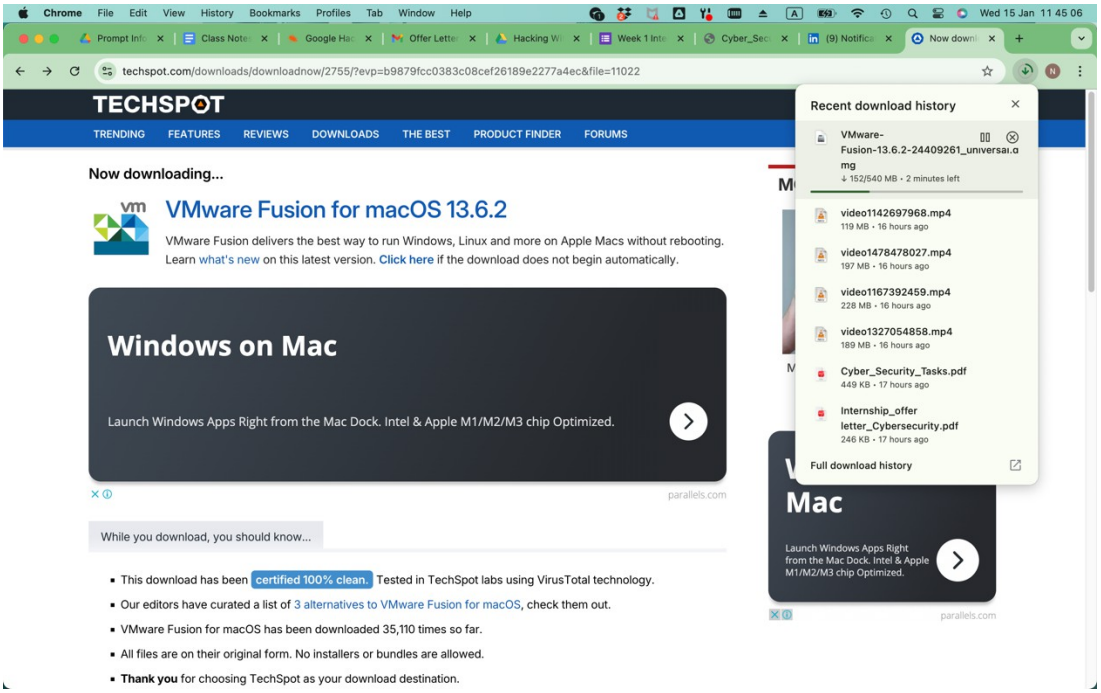
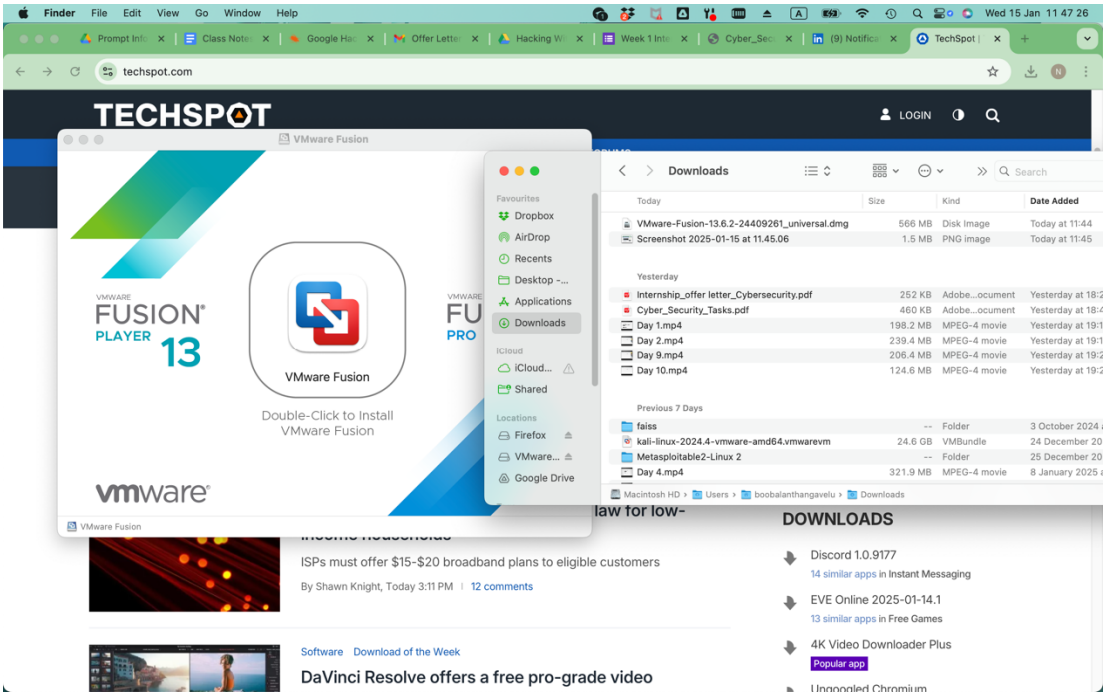
Week 1: Introduction to Cybersecurity and Virtualization

Cybersecurity Lab Setup Reports

Task 1: Setting Up Virtualization Software

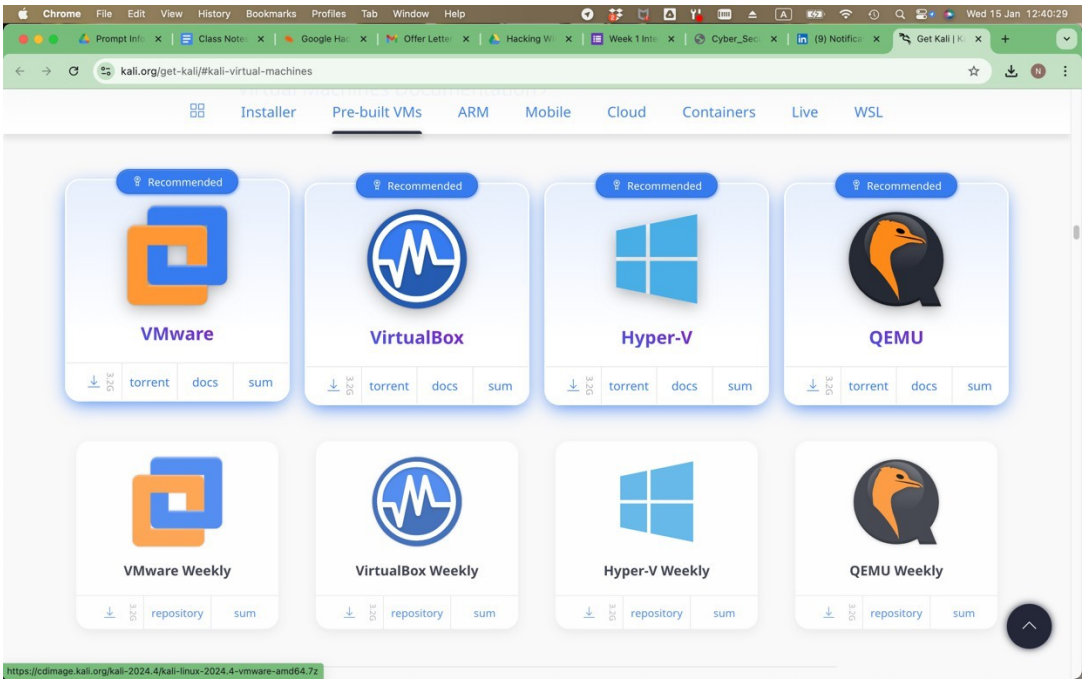
1. **Installed VMware Fusion**
    - Downloaded and installed VMware Fusion.



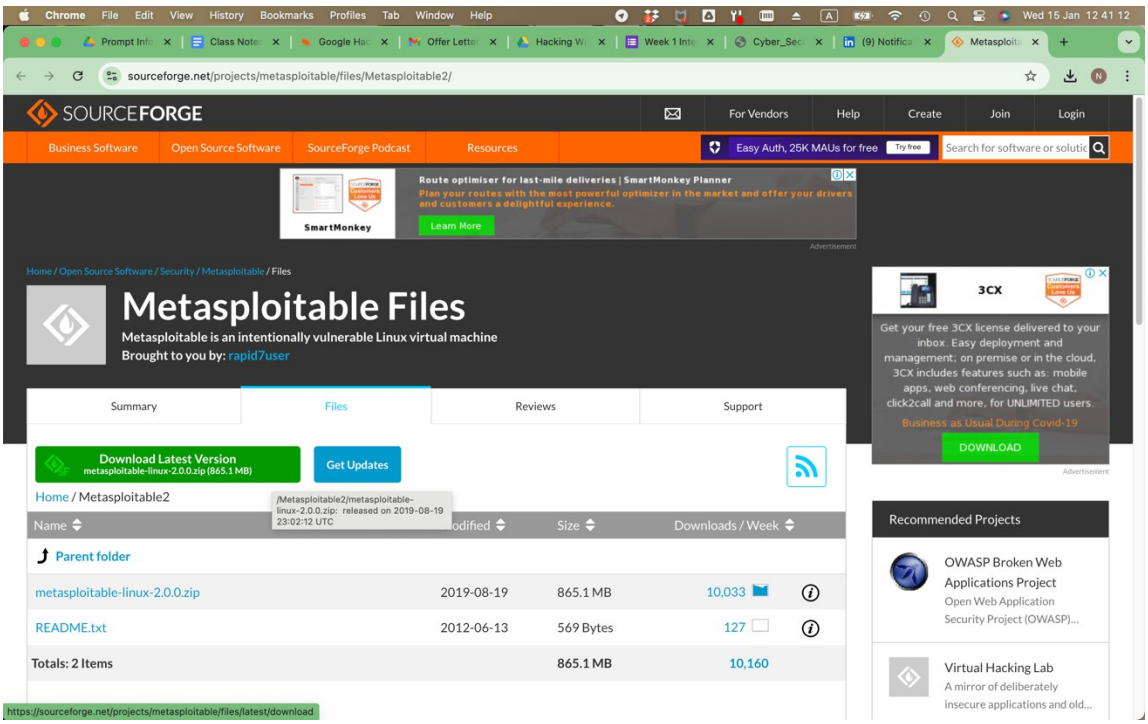


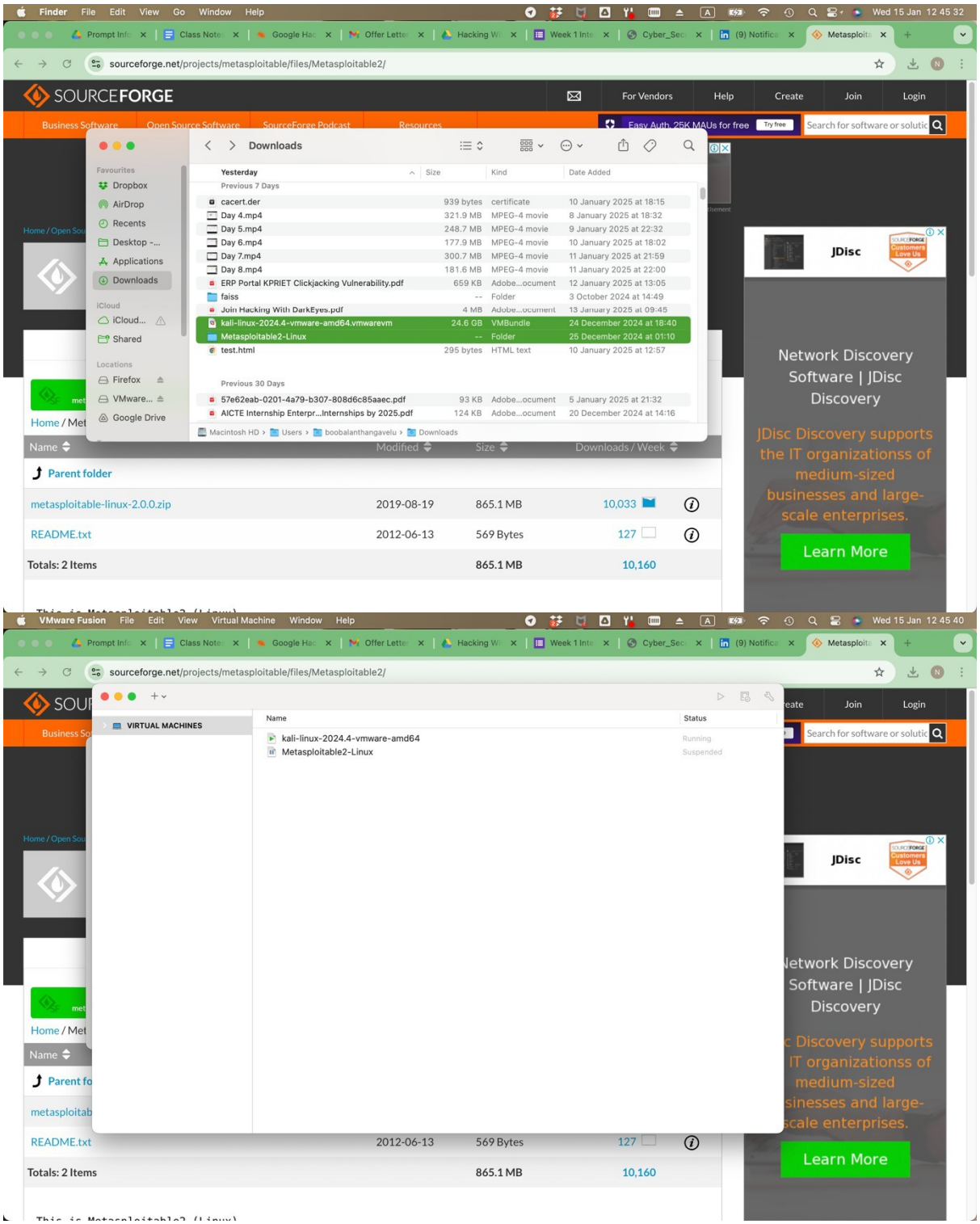
Task 2: Downloading Kali Linux and Metasploitable

1. **Downloaded Kali Linux**
   - Used the official website: Kali Linux Downloads.



2. **Downloaded Metasploitable**
   - Used the official repository: Metasploitable Downloads.





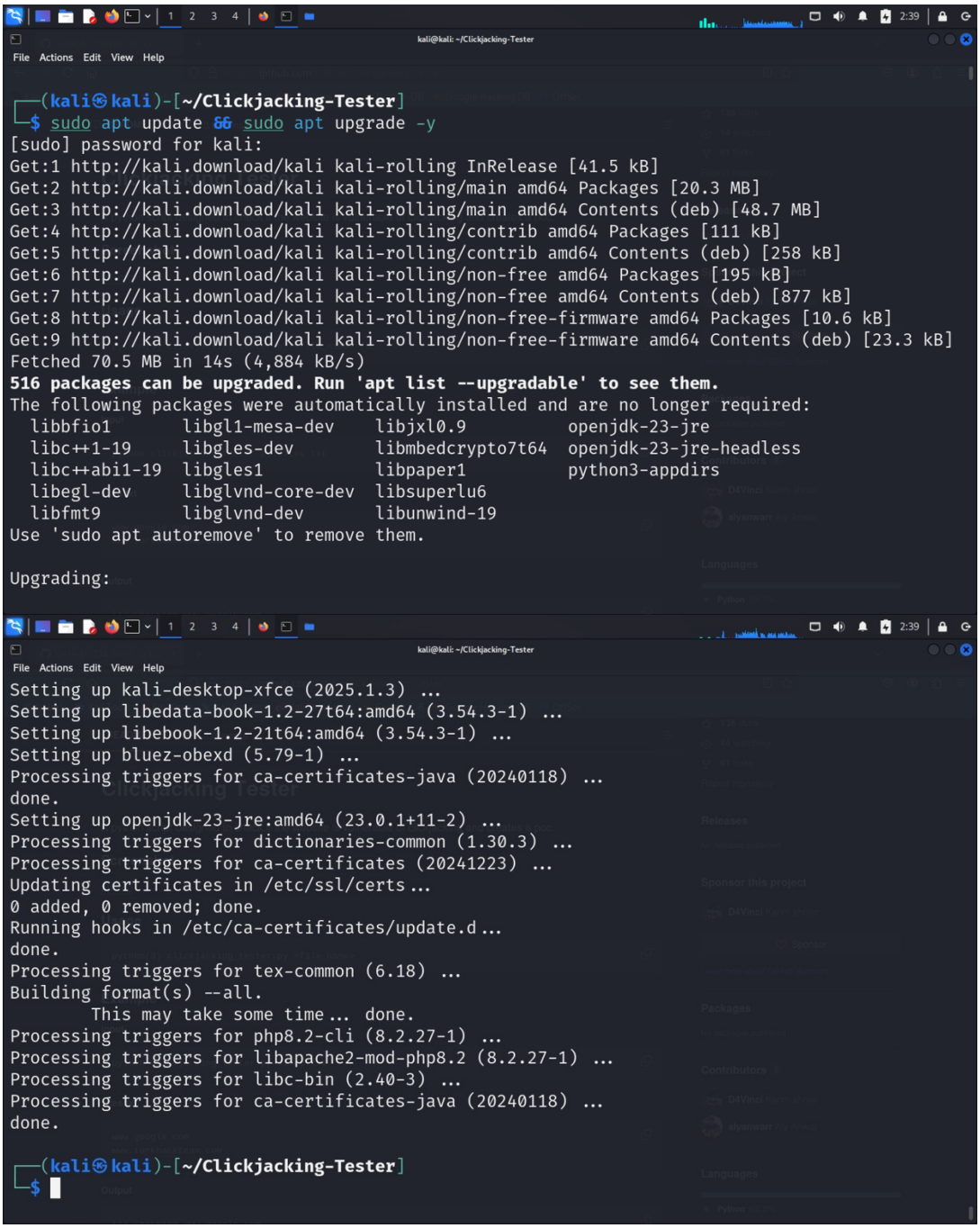
Task 3 & 4: Creating Virtual Machines

1. **Kali Linux Virtual Machine**:
   - Created a new VM in VMware Fusion.
   - Allocated resources:

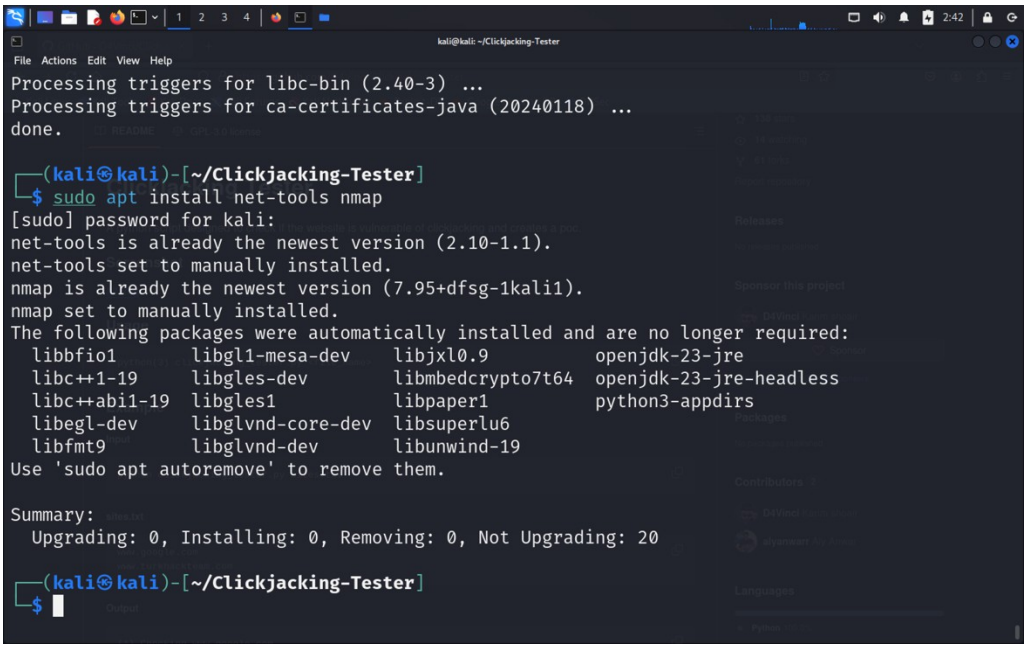
```
RAM: 4 GB
Disk Space: 50 GB
```

- 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
```



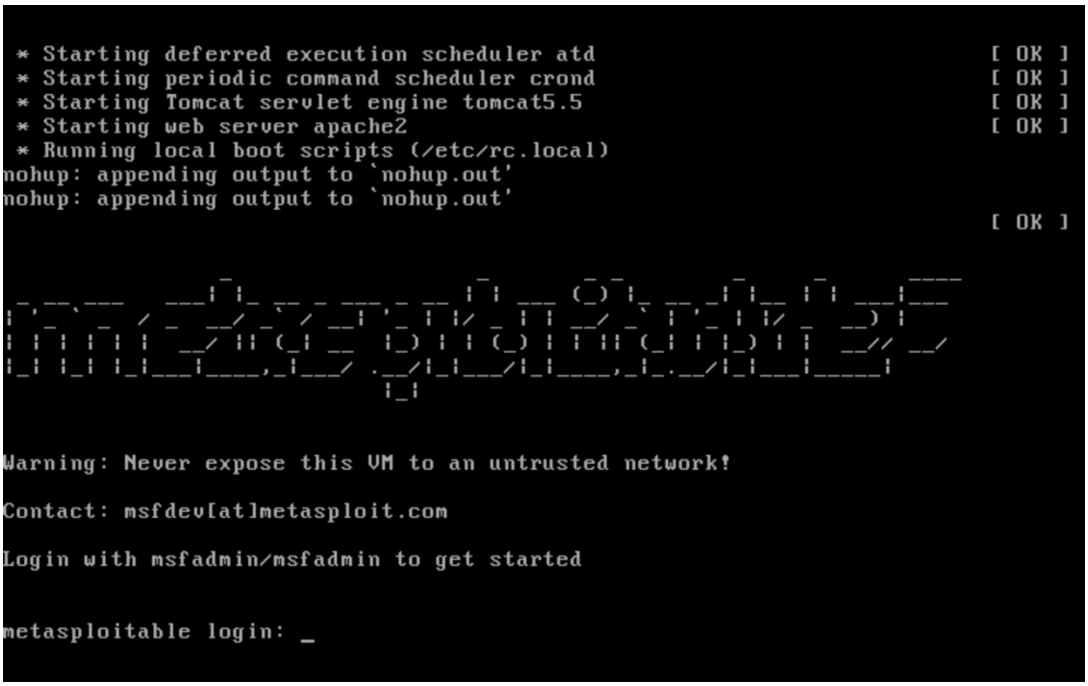

- ```
  # Install essential tools
  sudo apt install net-tools nmap
  ```
  ```



2. **Metasploitable Virtual Machine**:
   - Created another VM for Metasploitable.
   - Allocated resources:

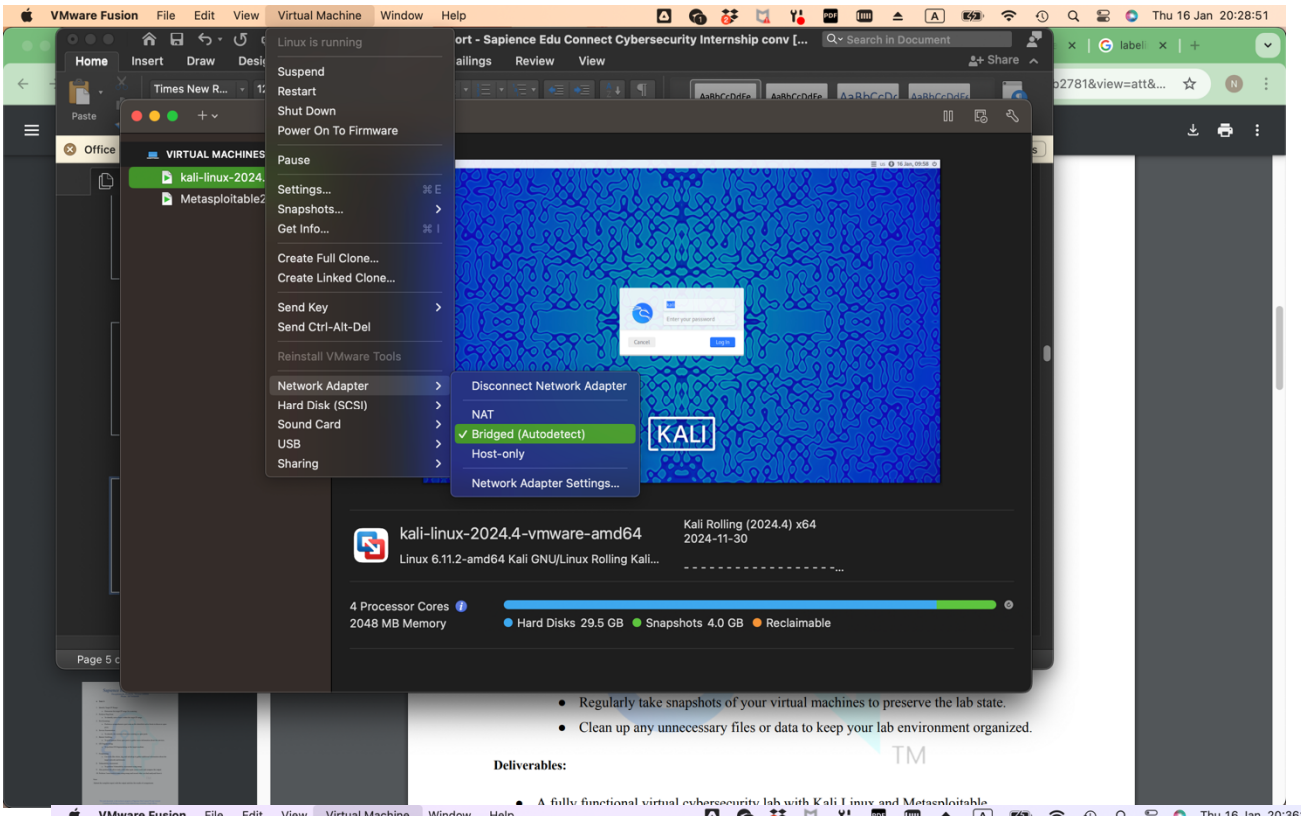
     ```
     RAM: 512 MB
     Disk Space: 8 GB
     ```

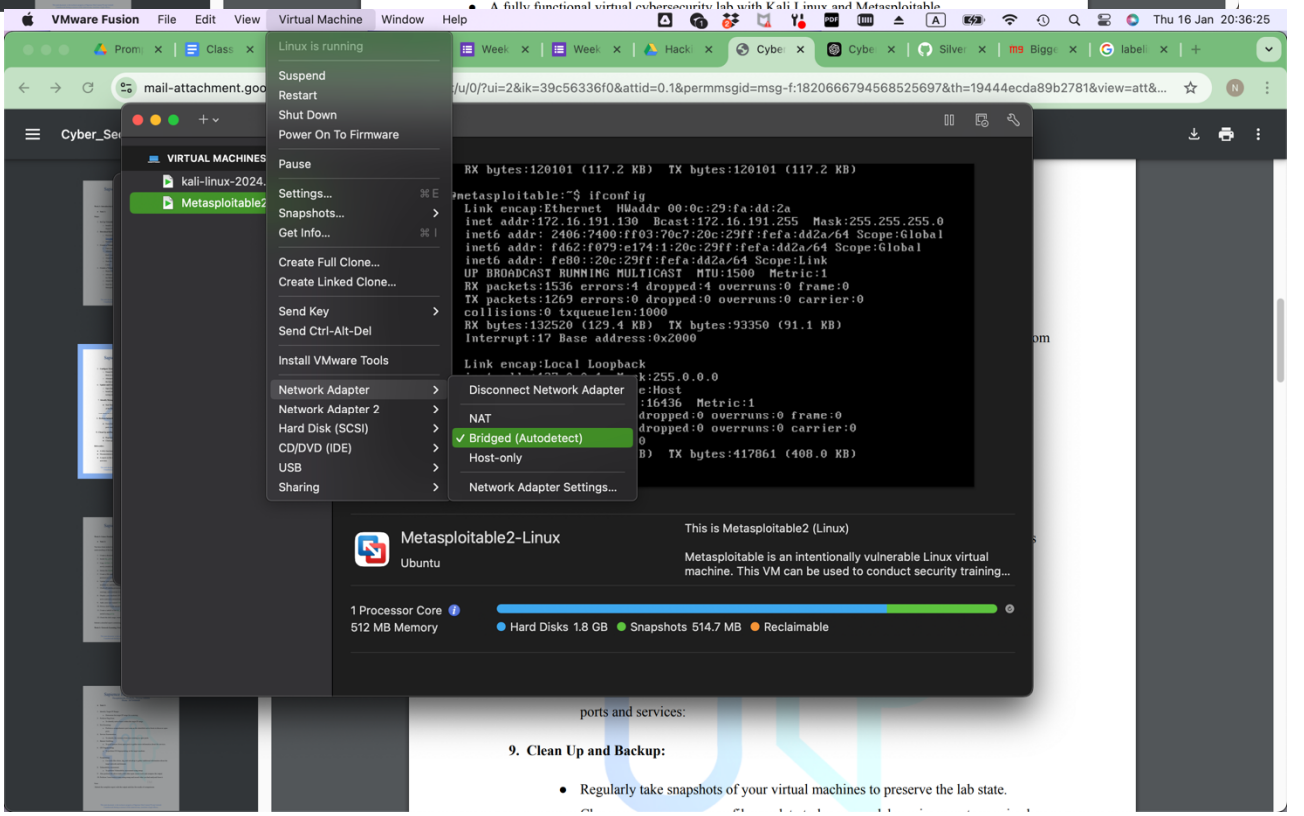
   - Attached the Metasploitable ISO and completed the installation.



Task 5: Configuring Networking

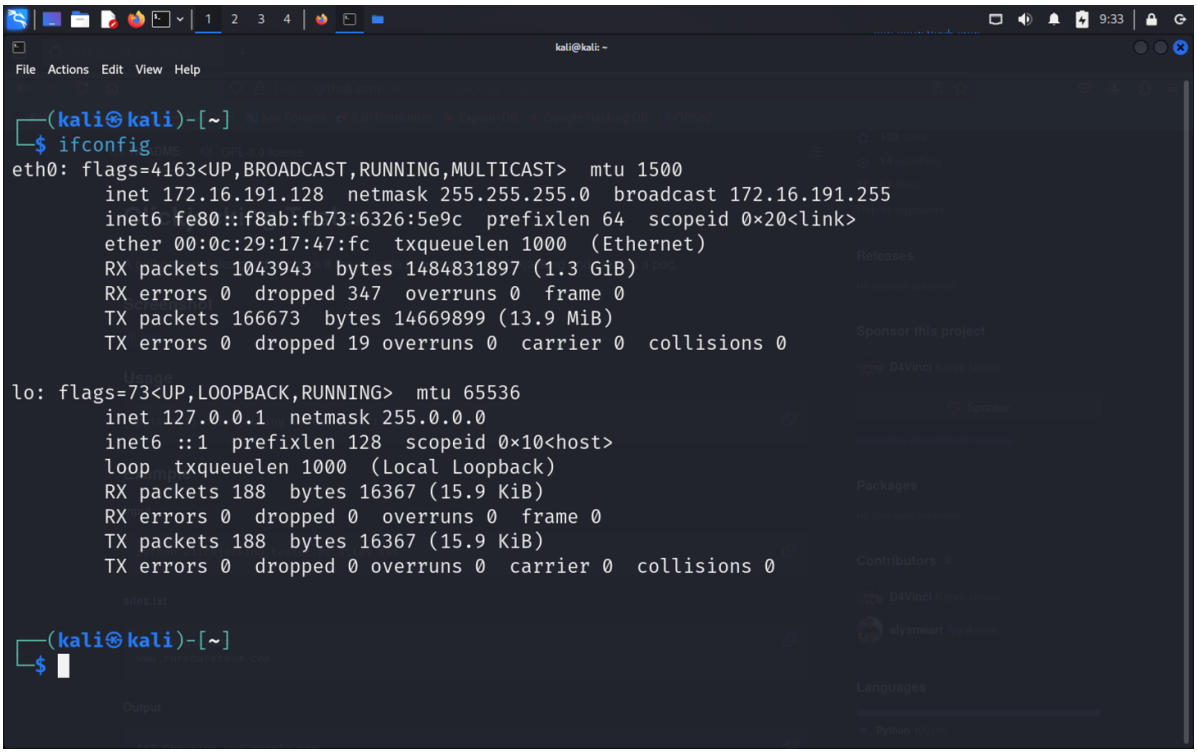
- Configured both VMs to use a bridged network adapter communicate with each other and the host.


VMware Fusion File Edit View Virtual Machine Window Help
Thu 16 Jan 20:28:51
Linux is running
Suspend
Restart
Shut Down
Power On To Firmware
Pause
Settings... ⌘E
Snapshots...
Get Info... ⌘I
Create Full Clone...
Create Linked Clone...
Send Key
Send Ctrl-Alt-Del
Reinstall VMware Tools
Network Adapter
Hard Disk (SCSI)
Sound Card
USB
Sharing
Disconnect Network Adapter
NAT
Bridged (Autodetect)
Host-only
Network Adapter Settings...
VIRTUAL MACHINES
kali-linux-2024.
Metasploitable2
KALI
kali-linux-2024.4-vmware-amd64
Linux 6.11.2-amd64 Kali GNU/Linux Rolling Kali...
Kali Rolling (2024.4) x64
2024-11-30
4 Processor Cores
2048 MB Memory
Hard Disks 29.5 GB
Snapshots 4.0 GB
Reclaimable
Regularly take snapshots of your virtual machines to preserve the lab state.
Clean up any unnecessary files or data to keep your lab environment organized.
Deliverables:

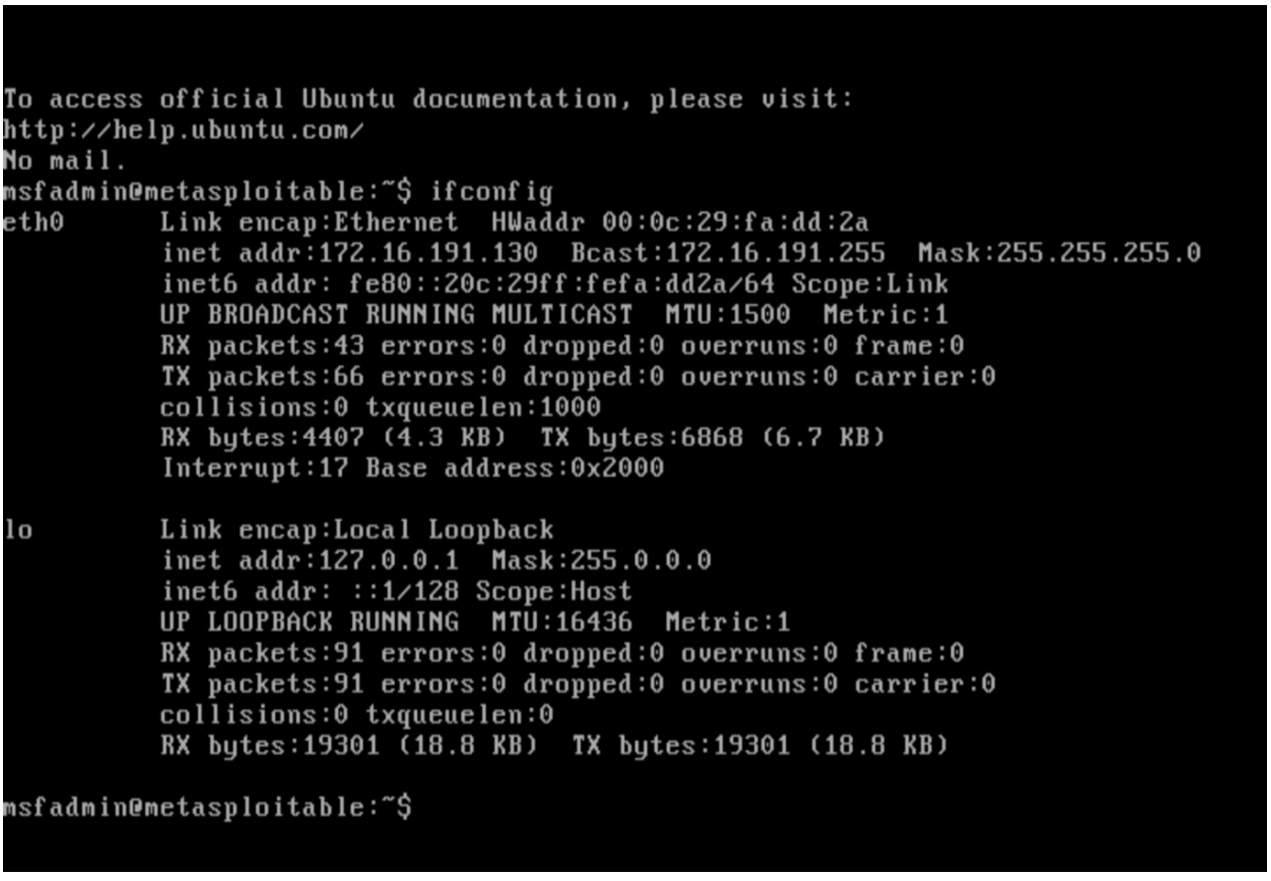

VMware Fusion File Edit View Virtual Machine Window Help
Thu 16 Jan 20:36:25
Linux is running
Suspend
Restart
Shut Down
Power On To Firmware
Pause
Settings... ⌘E
Snapshots...
Get Info... ⌘I
Create Full Clone...
Create Linked Clone...
Send Key
Send Ctrl-Alt-Del
Install VMware Tools
Network Adapter
Network Adapter 2
Hard Disk (SCSI)
CD/DVD (IDE)
USB
Sharing
Disconnect Network Adapter
NAT
Bridged (Autodetect)
Host-only
Network Adapter Settings...
VIRTUAL MACHINES
kali-linux-2024.
Metasploitable2
RX bytes:120101 (117.2 KB) TX bytes:120101 (117.2 KB)
msploitable:~$ ifconfig
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: 2406:7400:ff03:70c7:20c:29ff:fefa:dd2a/64 Scope:Global
inet6 addr: fd62:f079:e174:1:20c:29ff:fefa:dd2a/64 Scope:Global
inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1536 errors:4 dropped:4 overruns:0 frame:0
TX packets:1269 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:132520 (129.4 KB) TX bytes:93350 (91.1 KB)
Interrupt:17 Base address:0x2000
Link encap:Local Loopback
k:255.0.0.0
e:Host
:16436 Metric:1
dropped:0 overruns:0 frame:0
dropped:0 overruns:0 carrier:0
0
B) TX bytes:417861 (408.0 KB)
Metasploitable2-Linux
Ubuntu
This is Metasploitable2 (Linux)
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training...
1 Processor Core
512 MB Memory
Hard Disks 1.8 GB
Snapshots 514.7 MB
Reclaimable
ports and services:
9. Clean Up and Backup:
Regularly take snapshots of your virtual machines to preserve the lab state.

- Verified the IP addresses using:

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



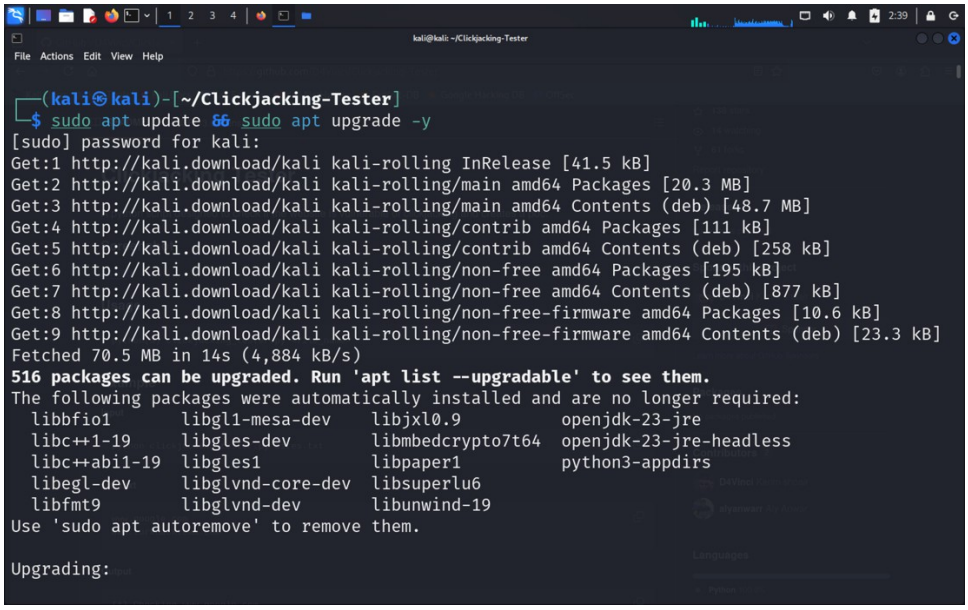

```
# On Metasploitable:
Ifconfig
```

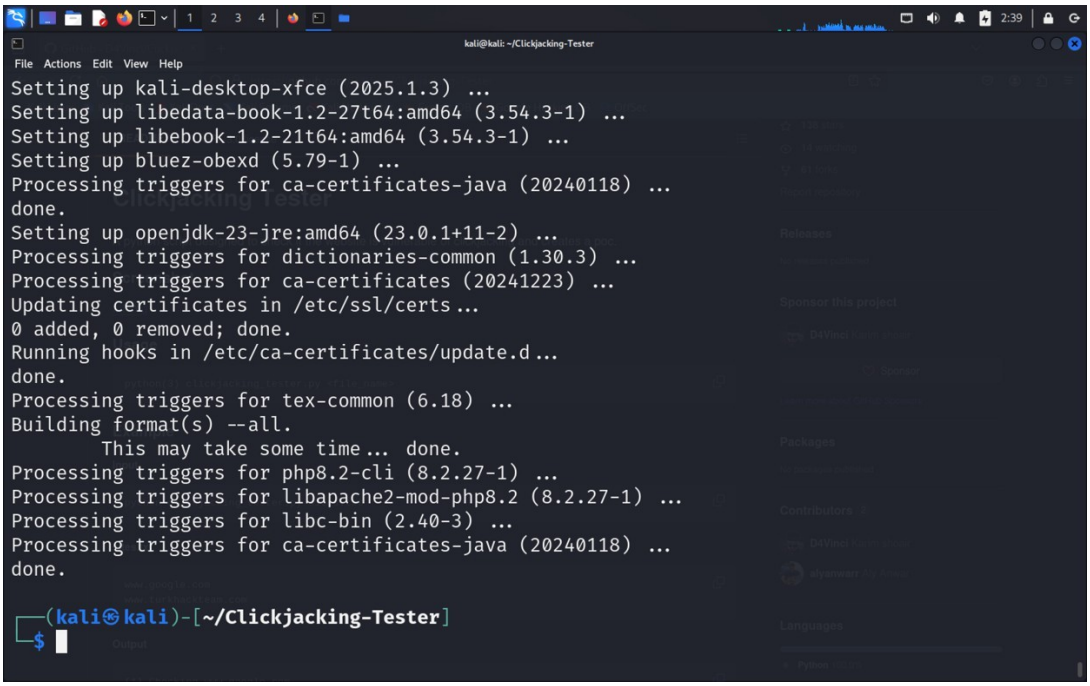


Task 6: Updating and Configuring Kali Linux

- Updated Kali Linux using:

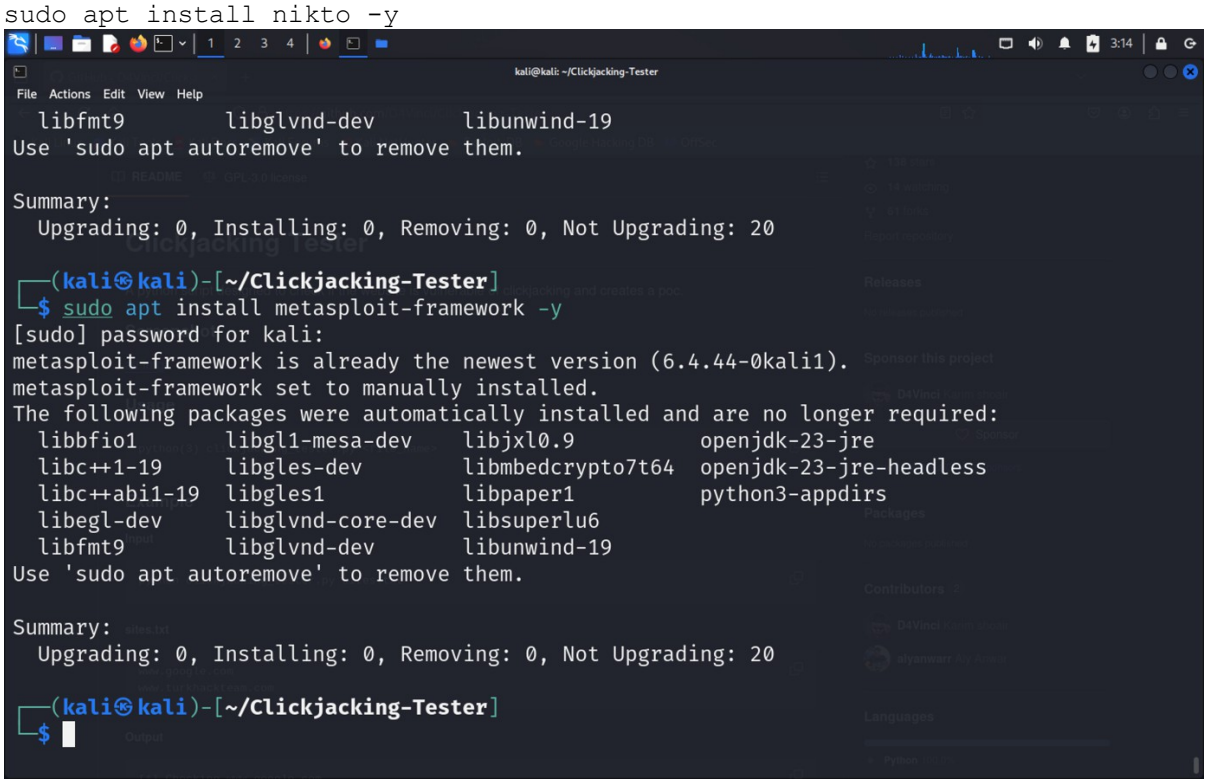
```
sudo apt update && sudo apt upgrade -y
```

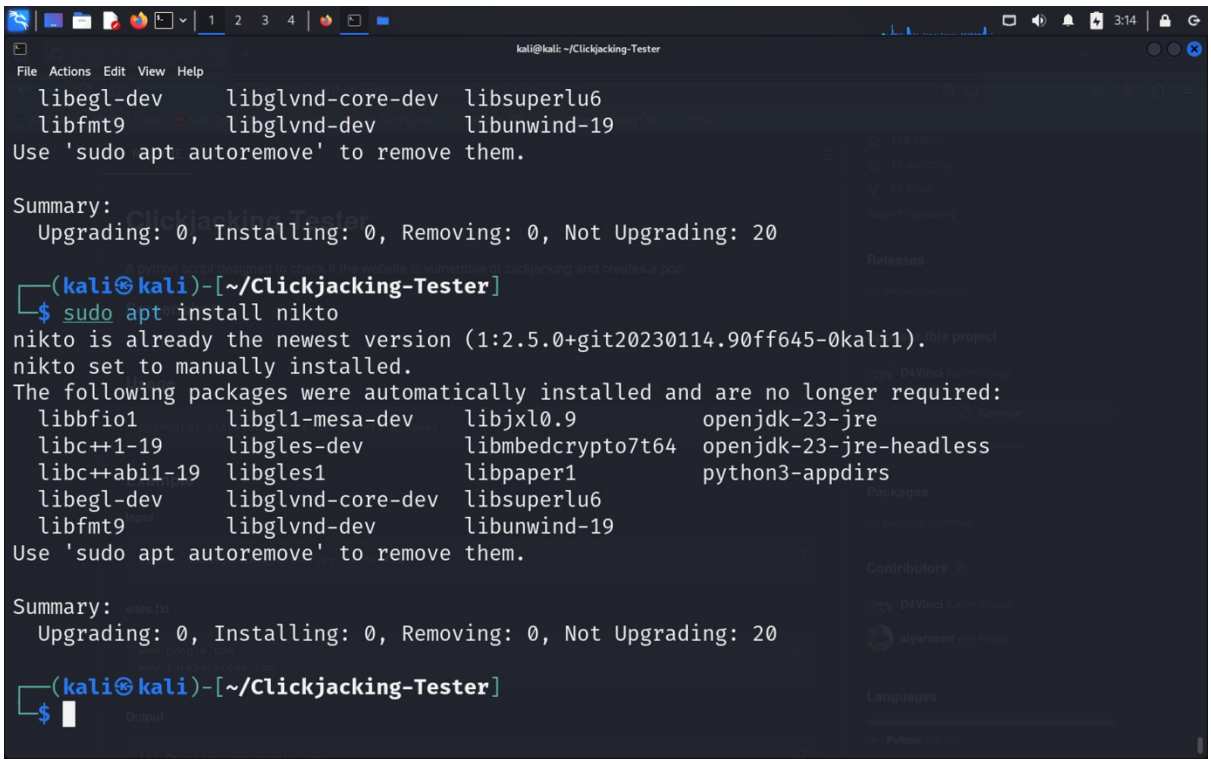




- Installed additional tools for penetration testing:

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





Task 7: Identifying Metasploitable's IP Address

- Logged into Metasploitable using default credentials:

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

- Identified IP address:

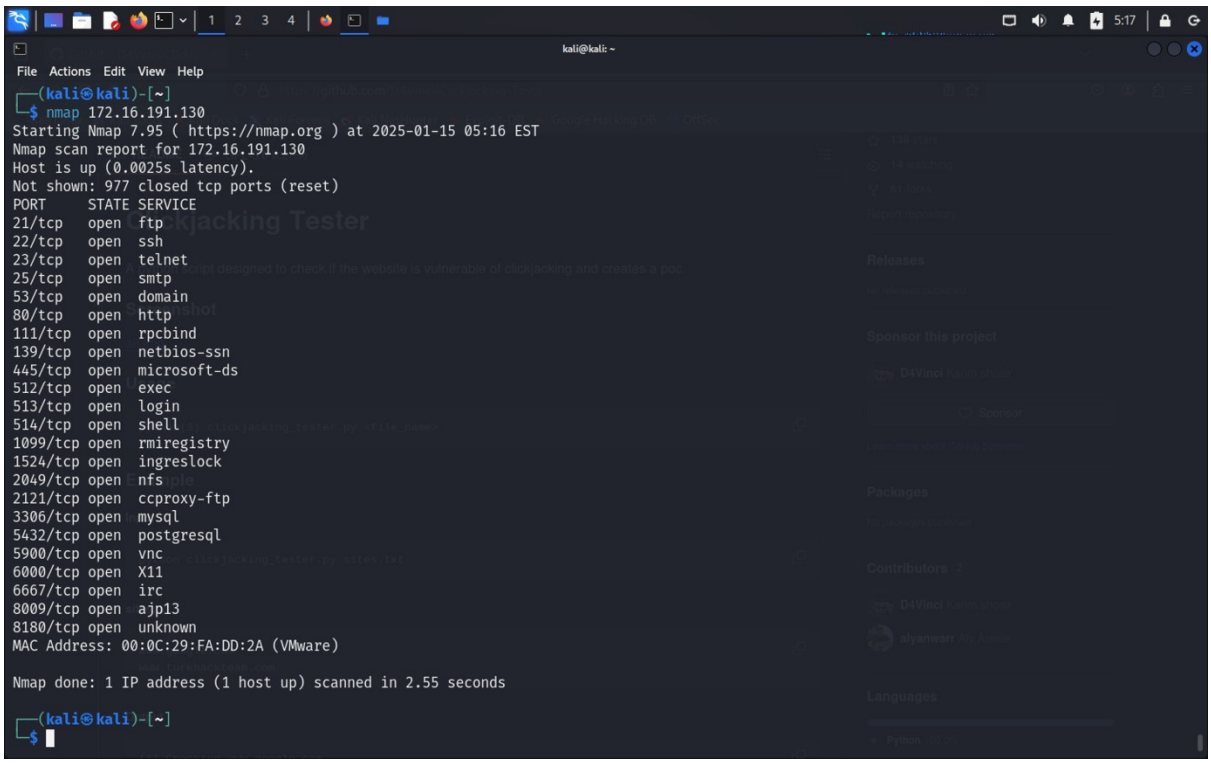
  ```
  ifconfig
  ```

Output: 172.16.191.130

Task 8: Initial Reconnaissance

- Performed a basic network scan from Kali Linux:

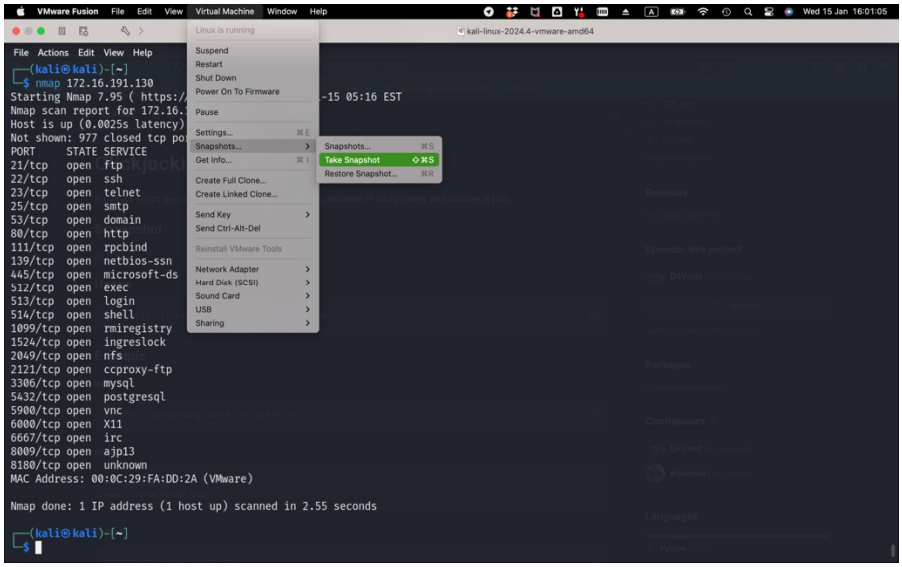
```
nmap 172.16.191.130
```

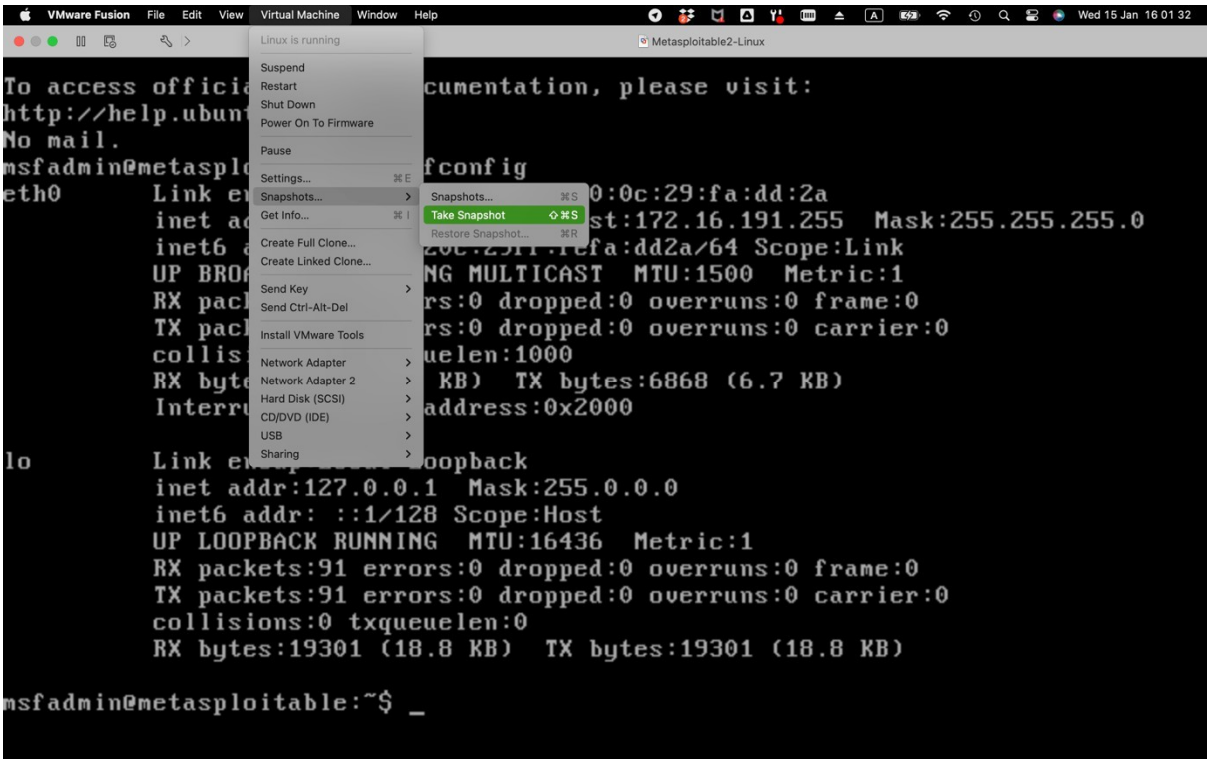


Output: Identified open ports, running services, and OS information of Metasploitable (Running In VMWare).

Task 9: Snapshots and Cleanup

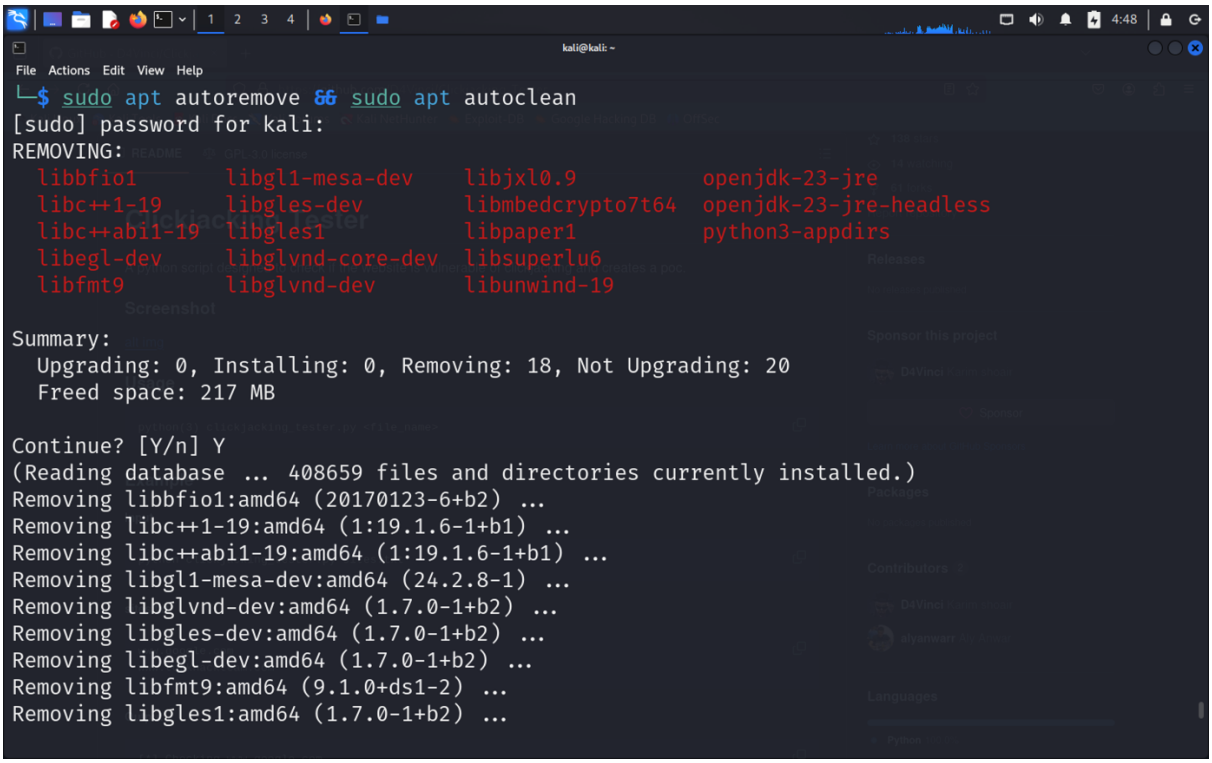
- Took snapshots of both VMs to save the current state.

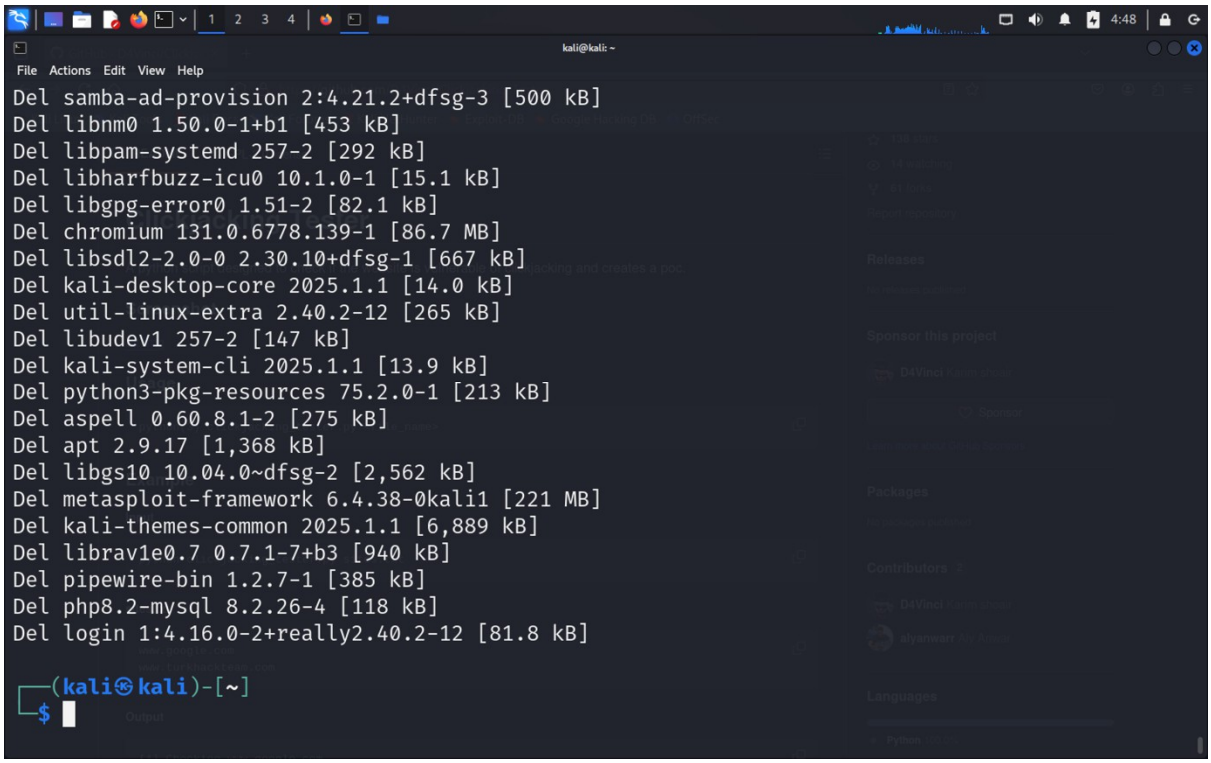




- Cleaned unnecessary files using:

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





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.