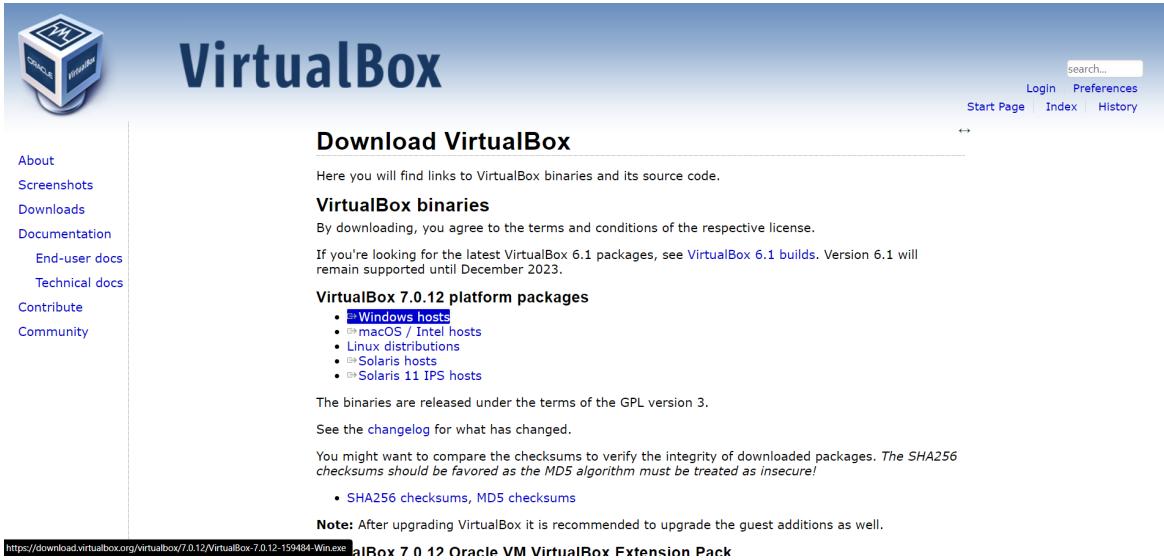


Software and Cybersecurity (CS/IT 445)

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

Task - Installation of the Kali Linux

1. Firstly install Virtual Box -



The screenshot shows the official VirtualBox website at <https://www.virtualbox.org/>. The main header features the "VirtualBox" logo. On the left, there's a sidebar with links to "About", "Screenshots", "Downloads", "Documentation", "End-user docs", "Technical docs", "Contribute", and "Community". The main content area has a large heading "Download VirtualBox". Below it, a sub-section titled "VirtualBox binaries" provides links to download binaries for various platforms. A note states that version 6.1 will remain supported until December 2023. Another section, "VirtualBox 7.0.12 platform packages", lists download links for "Windows hosts", "macOS / Intel hosts", "Linux distributions", "Solaris hosts", and "Solaris 11 IPS hosts". A note mentions that binaries are released under the terms of the GPL version 3. There's also a link to the "changelog". A note about SHA256 checksums is present, along with a note about upgrading guest additions. At the bottom, a link to the "VirtualBox Extension Pack" is shown.



Download

Here you will

VirtualBox

By downloading

If you're looking
remain support

VirtualBox

- Windows
- macOS
- Linux distros
- Solaris
- Solaris

Version 7.0.12

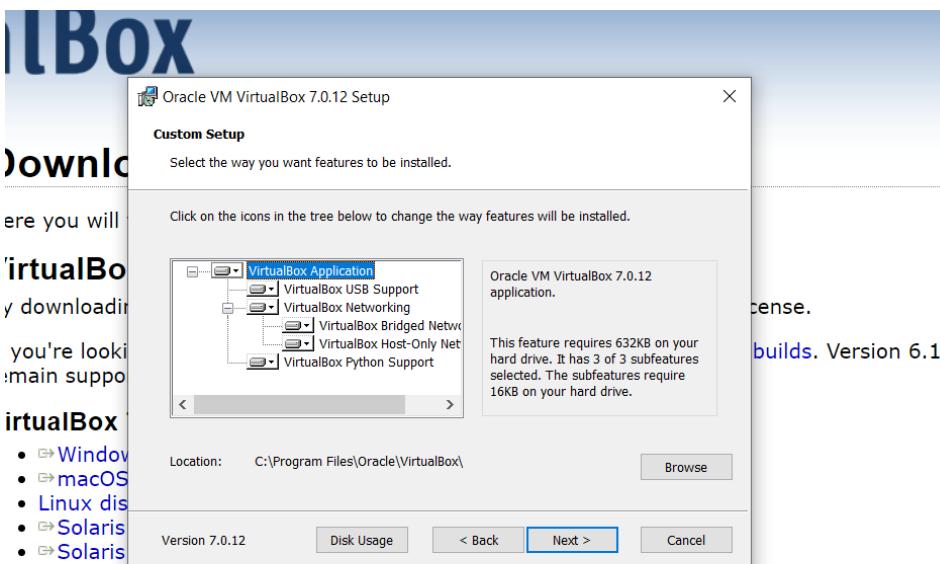
Next > Cancel

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 SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

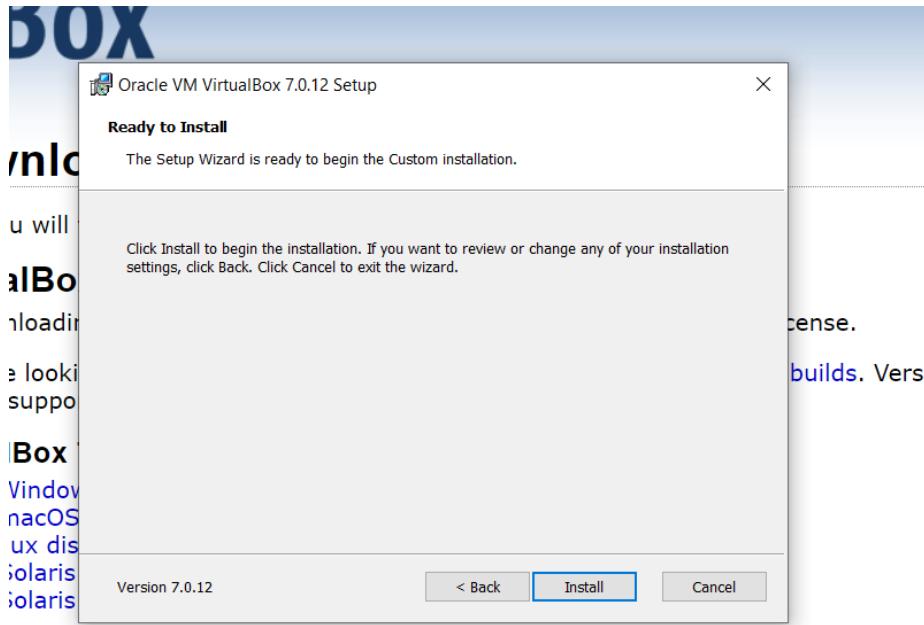
- [SHA256 checksums](#)
- [MD5 checksums](#)



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

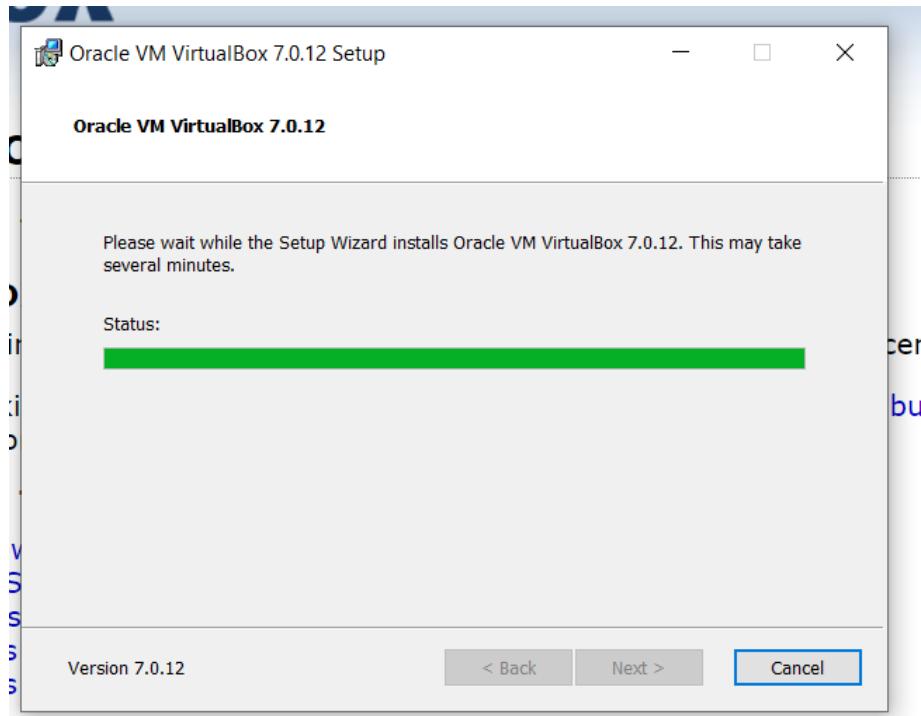
See the [changelog](#) for what has changed.

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



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

[changelog](#) for what has changed.

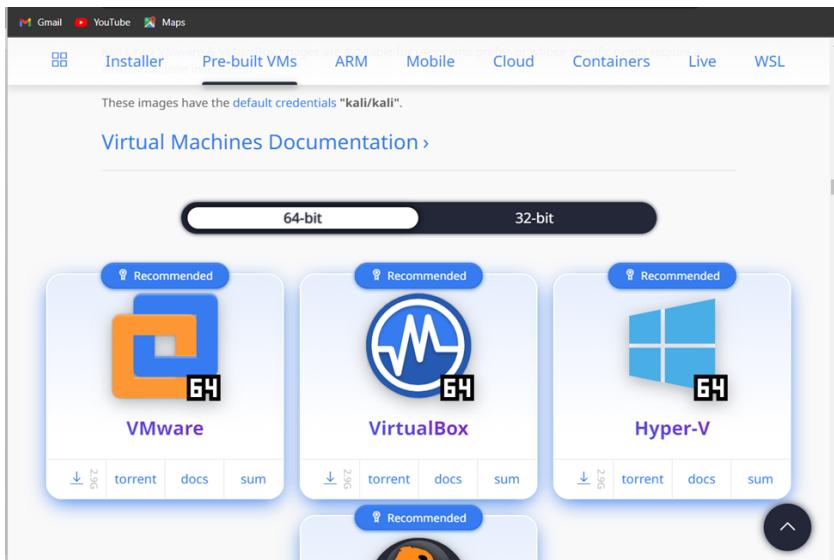




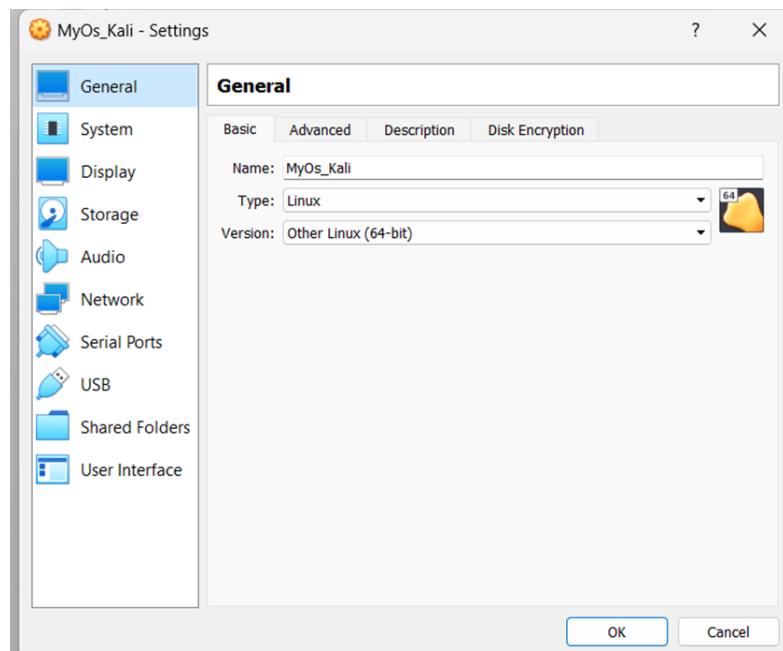
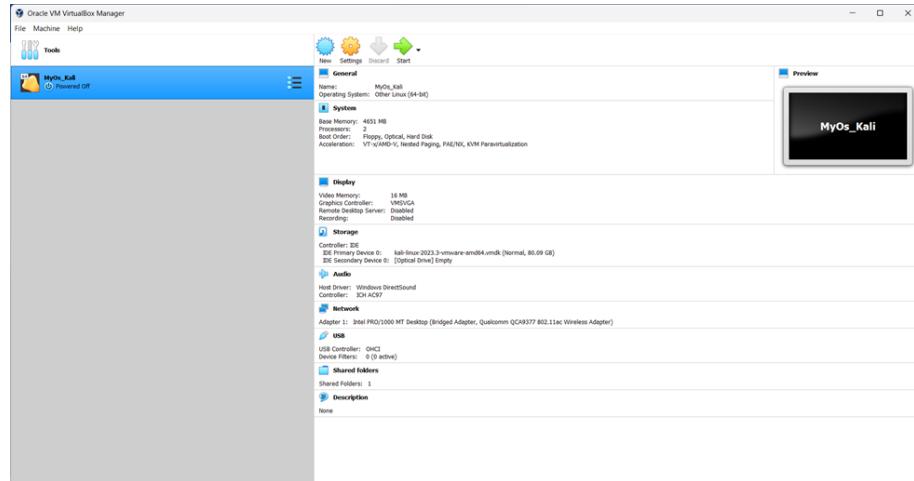
After Successfully Installation of Virtual Box Now Install Kali Linux .

Now, next step to install Kali Linux-

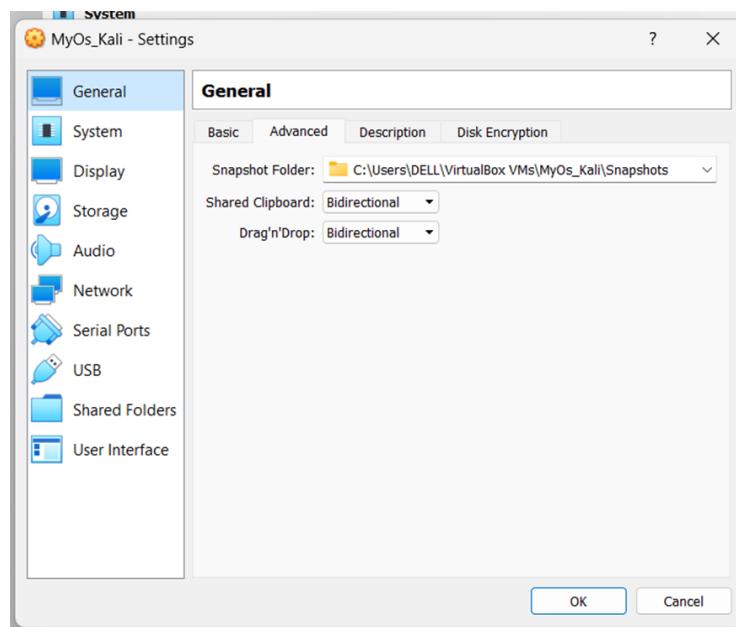
Step 1: Download the Kali Linux (VMware) package from its official website:
<https://www.kali.org/downloads/>



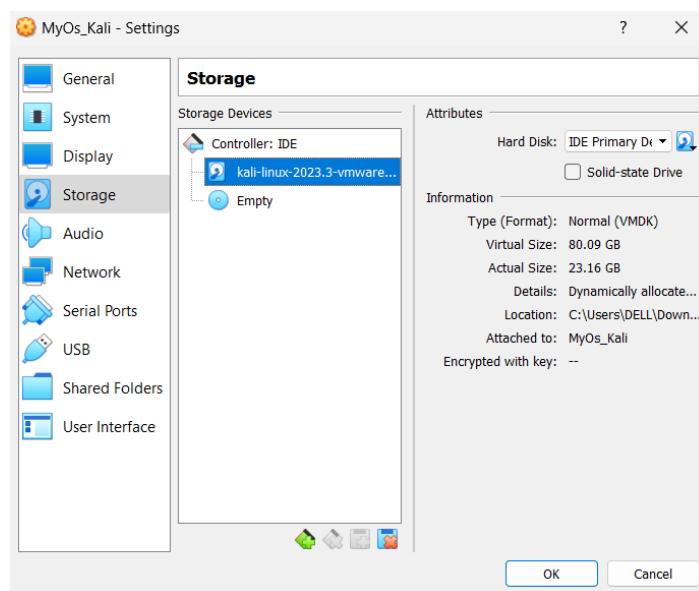
Step 2: Click VirtualBox -> New and create new Linux OS. And select necessary resources(eg: 2 CPU, 4GB RAM, etc.)



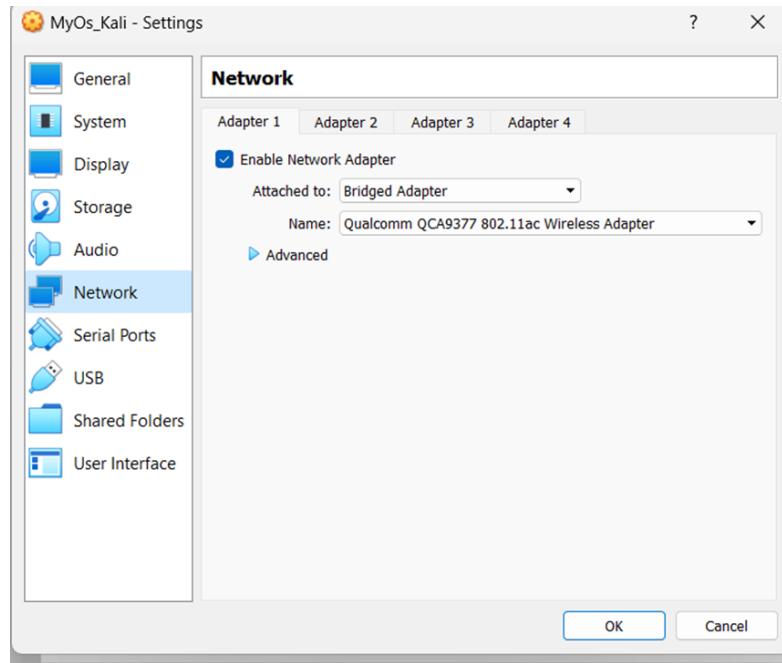
Step 3: Select Bidirectional in Shared Clipboard and Drag and Drop.



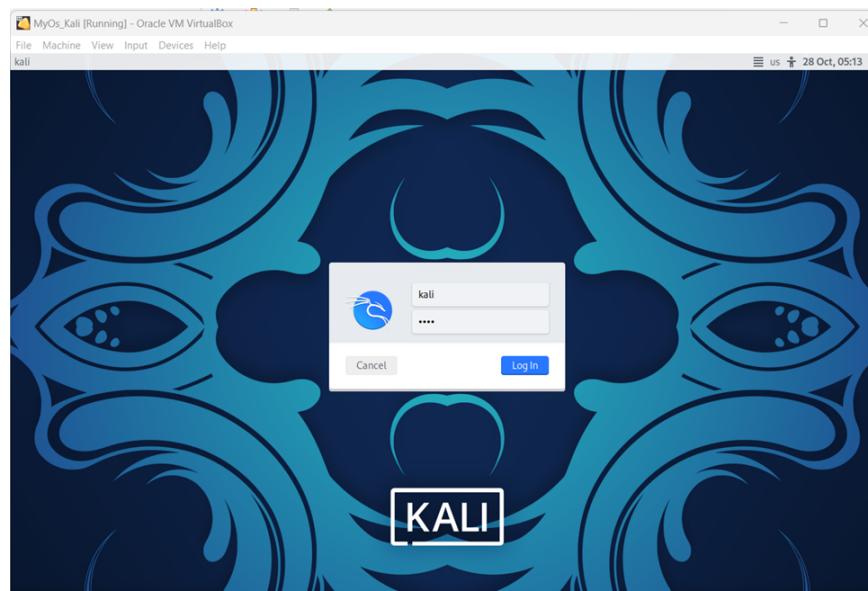
Step 4: In the Storage, select the storage file of Kali linux which we have already downloaded.



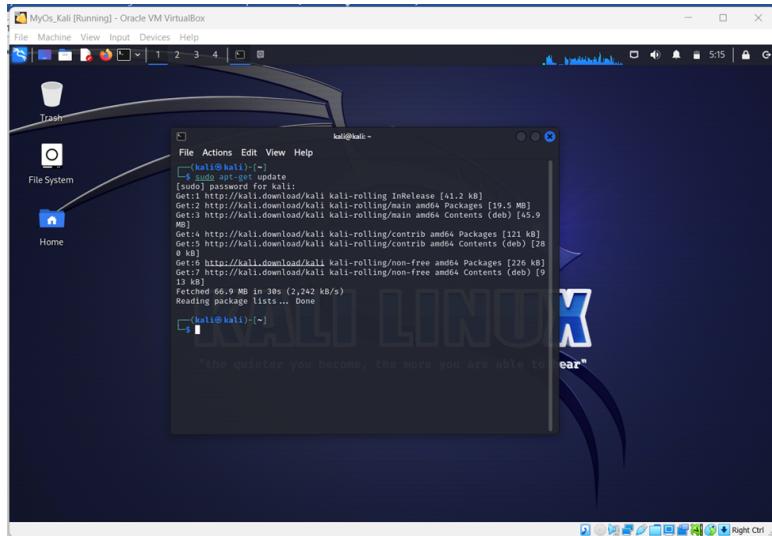
Step 5: In the Network, select the Bridged Adaptor.



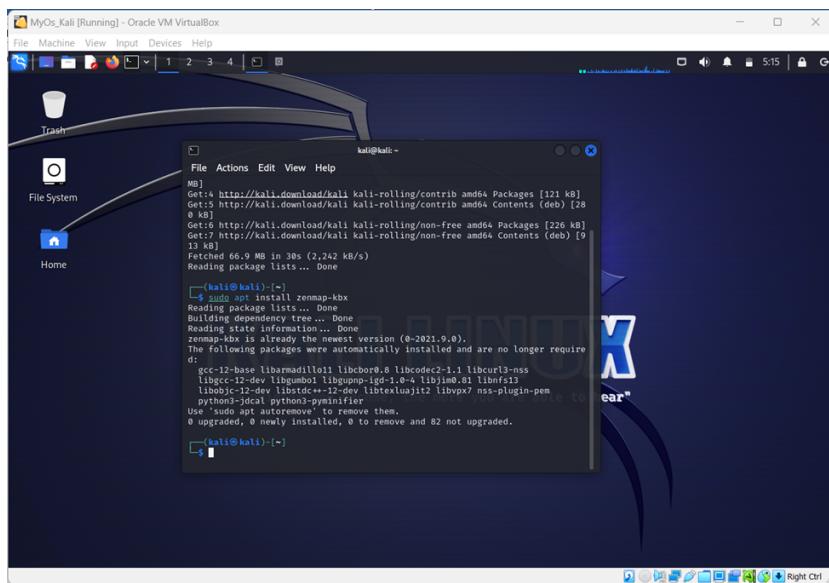
Step 6: Run the Kali-linux OS. And Enter the default username **kali** and password **kali**.



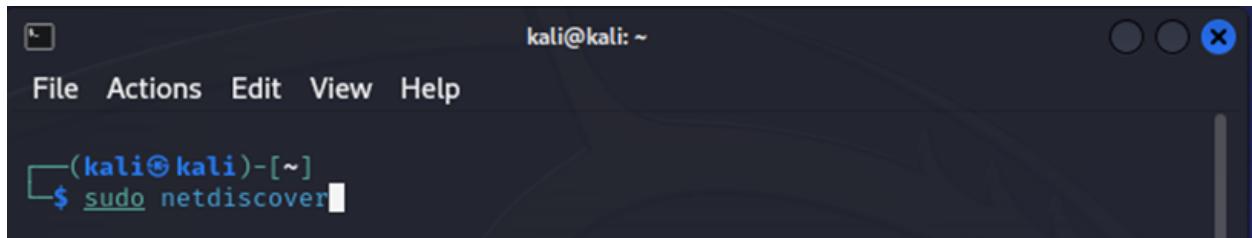
Step 7: Now to upgrade the tools, type “sudo apt-get upgrade” and the new packages will be downloaded.



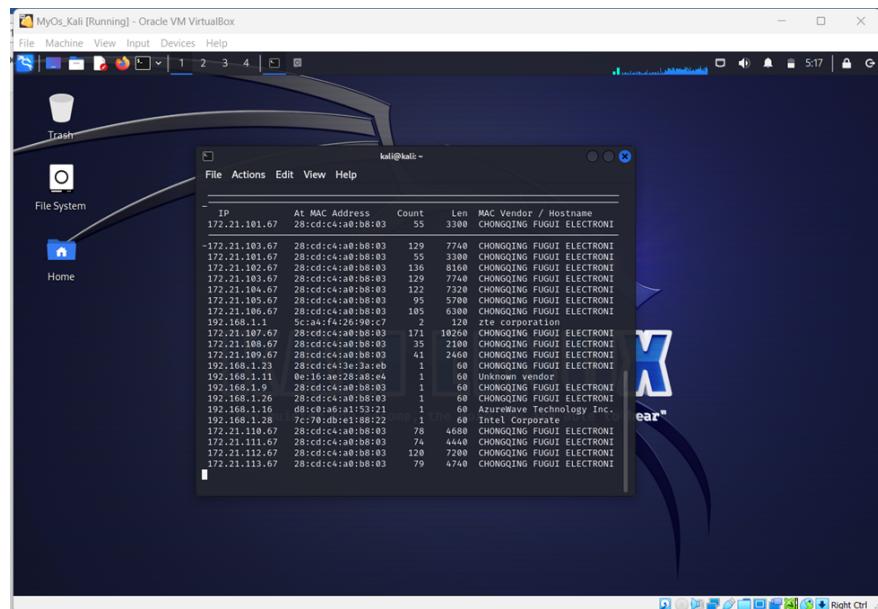
Step 8: Install the zenmap, type “sudo apt-install zenmap-kbx”



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

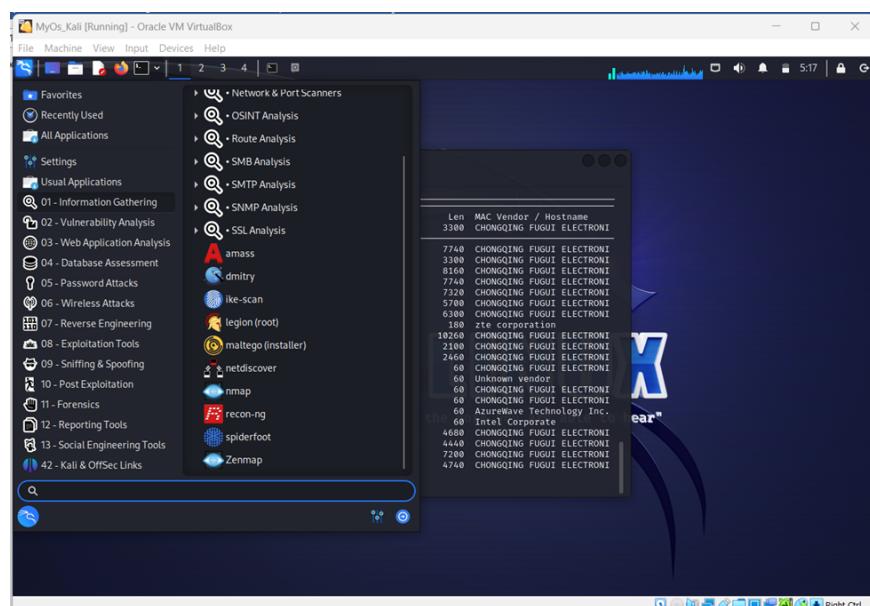


```
kali@kali: ~
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ sudo netdiscover
```



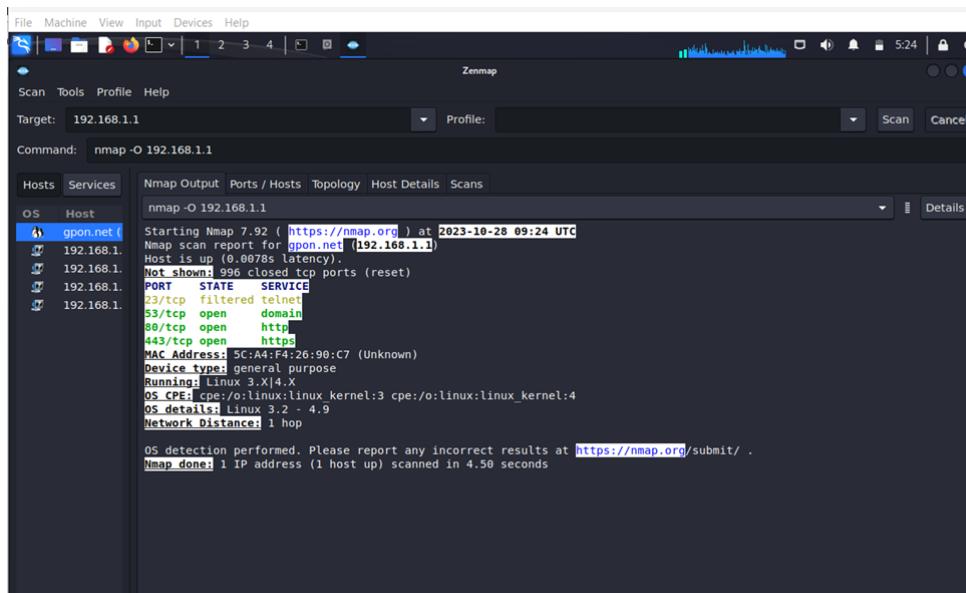
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
172.21.101.67	28:c:d:c:a:b:b:03	55	3308	CHONGMING FUGUI ELECTRONI
172.21.101.67	28:c:d:c:a:b:b:03	55	3308	CHONGMING FUGUI ELECTRONI
172.21.102.67	28:c:d:c:a:b:b:03	136	8168	CHONGMING FUGUI ELECTRONI
172.21.103.67	28:c:d:c:a:b:b:03	30	7748	CHONGMING FUGUI ELECTRONI
172.21.104.67	28:c:d:c:a:b:b:03	32	7748	CHONGMING FUGUI ELECTRONI
172.21.105.67	28:c:d:c:a:b:b:03	95	5708	CHONGMING FUGUI ELECTRONI
172.21.106.67	28:c:d:c:a:b:b:03	105	6308	CHONGMING FUGUI ELECTRONI
192.168.1.1	9c:a:4:f:26:98:c7	7	128	zte corporation
172.21.107.67	28:c:d:c:a:b:b:03	35	10080	CHONGMING FUGUI ELECTRONI
172.21.108.67	28:c:d:c:a:b:b:03	35	2108	CHONGMING FUGUI ELECTRONI
172.21.109.67	28:c:d:c:a:b:b:03	41	2468	CHONGMING FUGUI ELECTRONI
192.168.1.23	28:c:d:c:a:3:e:0e	1	68	CHONGMING FUGUI ELECTRONI
192.168.1.11	0e:1:ae:28:a8:e0	1	68	Unknown vendor
192.168.1.24	28:c:d:c:a:b:b:03	1	68	CHONGMING FUGUI ELECTRONI
192.168.1.26	28:c:d:c:a:b:b:03	1	68	CHONGMING FUGUI ELECTRONI
192.168.1.16	08:c:0:a:6:a:15:21	1	68	AzureWave Technology Inc.
192.168.1.28	9c:70:db:e1:88:27	1	68	Intel Corporate
172.21.110.67	28:c:d:c:a:b:b:03	40	4080	CHONGMING FUGUI ELECTRONI
172.21.111.67	28:c:d:c:a:b:b:03	74	4440	CHONGMING FUGUI ELECTRONI
172.21.112.67	28:c:d:c:a:b:b:03	128	7200	CHONGMING FUGUI ELECTRONI
172.21.113.67	28:c:d:c:a:b:b:03	79	4748	CHONGMING FUGUI ELECTRONI

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**

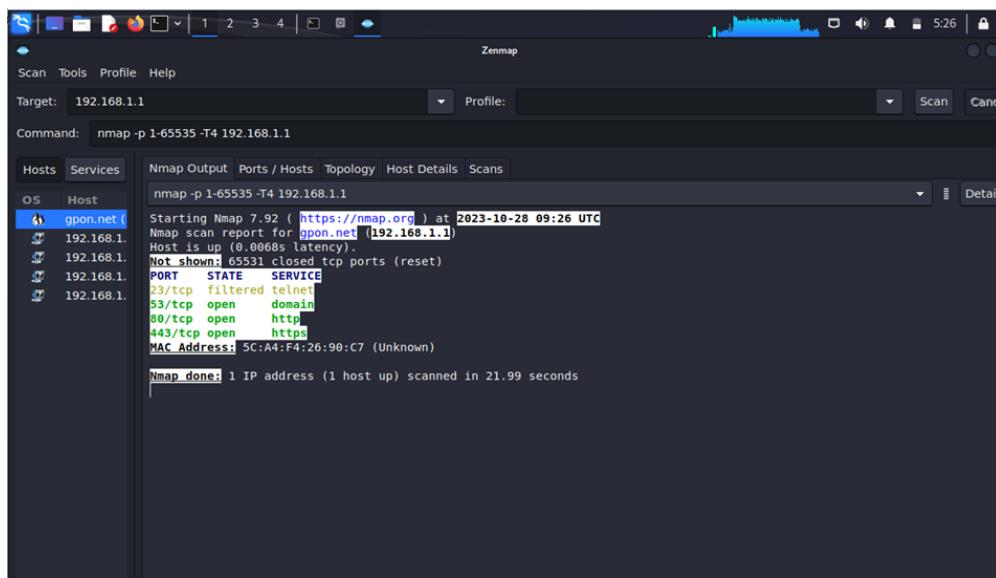


Zenmap interface showing the results of an OS detection scan on host 192.168.1.1. The output window displays the following details:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-28 09:24 UTC
Nmap scan report for gpon.net (192.168.1.1)
Host is up (0.0078s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE
23/tcp    filtered  telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
MAC Address: 5C:A4:F4:26:90:C7 (Unknown)
Device type: general-purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
```

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**

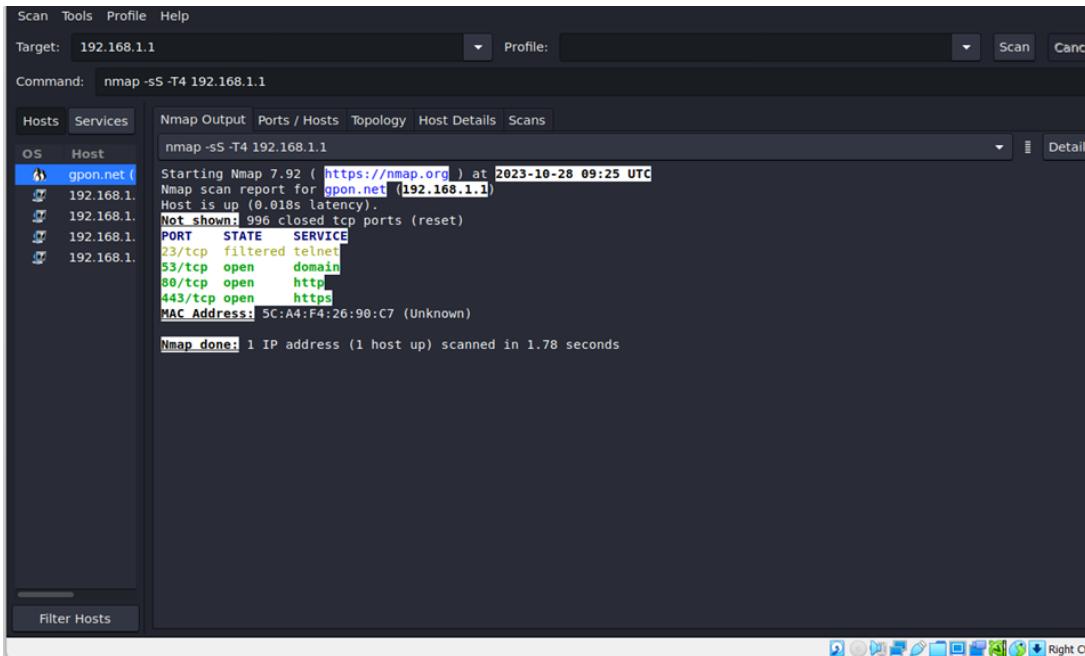


Zenmap interface showing the results of a full TCP port scan (-p 1-65535) on host 192.168.1.1. The output window displays the following details:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-28 09:26 UTC
Nmap scan report for gpon.net (192.168.1.1)
Host is up (0.0068s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE    SERVICE
23/tcp    filtered  telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
MAC Address: 5C:A4:F4:26:90:C7 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.99 seconds
```

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**



The screenshot shows the Nmap interface with the following details:

- Scan Menu:** Scan, Tools, Profile, Help
- Target:** 192.168.1.1
- Profile:** (empty)
- Command:** nmap -sS -T4 192.168.1.1
- Hosts Tab:** Shows a list of hosts under the OS column, including gpon.net (Windows 7 Home Premium SP1), 192.168.1.1, 192.168.1.2, 192.168.1.3, and 192.168.1.4.
- Services Tab:** Displays the Nmap Output. The output shows the following information:
 - Starting Nmap 7.92 (https://nmap.org) at 2023-10-28 09:25 UTC
 - Nmap scan report for gpon.net (192.168.1.1)
 - Host is up (0.018s latency).
 - Not shown: 996 closed tcp ports (reset)
 - PORT STATE SERVICE
 - 23/tcp filtered telnet
 - 53/tcp open domain
 - 80/tcp open http
 - 443/tcp open https
 - MAC Address: 5C:A4:F4:26:90:C7 (Unknown)
- Bottom Status:** Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds