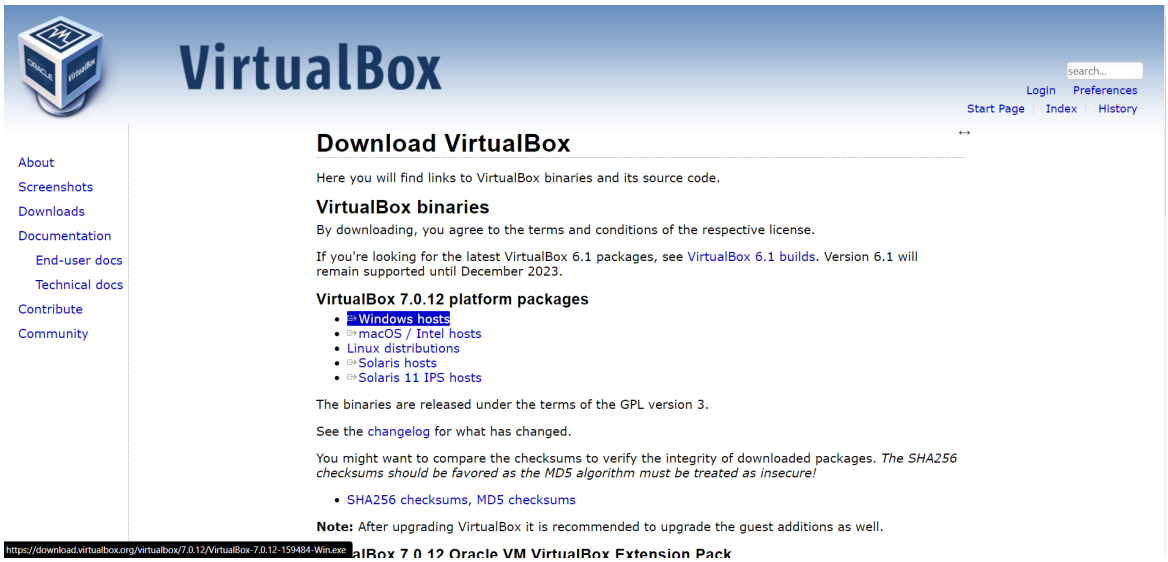
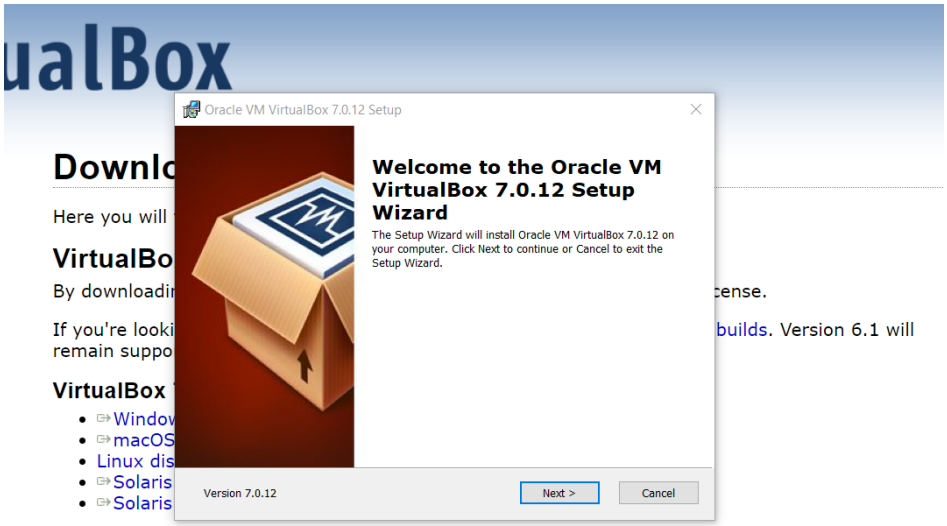
Software and Cybersecurity (CS/IT 445)

Name - Aradhya Mishra
ROLL NO - 202051034
Lab Assignment - 7

Task - Installation of the Kali Linux

1. Firstly install Virtual Box -





Here you will

VirtualBo

By downloadi cense.

If you're looki builds. Version 6.1 will remain suppo

VirtualBox

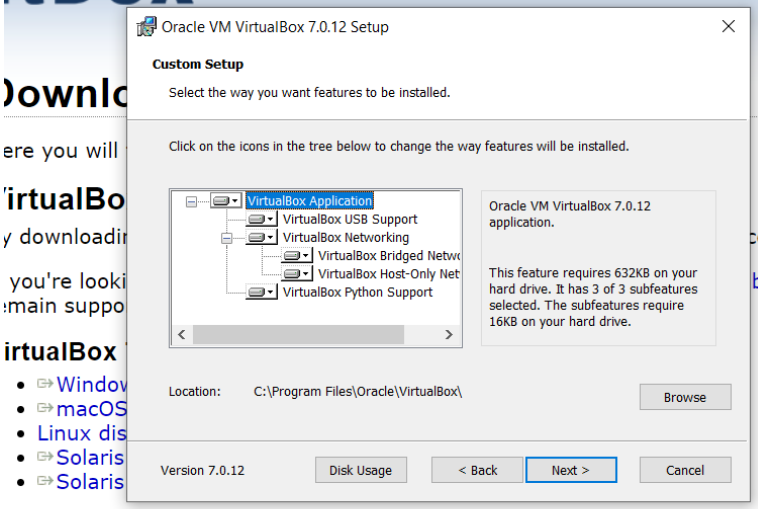
- Windov
- macOS
- Linux dis
- Solaris
- Solaris

The binaries are released under the terms of the GPL version 3.

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA2 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums



ere you will

irtualBo

y downloadi cense.

you're looki builds. Version 6.1 w
main suppo

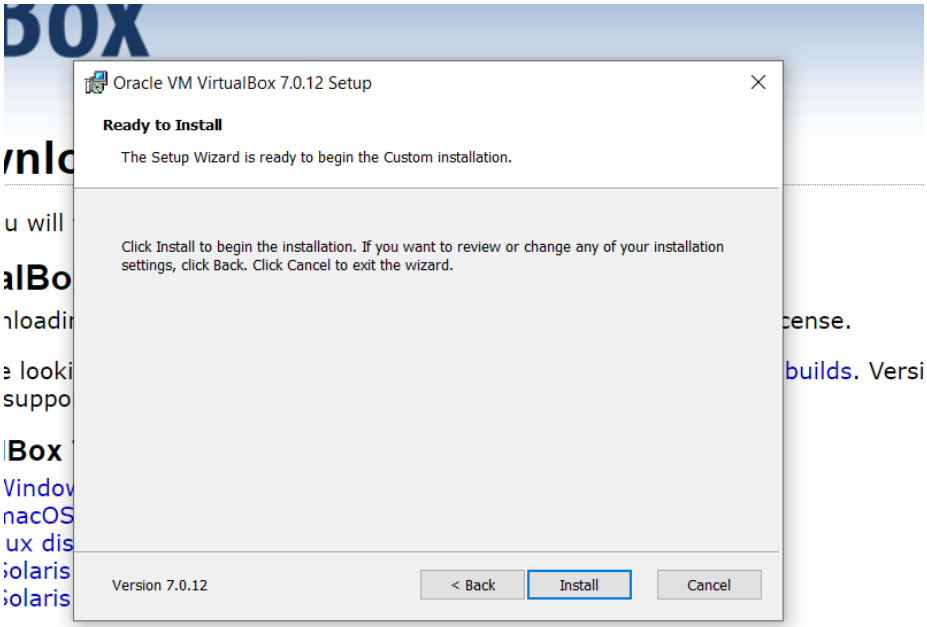
irtualBox

- Windov
- macOS
- Linux dis
- Solaris
- Solaris

he binaries are released under the terms of the GPL version 3.

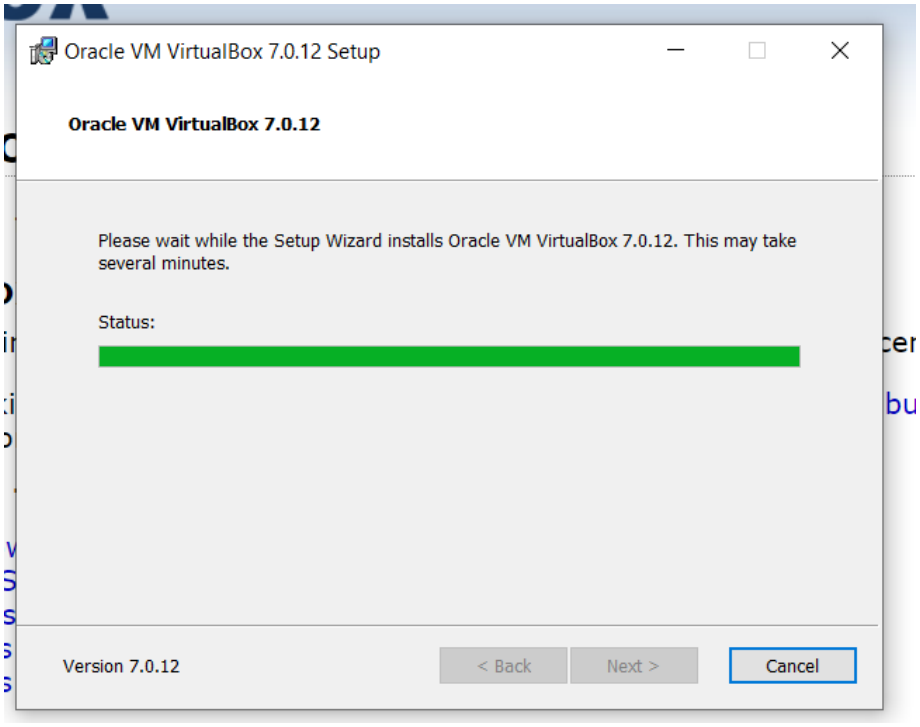
ee the changelog for what has changed.

ou might want to compare the checksums to verify the integrity of downloaded packages. *The*



aries are released under the terms of the GPL version 3.

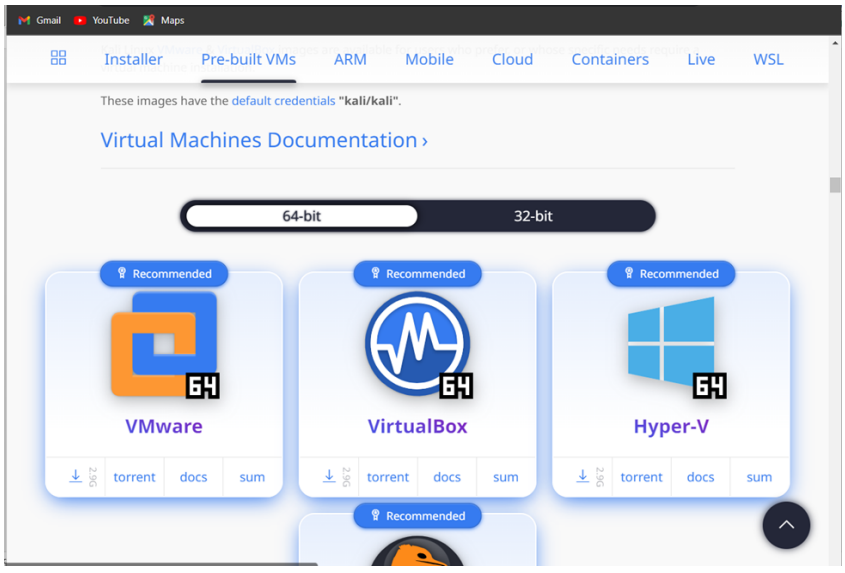
changelog for what has changed.



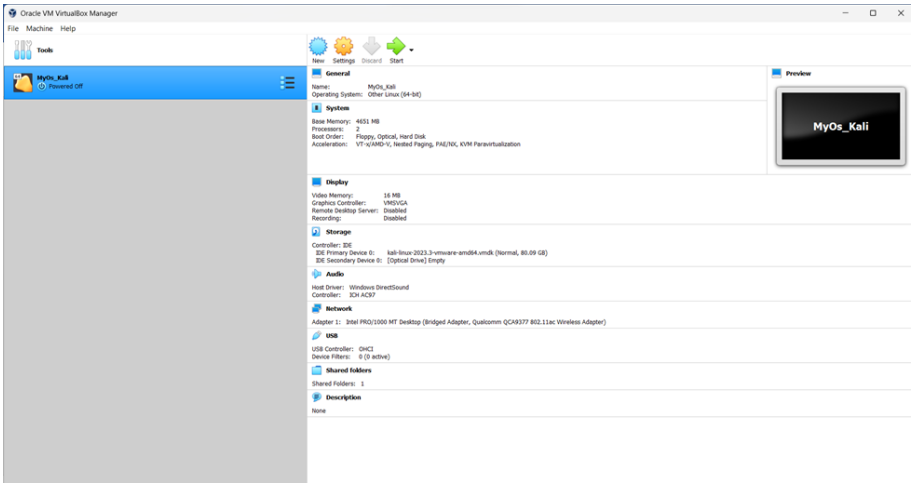
After Successfully Installation of Virtual Box Now Install Kali Linux .

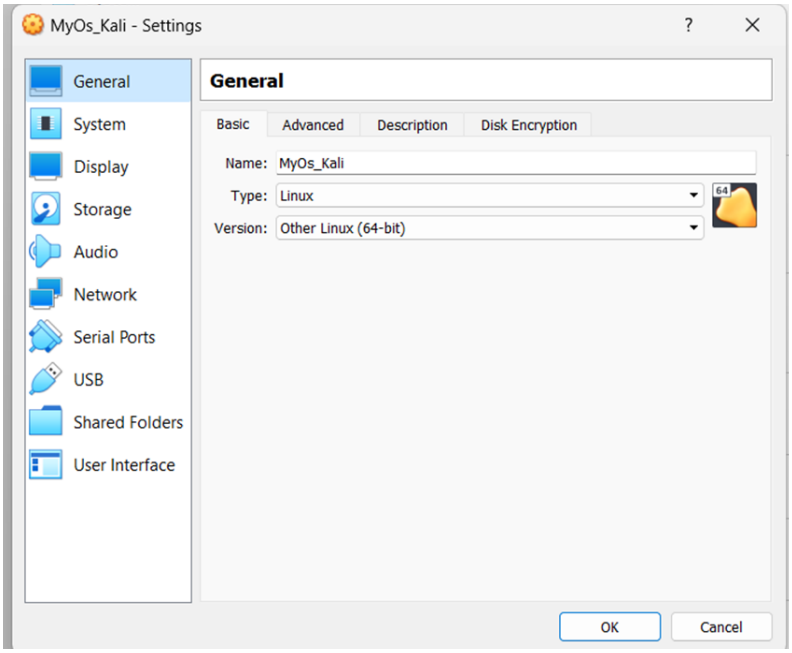
Now, next step to install Kali Linux-

Step 1: Download the Kali Linux (VMware) package from its official website: https://www.kali.org/downloads/

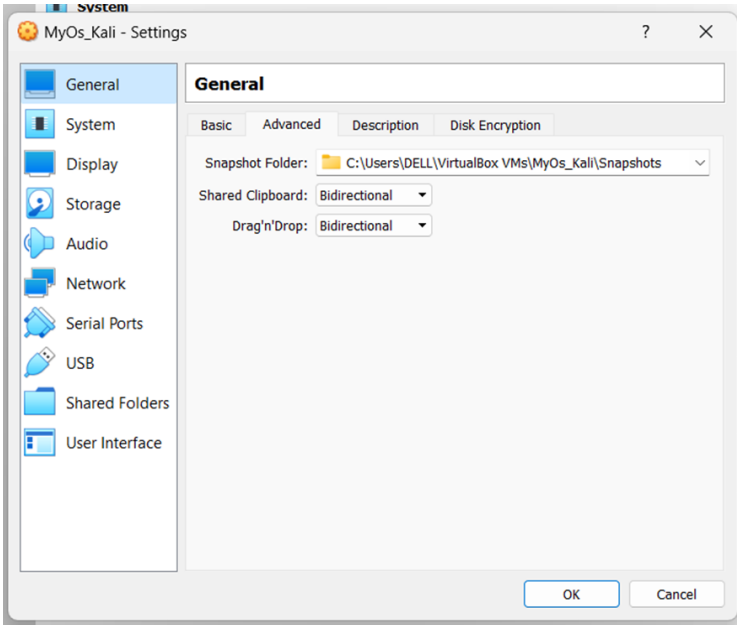


Step 2: Click VirtualBox -> New and create new Linux OS. And select necessary resources(eg: 2 CPU, 4GB RAM, etc.)

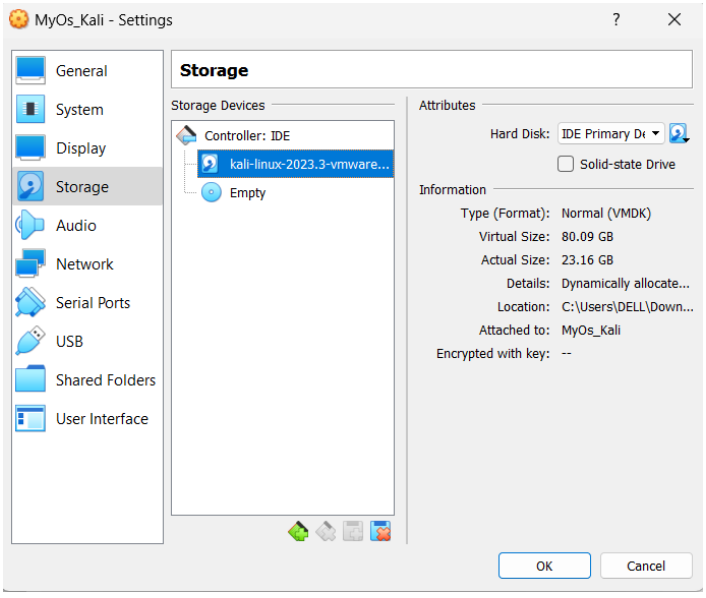




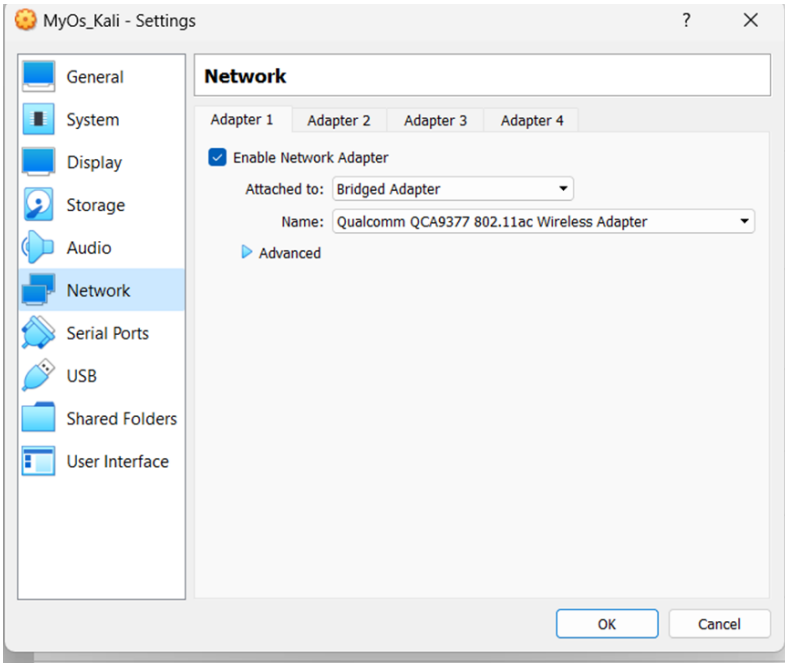
Step 3: Select Bidirectional in Shared Clipboard and Drag and Drop.



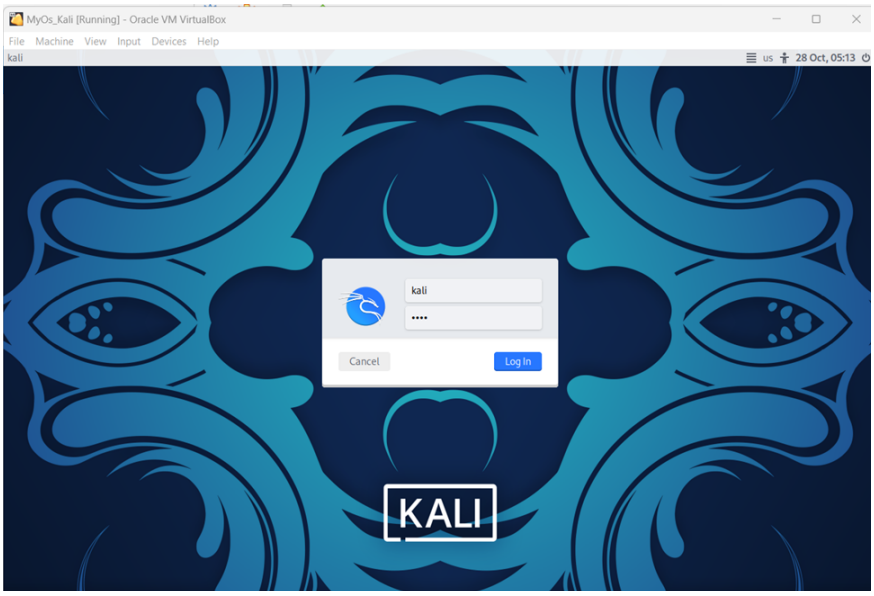
Step 4: In the Storage, select the storage file of Kali linux which we have already downloaded.



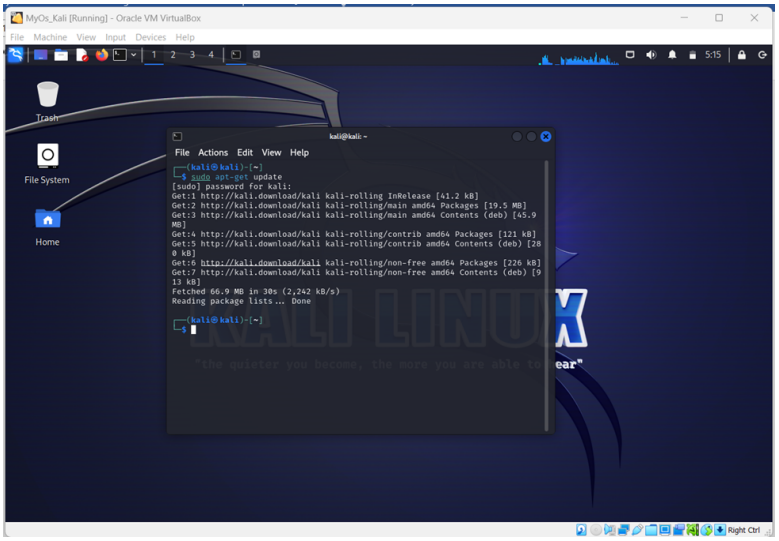
Step 5: In the Network, select the Bridged Adaptor.



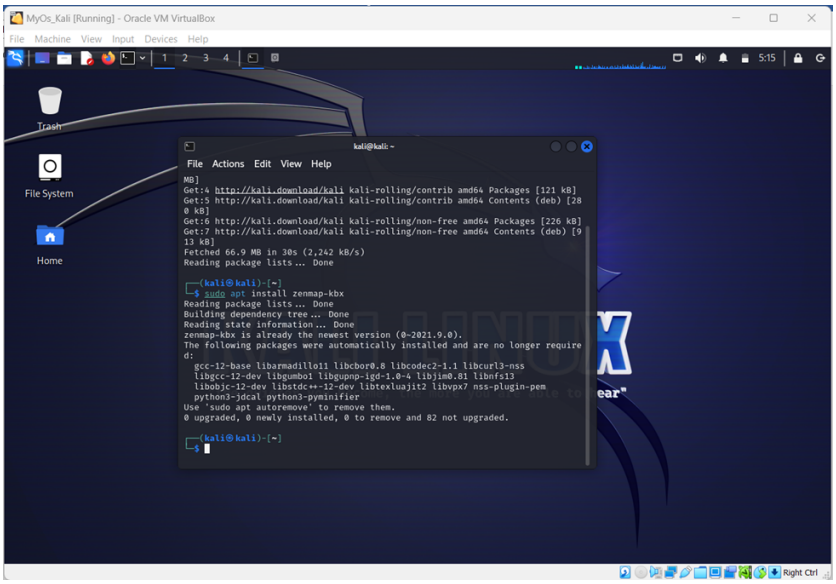
Step 6: Run the Kali-linux OS. And Enter the default username **kali** and password **kali**.



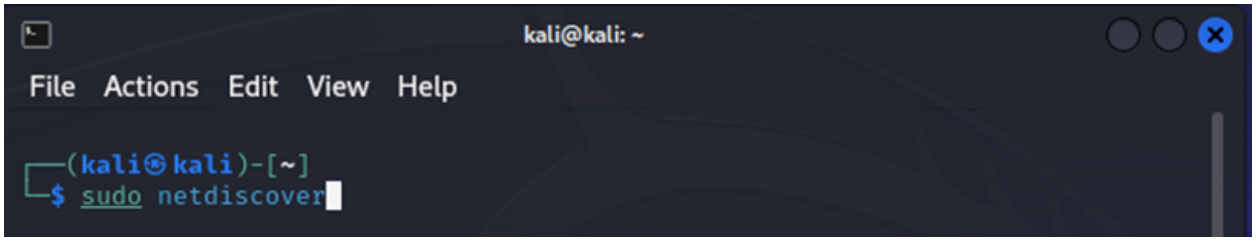
Step 7: Now to upgrade the tools, type “sudo apt-get upgrade” and the new packages will be downloaded.

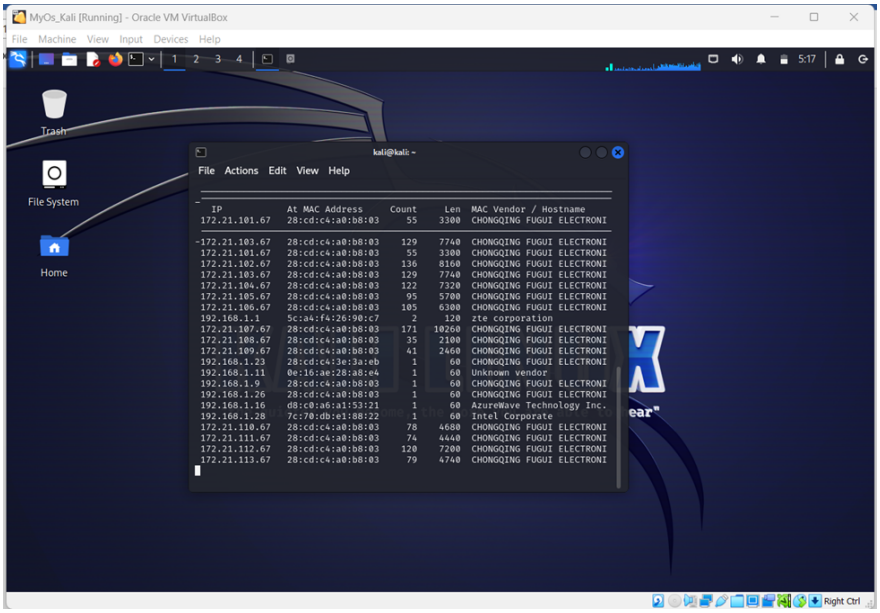


Step 8: Install the zenmap, type “sudo apt-install zenmap-kbx”

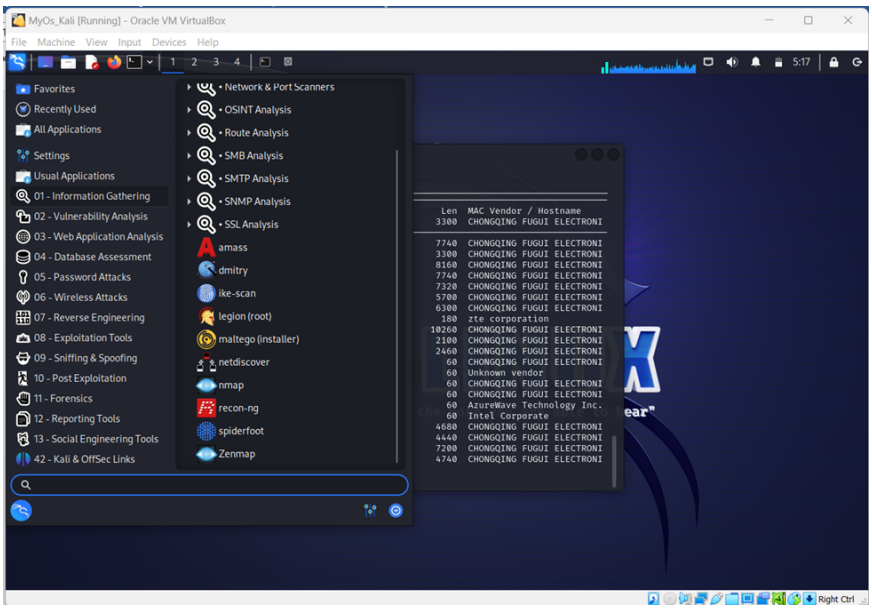


Step 9: Discover the IP which can be made as target, type “sudo netdiscover”



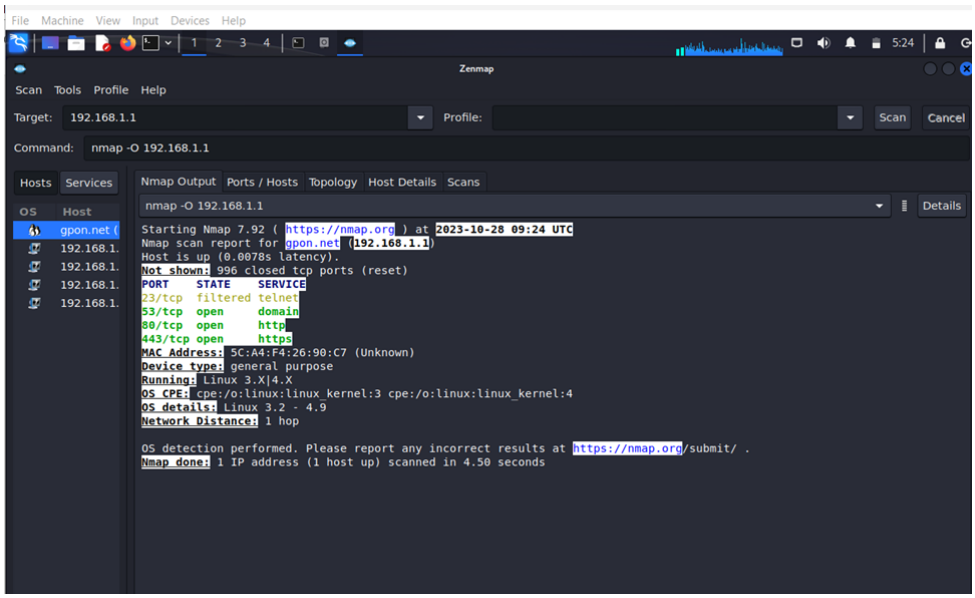


Step 10: Open zenmap.

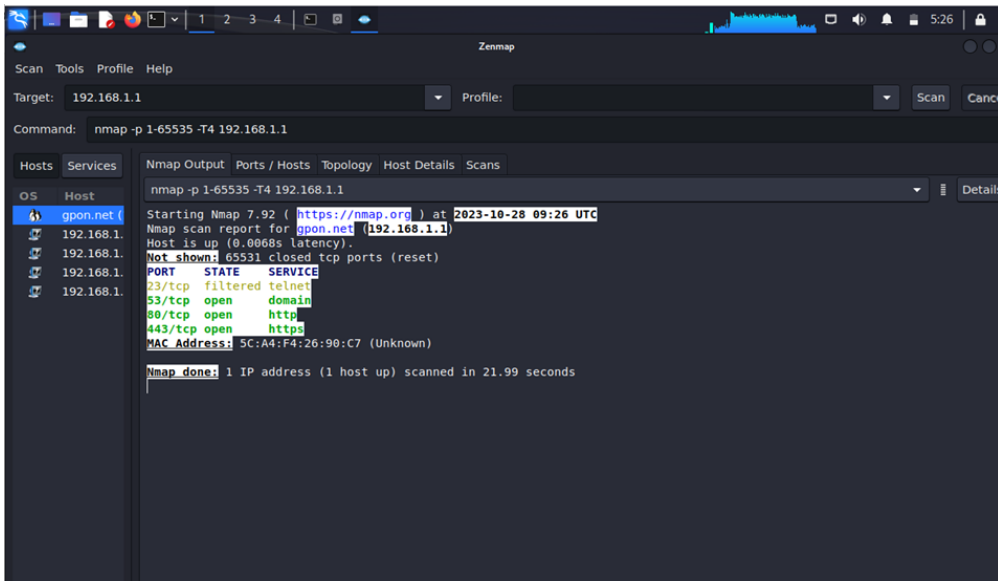


Step 11: The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable “-O”. For more information, use this link: https://nmap.org/book/man-os-detection.html

The command that we will use is: **nmap -O 192.168.1.1**



Step 12: Next, open the TCP and UDP ports. To scan all the TCP ports based on NMAP, use the following command: nmap -p 1-65535 -T4 192.168.1.1



Step 13: Now to see the SYN scan in practice, use the parameter –sS in NMAP. Following is the full command – **nmap -sS -T4 192.168.1.1**