



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-vertas
5357/tcp  open  wsdapi
5980/tcp  open  vnc
8080/tcp  filtered simplifimedia
32780/tcp filtered sometimes-ipc23
MAC Address: E8:70: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: E8:70: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?

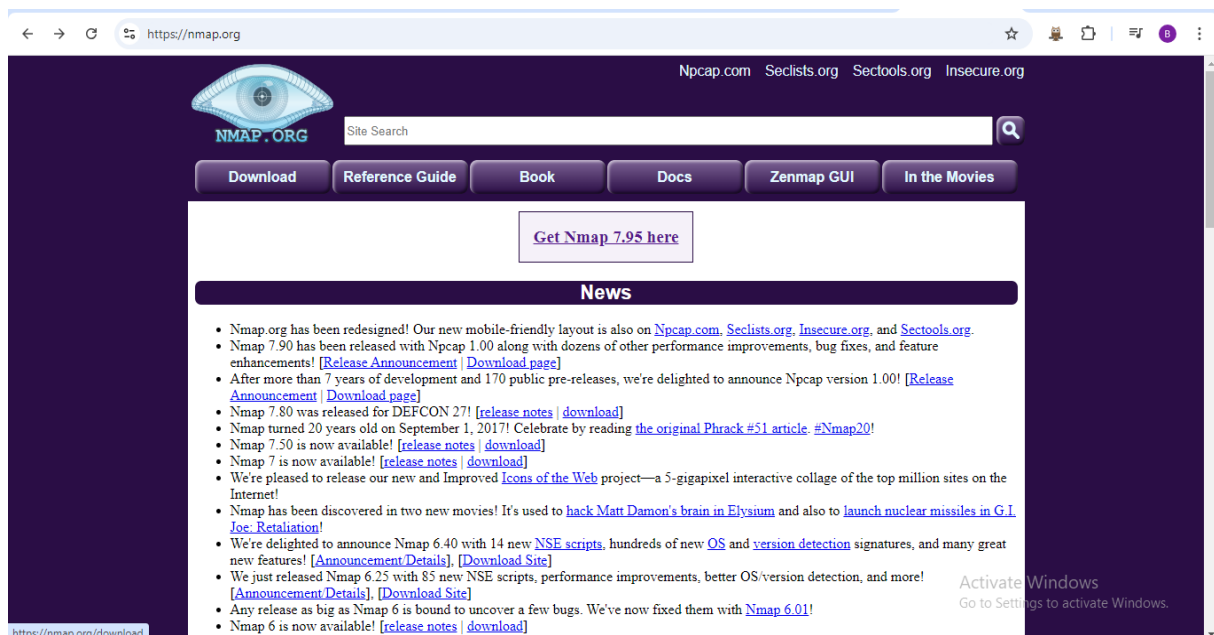
Task 4: Single Host Scan

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

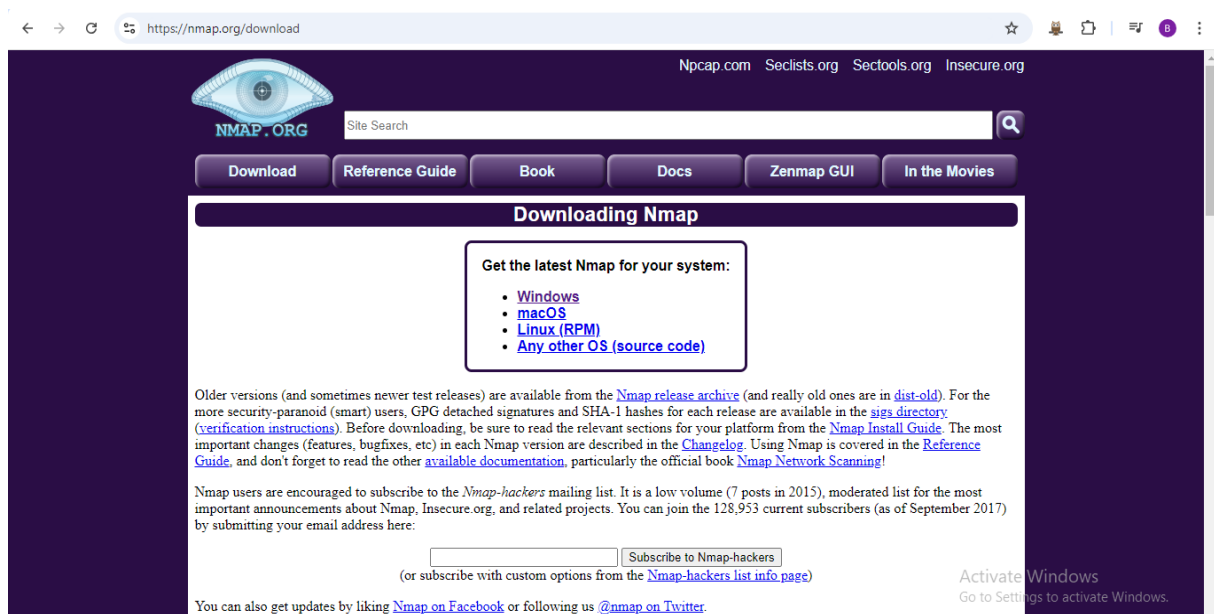
Task 5: Saving Scan Results

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

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



The screenshot shows the nmap.org homepage. At the top, there is a navigation bar with links to Npcap.com, Seclists.org, Sectools.org, and Insecure.org. Below this is a search bar and a menu with buttons for Download, Reference Guide, Book, Docs, Zenmap GUI, and In the Movies. A prominent button in the center says "Get Nmap 7.95 here". Below the menu is a "News" section with a list of recent updates and announcements, including new releases of Nmap and Npcap, and mentions of DEFCON 27 and various security events.



The screenshot shows the nmap.org/download page. It features the same navigation bar as the homepage. Below the menu, there is a section titled "Downloading Nmap" with a box that says "Get the latest Nmap for your system:" followed by a list of links for Windows, macOS, Linux (RPM), and Any other OS (source code). Below this, there is a paragraph of text providing instructions on how to download and verify the software, including links to the release archive, dist-old, verification instructions, Nmap Install Guide, and ChangeLog. At the bottom, there is a form to subscribe to the Nmap-hackers mailing list, with a button labeled "Subscribe to Nmap-hackers" and a note about custom options. A footer note mentions following Nmap on Facebook and Twitter.

Microsoft Windows binaries

Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

Latest stable release self-installer: [nmap-7.95-setup.exe](#)
Latest Npcap release self-installer: [npcap-1.80.exe](#)

We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the [RPM](#) package management system for quick and easy binary package installation. We have written a detailed [guide to installing our RPM packages](#), though these simple commands usually do the trick:

```
rpm -vhU https://nmap.org/dist/nmap-7.95-2.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.95-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.95-2.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.95-2.x86_64.rpm
```

You can also download and install the RPMs yourself:

Latest stable release:
x86-64 (64-bit Linux) **Nmap** RPM: [nmap-7.95-2.x86_64.rpm](#)
x86-64 (64-bit Linux) **Ncat** RPM: [ncat-7.95-2.x86_64.rpm](#)
x86-64 (64-bit Linux) **Nping** RPM: [nping-0.7.95-2.x86_64.rpm](#)
Optional **Zenmap GUI** (all platforms): [zenmap-7.95-1.noarch.rpm](#)
Source RPM (includes Nmap, Zenmap, Ncat, and Nping): [nmap-7.95-1.src.rpm](#)

Mac OS X Binaries

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

Nmap Setup

License Agreement

Please review the license terms before installing Nmap.

Press Page Down to see the rest of the agreement.

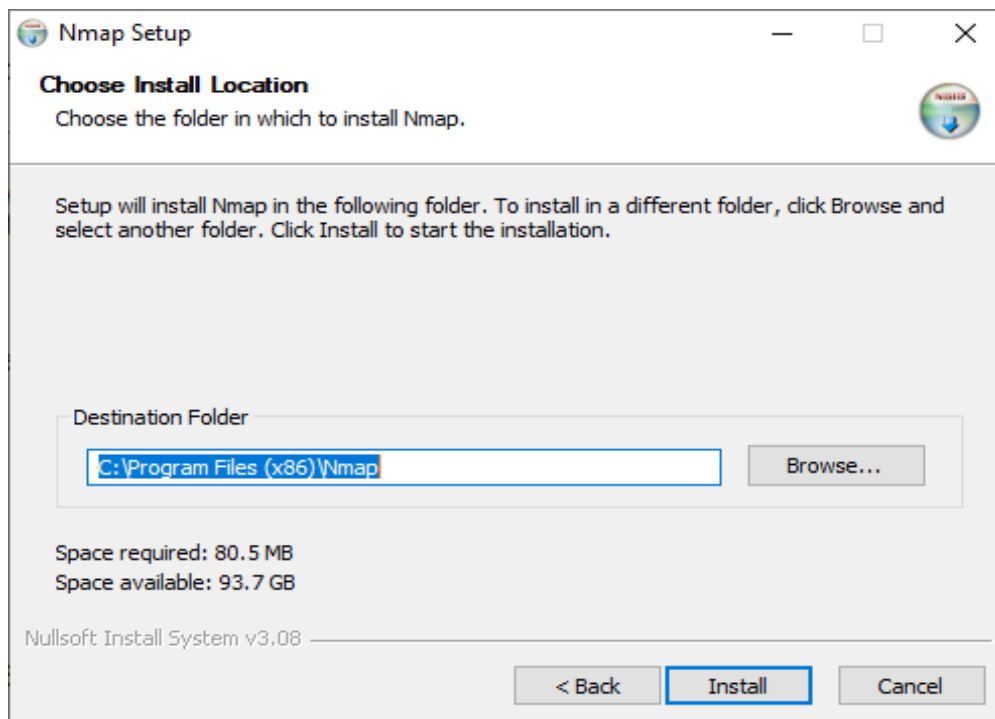
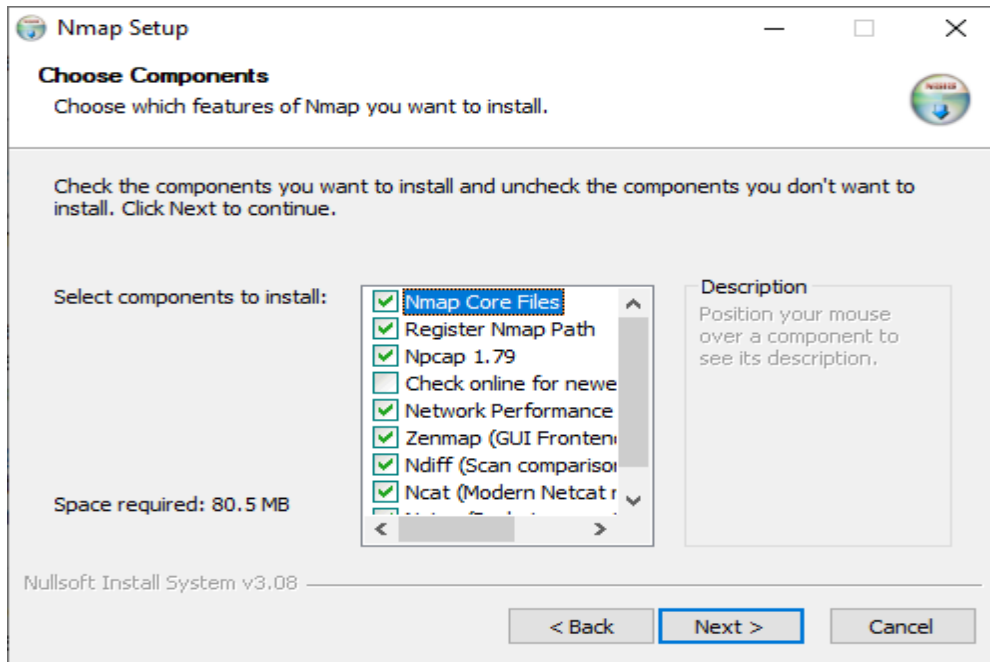
For more information on this license, see <https://nmap.org/npsl/>

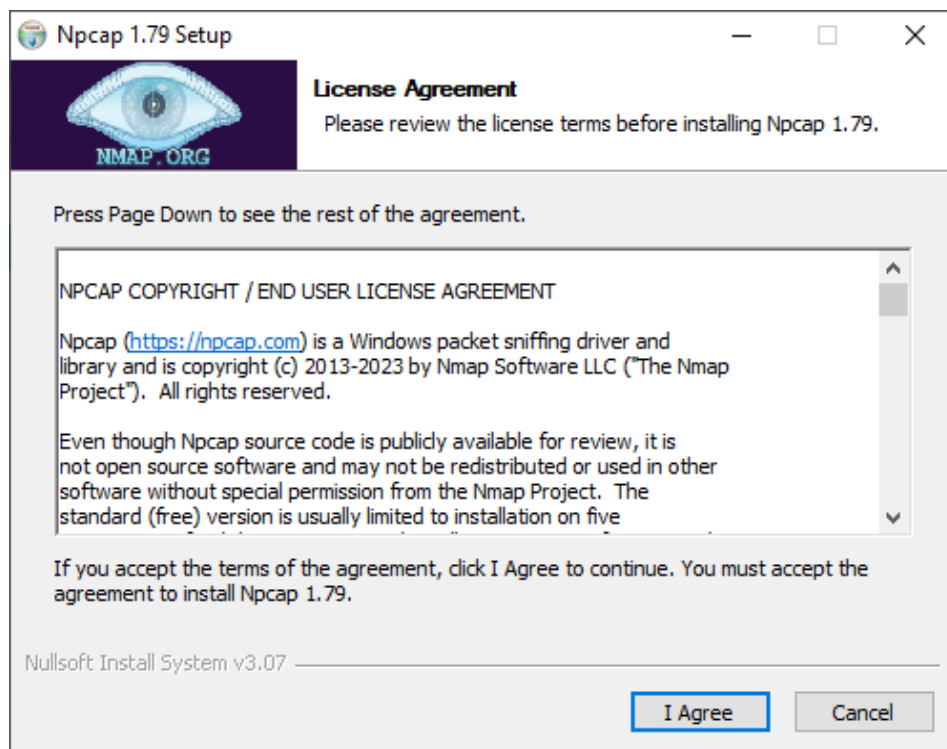
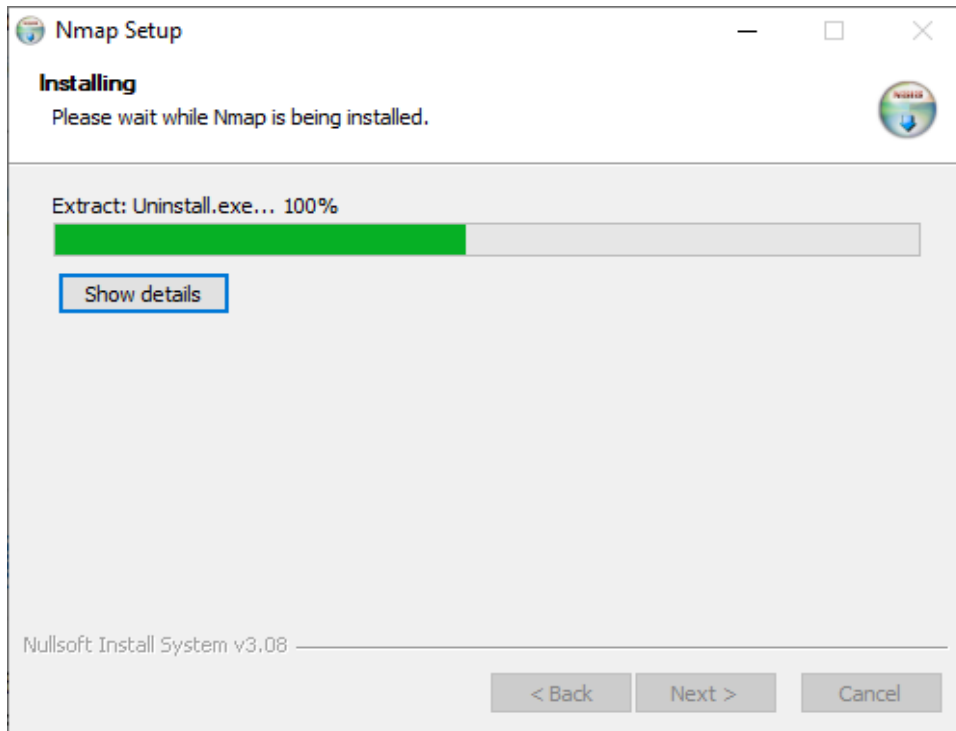
0. Preamble

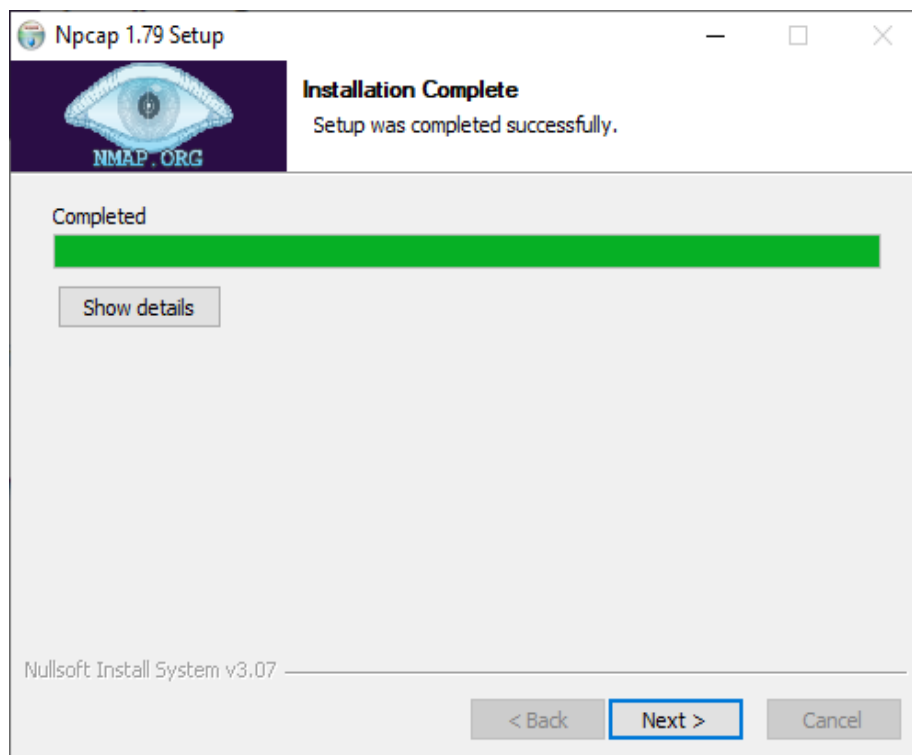
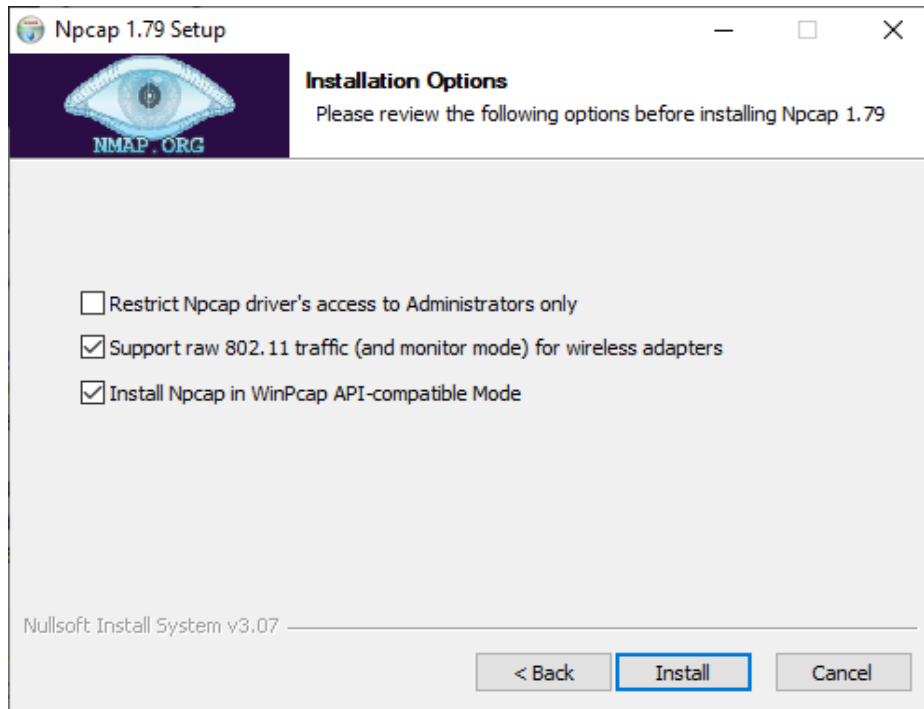
The intent of this license is to establish freedom to share and change the software regulated by this license under the open source model. It also includes a Contributor Agreement and disclaims any warranty on Covered Software. Companies wishing to use or incorporate Covered Software within their own products may find that our Nmap OEM product (<https://nmap.org/oem/>) better suits their needs. Open source developers who wish to incorporate parts of Covered Software into free software with conflicting licenses may write Licensor to request a waiver of terms.

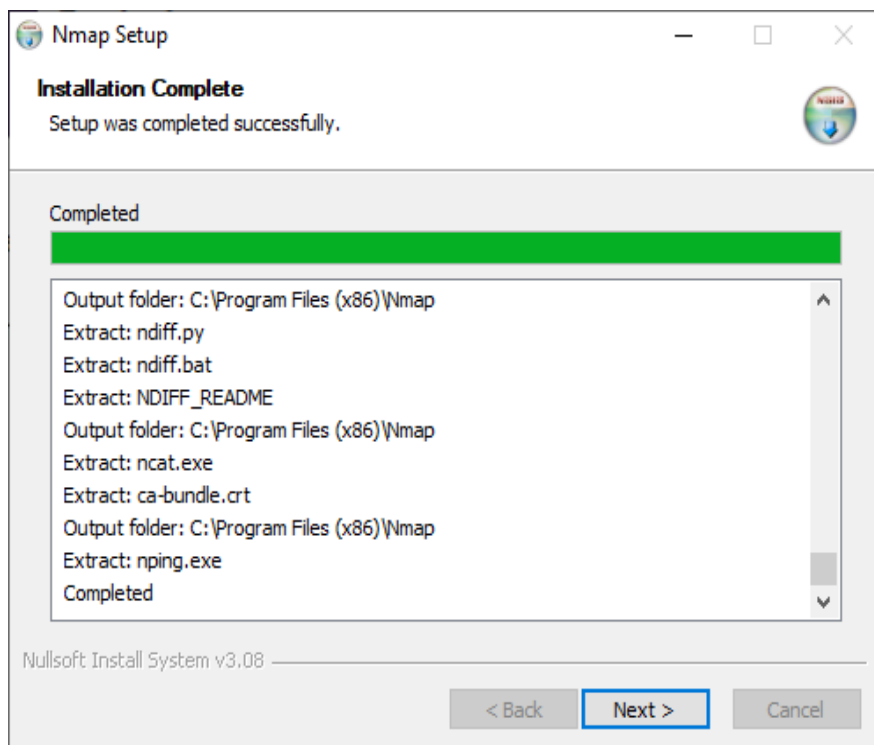
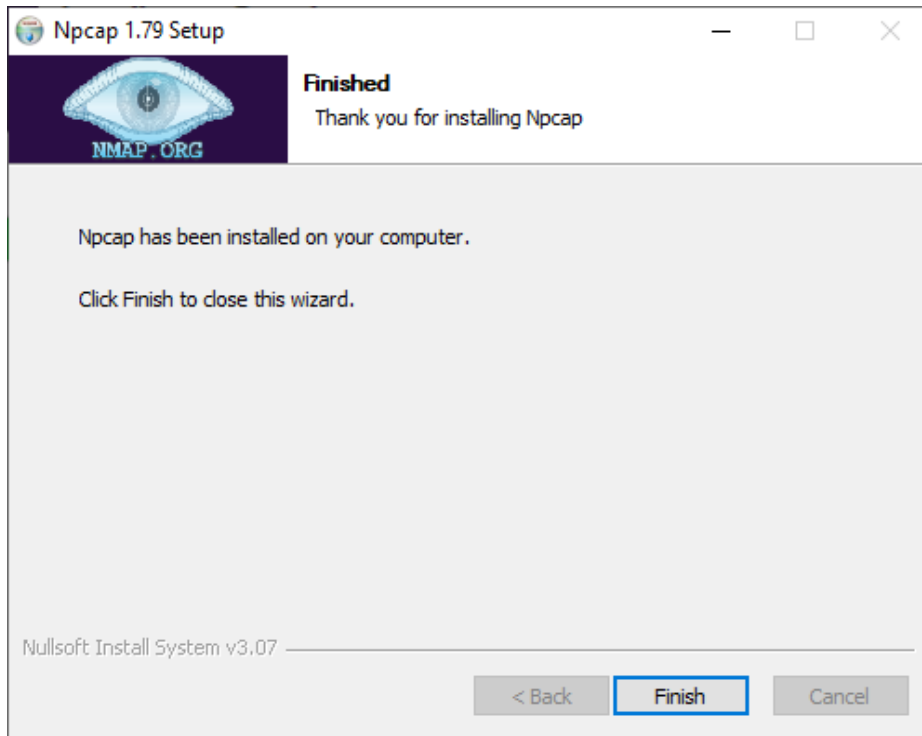
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

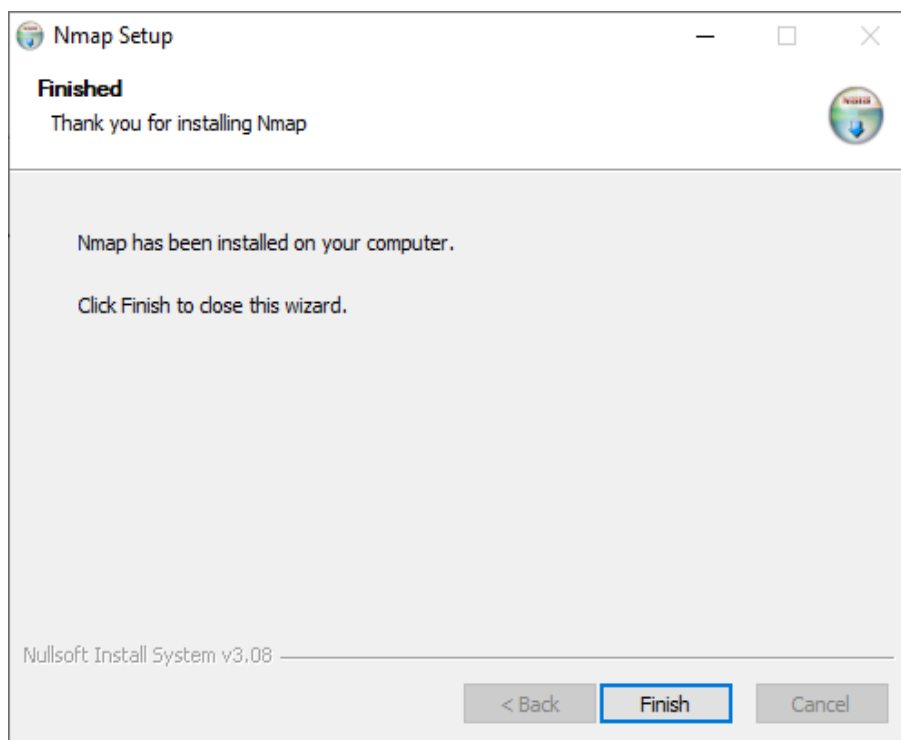
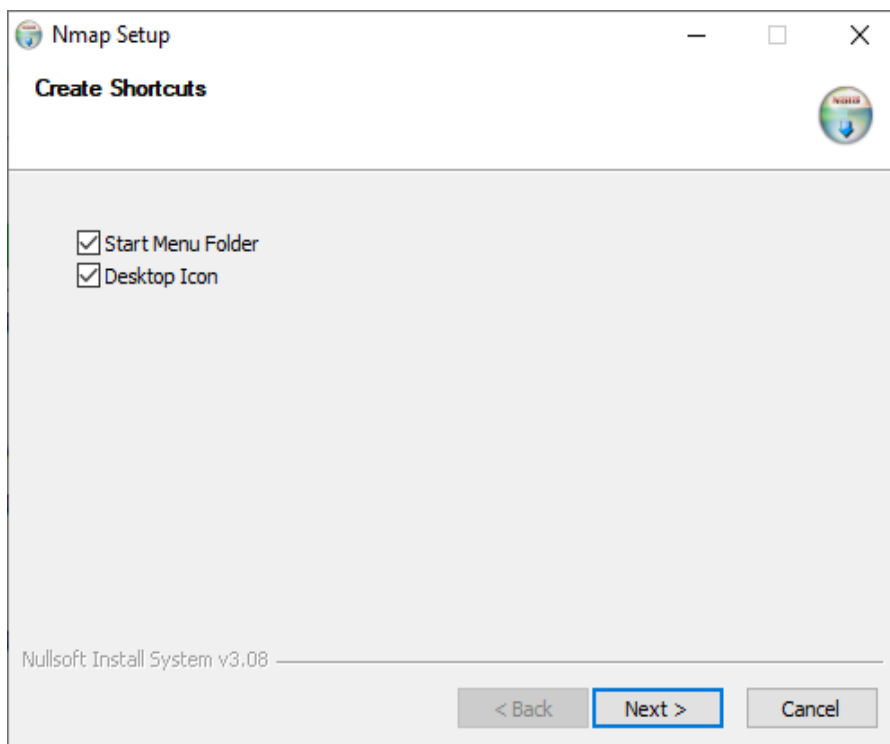
Nullsoft Install System v3.08



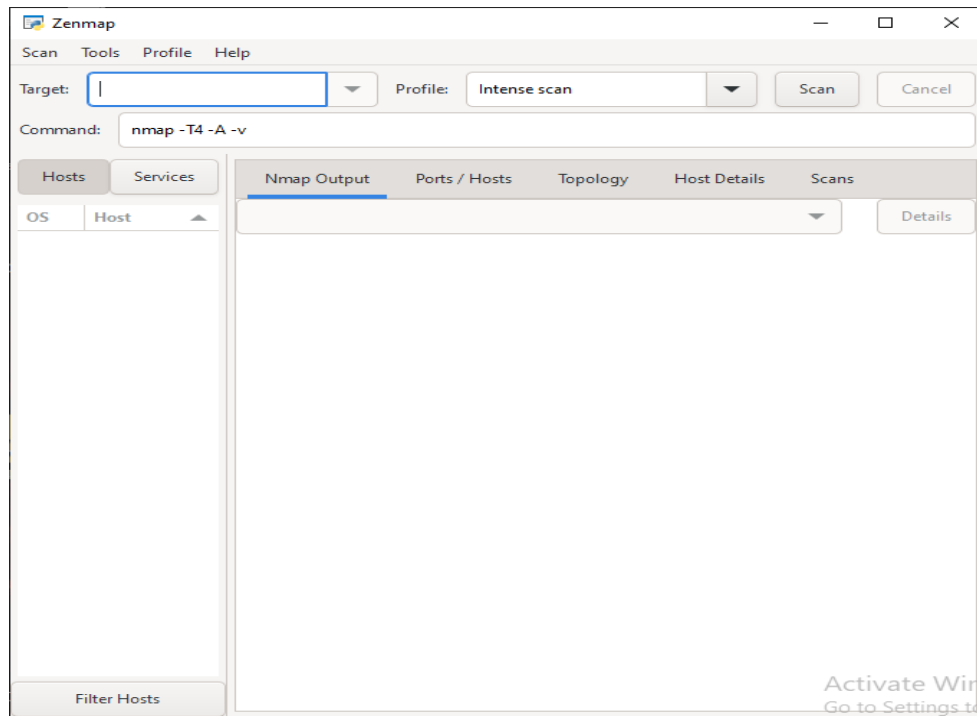








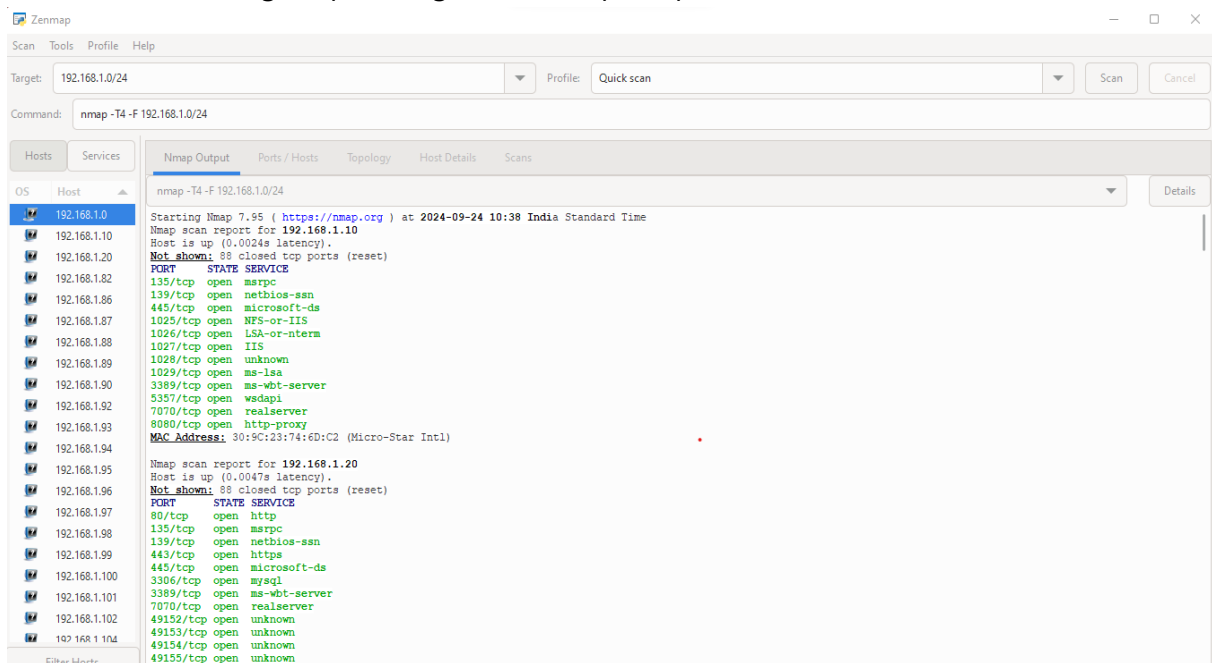
Step 3: The Zenmap has been installed



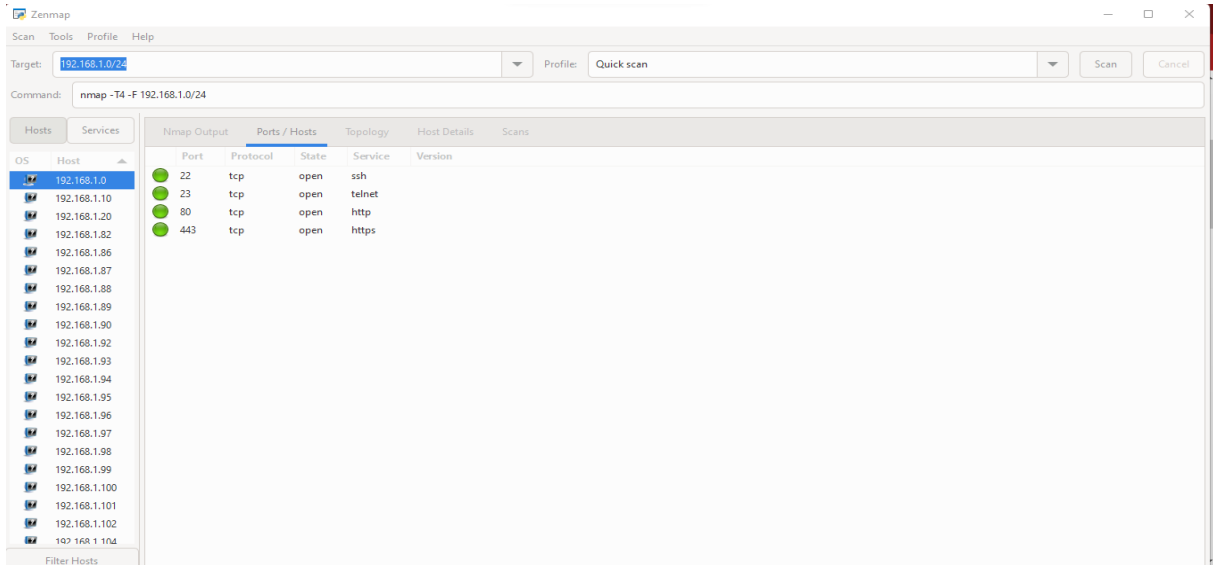
Step 4: Scan a network and find out which servers and devices are up and running:

In Target give 192.168.1.0/24 , Profile give Quick Scan

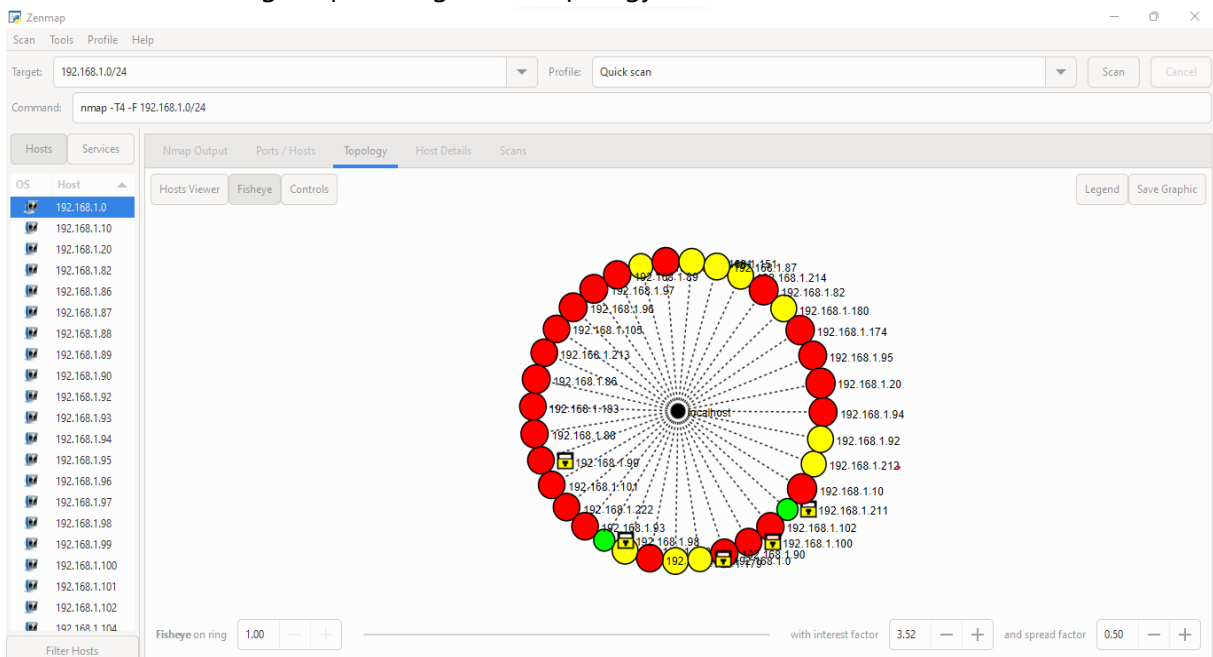
a. The following output will give for Nmap Output



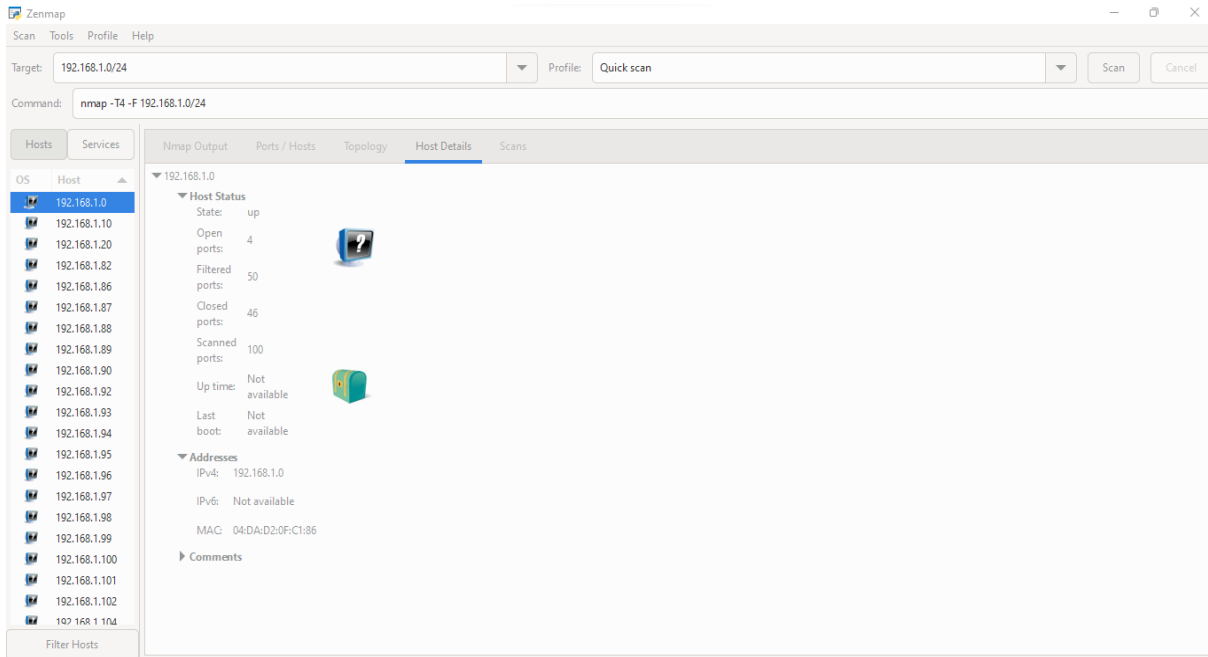
b. The following output will give for Ports/Hosts Output



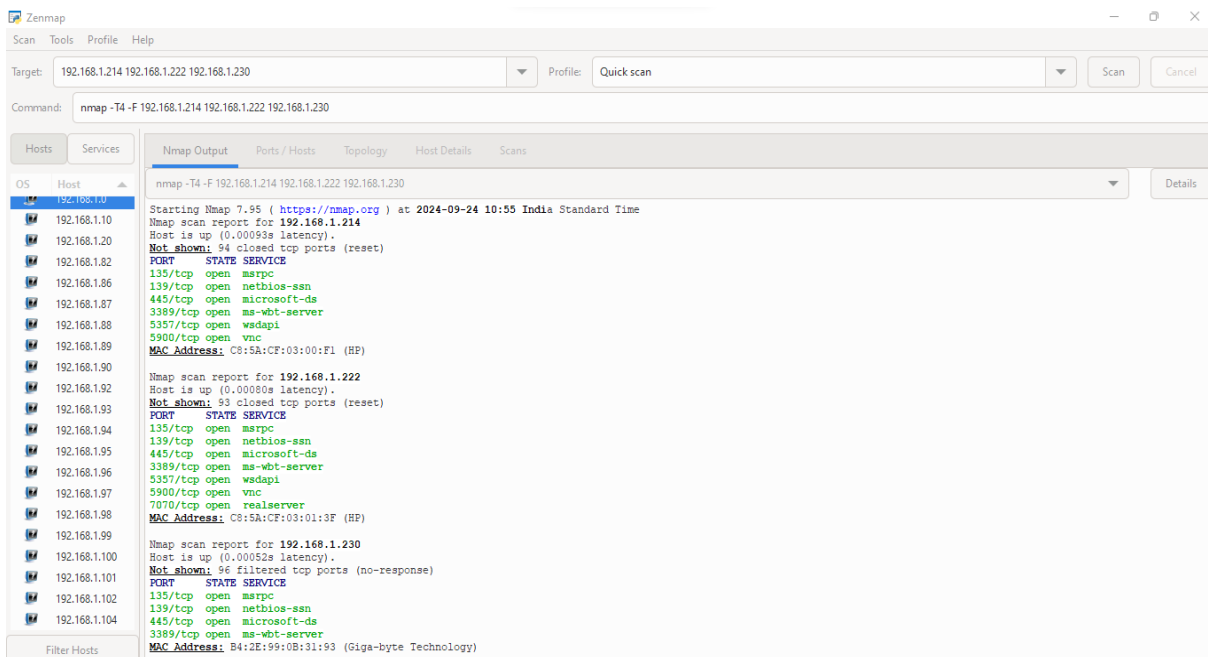
c. The following output will give for topology



d. The following output will give for Host details



Step 5: Scan multiple IP addresses or subnets:



Target: 192.168.1.214 192.168.1.222 192.168.1.230 Profile: Quick scan

Command: nmap -T4 -F 192.168.1.214 192.168.1.222 192.168.1.230

OS	Host	Port	Protocol	State	Service	Version
	192.168.1.10	22	tcp	open	ssh	
	192.168.1.10	23	tcp	open	telnet	
	192.168.1.20	80	tcp	open	http	
	192.168.1.82	443	tcp	open	https	

Target: 192.168.1.214 192.168.1.222 192.168.1.230 Profile: Quick scan

Command: nmap -T4 -F 192.168.1.214 192.168.1.222 192.168.1.230

Topology view showing a circular network diagram with nodes for each host (e.g., 192.168.1.10, 192.168.1.20, 192.168.1.82, 192.168.1.170) and their connections. The diagram is a circular fisheye projection of the network topology.

Legend Save Graphic

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.

The screenshot shows the Zenmap interface with the target set to `nmap 192.168.1.0/24 --exclude 192.168.1.101`. The command field contains `nmap -T4 -F --exclude 192.168.1.10 nmap 192.168.1.0/24 --exclude 192.168.1.101 --exclude 192.168.1.10 --exclude 192.168.1.10 --exclude 192.168.1.10 --exclude 192.168.1.10 --exclude 192.168.1.10 --exclude 192.168.1.10 --exclude 192.168.1.10 --exclude 192.168.1.10 --exclude 192.168.1.10`. The Nmap Output pane shows the scan results for 192.168.1.0/24, including the MAC address 00:D8:61:ED:BC:76 (Micro-Star Intl).

Step 7: Fast nmap scanning for a network range:

`nmap -F 192.168.1.10/24`

The screenshot shows the Zenmap interface with the target set to `192.168.1.10/24`. The command field contains `nmap -T4 -F 192.168.1.10/24`. The Nmap Output pane shows the scan results for 192.168.1.10/24, including the MAC address 30:9C:23:74:ED:C2 (Micro-Star Intl).

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

`nmap --packet-trace 192.168.1.10`

Target: `nmap --packet-trace 192.168.1.10` Profile: Quick scan

Command: `nmap -T4 -F --packet-trace nmap --packet-trace 192.168.1.10`

Hosts: 192.168.1.10

Nmap Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-24 11:19 India Standard Time
Failed to resolve "nmap".
SENT (2.3650s) ARP who-has 192.168.1.10 tell 192.168.1.213
RCVD (2.3650s) ARP reply 192.168.1.10 is-at 30:9c:23:74:6d:c2
NSOCK INFO [2.3950s] nssock_io_new2(): nssock_io_new (IOD #1)
NSOCK INFO [2.3950s] nssock_connect_udp(): UDP connection requested to 8.8.8.8:53 (IOD #1) EID 8
NSOCK INFO [2.3950s] nssock_read(): Read request from IOD #1 [8.8.8.8:53] (timeout: -1ms) EID 18
NSOCK INFO [2.3950s] nssock_io_new2(): nssock_io_new (IOD #2)
NSOCK INFO [2.3950s] nssock_connect_udp(): UDP connection requested to 4.2.2.2:53 (IOD #2) EID 24
NSOCK INFO [2.4020s] nssock_read(): Read request from IOD #2 [4.2.2.2:53] (timeout: -1ms) EID 34
NSOCK INFO [2.4020s] nssock_write(): Write request for 43 bytes to IOD #1 EID 43 [8.8.8.8:53]
NSOCK INFO [2.4020s] nssock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [8.8.8.8:53]
NSOCK INFO [2.4020s] nssock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [8.8.8.8:53]
NSOCK INFO [2.4090s] nssock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [8.8.8.8:53] (43 bytes): F.....10.1.168.192.in-addr.arpa.....
NSOCK INFO [2.4080s] nssock_read(): Read request from IOD #1 [8.8.8.8:53] (timeout: -1ms) EID 50
NSOCK INFO [2.4080s] nssock_io_delete(): nssock_io_delete (IOD #1)
NSOCK INFO [2.4080s] nssock_event_delete(): nssock_event_delete on event #50 (type READ)
NSOCK INFO [2.4080s] nssock_io_delete(): nssock_io_delete (IOD #2)
NSOCK INFO [2.4080s] nssock_event_delete(): nssock_event_delete on event #34 (type READ)
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:1199 S ttl=45 id=53090 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:1199 S ttl=45 id=53090 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:8888 S ttl=49 id=47811 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:1199 S ttl=51 id=7387 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:25 S ttl=39 id=61454 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:22 S ttl=57 id=25503 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:111 S ttl=41 id=52889 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:336 S ttl=43 id=49584 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:135 S ttl=50 id=36545 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
SENT (2.4090s) TCP 192.168.1.213:46003 > 192.168.1.10:80 S ttl=48 id=48108 ipLen=44 seq=1323180590 win=1024 cmsg 1460>
RCVD (2.4100s) TCP 192.168.1.10:1199 > 192.168.1.213:46003 RA ttl=128 id=8669 ipLen=40 seq=0 win=0
RCVD (2.4100s) TCP 192.168.1.10:1199 > 192.168.1.213:46003 RA ttl=128 id=8669 ipLen=40 seq=0 win=0
RCVD (2.4100s) TCP 192.168.1.10:8888 > 192.168.1.213:46003 RA ttl=128 id=8670 ipLen=40 seq=0 win=0
RCVD (2.4100s) TCP 192.168.1.10:25 > 192.168.1.213:46003 RA ttl=128 id=8672 ipLen=40 seq=0 win=0
```

Target: `nmap --packet-trace 192.168.1.10` Profile: Quick scan

Command: `nmap -T4 -F --packet-trace nmap --packet-trace 192.168.1.10`

Hosts: 192.168.1.10

Nmap Output:

```
RCVD (2.4150s) TCP 192.168.1.10:544 > 192.168.1.213:46003 RA ttl=128 id=8753 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:646 > 192.168.1.213:46003 RA ttl=128 id=8754 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:5900 > 192.168.1.213:46003 RA ttl=128 id=8755 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:9100 > 192.168.1.213:46003 RA ttl=128 id=8756 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:6646 > 192.168.1.213:46003 RA ttl=128 id=8757 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:8443 > 192.168.1.213:46003 RA ttl=128 id=8758 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:444 > 192.168.1.213:46003 RA ttl=128 id=8759 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:9 > 192.168.1.213:46003 RA ttl=128 id=8760 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:427 > 192.168.1.213:46003 RA ttl=128 id=8761 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:2121 > 192.168.1.213:46003 RA ttl=128 id=8762 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:514 > 192.168.1.213:46003 RA ttl=128 id=8763 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:1433 > 192.168.1.213:46003 RA ttl=128 id=8764 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:8009 > 192.168.1.213:46003 RA ttl=128 id=8765 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:5432 > 192.168.1.213:46003 RA ttl=128 id=8766 ipLen=40 seq=0 win=0
RCVD (2.4150s) TCP 192.168.1.10:1029 > 192.168.1.213:46003 SR ttl=128 id=8767 ipLen=44 seq=3417024683 win=8192 cmsg 1460>
Nmap scan report for 192.168.1.10
Host is up (0.00024s latency).
Not shown: 88 closed tcp ports (reset)
PORT STATE SERVICE
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-isa
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
7070/tcp open  realserver
8080/tcp open  http-proxy
MAC Address: 30:9C:23:74:6D:C2 (Micro-Star Int'l)

Nmap done: 1 IP address (1 host up) scanned in 2.42 seconds
```

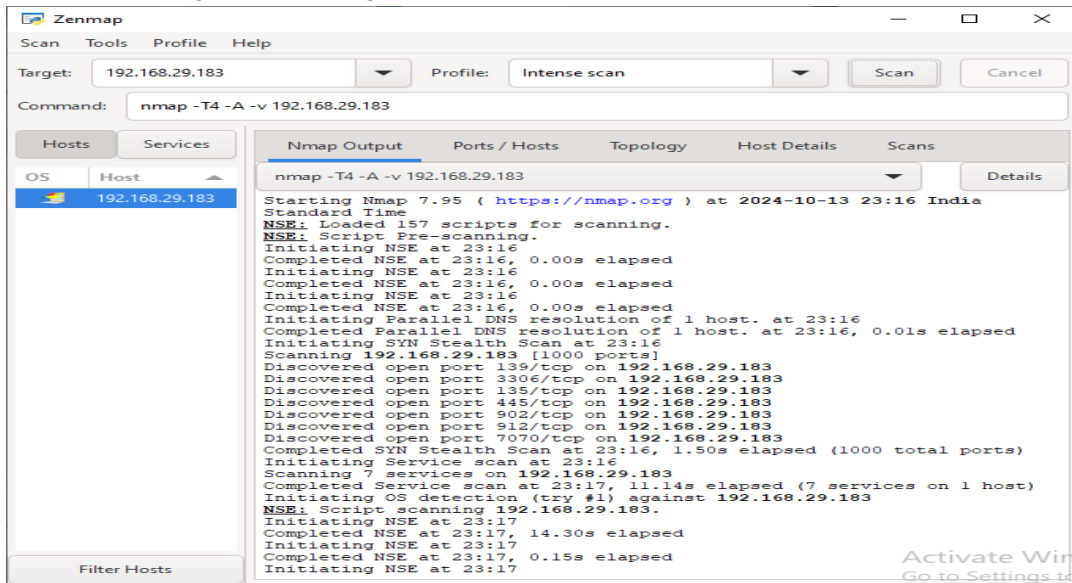
Step 9:

Now let's Scan a single host:

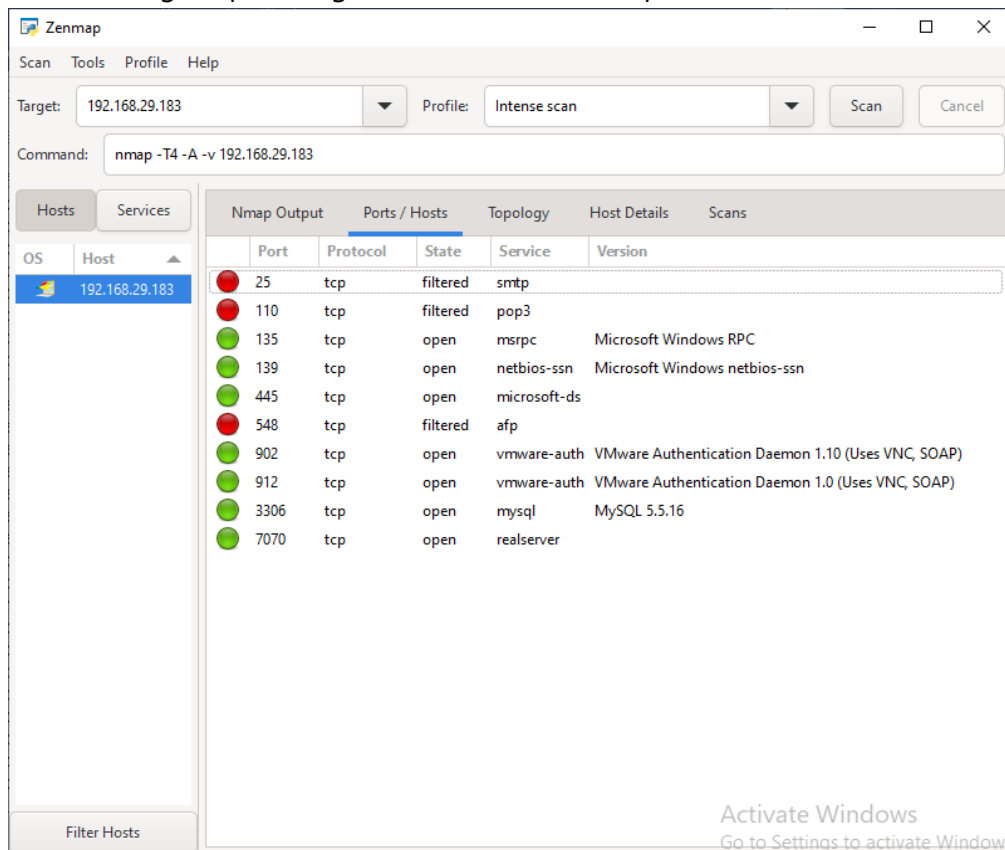
Here we have added our systems IP address

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

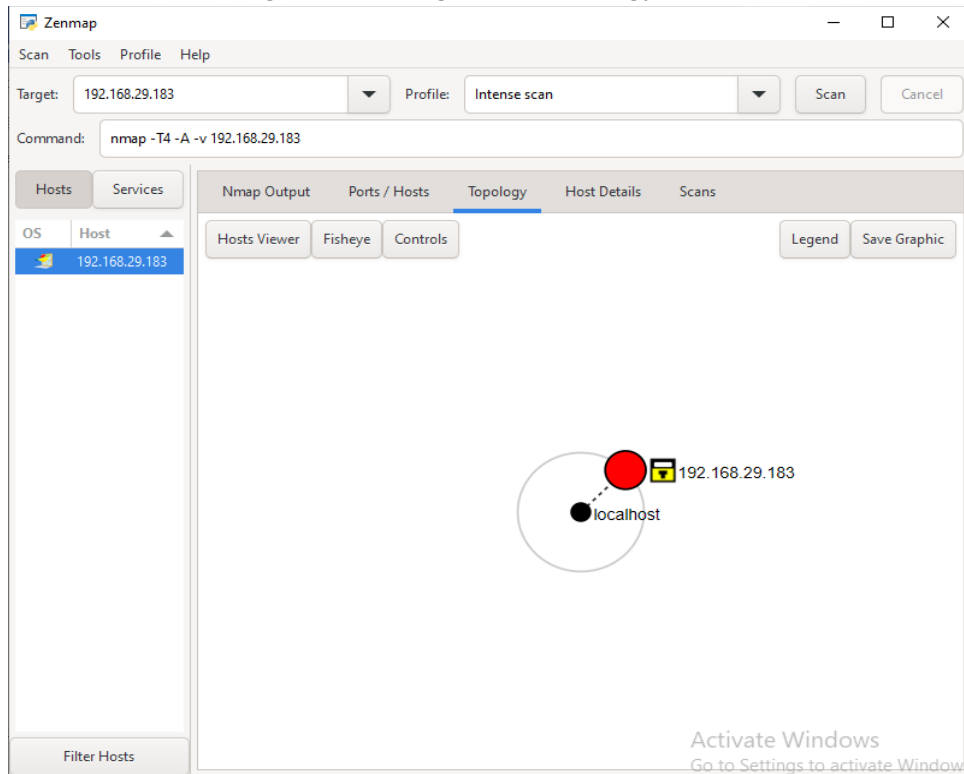
a. The following output will give for Nmap Output



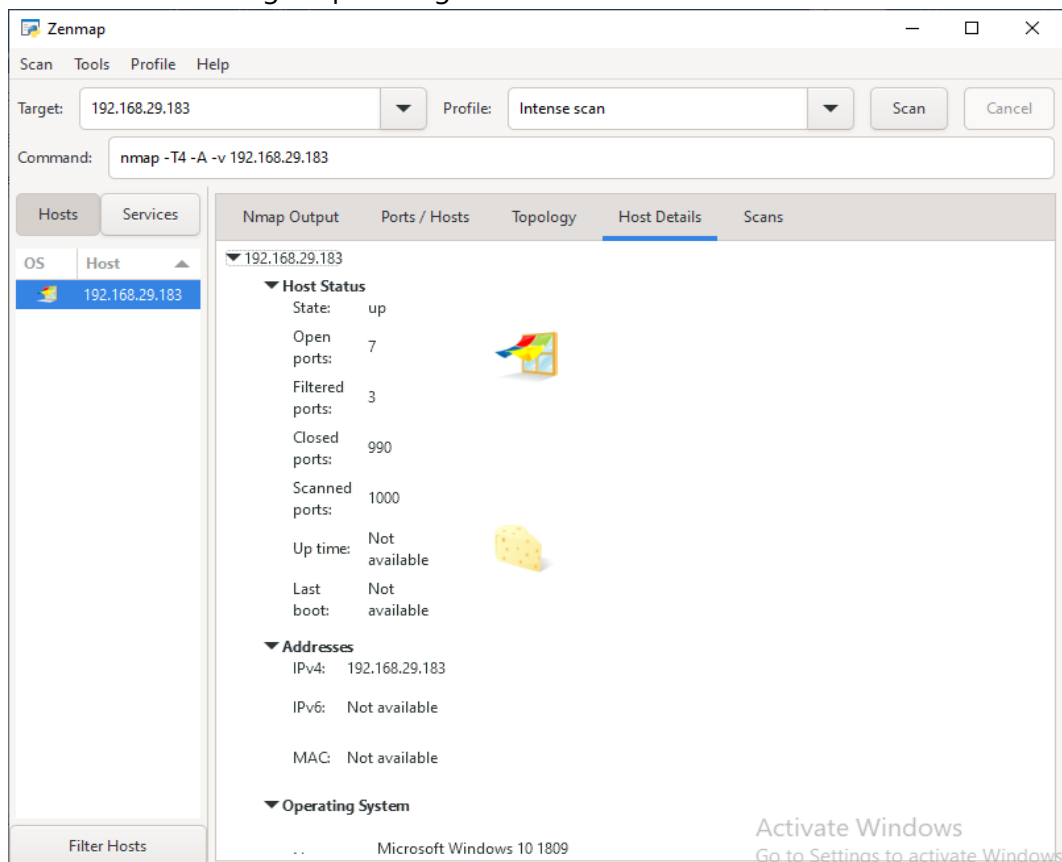
b. The following output will give for Ports/Hosts Output



c. The following output will give for topology

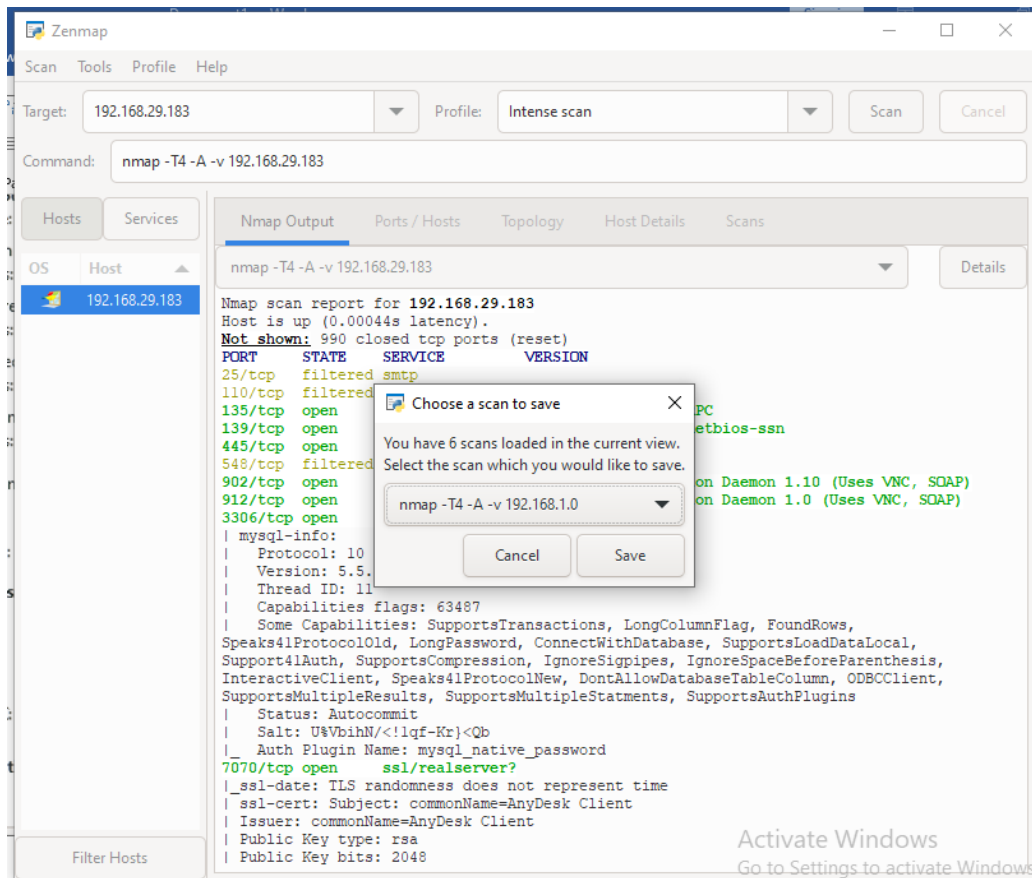


d. The following output will give for Host details



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

Go to Scan -> Save Scan and Save



The screenshot shows the Zenmap application window. The main area displays the output of an Nmap scan for target 192.168.29.183. The scan command is `nmap -T4 -A -v 192.168.29.183`. The output shows that the host is up and 990 TCP ports are closed. Several ports are open, including 135/tcp, 139/tcp, 445/tcp, 902/tcp, 912/tcp, and 3306/tcp. A dialog box titled "Choose a scan to save" is overlaid on the scan output, showing a list of scans with "nmap -T4 -A -v 192.168.1.0" selected. The dialog box has "Cancel" and "Save" buttons.

```
nmap -T4 -A -v 192.168.29.183
Nmap scan report for 192.168.29.183
Host is up (0.00044s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
25/tcp    filtered smtp
110/tcp   filtered
135/tcp   open
139/tcp   open
445/tcp   open
548/tcp   filtered
902/tcp   open
912/tcp   open
3306/tcp  open
| mysql-info:
| Protocol: 10
| Version: 5.5.
| Thread ID: 11
| Capabilities flags: 63487
| Some Capabilities: SupportsTransactions, LongColumnFlag, FoundRows,
Speaks41ProtocolOld, LongPassword, ConnectWithDatabase, SupportsLoadDataLocal,
Support41Auth, SupportsCompression, IgnoreSigpipes, IgnoreSpaceBeforeParenthesis,
InteractiveClient, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, ODBCClient,
SupportsMultipleResults, SupportsMultipleStatements, SupportsAuthPlugins
| Status: Autocommit
| Salt: U%VbihN/<!lqf-Krj<Qb
|_ Auth Plugin Name: mysql_native_password
7070/tcp  open  ssl/realserver?
|_ ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Issuer: commonName=AnyDesk Client
| Public Key type: rsa
| Public Key bits: 2048
```