered maybe-veritas
5357/tcp  open     wsdapi
5900/tcp  open     vnc
8087/tcp  filtered simplifymedia
32780/tcp filtered sometimes-rpc23
MAC Address: E0:70:EA:59:48:E2 (HP)

Nmap scan report for 192.168.1.65
Host is up (0.020s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: D8:D0:90:13:DC:43 (Dell)

Nmap scan report for 192.168.1.70
Host is up (0.021s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: E0:70:EA:59:43:E8 (HP)

Nmap scan report for 192.168.1.82
Host is up (0.019s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
3389/tcp  open     ms-wbt-server
```

2. ZENMAP

Zenmap is the graphical user interface (GUI) for Nmap, designed to make network scanning easier and more accessible. It allows users to visualize and interact with Nmap's powerful features without needing to use command-line instructions. Key functionalities include User-Friendly Interface, Profile Selection, Target Specification, Visual Outputs. Zenmap is a valuable tool for network administrators and security professionals, facilitating effective network monitoring and vulnerability assessments.

Task 1: Download and Installation

1. Where can you download Zenmap?
2. What steps must you follow to install Zenmap on your system?

Task 2: Basic Network Scan

3. Which profile should you select for a quick scan?
4. What types of output will you receive after performing the scan? (List them.)

Task 3: Scanning Techniques

5. How can you scan multiple IP addresses or subnets using Zenmap?
6. What command can you use to scan the subnet while excluding a specific host (e.g., 192.168.1.101)?
7. What command would you use for a fast scan on the network range 192.168.1.10/24?
8. How can you observe packets sent and received during a scan?

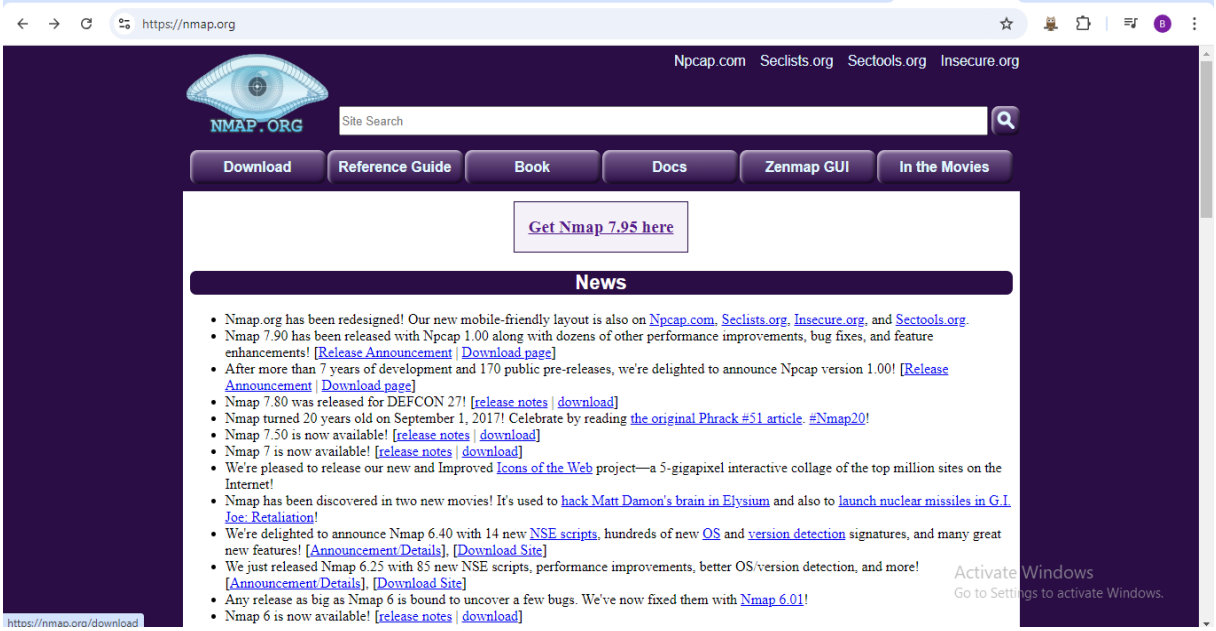
Task 4: Single Host Scan

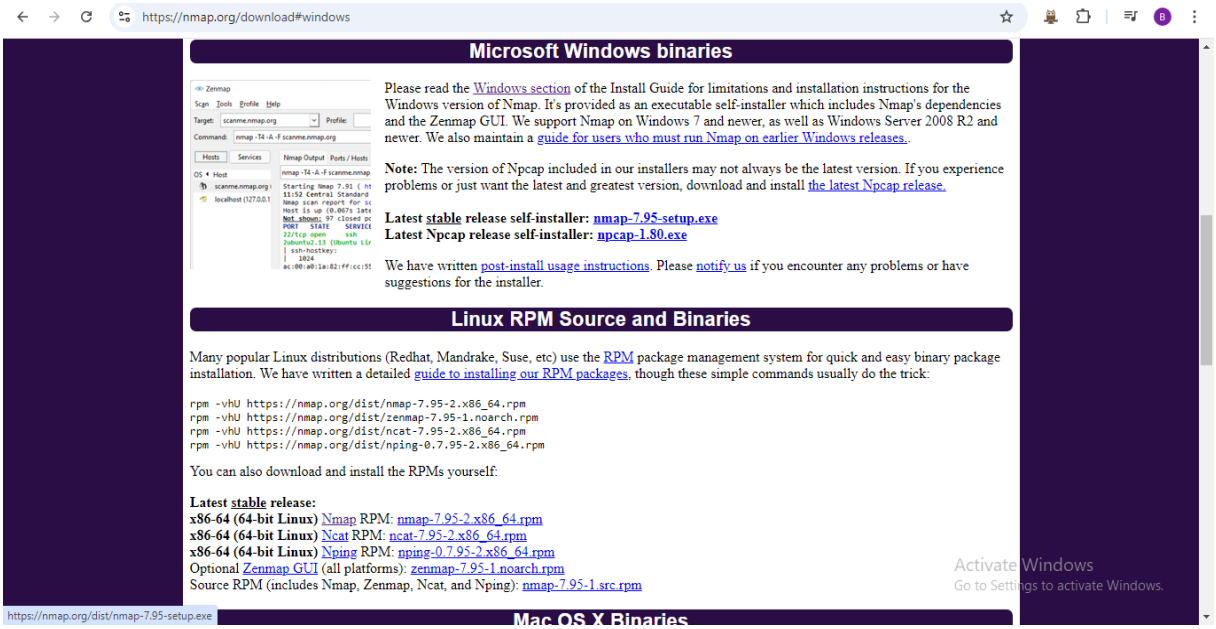
9. How do you scan a single host in Zenmap?

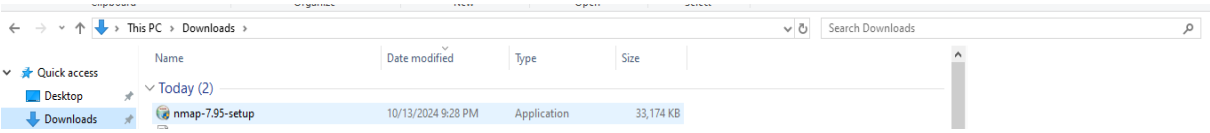
Task 5: Saving Scan Results

10. What steps do you follow to save your scan results in Zenmap?

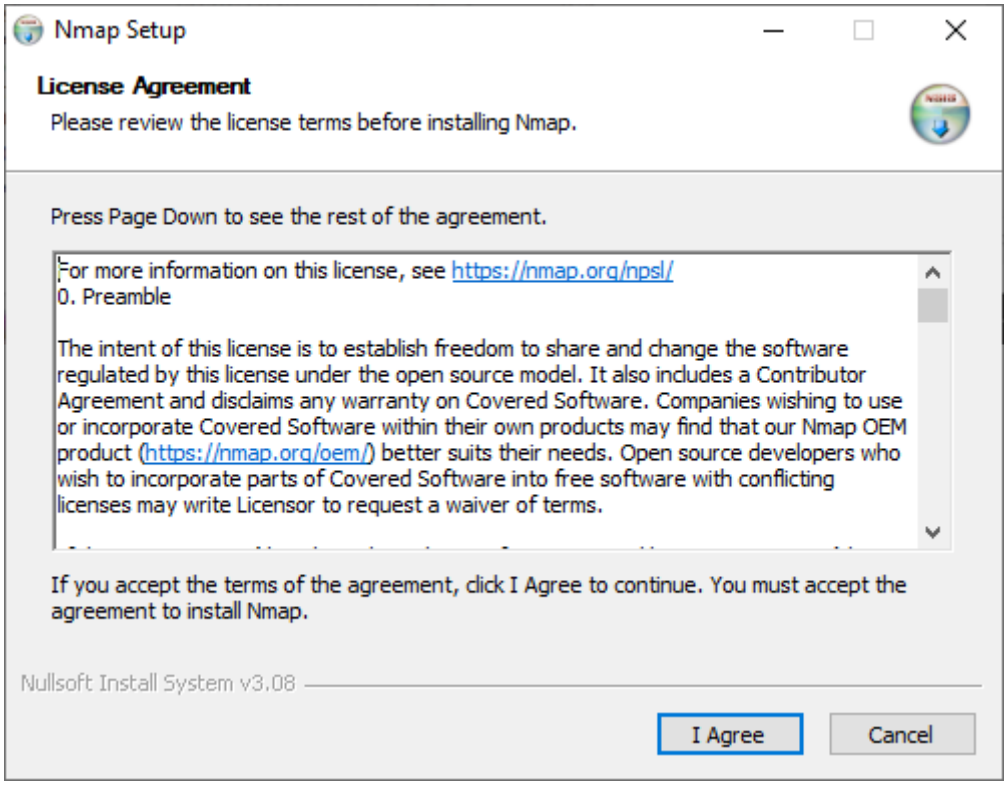
Step 1: Download Zenmap from https://nmap.org

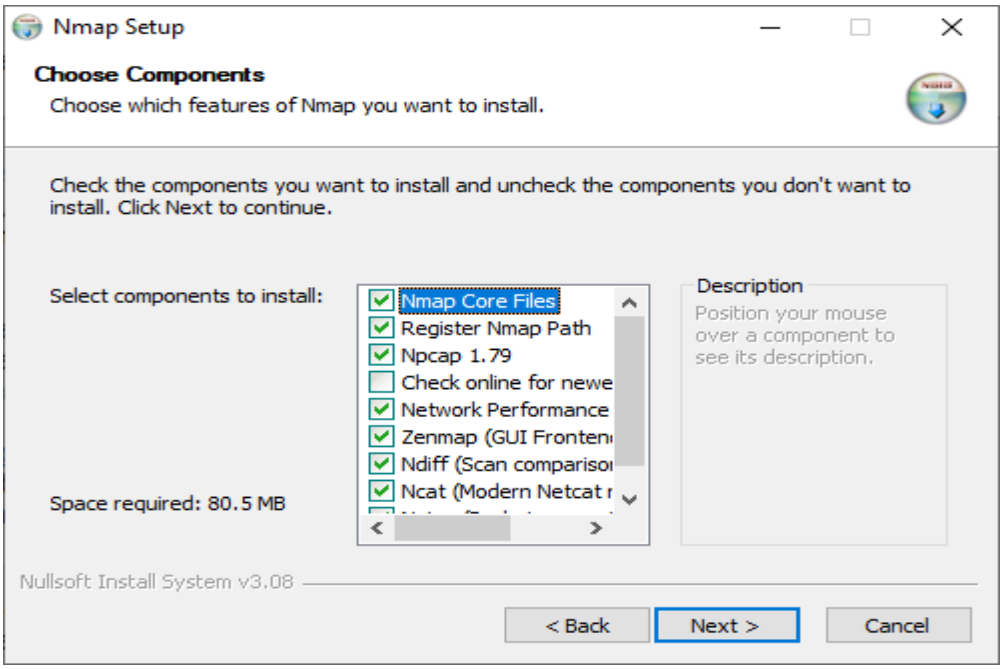


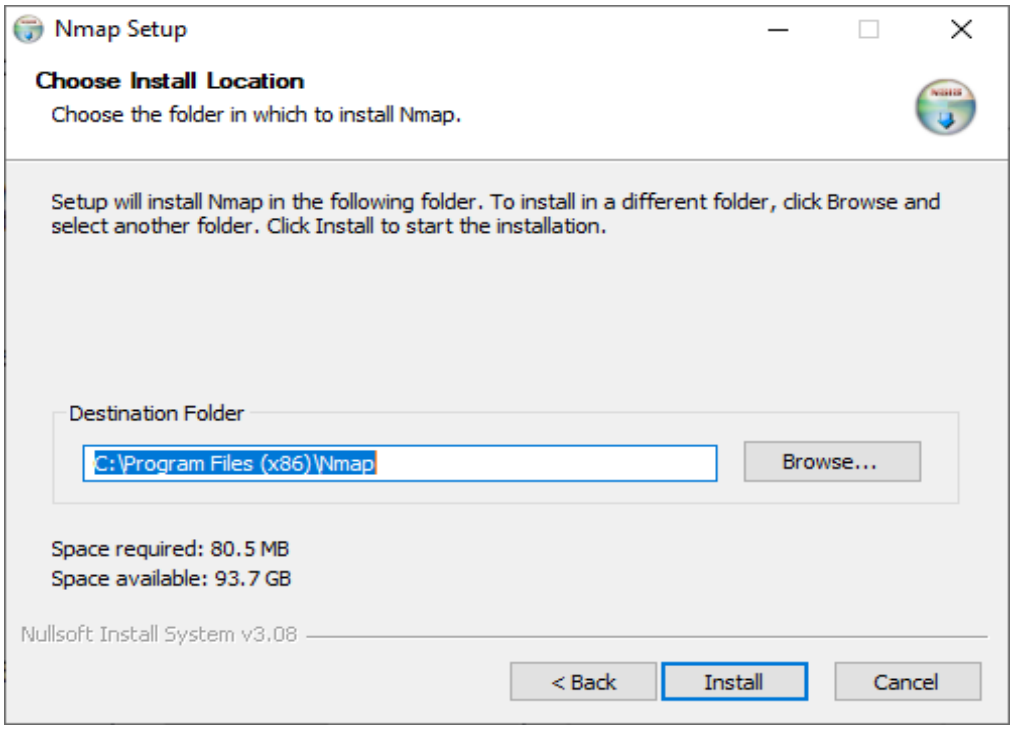


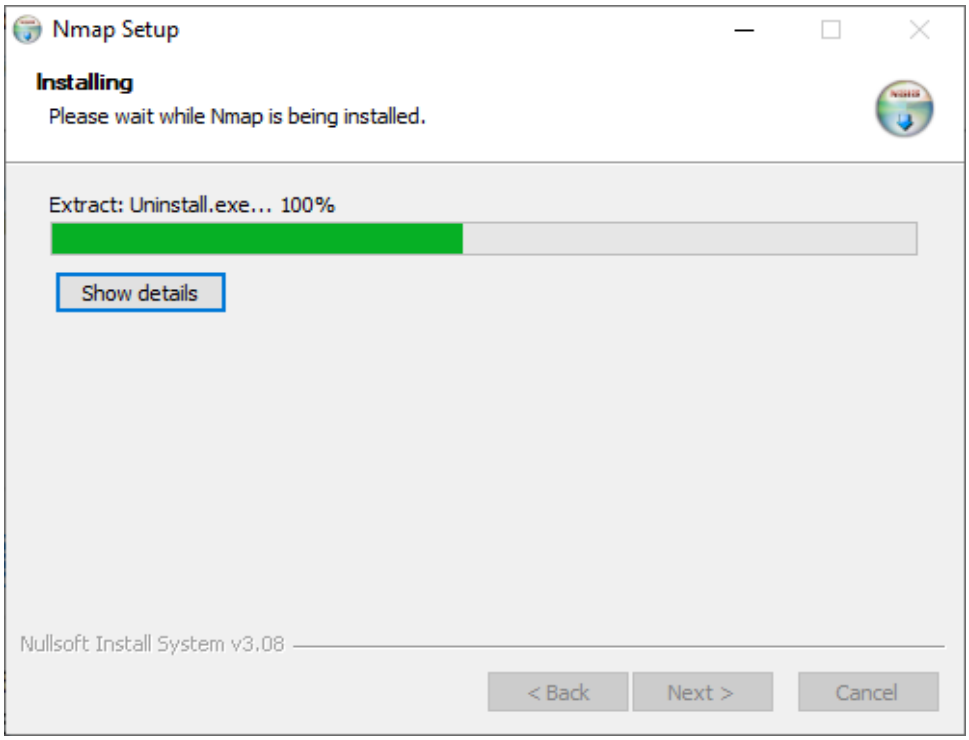


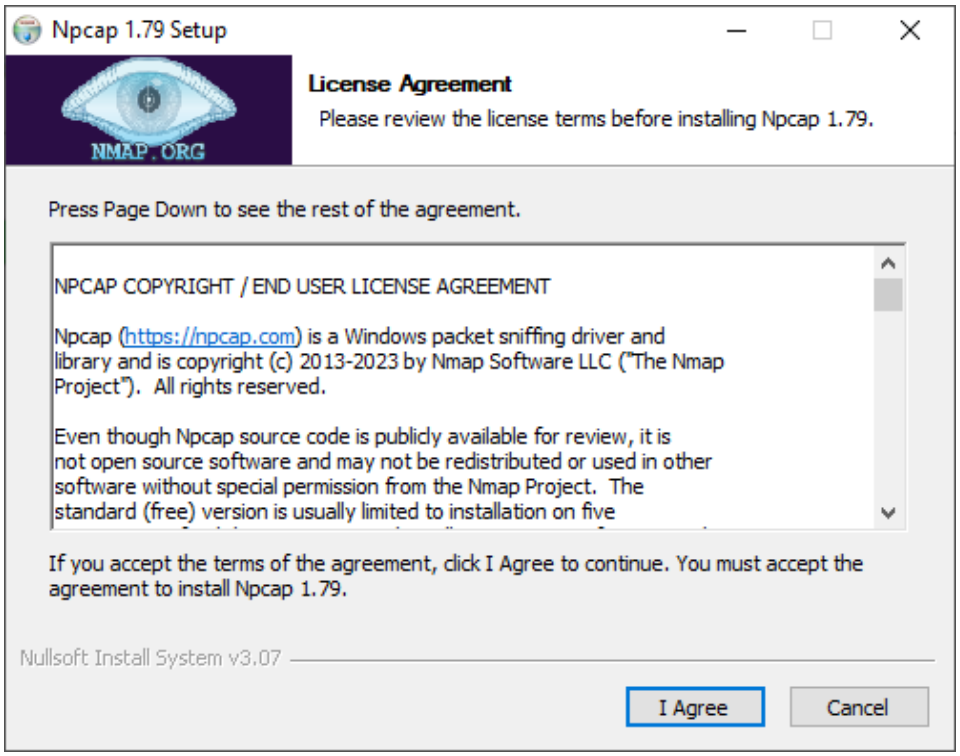
Step 2: After downloading the application, install it in the system.

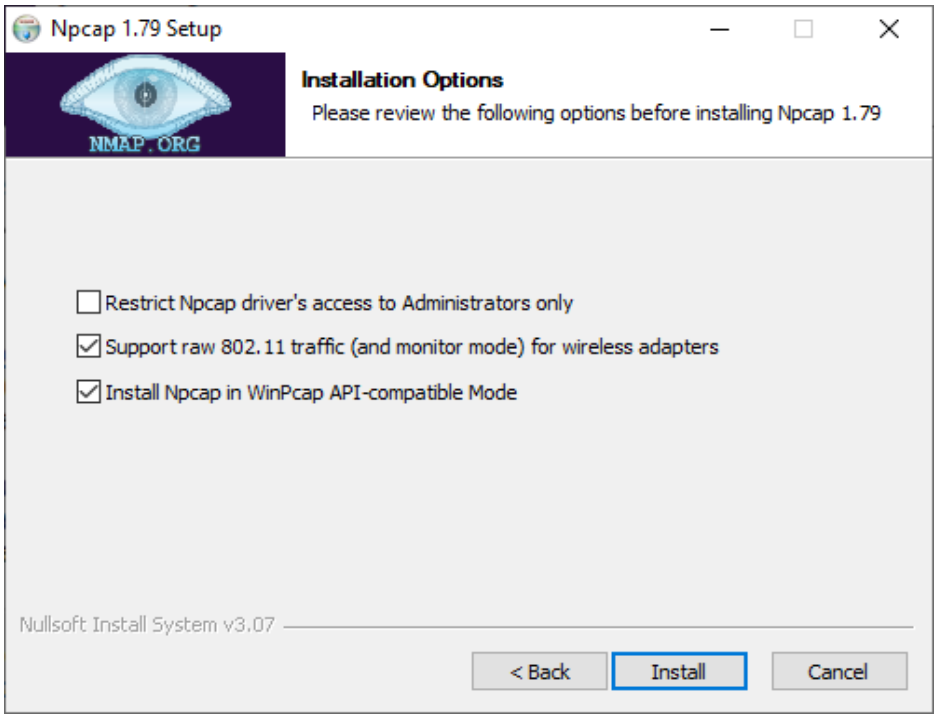


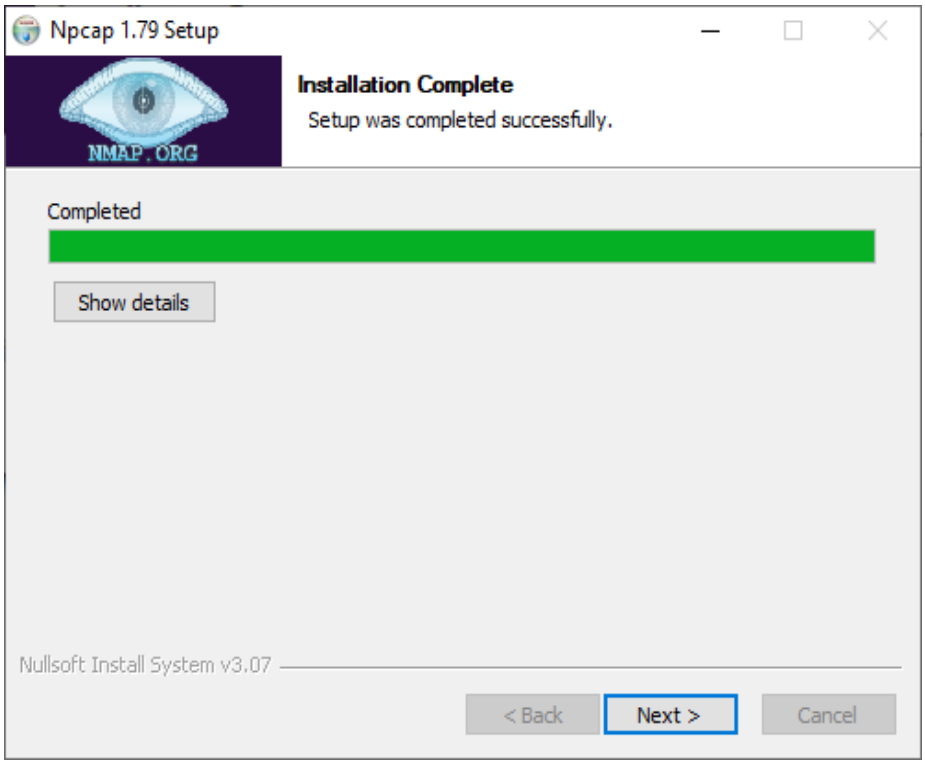

Nmap Setup
Choose Components
Choose which features of Nmap you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
Nmap Core Files
Register Nmap Path
Npcap 1.79
Check online for newe
Network Performance
Zenmap (GUI Fronten
Ndiff (Scan compariso
Ncat (Modern Netcat
Description
Position your mouse over a component to see its description.
Space required: 80.5 MB
Nullsoft Install System v3.08
< Back
Next >
Cancel

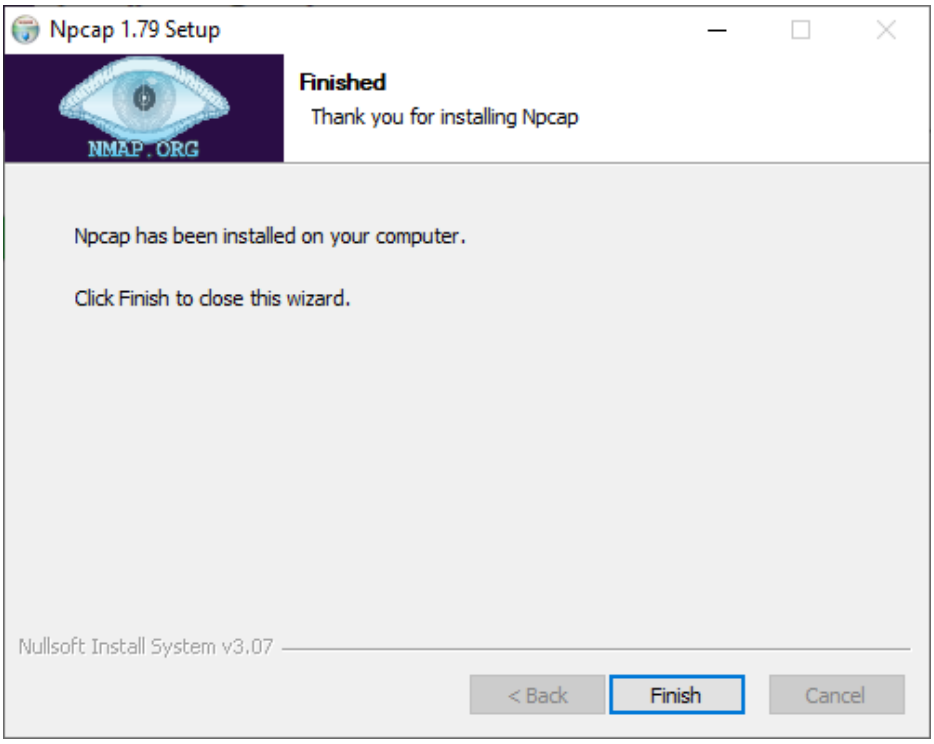

Nmap Setup
Choose Install Location
Choose the folder in which to install Nmap.
Setup will install Nmap in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files (x86)\Nmap
Browse...
Space required: 80.5 MB
Space available: 93.7 GB
Nullsoft Install System v3.08
< Back
Install
Cancel

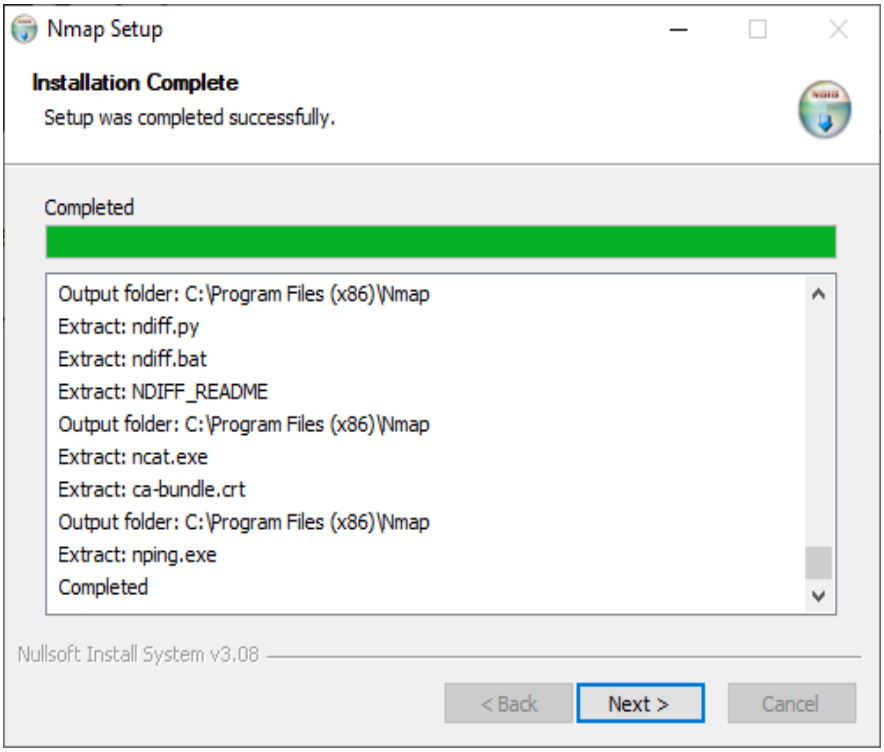

Nmap Setup
Installing
Please wait while Nmap is being installed.
Extract: Uninstall.exe... 100%
Show details
Nullsoft Install System v3.08
< Back
Next >
Cancel

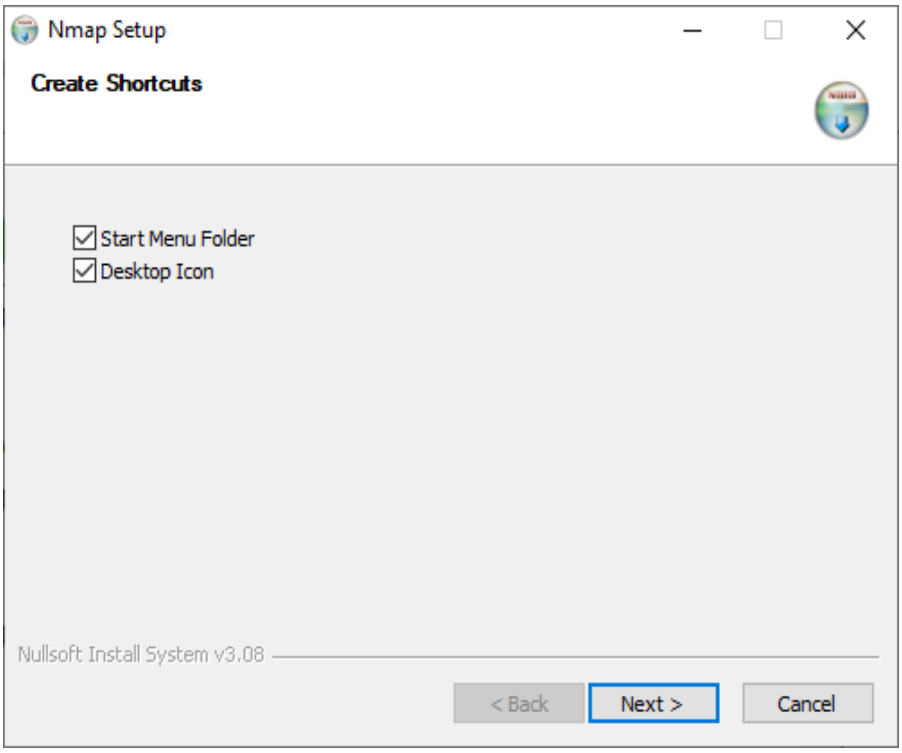

Npcap 1.79 Setup
NMAP.ORG
License Agreement
Please review the license terms before installing Npcap 1.79.
Press Page Down to see the rest of the agreement.
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT
Npcap (https://npcap.com) is a Windows packet sniffing driver and library and is copyright (c) 2013-2023 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 accept the agreement to install Npcap 1.79.
Nullsoft Install System v3.07
I Agree
Cancel

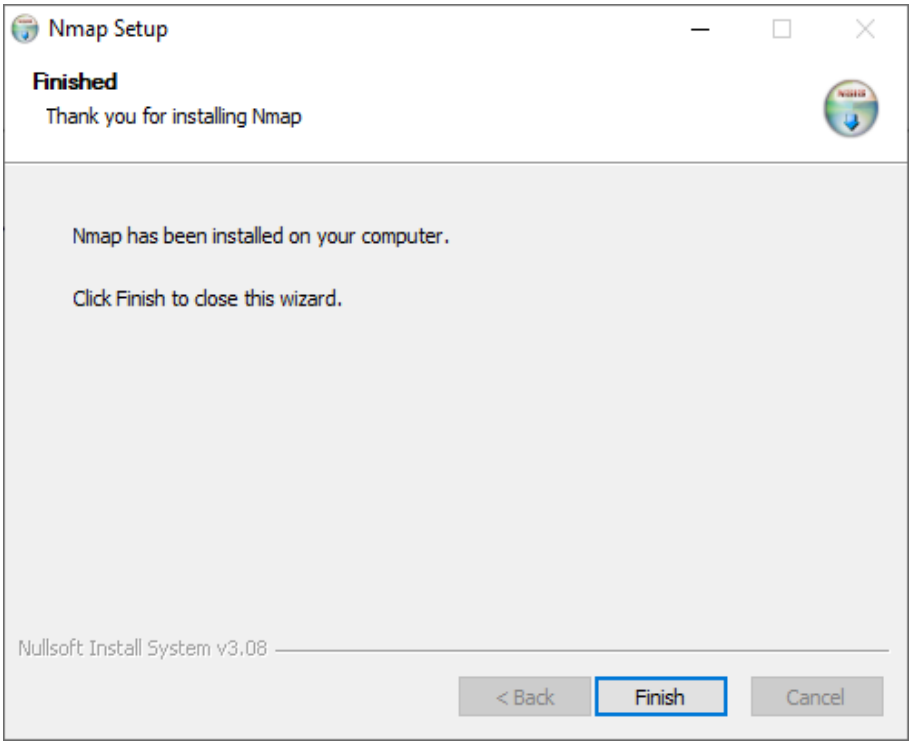

Npcap 1.79 Setup
NMAP.ORG
Installation Options
Please review the following options before installing Npcap 1.79
Restrict Npcap driver's access to Administrators only
Support raw 802.11 traffic (and monitor mode) for wireless adapters
Install Npcap in WinPcap API-compatible Mode
Nullsoft Install System v3.07
< Back
Install
Cancel


Npcap 1.79 Setup
NMAP.ORG
Installation Complete
Setup was completed successfully.
Completed
Show details
Nullsoft Install System v3.07
< Back
Next >
Cancel

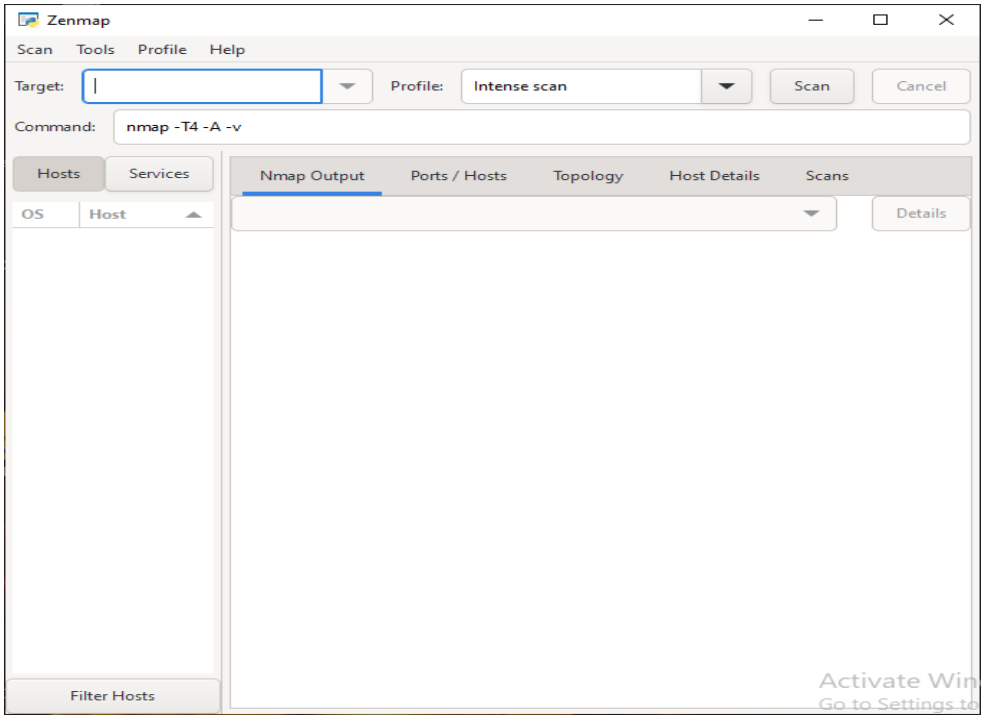

Npcap 1.79 Setup
NMAP.ORG
Finished
Thank you for installing Npcap
Npcap has been installed on your computer.
Click Finish to close this wizard.
Nullsoft Install System v3.07
< Back
Finish
Cancel


Nmap Setup
Installation Complete
Setup was completed successfully.
Completed
Output folder: C:\Program Files (x86)\Nmap
Extract: ndiff.py
Extract: ndiff.bat
Extract: NDIFF_README
Output folder: C:\Program Files (x86)\Nmap
Extract: ncat.exe
Extract: ca-bundle.crt
Output folder: C:\Program Files (x86)\Nmap
Extract: nping.exe
Completed
Nullsoft Install System v3.08
< Back
Next >
Cancel


Nmap Setup
Create Shortcuts
Start Menu Folder
Desktop Icon
Nullsoft Install System v3.08
< Back
Next >
Cancel


Nmap Setup
Finished
Thank you for installing Nmap
Nmap has been installed on your computer.
Click Finish to close this wizard.
Nullsoft Install System v3.08
< Back
Finish
Cancel

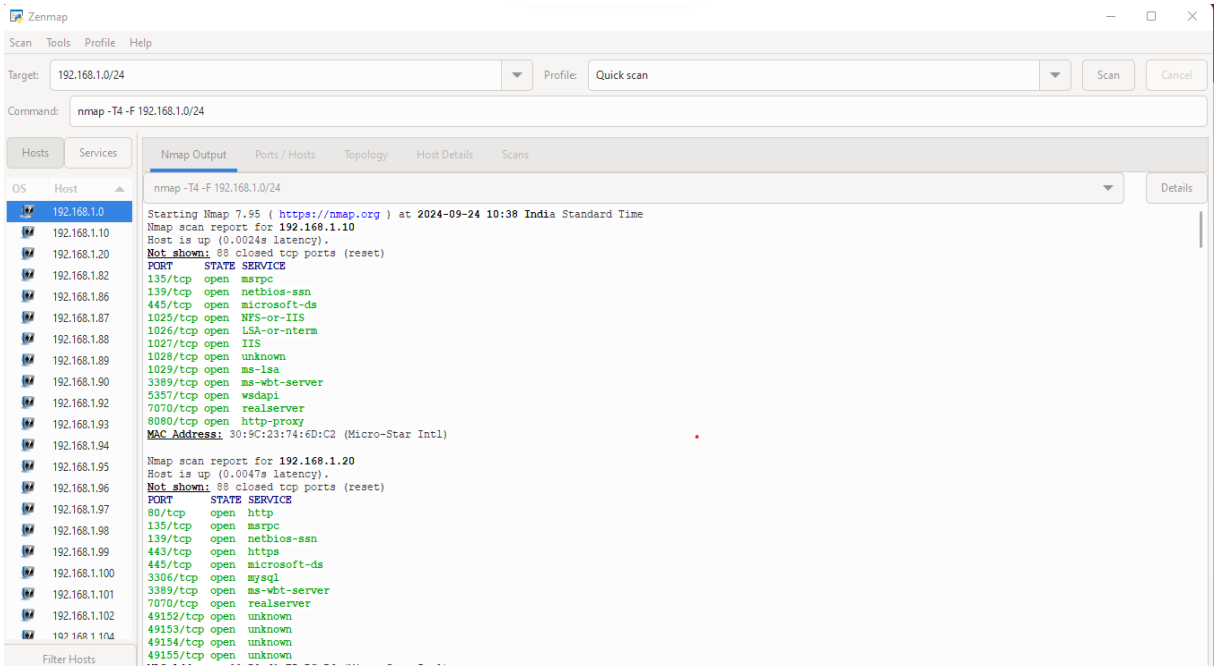
Step 3: The Zenmap has been installed



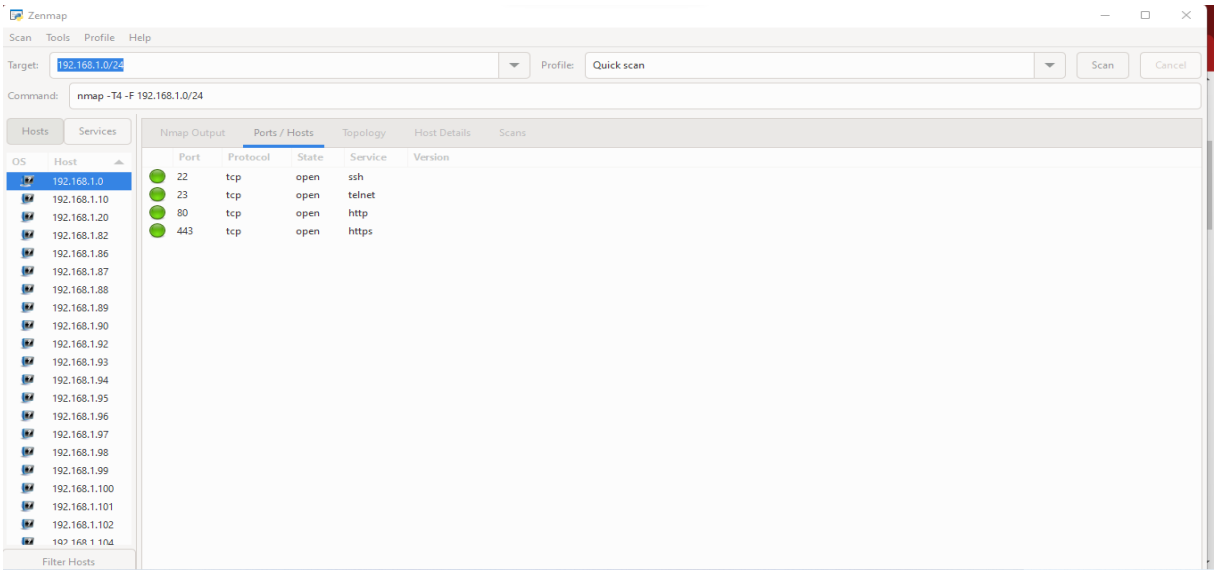
Step 4: Scan a network and find out which servers and devices are up and running:

In Target give 192.168.1.0/24 , Profile give Quick Scan

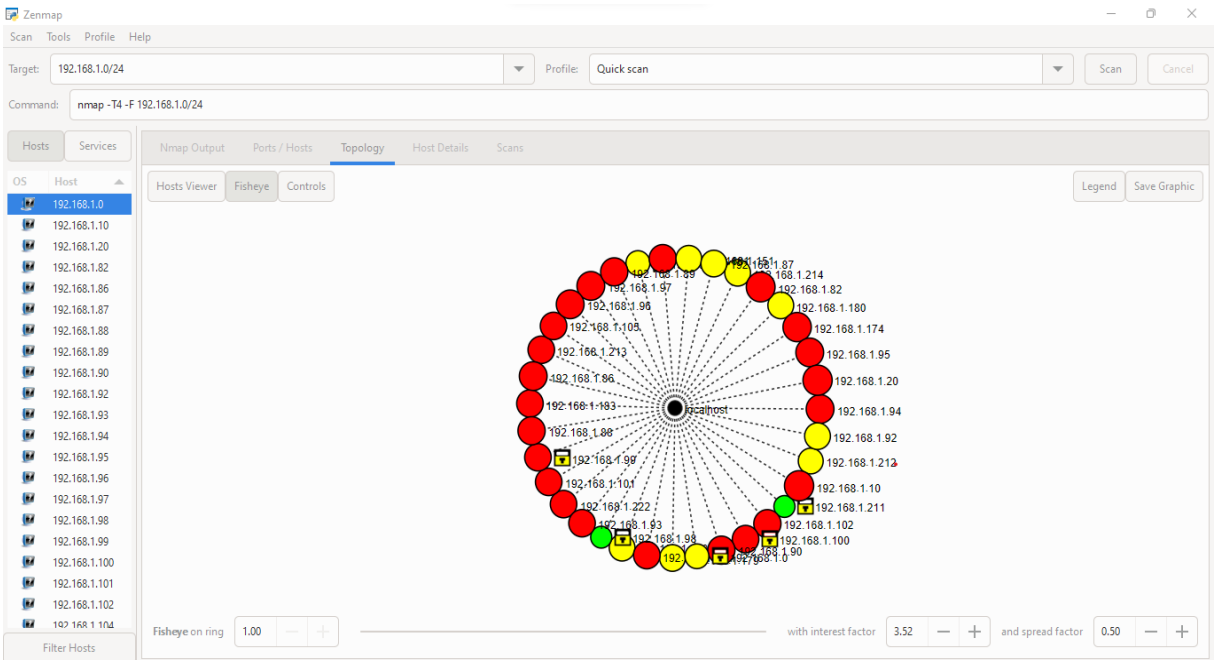
a. The following output will give for Nmap Output



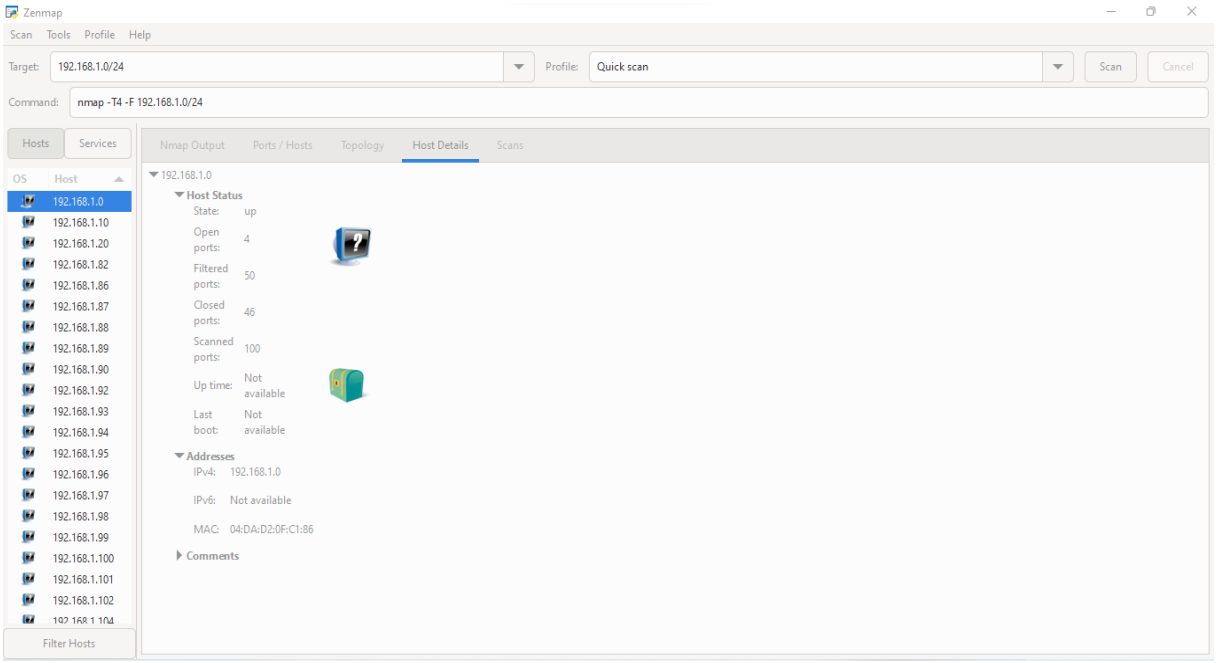
b. The following output will give for Ports/Hosts Output



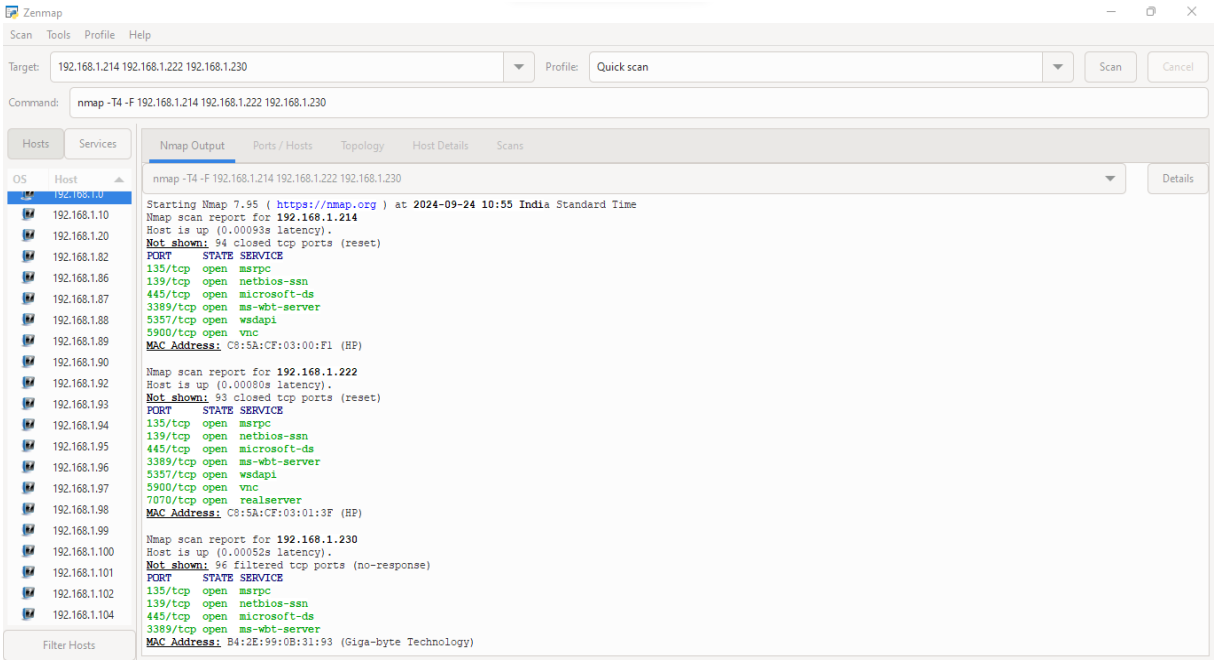
c. The following output will give for topology

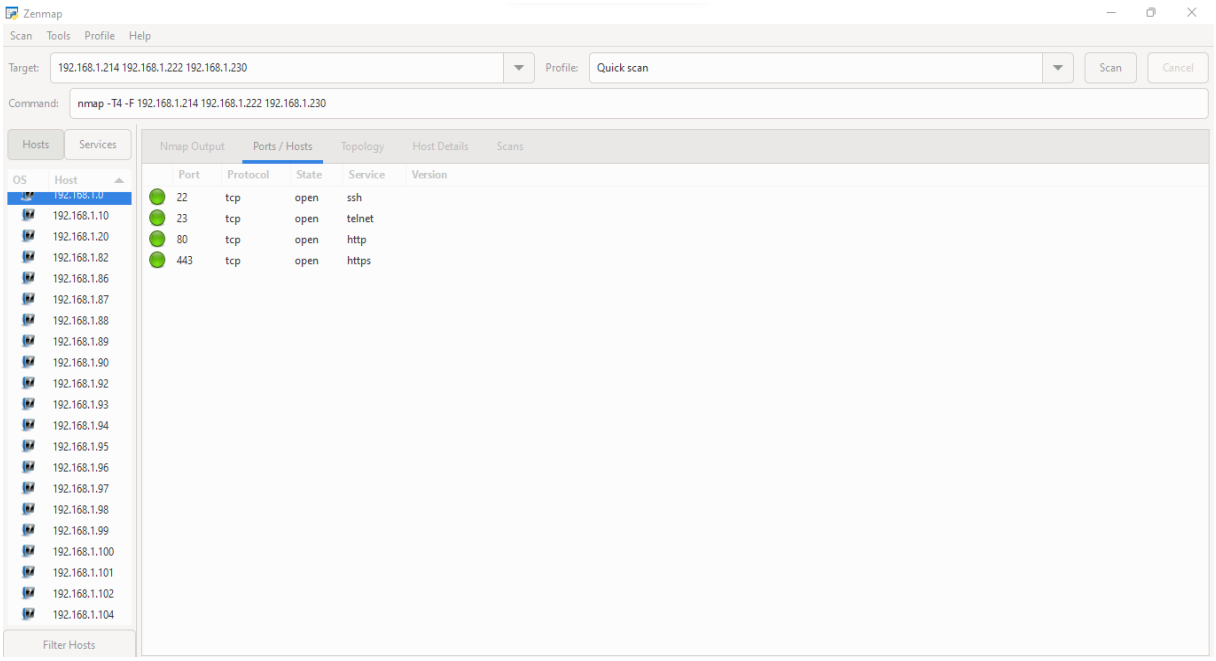


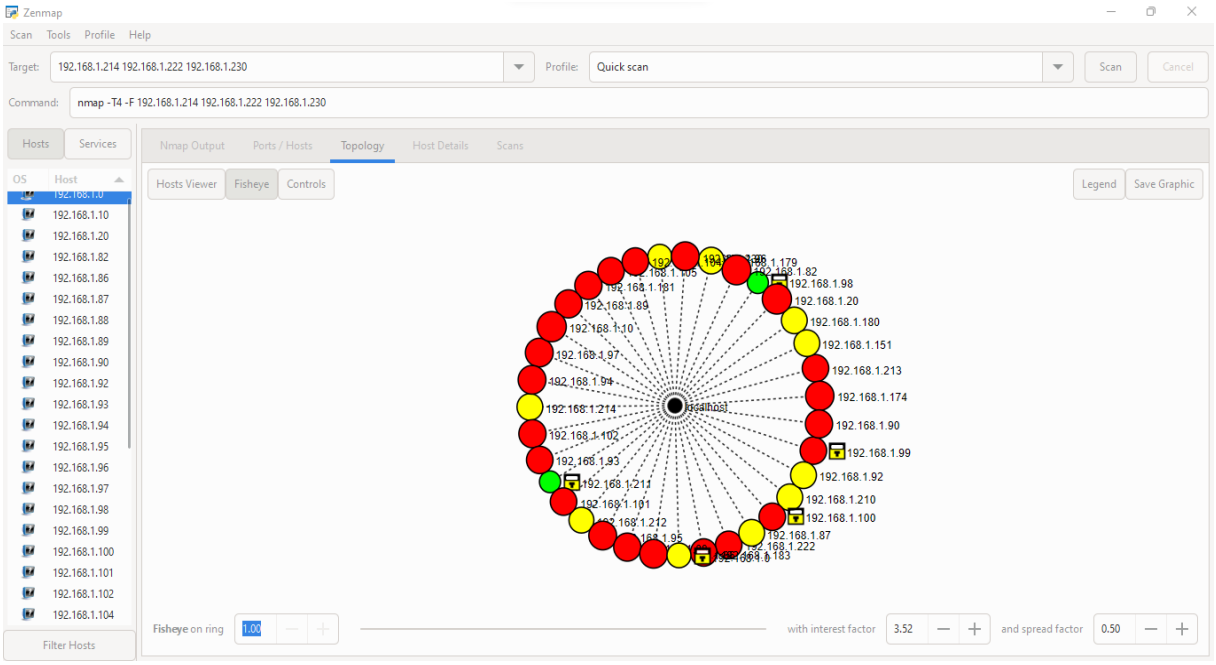
d. The following output will give for Host details



Step 5: Scan multiple IP addresses or subnets:



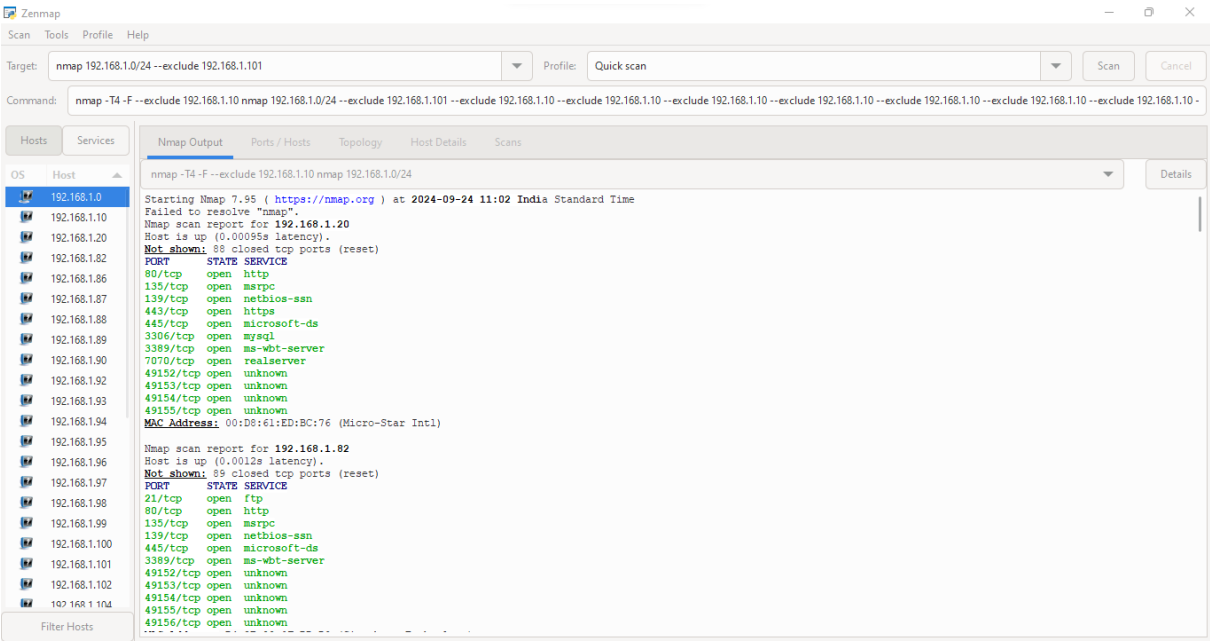

Zenmap
Scan Tools Profile Help
Target: 192.168.1.214 192.168.1.222 192.168.1.230
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 192.168.1.214 192.168.1.222 192.168.1.230
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
192.168.1.10
192.168.1.20
192.168.1.82
192.168.1.86
192.168.1.87
192.168.1.88
192.168.1.89
192.168.1.90
192.168.1.92
192.168.1.93
192.168.1.94
192.168.1.95
192.168.1.96
192.168.1.97
192.168.1.98
192.168.1.99
192.168.1.100
192.168.1.101
192.168.1.102
192.168.1.104
Filter Hosts
Port Protocol State Service Version
22 tcp open ssh
23 tcp open telnet
80 tcp open http
443 tcp open https


Zenmap
Scan Tools Profile Help
Target: 192.168.1.214 192.168.1.222 192.168.1.230
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 192.168.1.214 192.168.1.222 192.168.1.230
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
192.168.1.98
192.168.1.20
192.168.1.180
192.168.1.151
192.168.1.213
192.168.1.174
192.168.1.90
192.168.1.99
192.168.1.92
192.168.1.210
192.168.1.100
192.168.1.87
192.168.1.222
192.168.1.214
192.168.1.89
192.168.1.10
192.168.1.97
192.168.1.94
192.168.1.102
192.168.1.93
192.168.1.211
192.168.1.101
192.168.1.212
Fisheye on ring
1.00
with interest factor
3.52
and spread factor
0.50

Step 6: Scan by excluding a host:

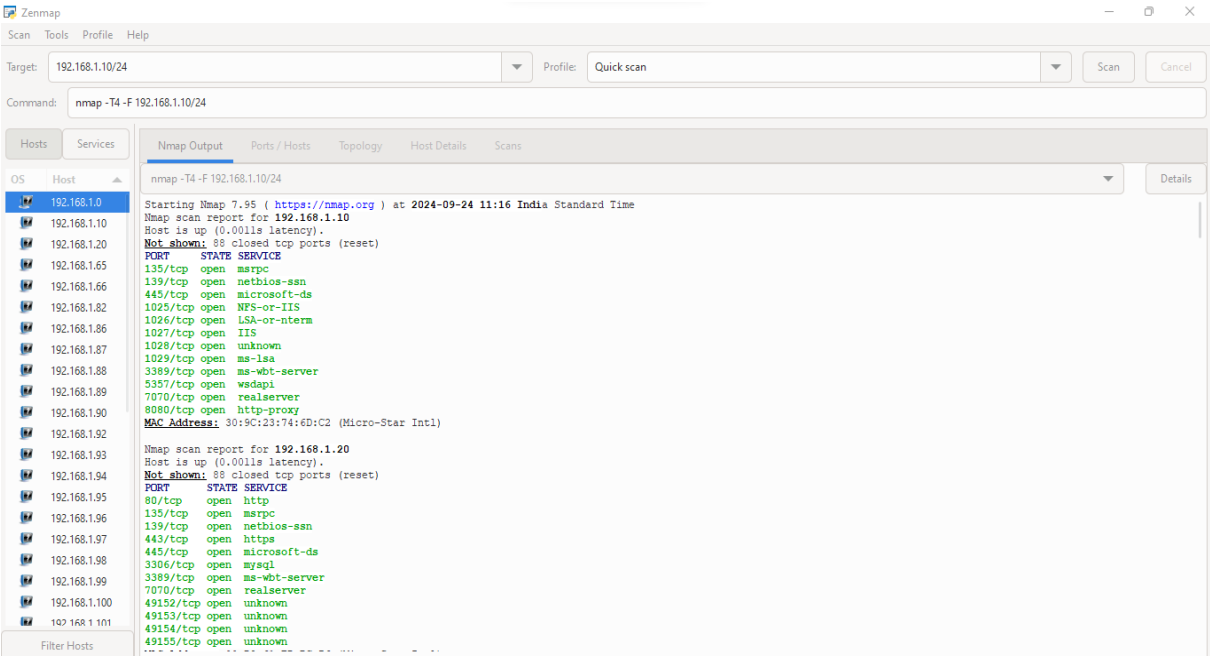
Command > nmap 192.168.1.0/24 --exclude 192.168.1.101

That will exclude the host while scanning.



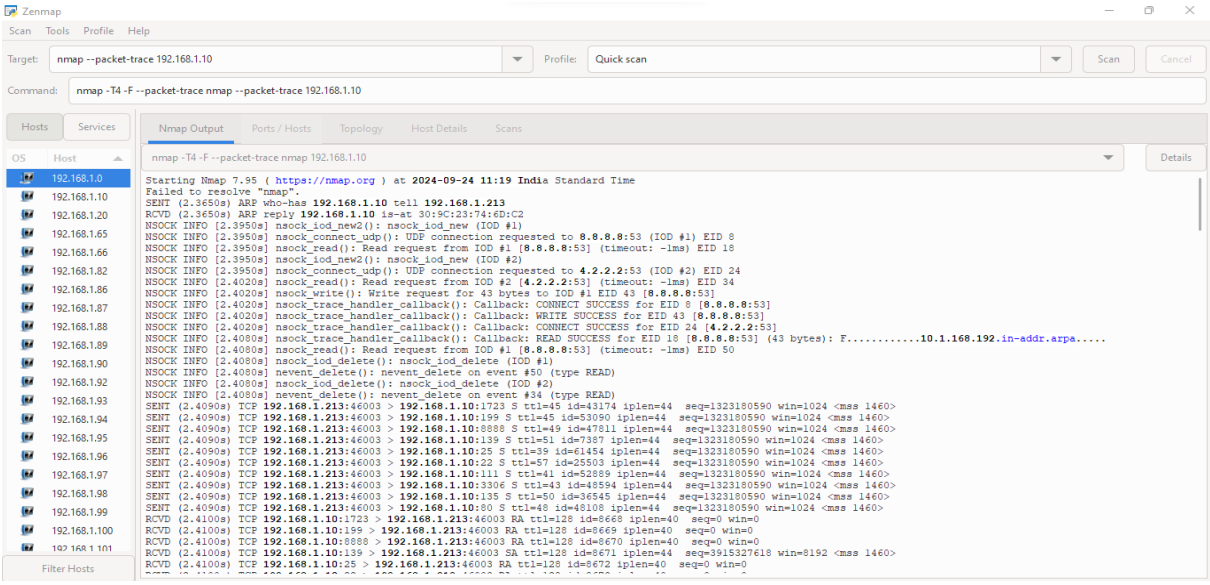
Step 7: Fast nmap scanning for a network range:

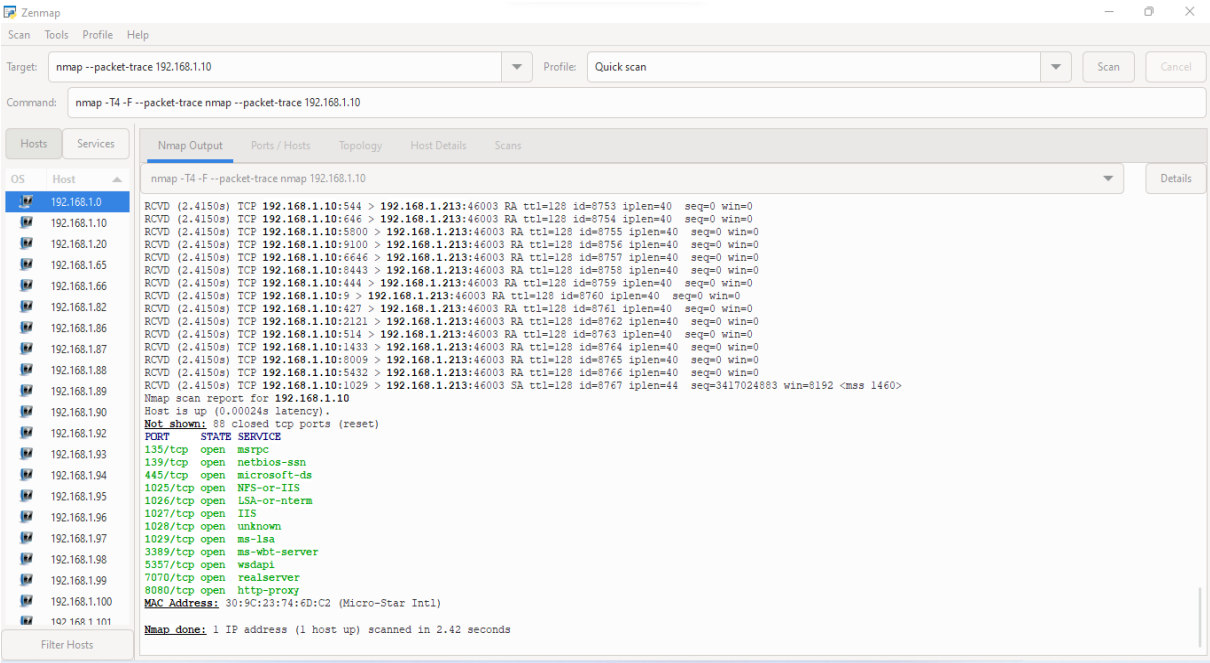
nmap -F 192.168.1.10/24



Step 8: To see packets sent and received r using nmap:

nmap --packet-trace 192.168.1.10





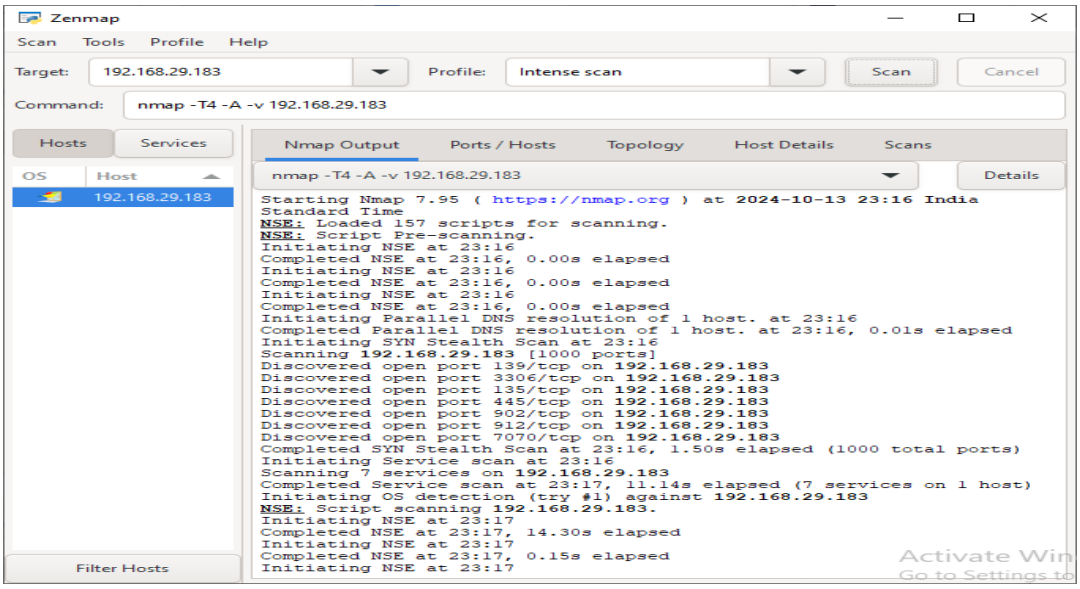
Step 9:

Now let's Scan a single host:

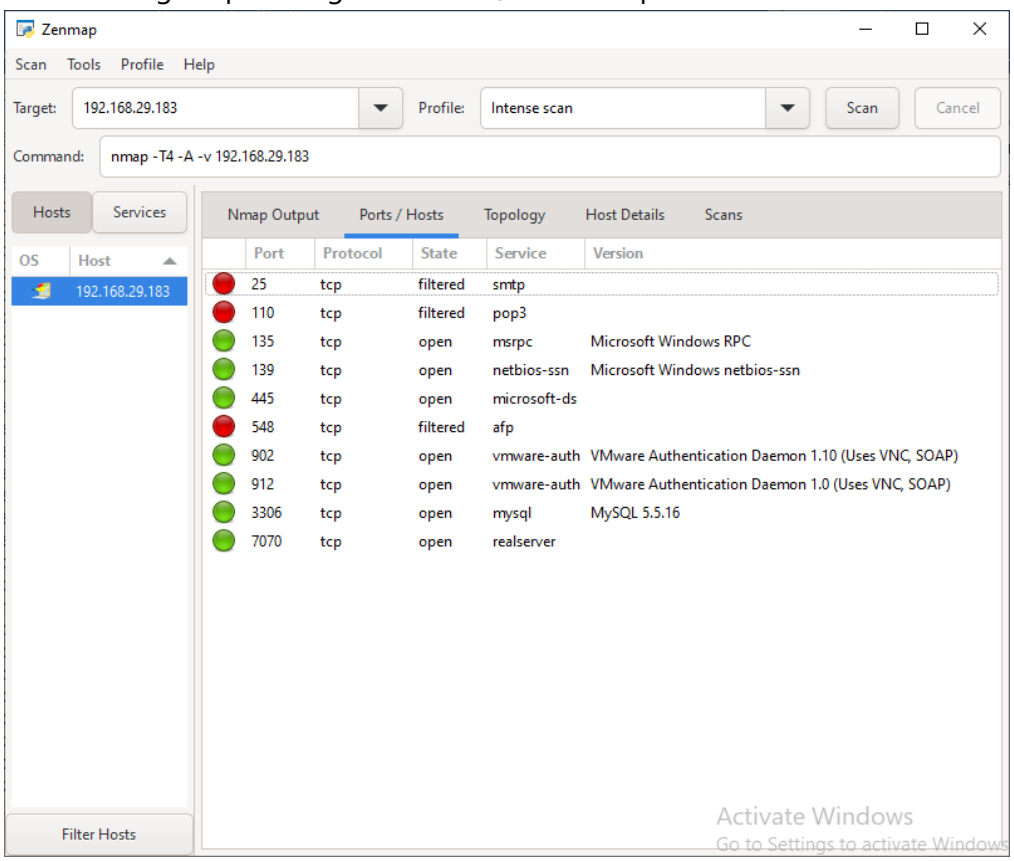
Here we have added our systems IP address

Go to Nmap and add the respective IP address > From Profile select Intense Scan > Click on Scan

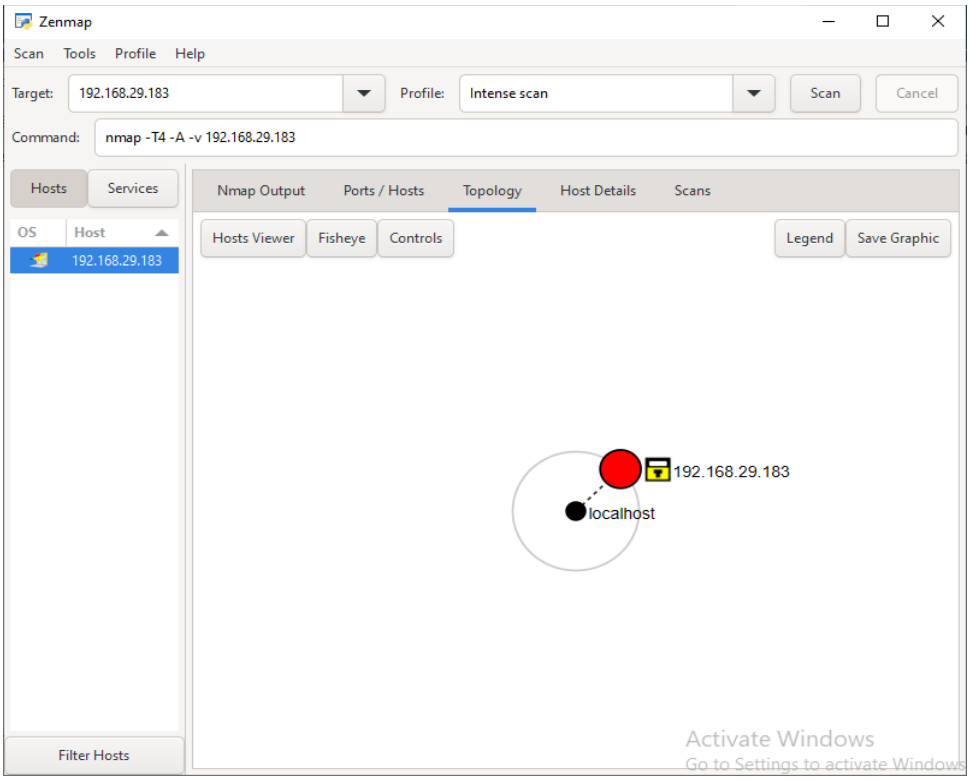
a. The following output will give for Nmap Output



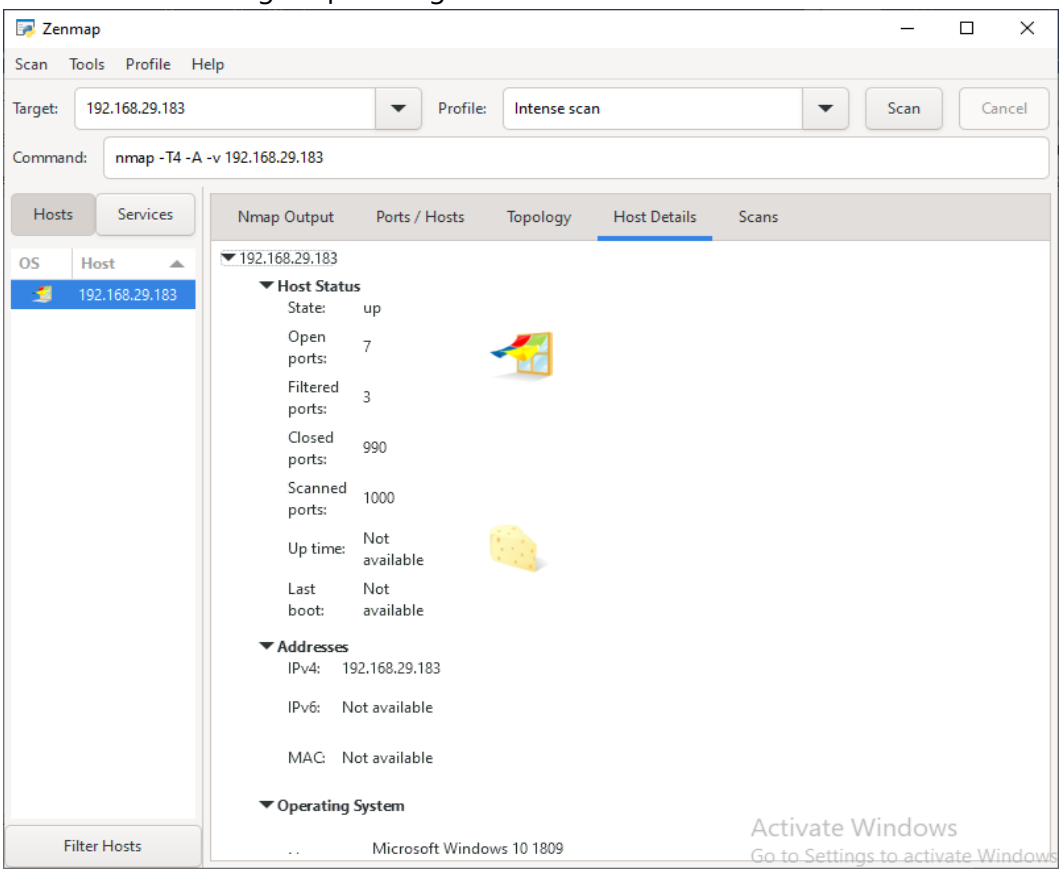
b. The following output will give for Ports/Hosts Output



c. The following output will give for topology



d. The following output will give for Host details



Step 10: The scan can be saved in system as follows

Go to Scan -> Save Scan and Save