

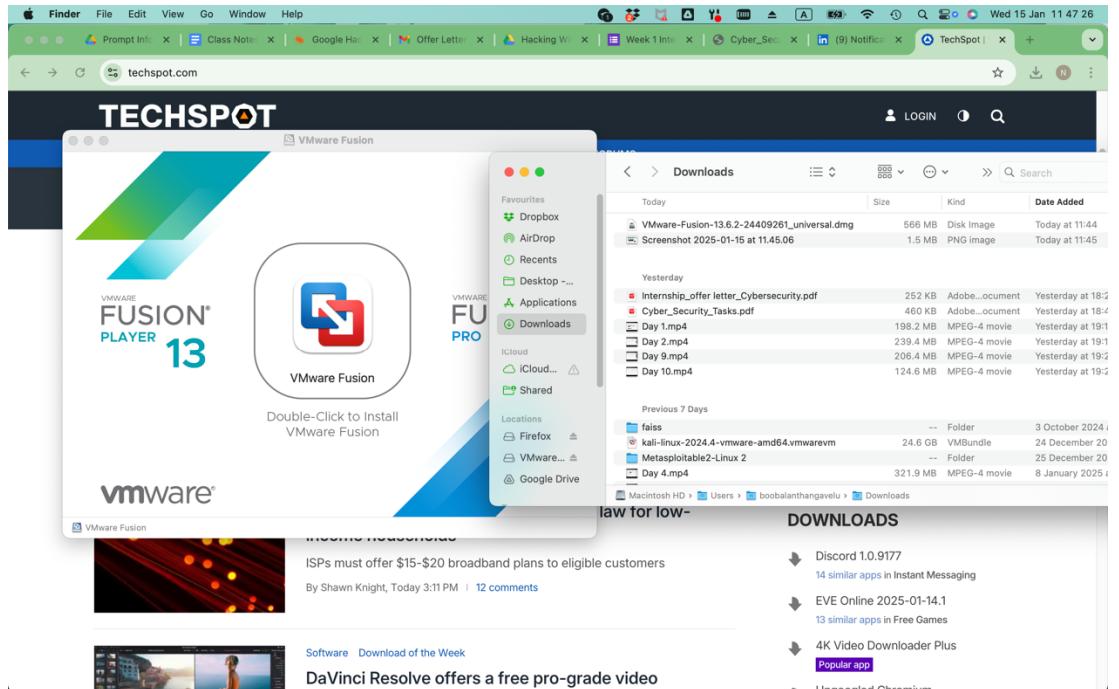
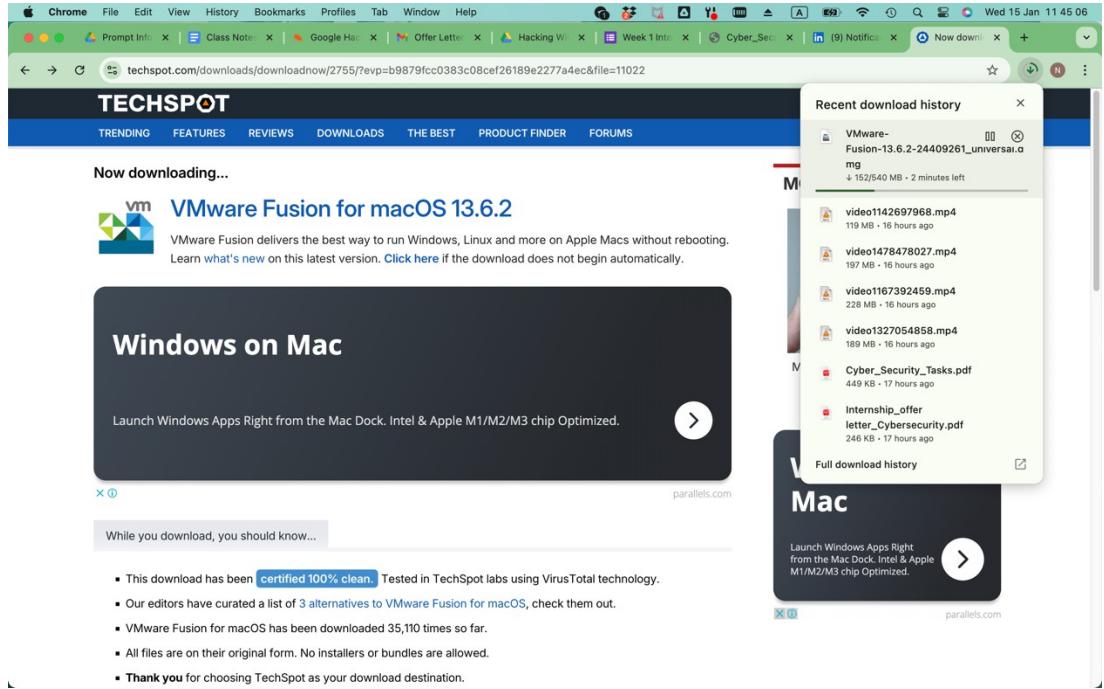
# Week 1: Introduction to Cybersecurity and Virtualization

## Cybersecurity Lab Setup Reports

### Task 1: Setting Up Virtualization Software

#### 1. Installed VMware Fusion

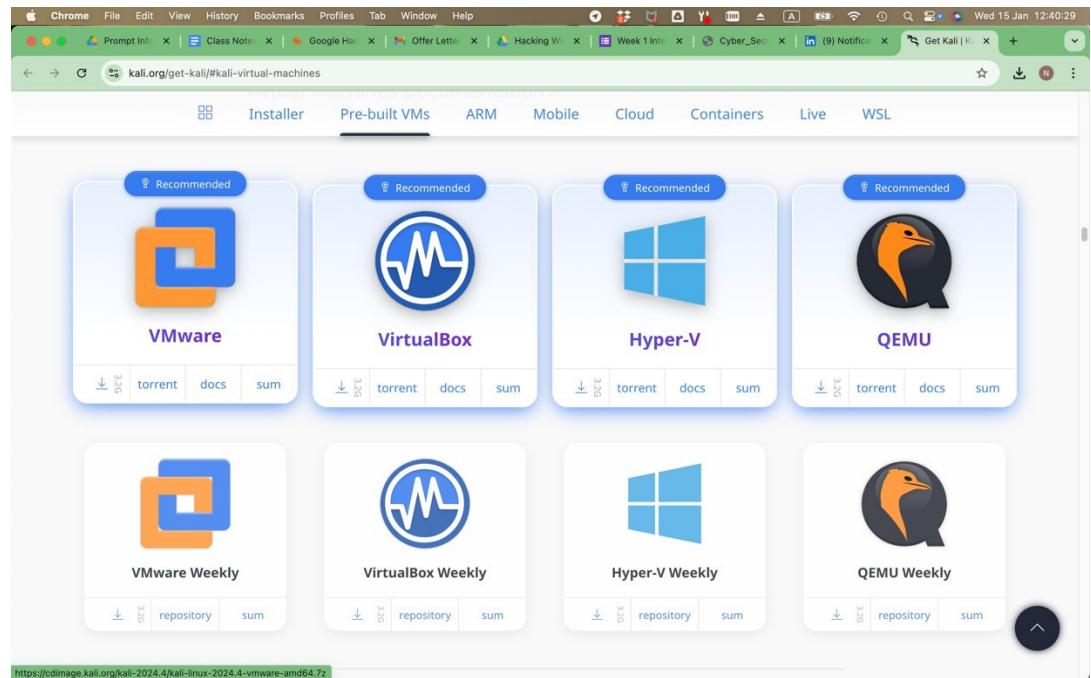
- Downloaded and installed VMware Fusion.



## Task 2: Downloading Kali Linux and Metasploitable

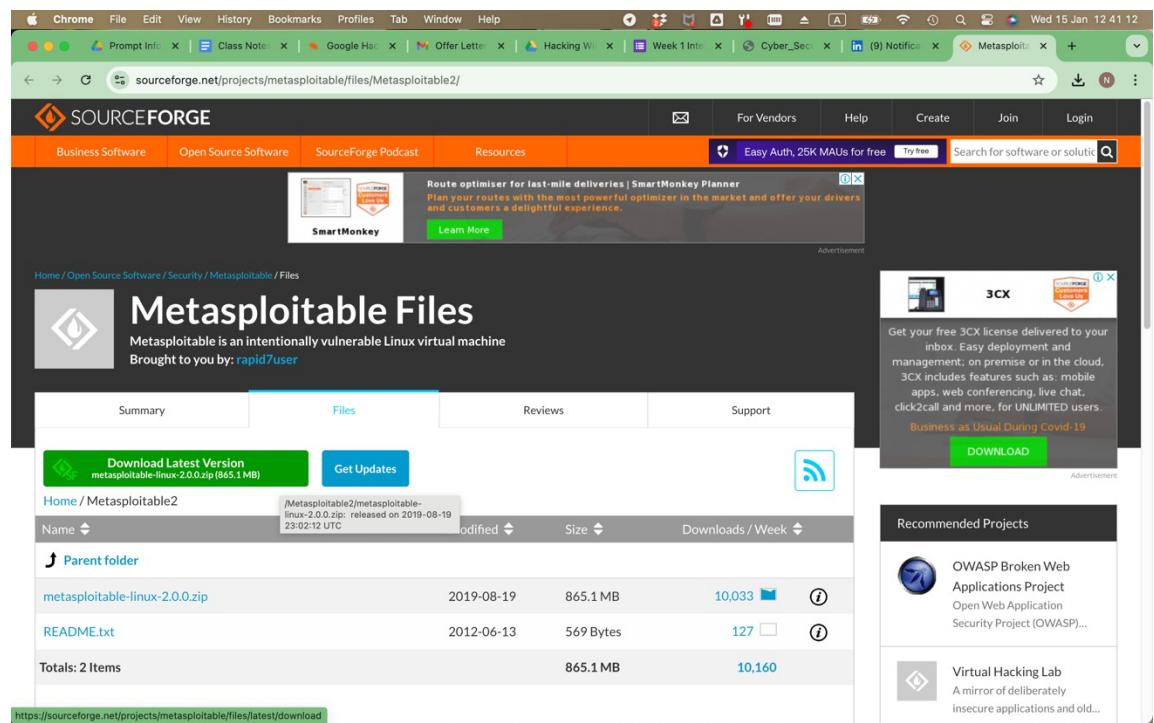
### 1. Downloaded Kali Linux

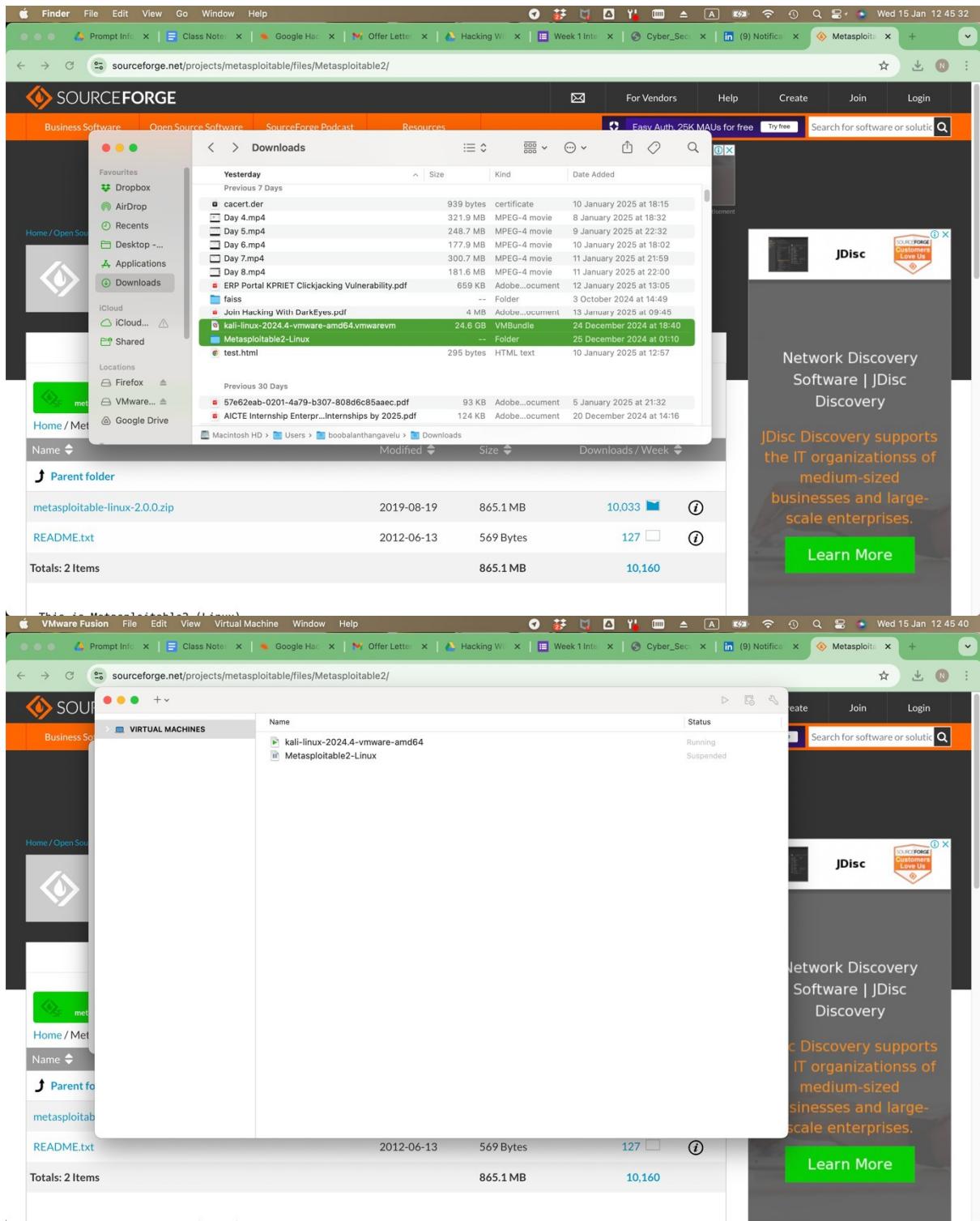
- Used the official website: [Kali Linux Downloads](https://kali.org/get-kali/#kali-virtual-machines).



### 2. Downloaded Metasploitable

- Used the official repository: [Metasploitable Downloads](https://sourceforge.net/projects/metasploitable/files/Metasploitable2/).





## Task 3 & 4: Creating Virtual Machines

### 1. Kali Linux Virtual Machine:

- Created a new VM in VMware Fusion.
- Allocated resources:

RAM: 4 GB

Disk Space: 50 GB

- Attached the Kali Linux ISO to the virtual CD/DVD drive.
- Booted the VM and followed the installation steps. Commands used:

```
# Update system
sudo apt update && sudo apt upgrade -y
```

```
(kali㉿kali)-[~/Clickjacking-Tester]
$ sudo apt update && sudo apt upgrade -y
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.7 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [258 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [877 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.3 kB]
Fetched 70.5 MB in 14s (4,884 kB/s)
516 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  libbbfi01   libgl1-mesa-dev   libjxl0.9      openjdk-23-jre
  libc++1-19   libgles-dev     libmbcrypto7t64  openjdk-23-jre-headless
  libc++abi1-19 libgles1       libpaper1      python3-appdirs
  libegl-dev    libglvnd-core-dev libsuperlu6
  libfmt9      libglvnd-dev    libunwind-19
Use 'sudo apt autoremove' to remove them.

Upgrading:
Setting up kali-desktop-xfce (2025.1.3) ...
Setting up libedata-book-1.2-27t64:amd64 (3.54.3-1) ...
Setting up libebook-1.2-21t64:amd64 (3.54.3-1) ...
Setting up bluez-obexd (5.79-1) ...
Processing triggers for ca-certificates-java (20240118) ...
done.
Setting up openjdk-23-jre:amd64 (23.0.1+11-2) ...
Processing triggers for dictionaries-common (1.30.3) ...
Processing triggers for ca-certificates (20241223) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d ...
done.
Processing triggers for tex-common (6.18) ...
Building format(s) --all.
  This may take some time... done.
Processing triggers for php8.2-cli (8.2.27-1) ...
Processing triggers for libapache2-mod-php8.2 (8.2.27-1) ...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for ca-certificates-java (20240118) ...
done.

(kali㉿kali)-[~/Clickjacking-Tester]
```

- # Install essential tools
 

```
sudo apt install net-tools nmap
```

```

Processing triggers for libc-bin (2.40-3) ...
Processing triggers for ca-certificates-java (20240118) ...
done.

[(kali㉿kali)-[~/Clickjacking-Tester]]$ sudo apt install net-tools nmap
[sudo] password for kali:
net-tools is already the newest version (2.10-1.1).
net-tools set to manually installed.
nmap is already the newest version (7.95+dfsg-1kali1).
nmap set to manually installed.
The following packages were automatically installed and are no longer required:
  libbfio1   libgl1-mesa-dev   libjxl0.9      openjdk-23-jre
  libc++1-19  libgles-dev     libmbcrypto7t64  openjdk-23-jre-headless
  libc++abi1-19 libgles1      libpaper1     python3-appdirs
  libegl-dev   libglvnd-core-dev libsperlu6
  libfmt9      libglvnd-dev    libunwind-19
Use 'sudo apt autoremove' to remove them.

Summary:           Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 20
[(kali㉿kali)-[~/Clickjacking-Tester]]$ 

```

## 2. Metasploitable Virtual Machine:

- Created another VM for Metasploitable.
- Allocated resources:

RAM: 512 MB  
Disk Space: 8 GB

- Attached the Metasploitable ISO and completed the installation.

```

* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

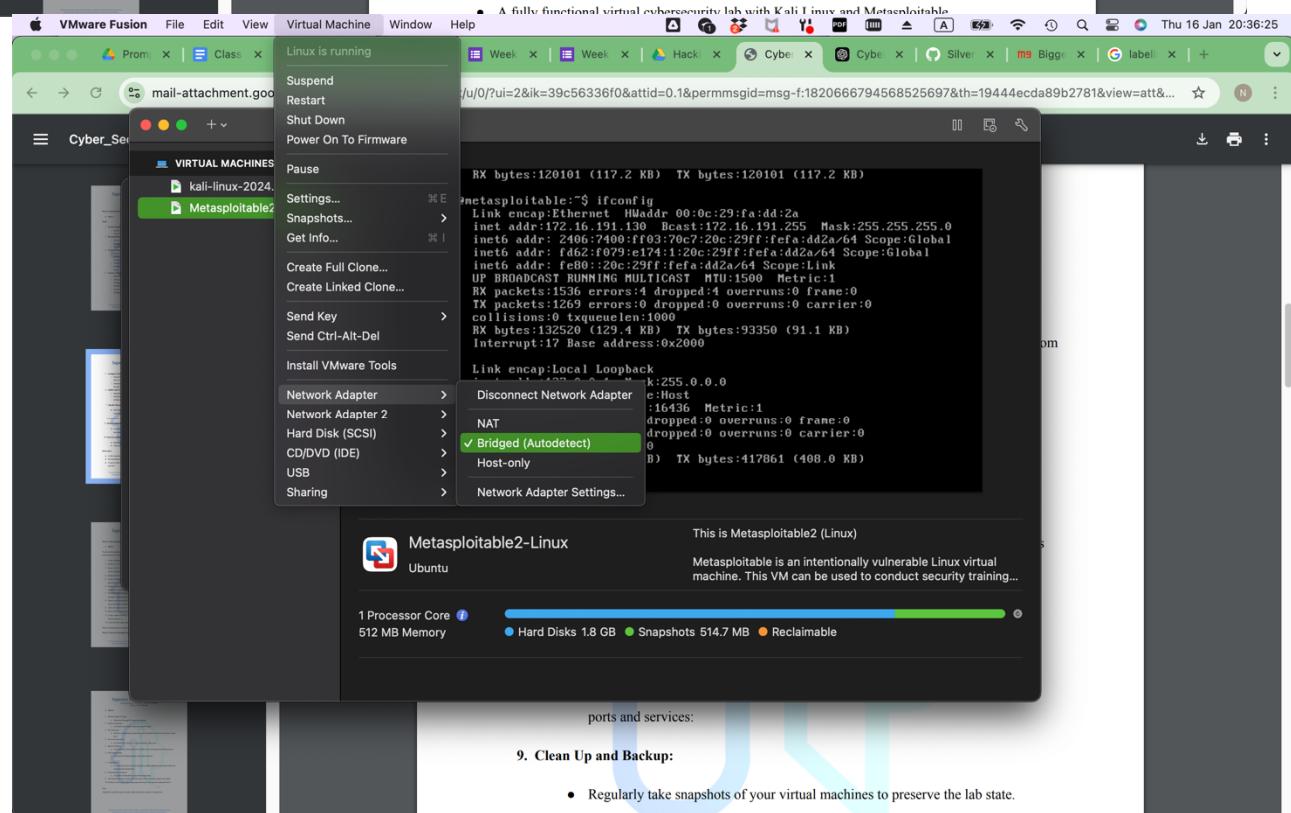
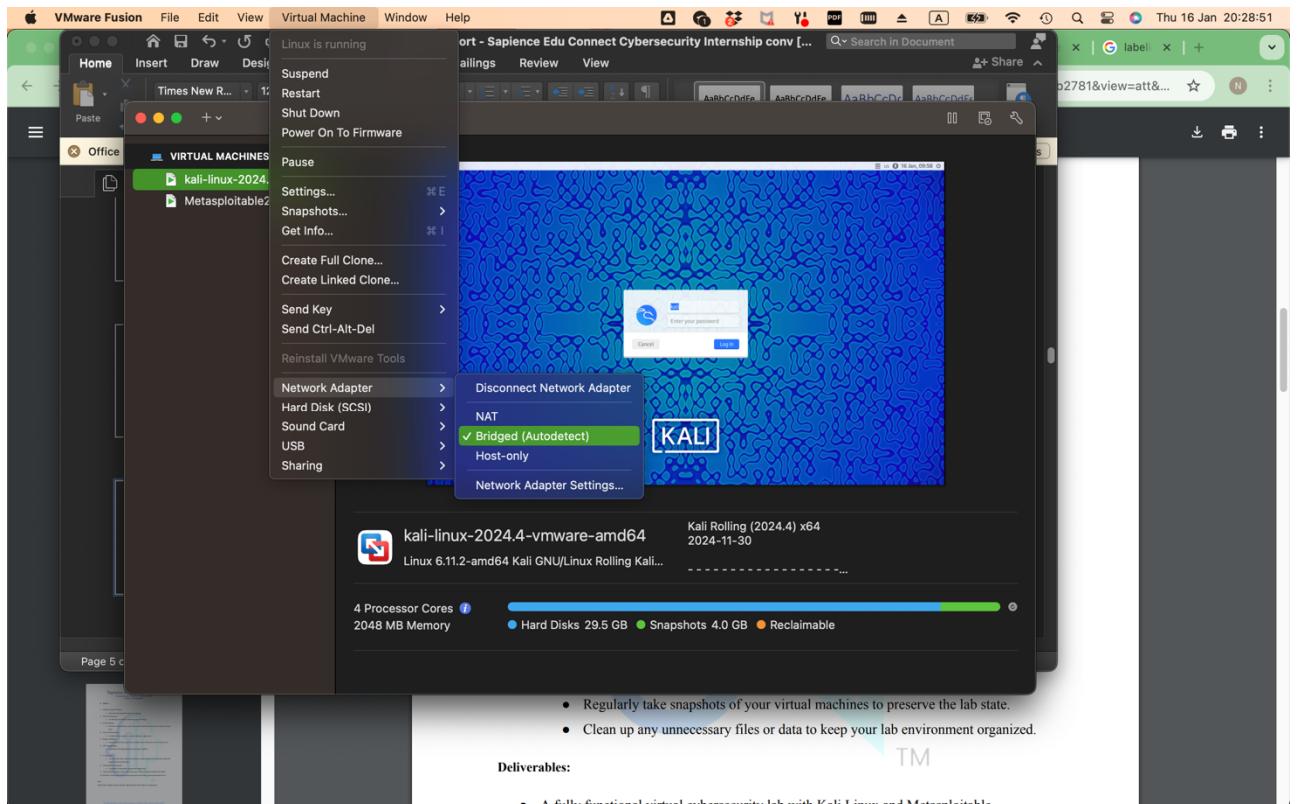
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _ 

```

## Task 5: Configuring Networking

- Configured both VMs to use a bridged network adapter communicate with each other and the host.



- Verified the IP addresses using:

```
# On Kali Linux:  
ifconfig
```

The screenshot shows a terminal window titled 'kali@kali:~'. The window displays the output of the 'ifconfig' command. It shows two interfaces: 'eth0' and 'lo'. 'eth0' has an IPv4 address of 172.16.191.128 and an IPv6 address of fe80::f8ab:fb73:6326:5e9c. 'lo' is the loopback interface with an IPv4 address of 127.0.0.1. The terminal window is part of a desktop environment with various icons and a status bar at the top.

```
(kali㉿kali)-[~]$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
        inet 172.16.191.128 netmask 255.255.255.0 broadcast 172.16.191.255  
        inet6 fe80::f8ab:fb73:6326:5e9c prefixlen 64 scopeid 0x20<link>  
              ether 00:0c:29:17:47:fc txqueuelen 1000 (Ethernet)  
        RX packets 1043943 bytes 148431897 (1.3 GiB)  
        RX errors 0 dropped 347 overruns 0 frame 0  
        TX packets 166673 bytes 14669899 (13.9 MiB)  
        TX errors 0 dropped 19 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
        inet 127.0.0.1 netmask 255.0.0.0  
        inet6 ::1 prefixlen 128 scopeid 0x10<host>  
          loop txqueuelen 1000 (Local Loopback)  
        RX packets 188 bytes 16367 (15.9 KiB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 188 bytes 16367 (15.9 KiB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
# On Metasploitable:  
Ifconfig
```

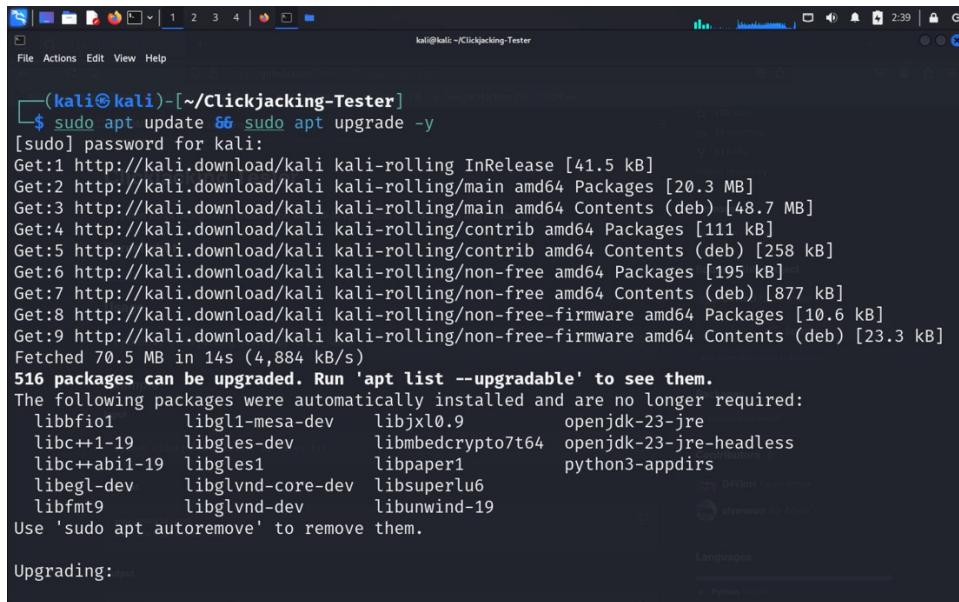
The screenshot shows a terminal window titled 'msfadmin@metasploitable:~\$'. The window displays the output of the 'ifconfig' command. It shows two interfaces: 'eth0' and 'lo'. 'eth0' has an IPv4 address of 172.16.191.130 and an IPv6 address of fe80::20c:29ff:fed2a/64. 'lo' is the loopback interface with an IPv4 address of 127.0.0.1. The terminal window is part of a desktop environment with various icons and a status bar at the top.

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:fa:dd:2a  
          inet addr:172.16.191.130 Bcast:172.16.191.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fed2a/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:43 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:66 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:4407 (4.3 KB) TX bytes:6868 (6.7 KB)  
            Interrupt:17 Base address:0x2000  
  
lo      Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:91 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
```

## Task 6: Updating and Configuring Kali Linux

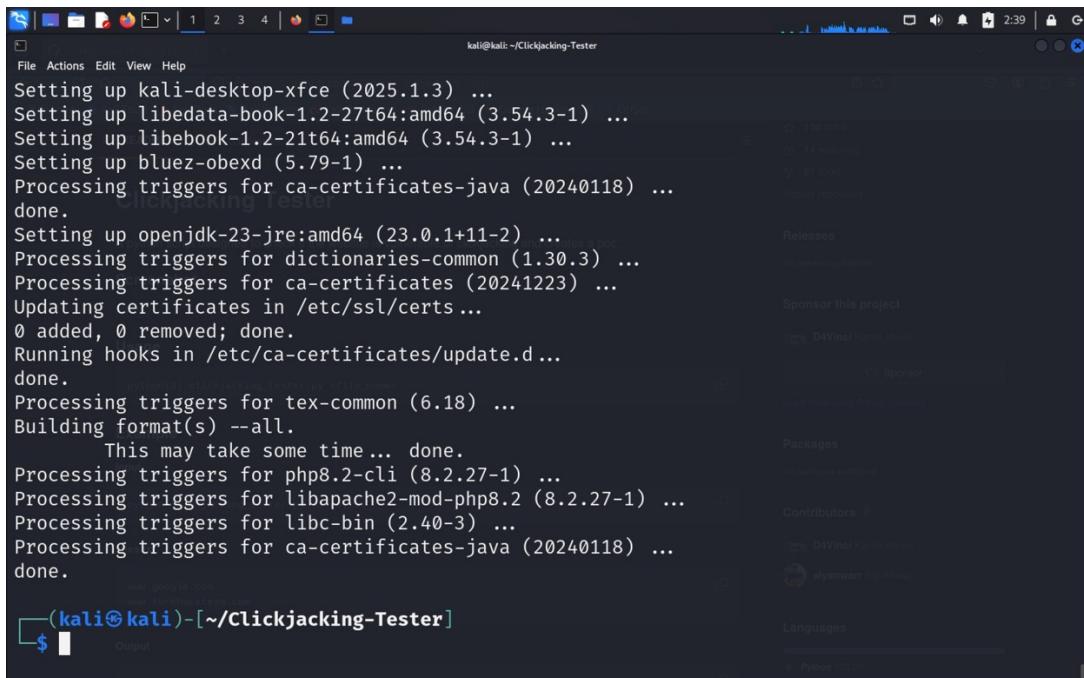
- Updated Kali Linux using:

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



```
(kali㉿kali)-[~/Clickjacking-Tester]
$ sudo apt update && sudo apt upgrade -y
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.7 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [258 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [877 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.3 kB]
Fetched 70.5 MB in 14s (4,884 kB/s)
516 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  libffio1      libgl1-mesa-dev    libjxl0.9      openjdk-23-jre
  libc++1-19    libgles-dev       libmbcrypto7t64  openjdk-23-jre-headless
  libc++abi1-19 libgles1         libpaper1      python3-appdirs
  libegl-dev    libglvnd-core-dev libsuperlu6
  libfmt9       libglvnd-dev     libunwind-19
Use 'sudo apt autoremove' to remove them.

Upgrading:
```



```
Setting up kali-desktop-xfce (2025.1.3) ...
Setting up libedata-book-1.2-27t64:amd64 (3.54.3-1) ...
Setting up libebook-1.2-21t64:amd64 (3.54.3-1) ...
Setting up bluez-obexd (5.79-1) ...
Processing triggers for ca-certificates-java (20240118) ...
done.
Setting up openjdk-23-jre:amd64 (23.0.1+11-2) ...
Processing triggers for dictionaries-common (1.30.3) ...
Processing triggers for ca-certificates (20241223) ...
Updating certificates in /etc/ssl/certs ...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d ...
done.
Processing triggers for tex-common (6.18) ...
Building format(s) --all.
      This may take some time... done.
Processing triggers for php8.2-cli (8.2.27-1) ...
Processing triggers for libapache2-mod-php8.2 (8.2.27-1) ...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for ca-certificates-java (20240118) ...
done.

(kali㉿kali)-[~/Clickjacking-Tester]
$
```

- Installed additional tools for penetration testing:

```
sudo apt install metasploit-framework -y
sudo apt install nikto -y
```

```
kali@kali: ~/Clickjacking-Tester
libfmt9      libglvnd-dev    libunwind-19
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 20

[(kali㉿kali)-~/Clickjacking-Tester]
$ sudo apt install metasploit-framework -y
[sudo] password for kali:
metasploit-framework is already the newest version (6.4.44-0kali1).
metasploit-framework set to manually installed.
The following packages were automatically installed and are no longer required:
  libbbfio1   libgl1-mesa-dev  libjxl0.9    openjdk-23-jre
  libc++1-19  libgles-dev     libmbcrypto7t64  openjdk-23-jre-headless
  libc++abi1-19 libgles1       libpaper1    python3-appdirs
  libegl-dev   libglvnd-core-dev  libsuperlu6
  libfmt9      libglvnd-dev    libunwind-19
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 20

[(kali㉿kali)-~/Clickjacking-Tester]
$
```

```
kali@kali: ~/Clickjacking-Tester
libegl-dev      libglvnd-core-dev  libsuperlu6
libfmt9         libglvnd-dev        libunwind-19
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 20

[(kali㉿kali)-~/Clickjacking-Tester]
$ sudo apt install nikto
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).
nikto set to manually installed.
The following packages were automatically installed and are no longer required:
  libbbfio1   libgl1-mesa-dev  libjxl0.9    openjdk-23-jre
  libc++1-19  libgles-dev     libmbcrypto7t64  openjdk-23-jre-headless
  libc++abi1-19 libgles1       libpaper1    python3-appdirs
  libegl-dev   libglvnd-core-dev  libsuperlu6
  libfmt9      libglvnd-dev    libunwind-19
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 20

[(kali㉿kali)-~/Clickjacking-Tester]
$
```

## Task 7: Identifying Metasploitable's IP Address

- Logged into Metasploitable using default credentials:

```
Username: msfadmin  
Password: msfadmin
```

- Identified IP address:

```
ifconfig
```

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:fa:dd:2a  
          inet addr:172.16.191.130 Bcast:172.16.191.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe:dd2a/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:4407 (4.3 KB) TX bytes:6868 (6.7 KB)  
          Interrupt:17 Base address:0x2000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING MTU:16436 Metric:1  
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)  
  
msfadmin@metasploitable:~$
```

Output: 172.16.191.130

## Task 8: Initial Reconnaissance

- Performed a basic network scan from Kali Linux:

```
nmap 172.16.191.130
```

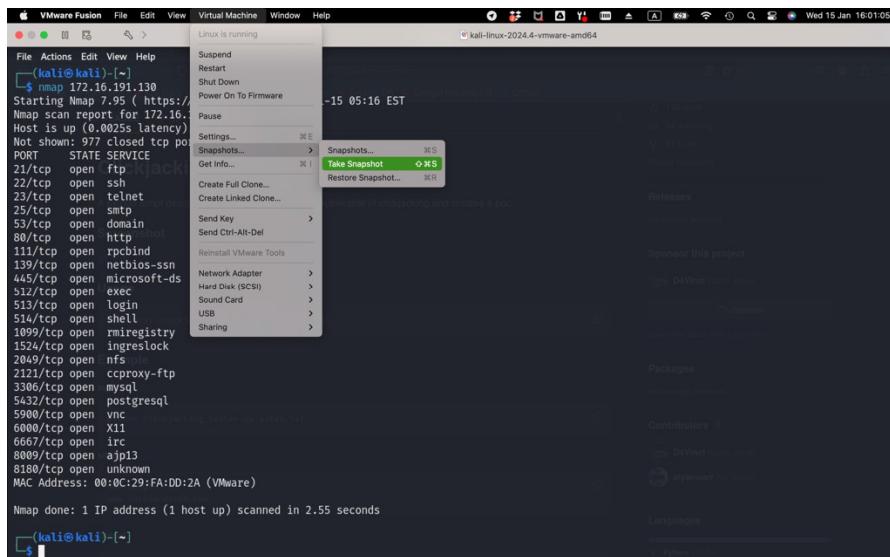
```
(kali㉿kali)-[~] $ nmap 172.16.191.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 05:16 EST
Nmap scan report for 172.16.191.130
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

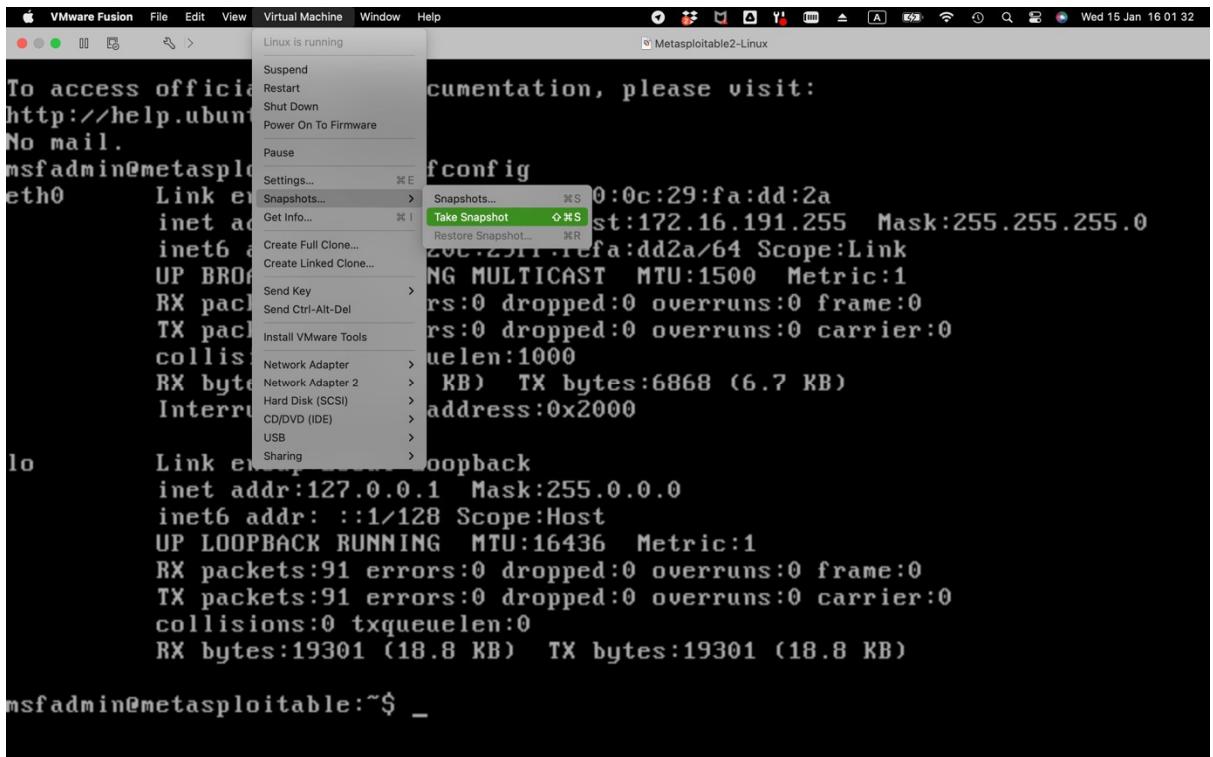
Nmap done: 1 IP address (1 host up) scanned in 2.55 seconds
(kali㉿kali)-[~]
```

Output: Identified open ports, running services, and OS information of Metasploitable (Running In VMWare).

## Task 9: Snapshots and Cleanup

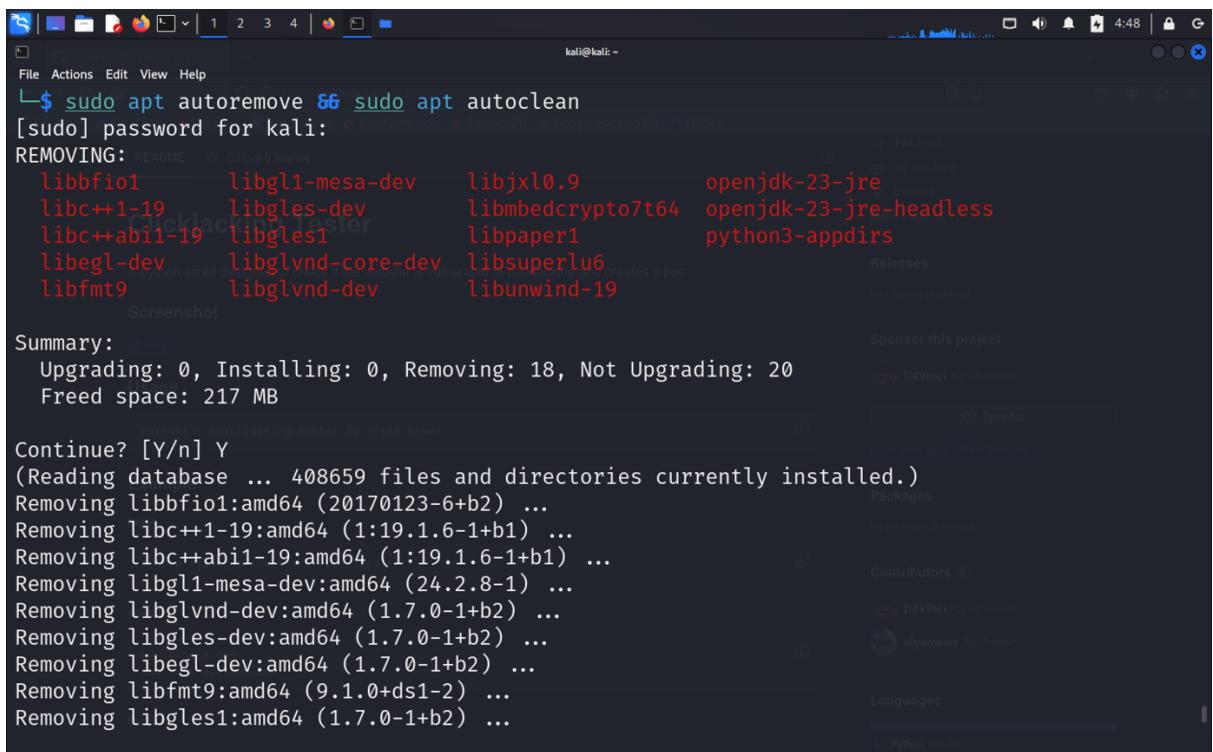
- Took snapshots of both VMs to save the current state.





- Cleaned unnecessary files using:

```
sudo apt autoremove && sudo apt autoclean
```



```
Del samba-ad-provision 2:4.21.2+dfsg-3 [500 kB]
Del libnm0 1.50.0-1+b1 [453 kB]
Del libpam-systemd 257-2 [292 kB]
Del libharfbuzz-icu0 10.1.0-1 [15.1 kB]
Del libgpg-error0 1.51-2 [82.1 kB]
Del chromium 131.0.6778.139-1 [86.7 MB]
Del libssl2-2.0-0 2.30.10+dfsg-1 [667 kB]
Del kali-desktop-core 2025.1.1 [14.0 kB]
Del util-linux-extra 2.40.2-12 [265 kB]
Del libudev1 257-2 [147 kB]
Del kali-system-cli 2025.1.1 [13.9 kB]
Del python3-pkg-resources 75.2.0-1 [213 kB]
Del aspell 0.60.8.1-2 [275 kB]
Del apt 2.9.17 [1,368 kB]
Del libgs10 10.04.0~dfsg-2 [2,562 kB]
Del metasploit-framework 6.4.38-0kali1 [221 MB]
Del kali-themes-common 2025.1.1 [6,889 kB]
Del librav1e0.7 0.7.1-7+b3 [940 kB]
Del pipewire-bin 1.2.7-1 [385 kB]
Del php8.2-mysql 8.2.26-4 [118 kB]
Del login 1:4.16.0-2+really2.40.2-12 [81.8 kB]
```

## Findings and Insights of Initial Reconnaissance:

Based on the scan output from **nmap** for the target IP 172.16.191.130, several critical findings can be observed. The target machine is hosting a wide range of services on multiple open ports. Key open ports include **21 (FTP)**, **22 (SSH)**, **23 (Telnet)**, **25 (SMTP)**, **80 (HTTP)**, **139 and 445 (NetBIOS and SMB)**, and **3306 (MySQL)**, among others. Each of these ports corresponds to a specific service that could potentially be exploited if vulnerabilities exist in the configurations or versions of the software being used.

The presence of **Telnet (port 23)**, which is an insecure protocol, suggests that the target machine may lack modern security measures, as Telnet transmits data, including credentials, in plain text. Similarly, the availability of **FTP (port 21)** and **SMB (ports 139 and 445)** could indicate weak authentication mechanisms or outdated software, making them potential targets for brute-force attacks or exploitation of known vulnerabilities. The inclusion of database services like **MySQL (port 3306)** and **PostgreSQL (port 5432)** highlights the need to assess database security, as exposed database ports can lead to unauthorized access or data breaches.

Moreover, **HTTP (port 80)** suggests the presence of a web server, which could provide further attack vectors if web applications hosted on the server have vulnerabilities like insecure configurations, outdated frameworks, or susceptible plugins. The **X11 (port 6000)** and other high-numbered ports indicate additional services that may be used for remote desktop-like functionality, which could also be investigated for misconfigurations.

In summary, this scan reveals that the target machine hosts numerous services, many of which are associated with well-known vulnerabilities. This information can be used for prioritizing further investigation into each service to identify specific security weaknesses, misconfigurations, or outdated software versions. The findings highlight the necessity for patching, hardening, and potentially disabling unnecessary or insecure services to enhance the overall security posture of the system.