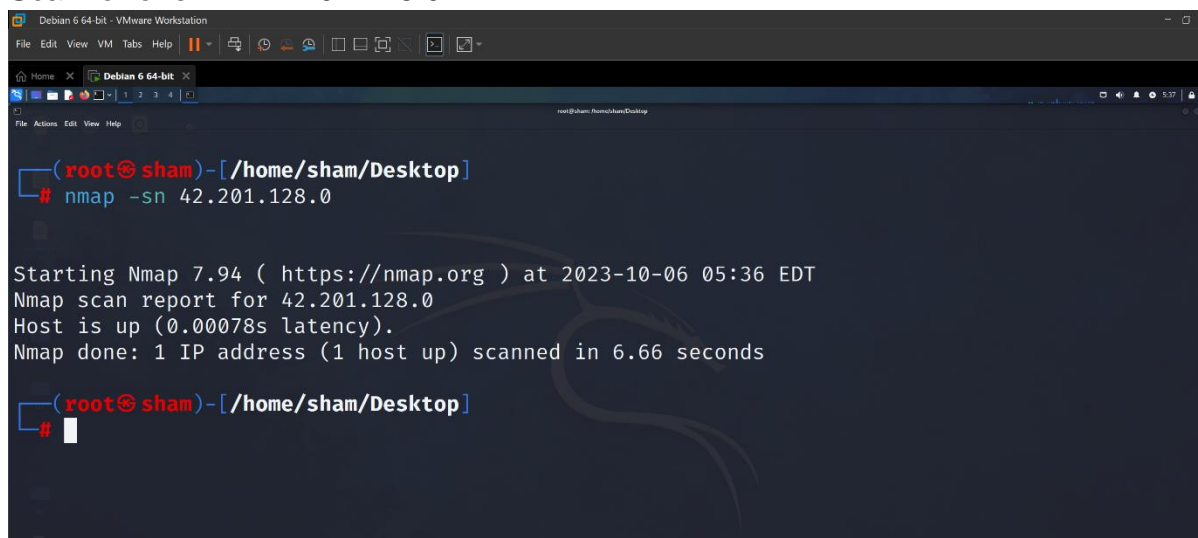


Activity 1 : Task Instructions:

1. Basic Host Discovery: Command: `nmap -sn [IP range]`

Scan for one IP : 42.201.128.0

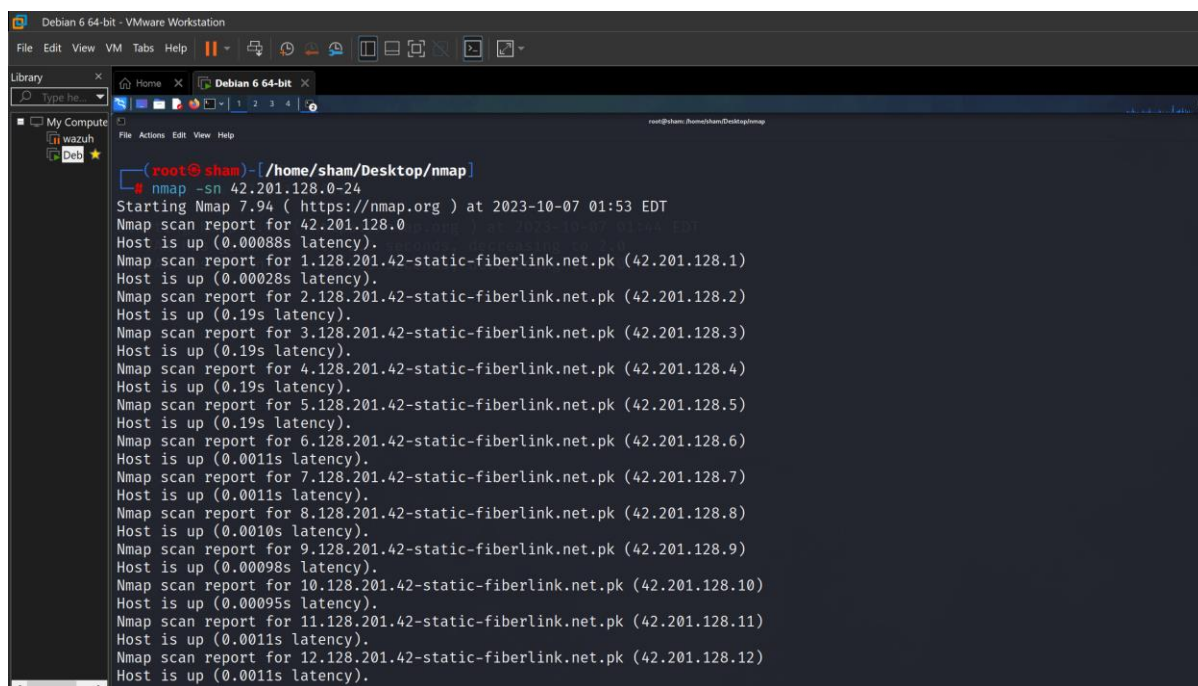


```
(root@sham)-[/home/sham/Desktop]
# nmap -sn 42.201.128.0

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-06 05:36 EDT
Nmap scan report for 42.201.128.0
Host is up (0.00078s latency).
Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds

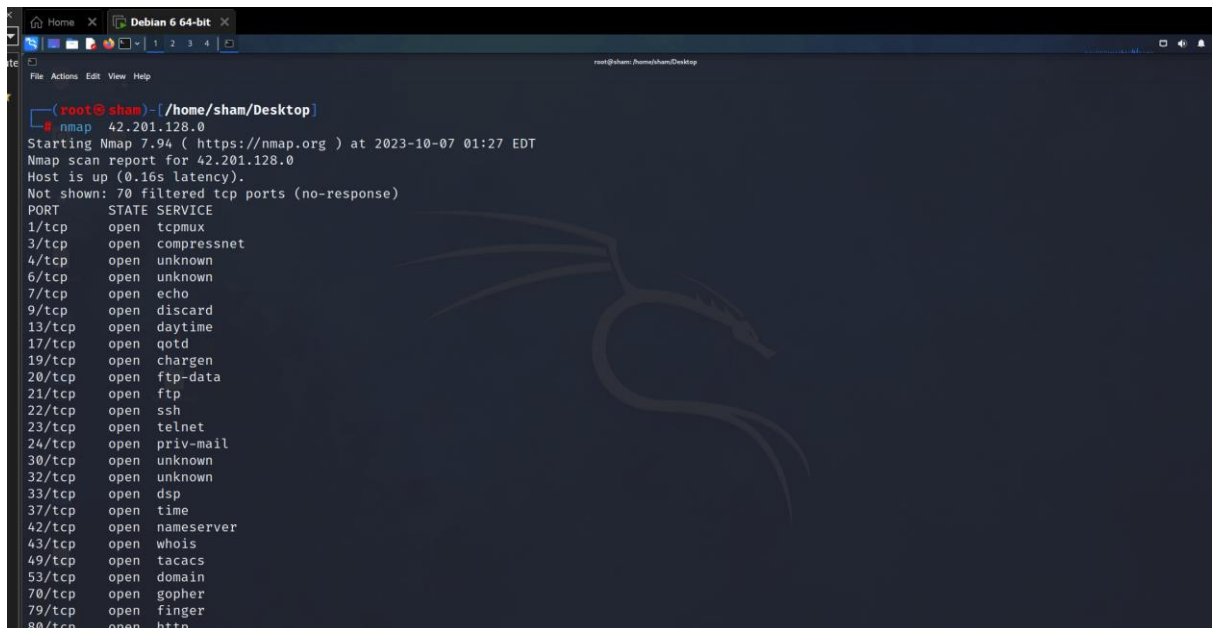
(root@sham)-[/home/sham/Desktop]
#
```

- Objective: Identify all active devices within the specified IP range. Nmap scan for 25 hosts



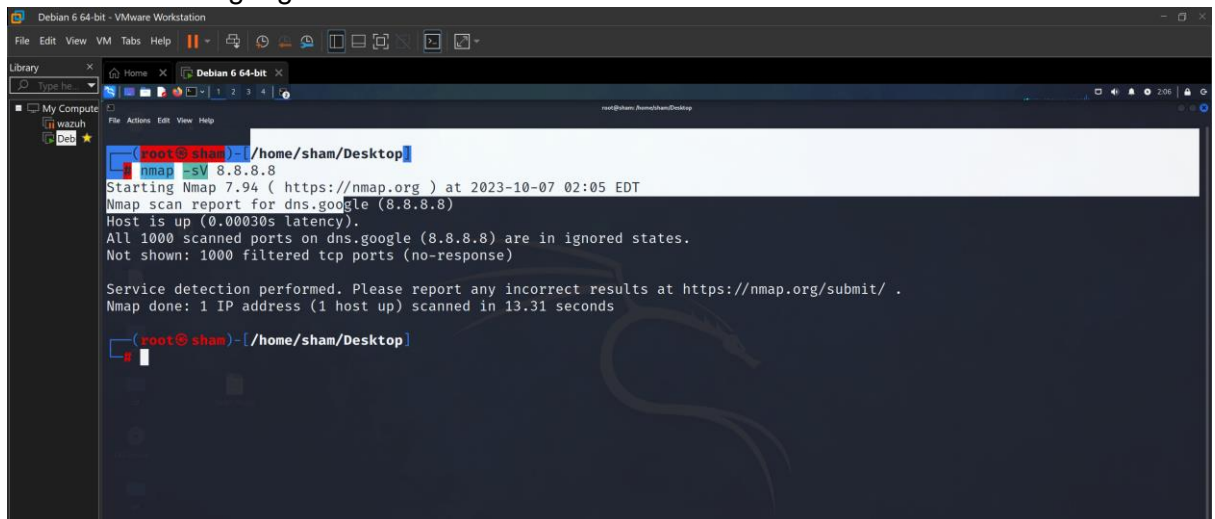
```
(root@sham)-[/home/sham/Desktop/nmap]
# nmap -sn 42.201.128.0-24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-07 01:53 EDT
Nmap scan report for 42.201.128.0
Host is up (0.00088s latency).
Nmap scan report for 1.128.201.42-static-fiberlink.net.pk (42.201.128.1)
Host is up (0.00028s latency).
Nmap scan report for 2.128.201.42-static-fiberlink.net.pk (42.201.128.2)
Host is up (0.19s latency).
Nmap scan report for 3.128.201.42-static-fiberlink.net.pk (42.201.128.3)
Host is up (0.19s latency).
Nmap scan report for 4.128.201.42-static-fiberlink.net.pk (42.201.128.4)
Host is up (0.19s latency).
Nmap scan report for 5.128.201.42-static-fiberlink.net.pk (42.201.128.5)
Host is up (0.19s latency).
Nmap scan report for 6.128.201.42-static-fiberlink.net.pk (42.201.128.6)
Host is up (0.0011s latency).
Nmap scan report for 7.128.201.42-static-fiberlink.net.pk (42.201.128.7)
Host is up (0.0011s latency).
Nmap scan report for 8.128.201.42-static-fiberlink.net.pk (42.201.128.8)
Host is up (0.0010s latency).
Nmap scan report for 9.128.201.42-static-fiberlink.net.pk (42.201.128.9)
Host is up (0.00098s latency).
Nmap scan report for 10.128.201.42-static-fiberlink.net.pk (42.201.128.10)
Host is up (0.00095s latency).
Nmap scan report for 11.128.201.42-static-fiberlink.net.pk (42.201.128.11)
Host is up (0.0011s latency).
Nmap scan report for 12.128.201.42-static-fiberlink.net.pk (42.201.128.12)
Host is up (0.0011s latency).
```

2. Basic Port Scanning: Command: `nmap [Target IP]`



```
(root@sham)-[/home/sham/Desktop]
# nmap 42.201.128.0
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-07 01:27 EDT
Nmap scan report for 42.201.128.0
Host is up (0.16s latency).
Not shown: 70 filtered tcp ports (no-response)
PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
30/tcp    open  unknown
32/tcp    open  unknown
33/tcp    open  dsp
37/tcp    open  time
42/tcp    open  nameserver
43/tcp    open  whois
49/tcp    open  tacacs
53/tcp    open  domain
70/tcp    open  gopher
79/tcp    open  finger
80/tcp    open  http
```

3. **Service Version Detection:** Command: `nmap -sV [Target ip]`
I tried on 8.8.8.8 google DNS



```
(root@sham)-[/home/sham/Desktop]
# nmap -sV 8.8.8.8
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-07 02:05 EDT
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.00030s latency).
All 1000 scanned ports on dns.google (8.8.8.8) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds

(root@sham)-[/home/sham/Desktop]
```

4. Operating System Detection:

Command: `nmap -O [Target IP]` example: 42.201.128.0

```
Debian 6 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
wazuh
Deb
61532/tcp open unknown
61900/tcp open unknown
62078/tcp open iphone-sync
63331/tcp open unknown
64623/tcp open unknown
65000/tcp open unknown
65129/tcp open unknown
65389/tcp open unknown
Device type: general purpose|WAP
Running (JUST GUESSING): Microsoft Windows XP|7|2012 (97%), Actiontec embedded (94%), Linux 2.4.X|3.X (94%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:li
nux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
Aggressive OS guesses: Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Actiontec MI42
4WR-GEN3I WAP (94%), DD-WRT v24-sp2 (Linux 2.4.37) (94%), Microsoft Windows XP SP3 (93%), Linux 3.2 (91%)
, Linux 4.4 (91%)
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 54.28 seconds

(root@sham)-[/home/sham/Desktop/nmap]
```

5. Aggressive Scan:

Command: `nmap -T4 -A [Target IP] ip= 42.201.128.0`

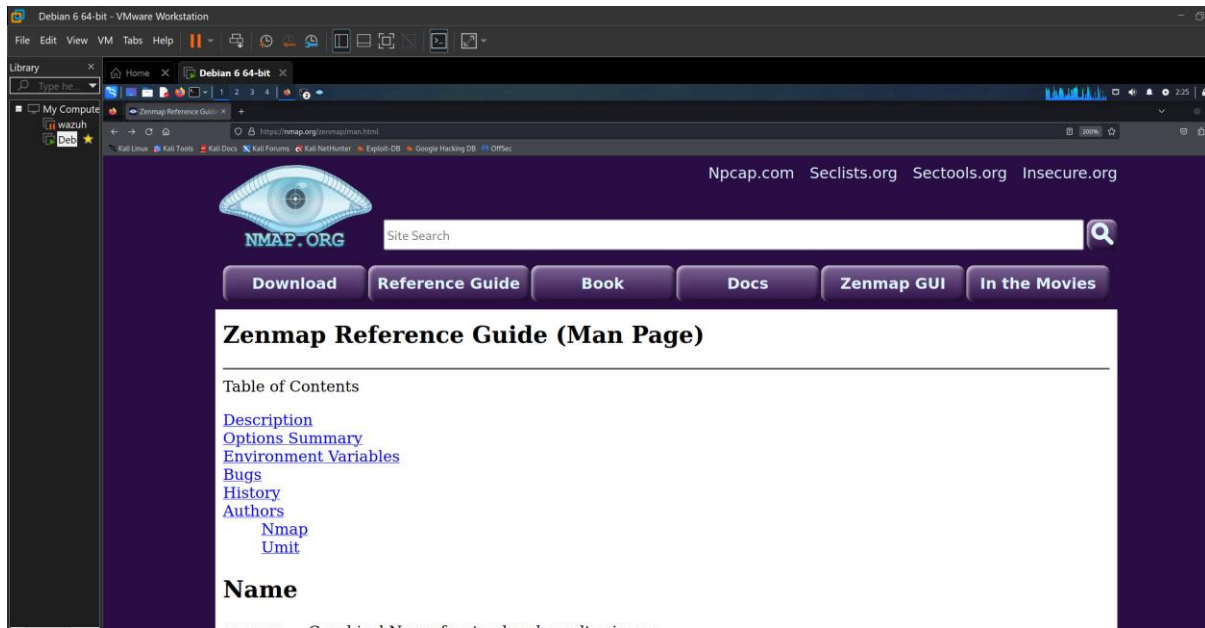
```
Debian 6 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
wazuh
Deb
(root@sham)-[/home/sham/Desktop/nmap]
nmap -T4 -A -v 42.201.128.0
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-07 02:20 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:20
Completed NSE at 02:20, 0.00s elapsed
Initiating NSE at 02:20
Completed NSE at 02:20, 0.00s elapsed
Initiating NSE at 02:20
Completed NSE at 02:20, 0.00s elapsed
Initiating Ping Scan at 02:20
Scanning 42.201.128.0 [4 ports]
Completed Ping Scan at 02:20, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:20
Completed Parallel DNS resolution of 1 host. at 02:20, 0.81s elapsed
Initiating SYN Stealth Scan at 02:20
Scanning 42.201.128.0 [1000 ports]
Discovered open port 554/tcp on 42.201.128.0
Discovered open port 80/tcp on 42.201.128.0
Discovered open port 1723/tcp on 42.201.128.0
Discovered open port 143/tcp on 42.201.128.0
Discovered open port 135/tcp on 42.201.128.0
Discovered open port 995/tcp on 42.201.128.0
Discovered open port 22/tcp on 42.201.128.0
Discovered open port 443/tcp on 42.201.128.0
Discovered open port 993/tcp on 42.201.128.0
Discovered open port 113/tcp on 42.201.128.0
Discovered open port 23/tcp on 42.201.128.0
```

Activity 2: Task Instructions:

1. Use Zenmap to generate a visual representation of the network

Nmap is the graphical representation of nmap tool.

- Download the latest version of Zenmap from the official website.



How to Install Zenmap in Kali Linux?

Here is the step-by-step process to install Zenmap on Kali Linux:

1. Update Kali Linux

Before Zenmap installation, it is highly recommended that you upgrade or update the packages index list in Kali Linux. For this, open a terminal and write the following command:

```
sudo apt update
```

To have a look at the packages available for update, write this command:

```
sudo apt list --upgradable
```

Now, you can easily update the packages on an individual basis with the `sudo apt install PACKAGE_NAME`. In order to update the entire system, run this command:

```
sudo apt full-upgrade -y
```

This will successfully update your Kali Linux system.

Furthermore, if you are looking for an all-in-one command to update the Kali Linux system, use this:

```
sudo apt update && sudo apt full-upgrade -y
```

2. Download Latest Version of Zenmap

Once you have updated the Kali Linux, it is time to download Zenmap. For this, visit the [official site](#) of Nmap.

Alternatively, you can download and install it using commands in the terminal:

```
wget https://nmap.org/dist/zenmap-7.91-1.noarch.rpm
```

3. Download & Install Essential Dependencies

To install and make the most out of Zenmap, you should download some dependencies as well. Run these commands to do so:

```
wget http://archive.ubuntu.com/ubuntu/pool/universe/p/pygtk/python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
```

```
wget http://archive.ubuntu.com/ubuntu/pool/universe/p/pycairo/python-cairo_1.16.2-2ubuntu2_amd64.deb
```

```
wget http://archive.ubuntu.com/ubuntu/pool/universe/p/pygobject-2/python-gobject-2_2.28.6-14ubuntu1_amd64.deb
```

After downloading these, it is time to install the packages. In order to do this, make the .deb files executable by running the below command:

```
sudo chmod +777
```

Once the .deb files have become executable, run the below commands to install the Zenmap dependencies:

```
sudo apt install ./python-cairo_1.16.2-2ubuntu2_amd64.deb
```

```
sudo apt install ./python-gobject-2_2.28.6-14ubuntu1_amd64.deb
```

```
sudo apt install ./python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
```

4. Convert Zenmap .rpm packages to .deb extension

The next step is the conversion of .rpm package lists to .deb extension. For this, you can use Alien Package, which is a computer program used to convert Linux package distribution files to Debian. Alien allows conversion of RPM, deb, slp, tgz, and Linux Standard Base.

To install Alien, run this command:

```
sudo apt install alien
```

After installing Alien, now convert the .rpm package to .deb by running this command:

```
sudo alien --to-deb zenmap-7.91-1.noarch.rpm
```

5. Execute .deb Files

Once the .deb files are ready, you need to make them executable using the below command:

```
sudo chmod +777 zenmap_7.91-2_all.deb
```

Finally, run the following command to mark the completion of Zenmap installation:

```
sudo apt install ./zenmap_7.91-2_all.deb
```

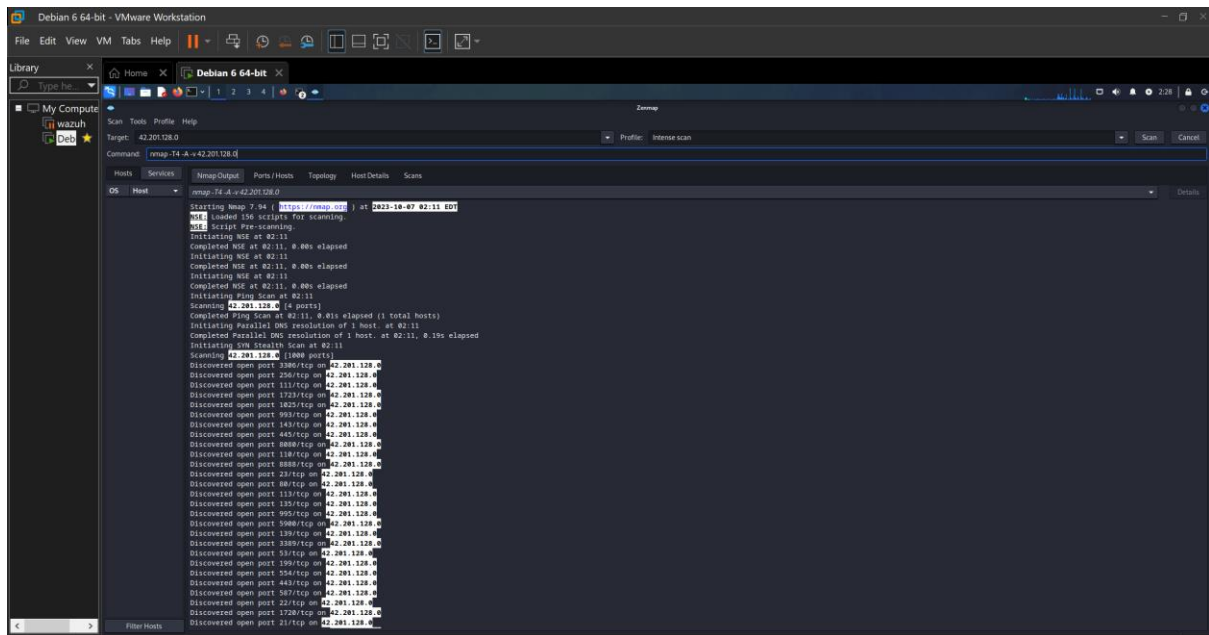
Zenmap is now ready for use. You can get started with it by simply searching for it from the Search bar or running the command line.

Source : <https://www.tutorialsfreak.com/nmap-tutorial/zenmap-installation>

Run: \$sudo zenmap

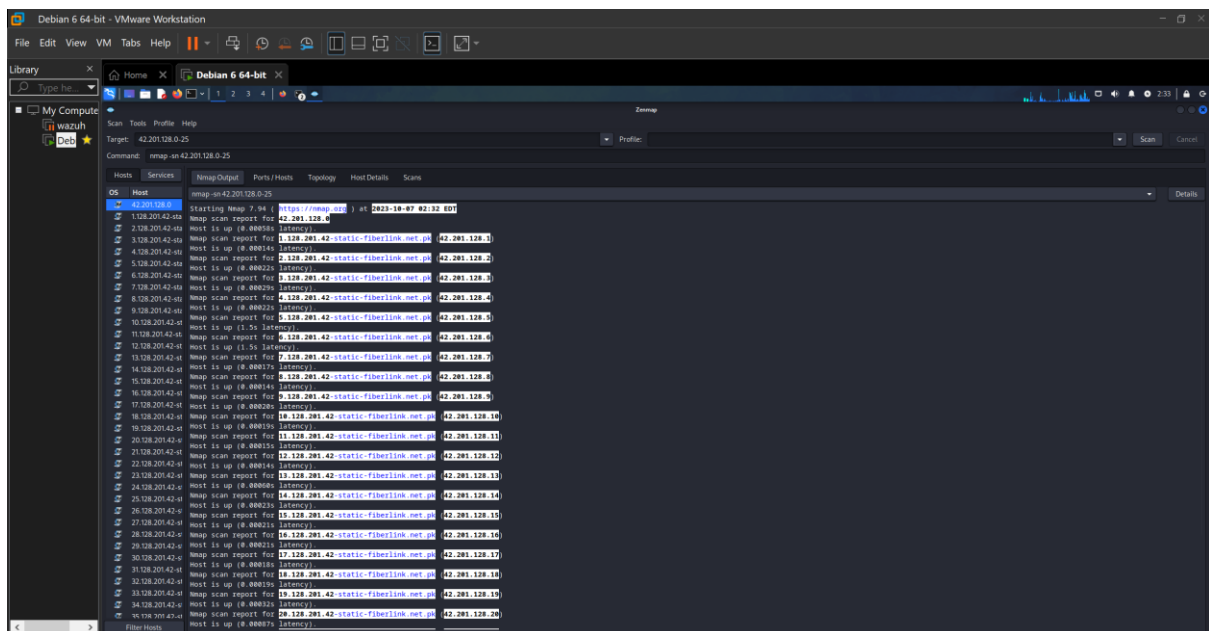
1. Basic Host Discovery:

- Command: nmap -sn [IP range]
- Objective: Identify all active devices within the specified IP range.
- Deliverable: List the IP addresses of all discovered devices



2. Network Scanning with Zenmap:

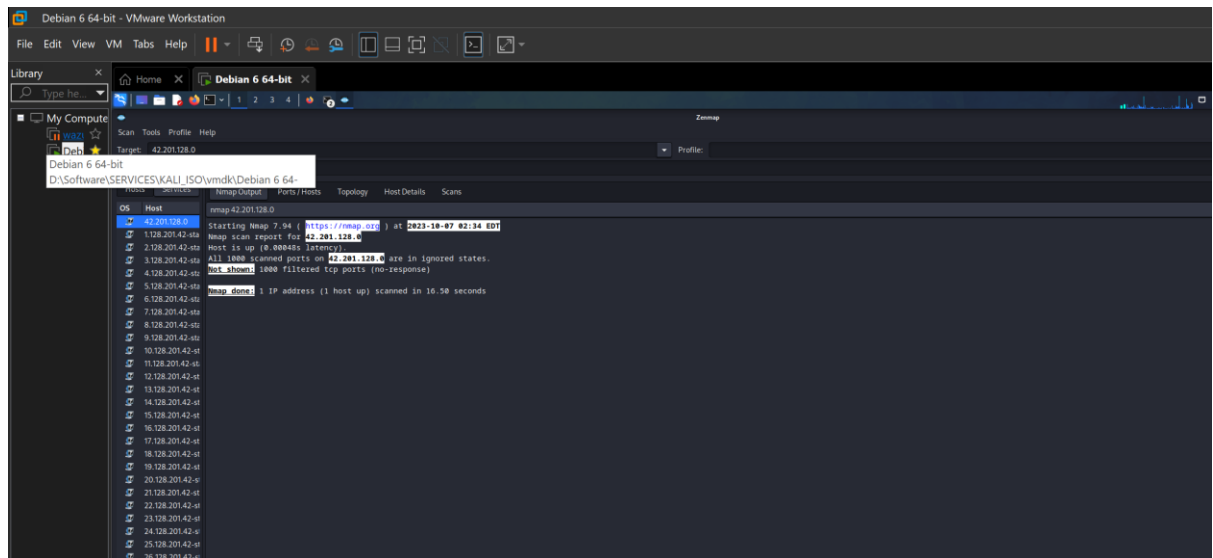
- Launch Zenmap
- Input your target IP range or specific IP address in the 'Target' field
- Select a scan profile, for instance, 'Quick Scan'.
- Initiate the scan and wait for it to complete.
- Review and save the results.



3. Network Scanning with Nmap:

- Open your command-line or terminal.
- Use the command: nmap [Target IP or IP range]. For instance, nmap 192.168.1.0/24.

- Wait for the scan to finish and review the results.



Comparison of Zenmap and Nmap:

- Based on your experience with both tools, compare them in terms of:
- User interface and ease of use.
- Flexibility and customization of scan options.
- Presentation and interpretation of scan results.
- Record your observations and finding

Following are the points:

Comparison between Zenmap and Nmap:

1. User Interface and Ease of Use:

- Zenmap: Offers a graphical user interface (GUI) for ease of use.
- Nmap: Command-line-based and less intuitive for beginners.

2. Flexibility and Customization of Scan Options:

- Zenmap: Provides pre-configured scan profiles and options for customization.
- Nmap: Highly flexible with extensive control over scan parameters via command line.

3. Presentation and Interpretation of Scan Results:

- Zenmap: Presents results in a user-friendly, graphical format.
- Nmap: Generates text-based reports, which may require additional tools for interpretation.

4. Observations and Findings:

- Zenmap is user-friendly and suitable for beginners.
- Nmap offers advanced customization and control for experienced users.
- Zenmap can serve as a stepping stone to learning Nmap's capabilities.

THE END!