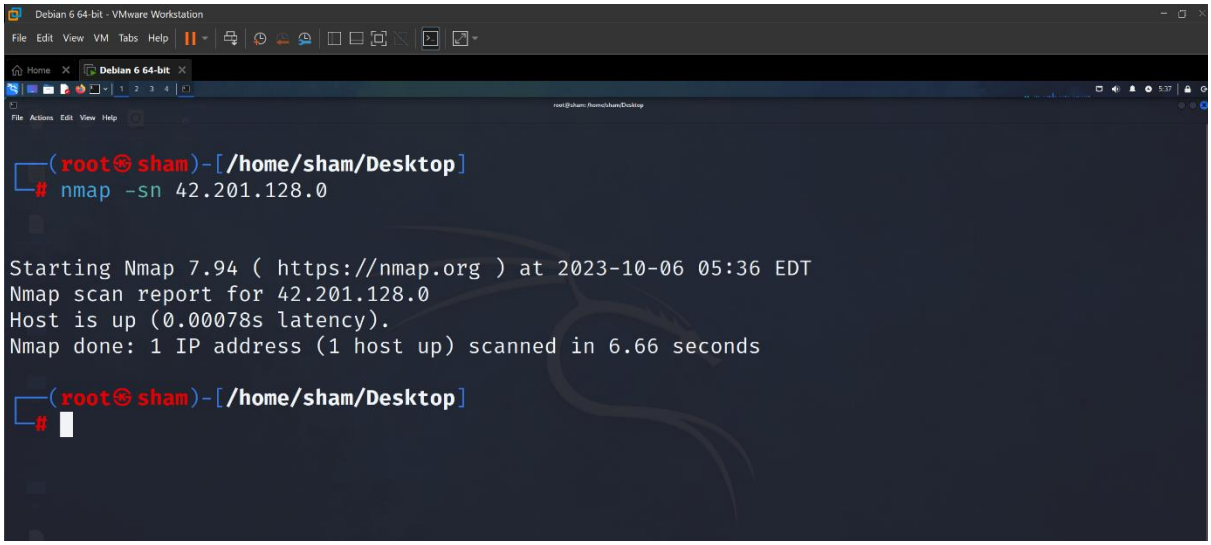
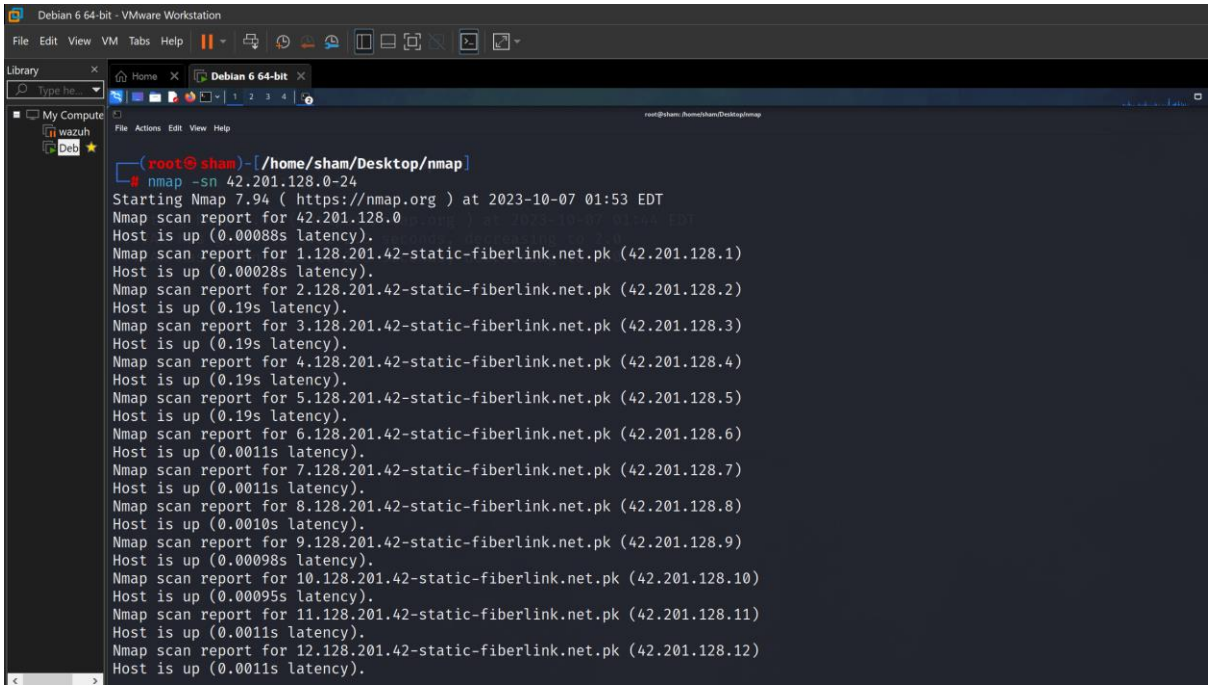
Activity 1 : Task Instructions:

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

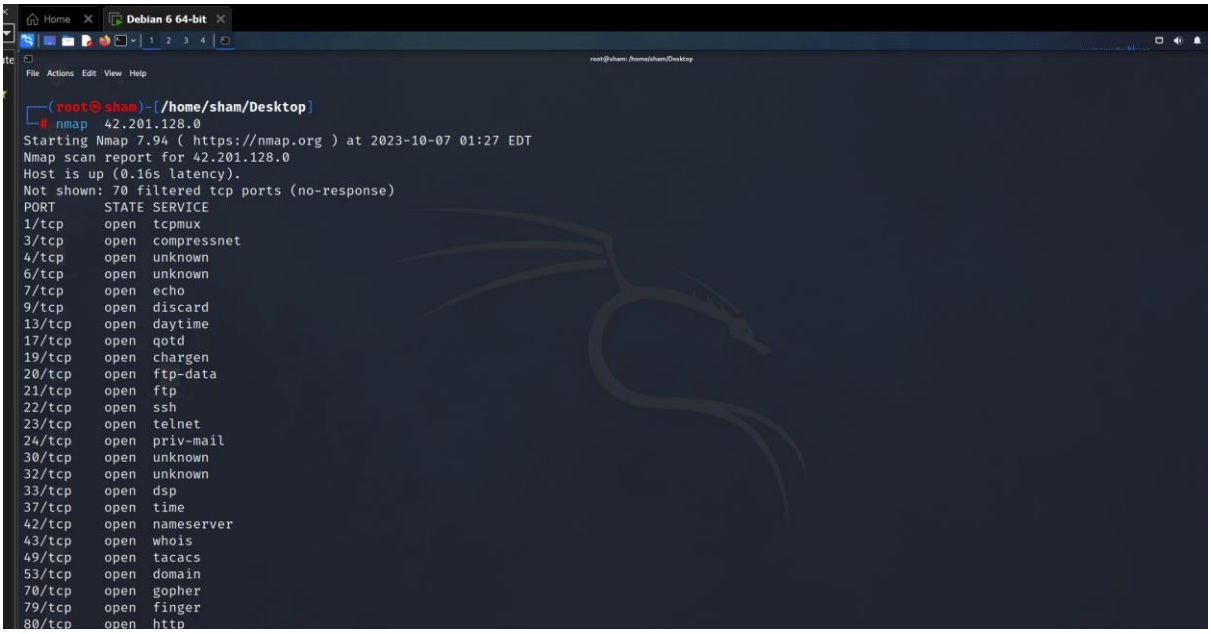
Scan for one IP : 42.201.128.0



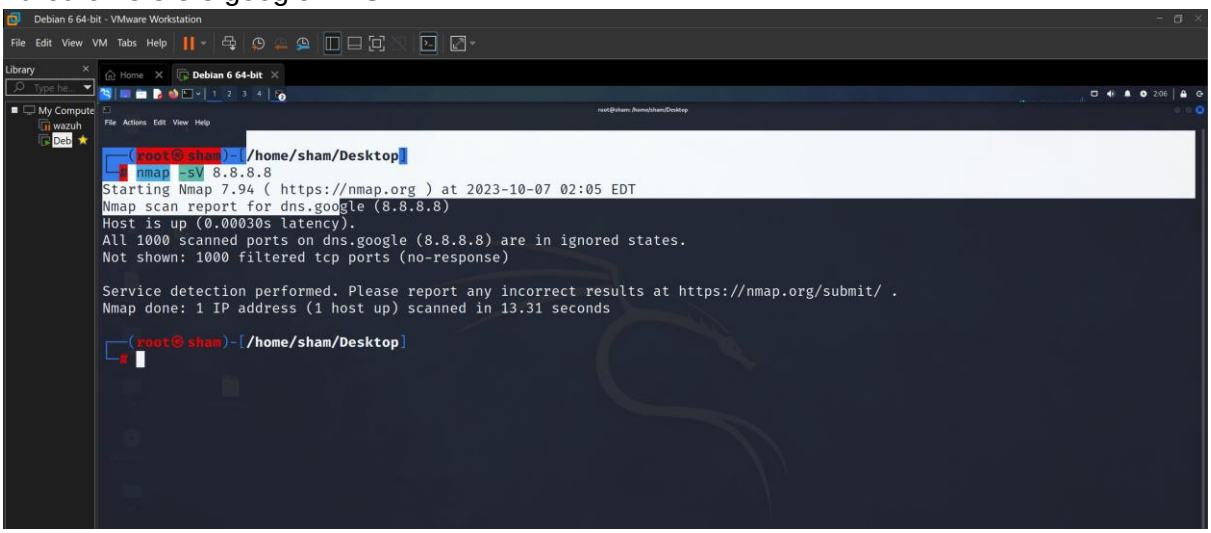
• Objective: Identify all active devices within the specified IP range.Nmap scan for 25 hosts



2. **<u>Basic Port Scanning:</u>** Command: nmap [Target IP]

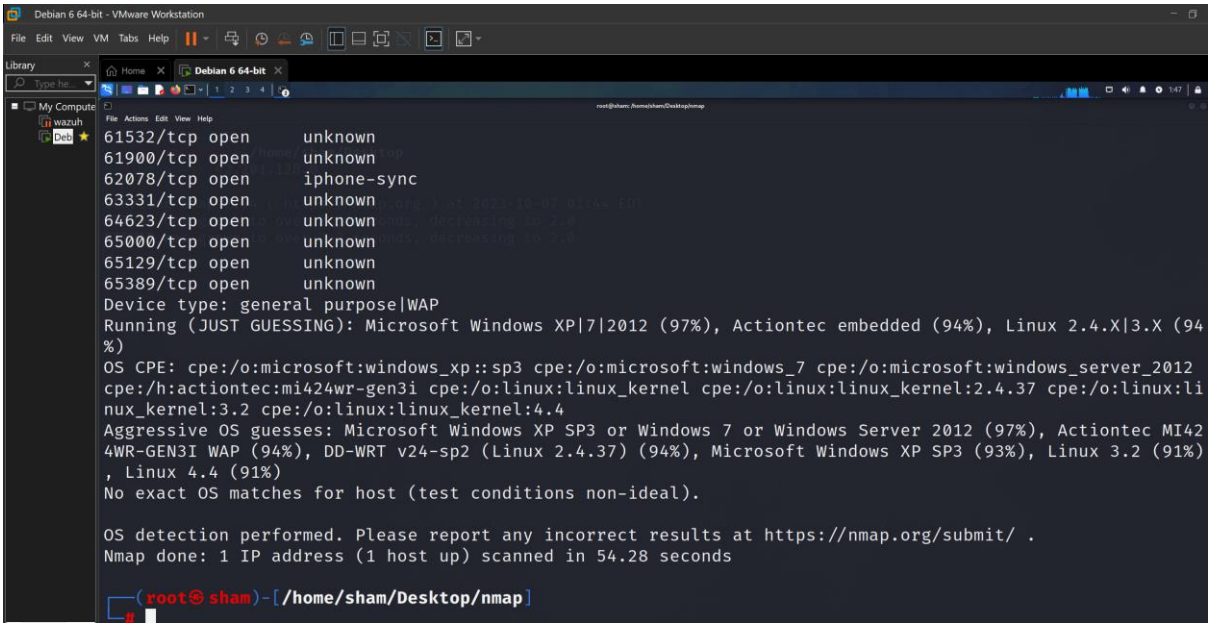


3. **<u>Service Version Detection</u>**: Command: nmap -sV [Target ip]
   I tried on 8.8.8.8 google DNS



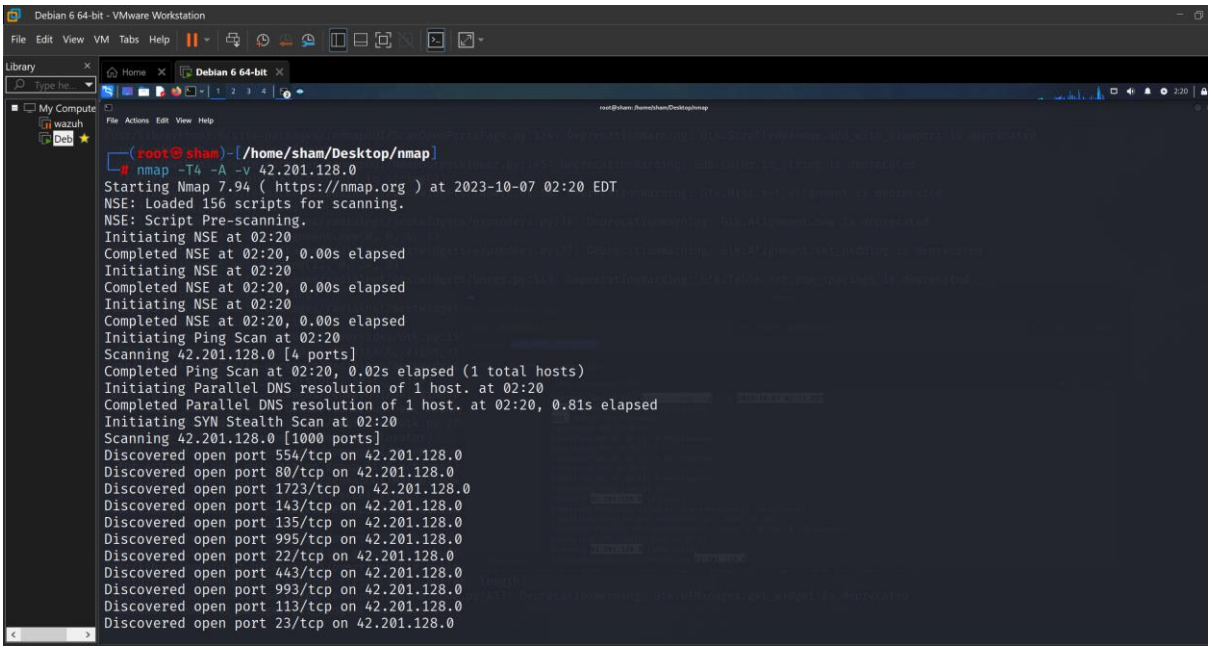
<u>4.Operating System Detection</u>:

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



5. Aggressive Scan:

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

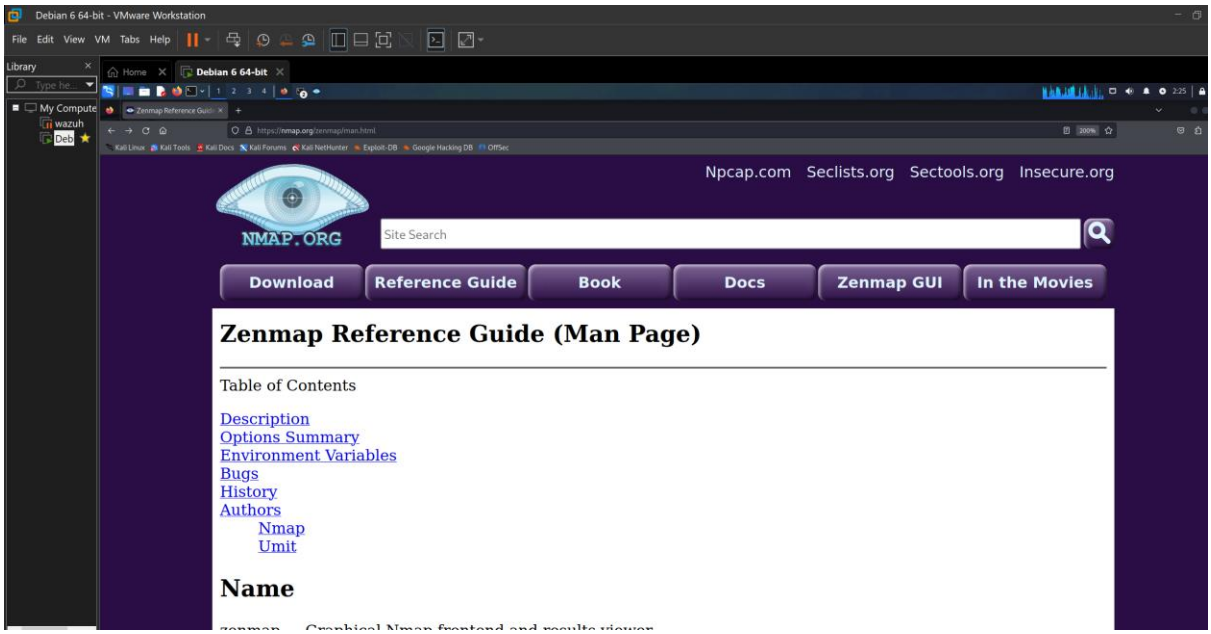


Activity 2: Task Instructions:

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 PCKAGE_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 Alient, 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 competition of Zenmap installation:

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

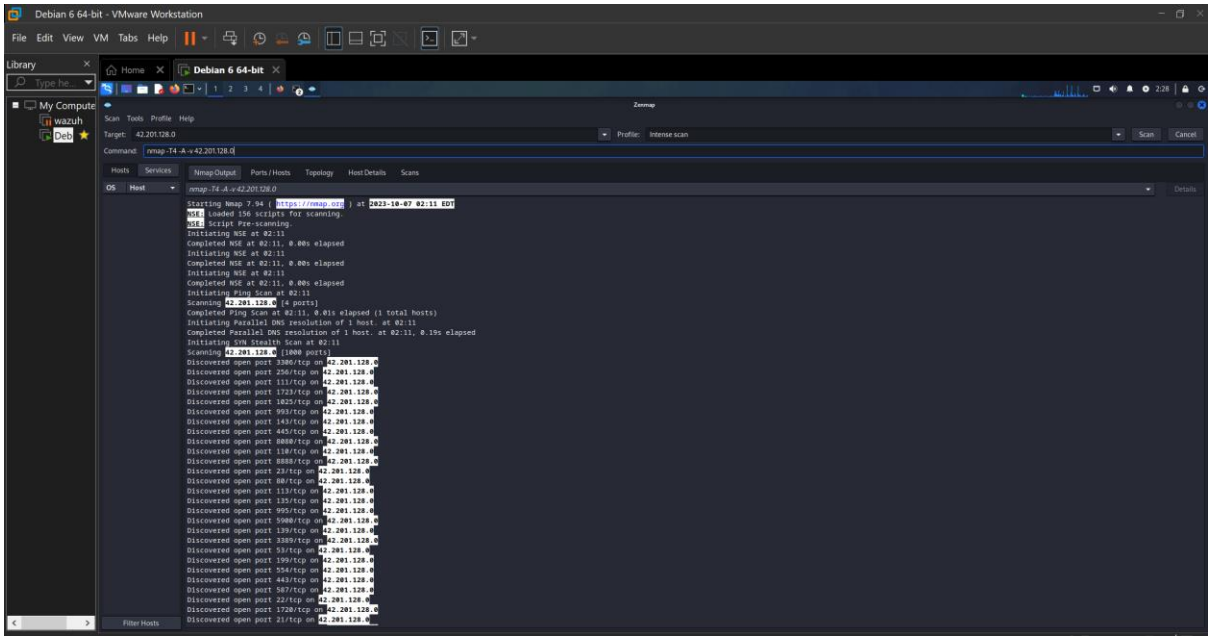
Zenmap is now ready for use. You can get started with it by simply searching for it from the Search bar or running the command line.

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

Run: $sudo zenmap

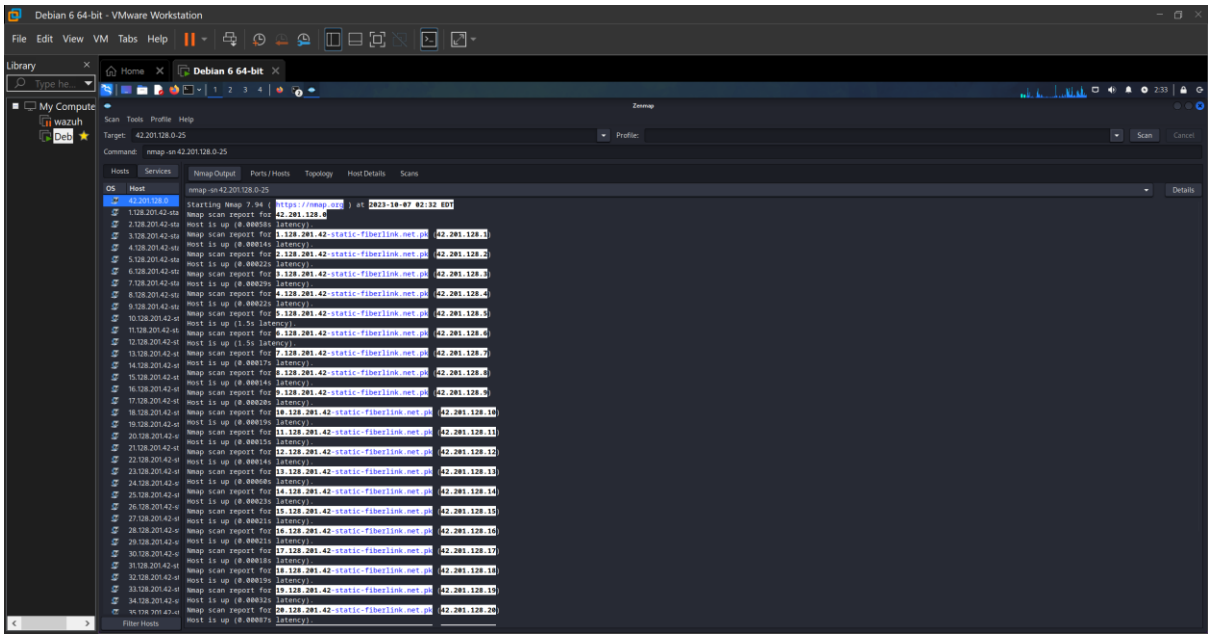
1. **Basic Host Discovery**:

- 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:

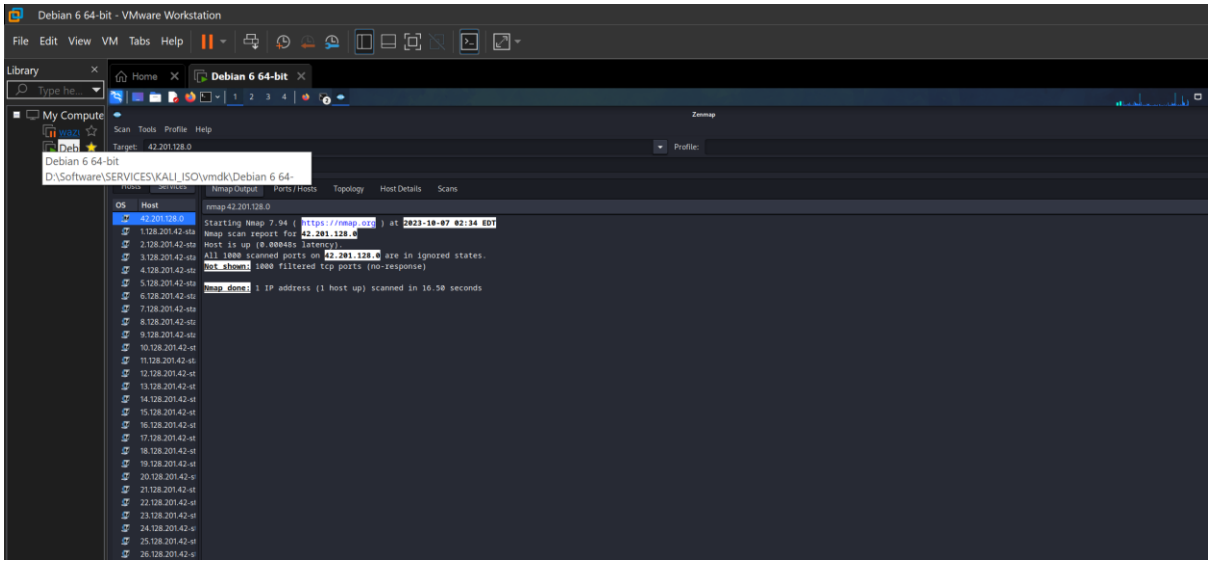
- Launch Zenmap
- Input your target IP range or specific IP address in the 'Target' field
- Select a scan profile, for instance, 'Quick Scan'.
- Initiate the scan and wait for it to complete.
- Review and save the results.



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!