Week 1: Introduction to Cybersecurity and Virtualization

Name: V. Risvanth

Introduction

This internship focused on setting up a virtualized penetration testing lab using VirtualBox, Kali Linux, and Metasploitable 2. The primary objective was to understand the process of ethical hacking, security assessment, and vulnerability exploitation in a controlled environment. This report provides a detailed step-by-step guide to setting up the lab, performing reconnaissance, and conducting security assessments using Metasploit.

Table of Contents

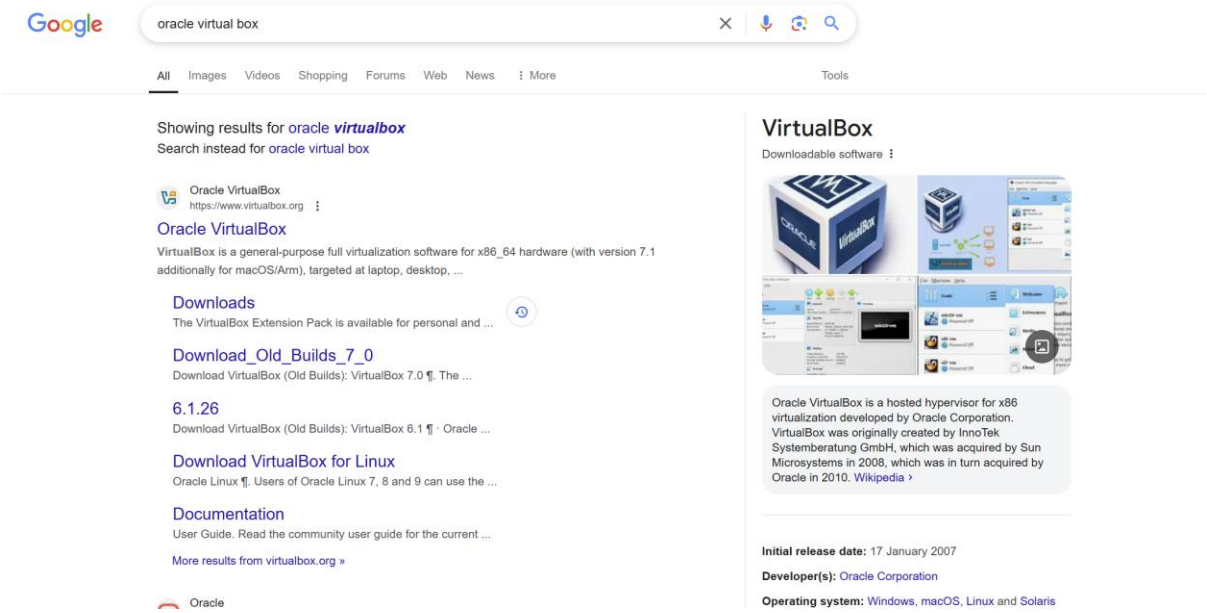
1. Virtualization Software Setup

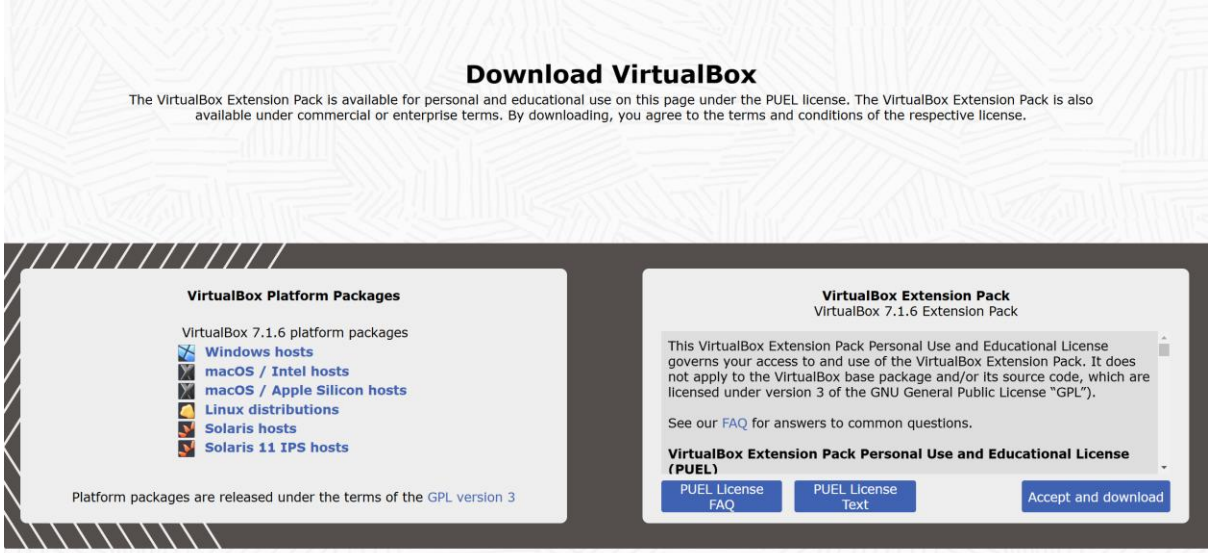
To enable the execution of multiple operating systems, a virtualization platform was installed. VirtualBox was chosen due to its ease of use and compatibility with various operating systems.

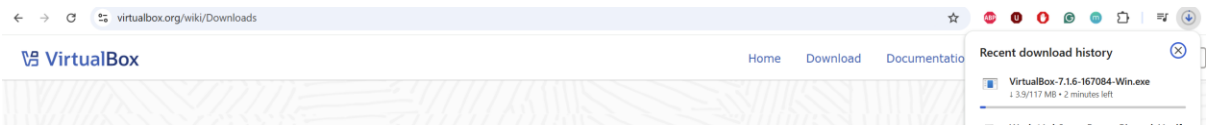
Steps to Install VirtualBox:

1. Download VirtualBox from the official website: https://www.virtualbox.org/.

2. Install VirtualBox by following the on-screen instructions.
3. Download and install the VirtualBox Extension Pack for additional features.
4. Verify the installation and ensure VirtualBox is running properly.







2. Kali Linux Setup

Kali Linux is a penetration testing and security auditing operating system. It was set up within VirtualBox to conduct security assessments.

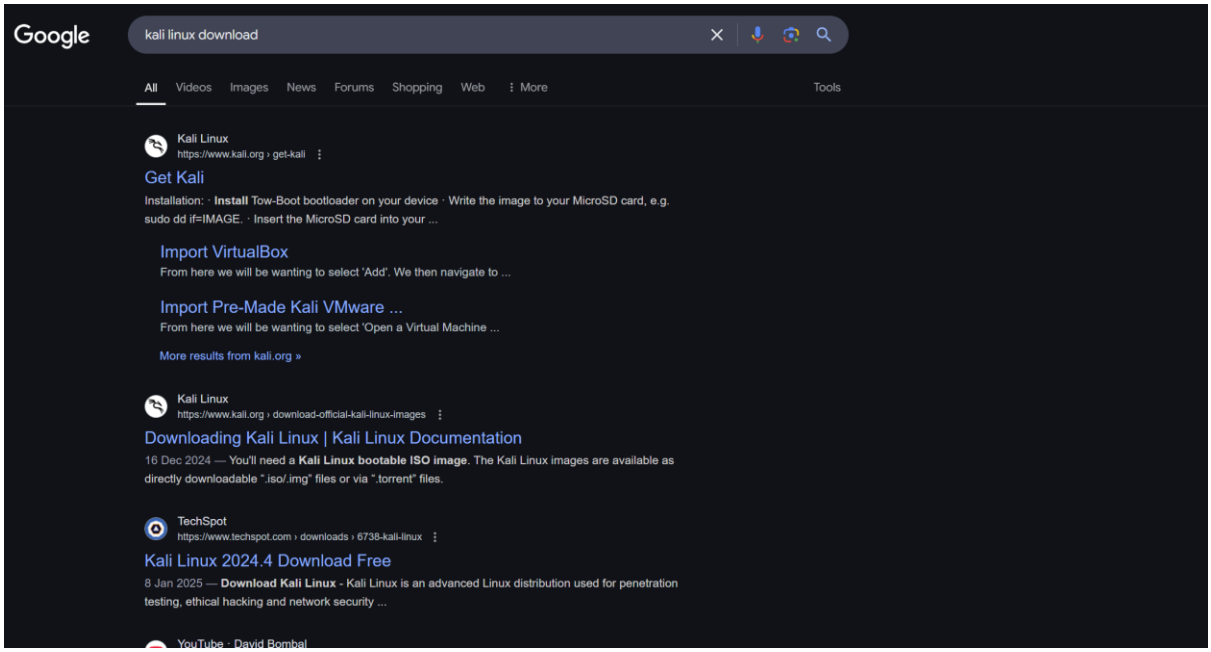
Steps to Install Kali Linux:

1. Download the Kali Linux ISO file from the official website: https://www.kali.org/getkali/.

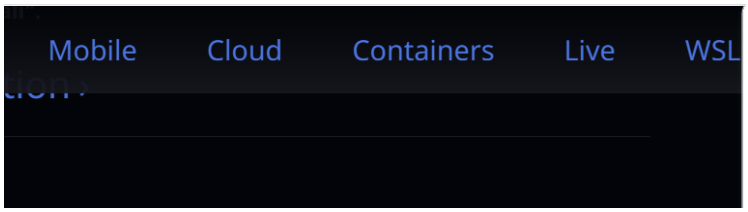
2. Open VirtualBox and create a new virtual machine.
3. Set the following VM configurations:
    - Name: Kali Linux
    - Type: Linux
    - Version: Debian (64-bit)
    - RAM: 4GB
    - Storage: 50GB (Dynamically Allocated)

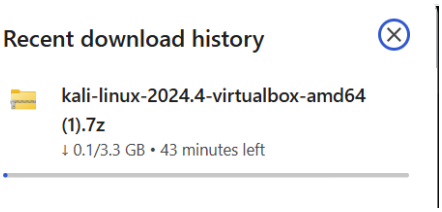
4. Attach the Kali Linux ISO file to the virtual machine.

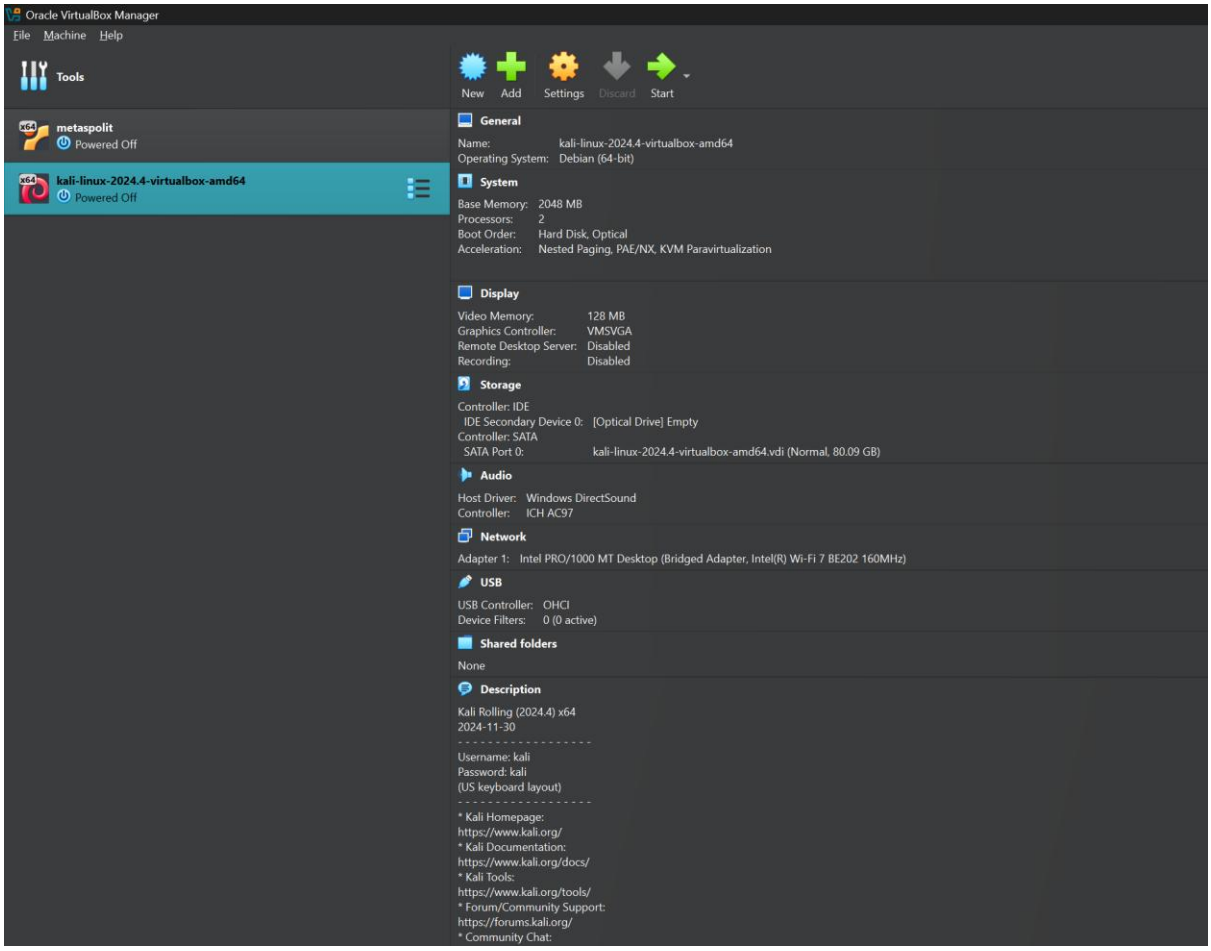
5. Start the VM and follow the installation steps:
    - Select graphical install
    - Configure language, region, and keyboard layout
    - Create a username and password
    - Select disk partitioning (use entire disk)
    - Complete the installation and reboo

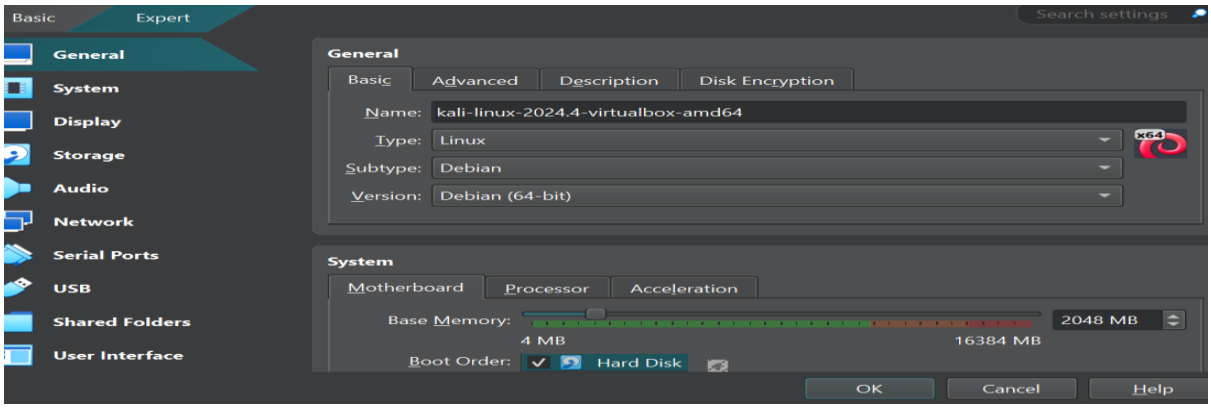

Google
kali linux download
All
Videos
Images
News
Forums
Shopping
Web
More
Tools
Kali Linux
https://www.kali.org › get-kali
Get Kali
Installation: · Install Tow-Boot bootloader on your device · Write the image to your MicroSD card, e.g. sudo dd if=IMAGE. · Insert the MicroSD card into your ...
Import VirtualBox
From here we will be wanting to select 'Add'. We then navigate to ...
Import Pre-Made Kali VMware ...
From here we will be wanting to select 'Open a Virtual Machine ...
More results from kali.org »
Kali Linux
https://www.kali.org › download-official-kali-linux-images
Downloading Kali Linux | Kali Linux Documentation
16 Dec 2024 — You'll need a Kali Linux bootable ISO image. The Kali Linux images are available as directly downloadable ".iso/.img" files or via ".torrent" files.
TechSpot
https://www.techspot.com › downloads › 6738-kali-linux
Kali Linux 2024.4 Download Free
8 Jan 2025 — Download Kali Linux - Kali Linux is an advanced Linux distribution used for penetration testing, ethical hacking and network security ...

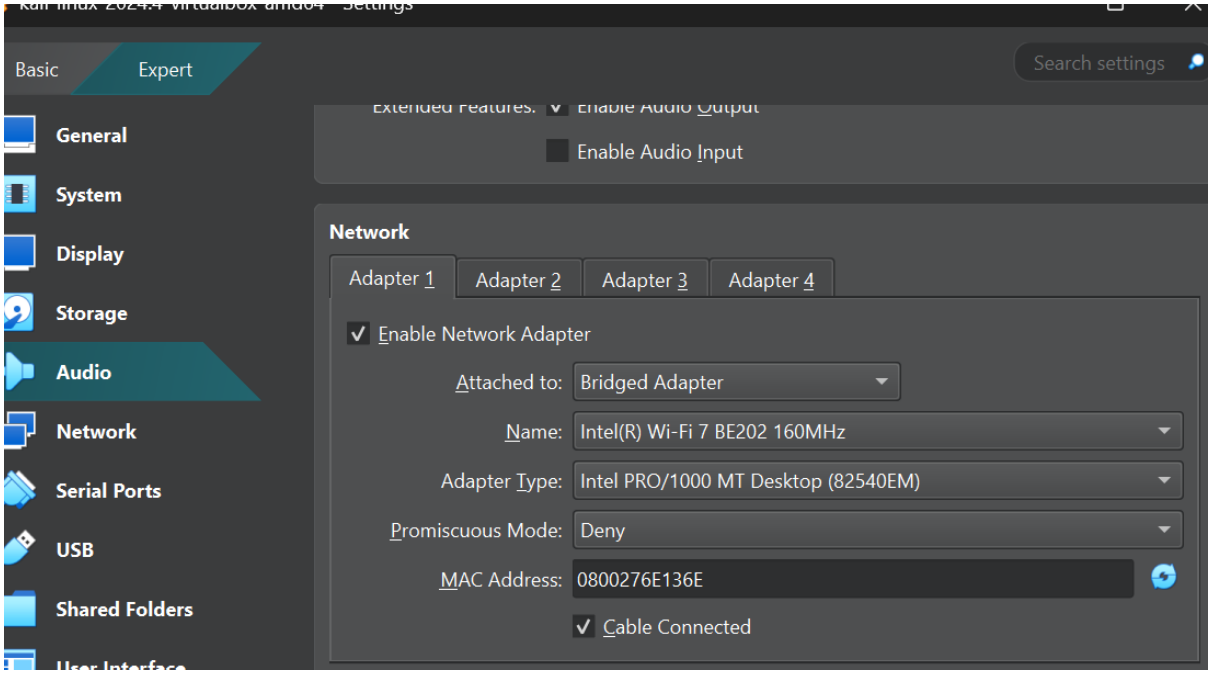

Recommended
VMware
torrent
docs
sum
Recommended
VirtualBox
torrent
docs
sum
Recommended
Hyper-V
torrent
docs
sum
Recommended
QEMU
torrent
docs
sum
VMware Weekly
repository
sum
VirtualBox Weekly
repository
sum
Hyper-V Weekly
repository
sum
QEMU Weekly
repository
sum

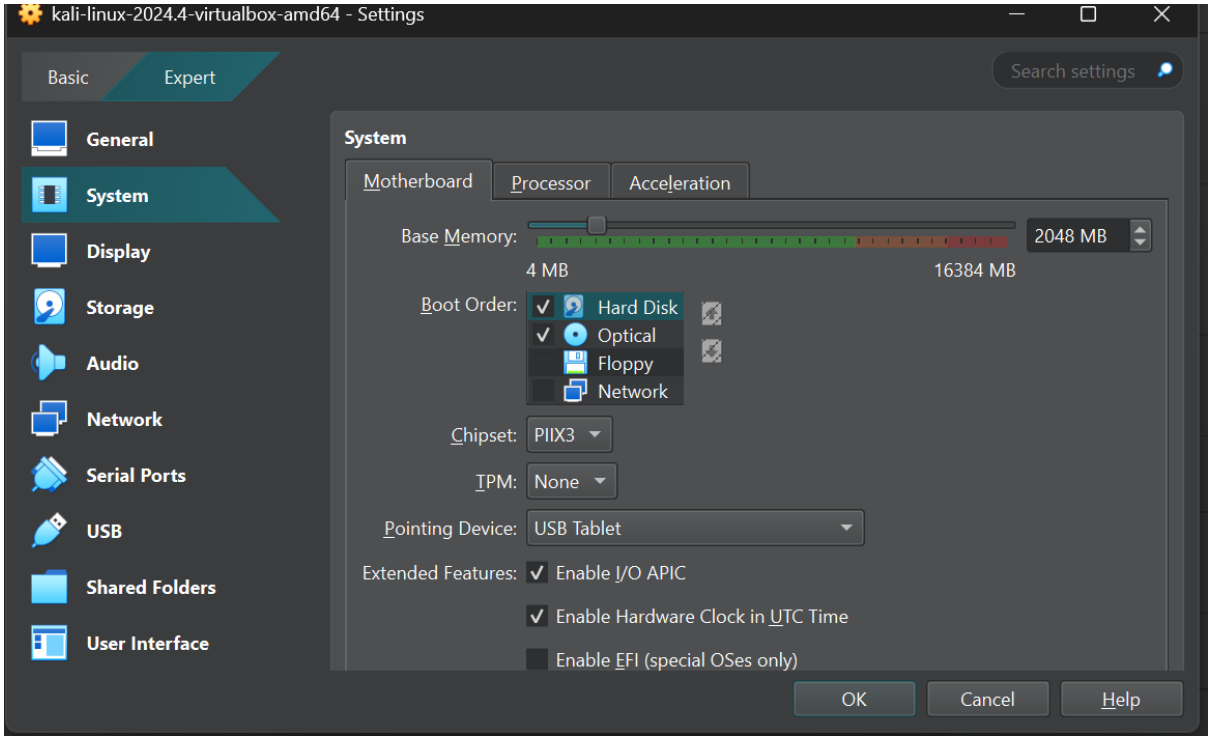

Mobile
Cloud
Containers
Live
WSL

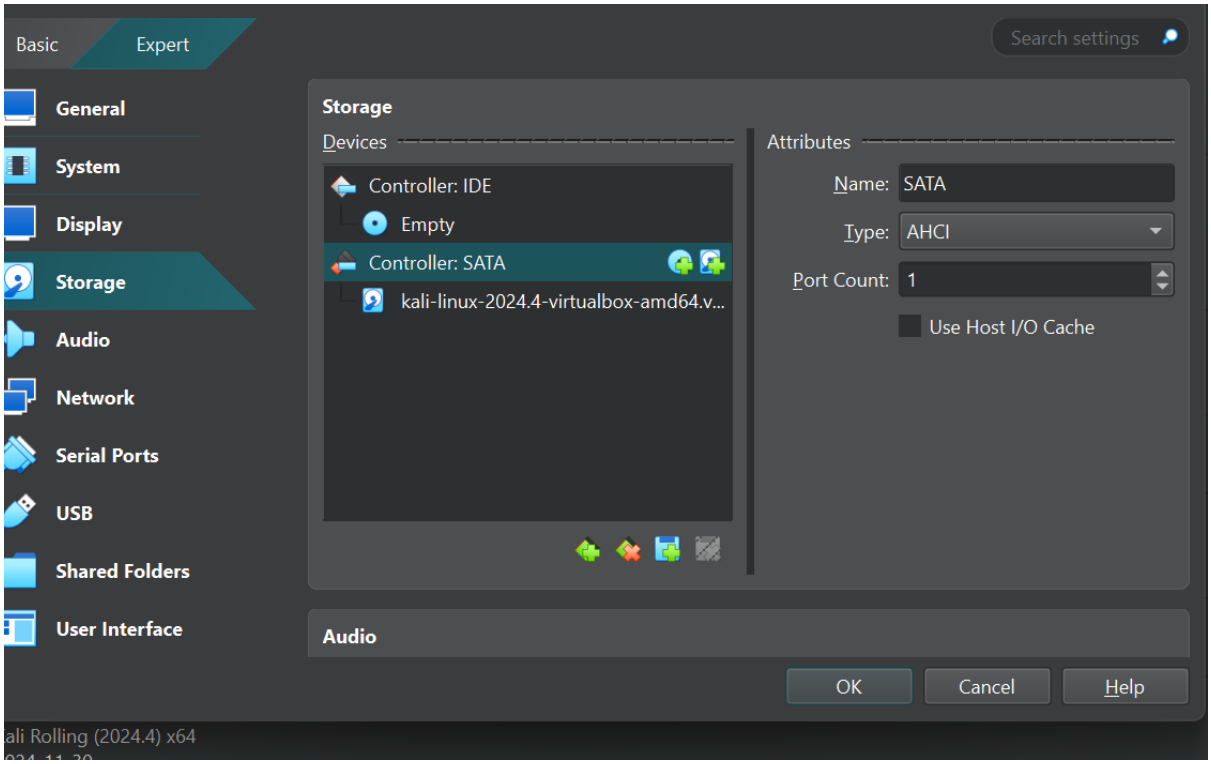

Recent download history
kali-linux-2024.4-virtualbox-amd64 (1).7z
↓ 0.1/3.3 GB • 43 minutes left

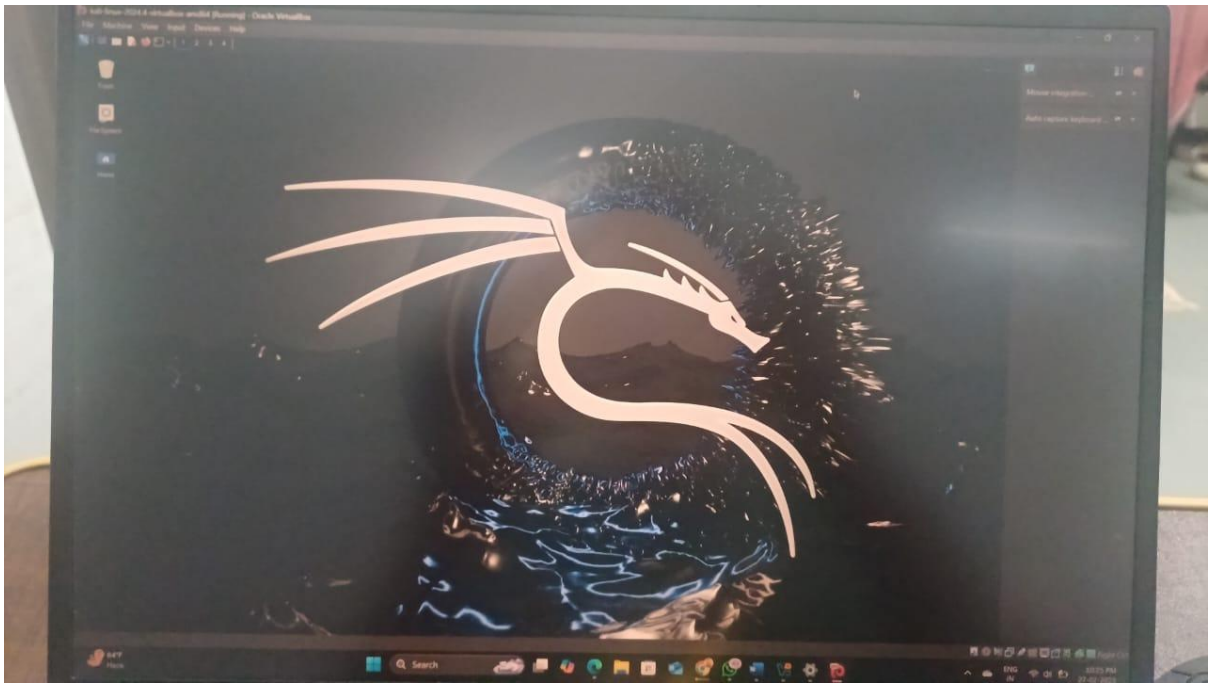

Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Start
metaspolit
Powered Off
kali-linux-2024.4-virtualbox-amd64
Powered Off
General
Name: kali-linux-2024.4-virtualbox-amd64
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2024.4-virtualbox-amd64.vdi (Normal, 80.09 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Wi-Fi 7 BE202 160MHz)
USB
USB Controller: OHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
Kali Rolling (2024.4) x64
2024-11-30
Username: kali
Password: kali
(US keyboard layout)
* Kali Homepage:
https://www.kali.org/
* Kali Documentation:
https://www.kali.org/docs/
* Kali Tools:
https://www.kali.org/tools/
* Forum/Community Support:
https://forums.kali.org/
* Community Chat:


Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
General
Basic
Advanced
Description
Disk Encryption
Name: kali-linux-2024.4-virtualbox-amd64
Type: Linux
Subtype: Debian
Version: Debian (64-bit)
System
Motherboard
Processor
Acceleration
Base Memory:
2048 MB
4 MB
16384 MB
Boot Order:
Hard Disk
OK
Cancel
Help


Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
Enable Audio Input
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: Intel(R) Wi-Fi 7 BE202 160MHz
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 0800276E136E
Cable Connected


kali-linux-2024.4-virtualbox-amd64 - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
2048 MB
4 MB
16384 MB
Boot Order:
Hard Disk
Optical
Floppy
Network
Chipset: PIIX3
TPM: None
Pointing Device: USB Tablet
Extended Features: Enable I/O APIC
Enable Hardware Clock in UTC Time
Enable EFI (special OSes only)
OK
Cancel
Help


Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Devices
Controller: IDE
Empty
Controller: SATA
kali-linux-2024.4-virtualbox-amd64.v...
Attributes
Name: SATA
Type: AHCI
Port Count: 1
Use Host I/O Cache
Audio
OK
Cancel
Help
ali Rolling (2024.4) x64

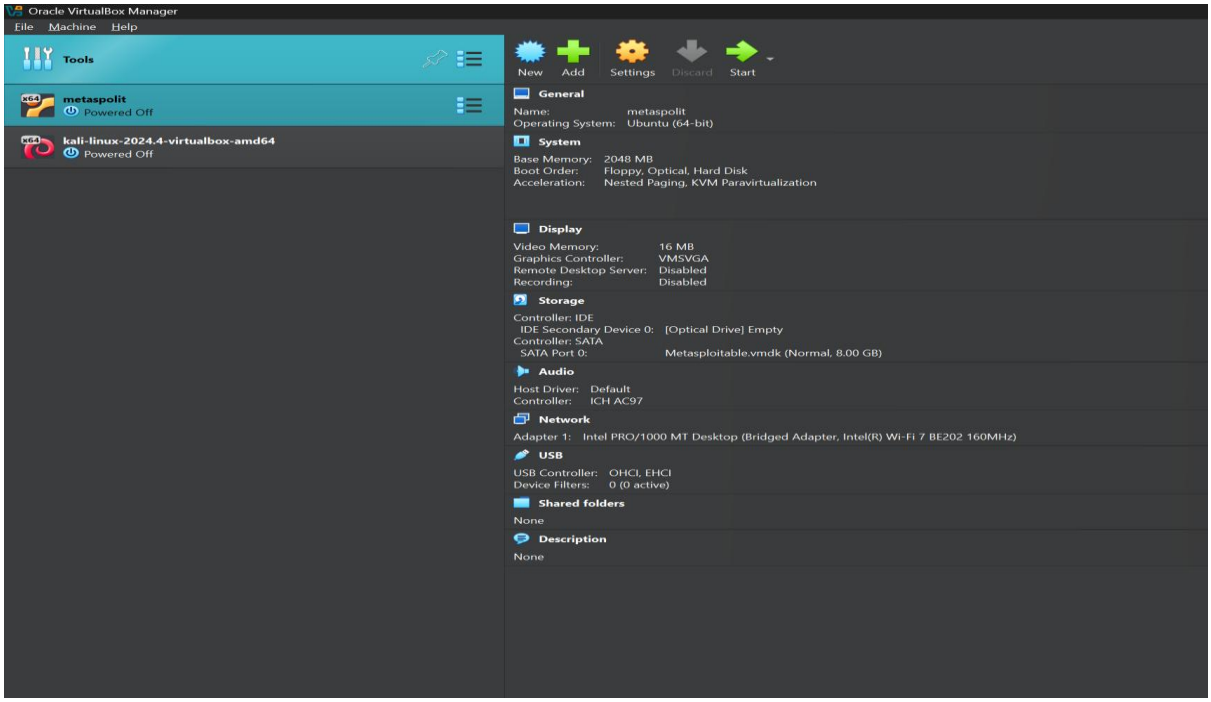


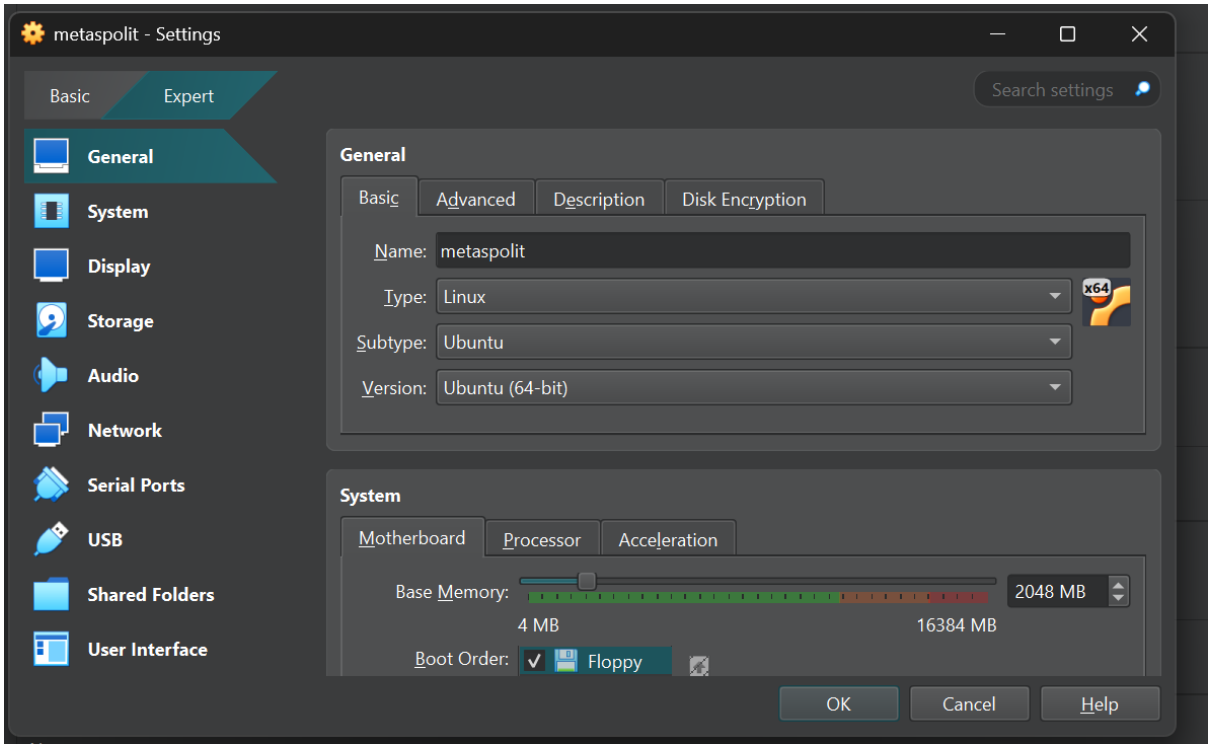
3. Metasploitable 2 Setup

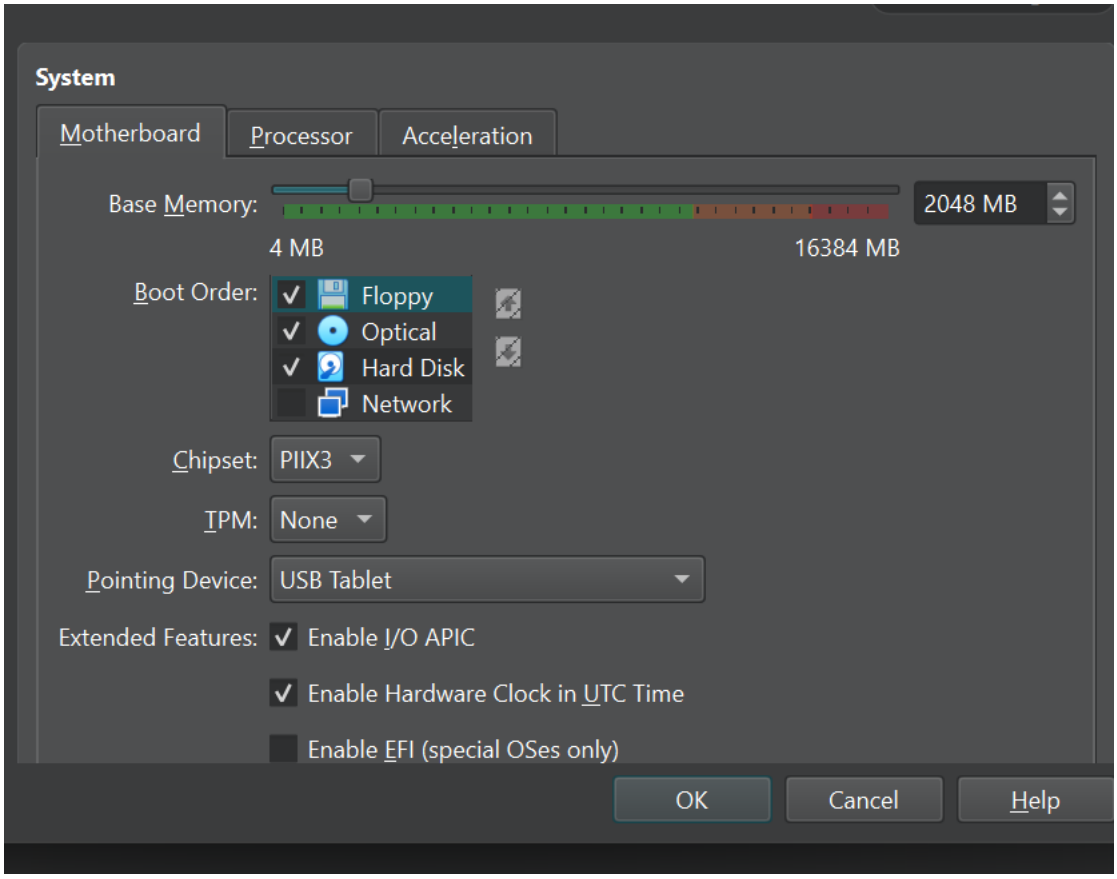
Metasploitable 2 is a deliberately vulnerable virtual machine used for penetration testing practice. It was installed to serve as a target for security assessments.

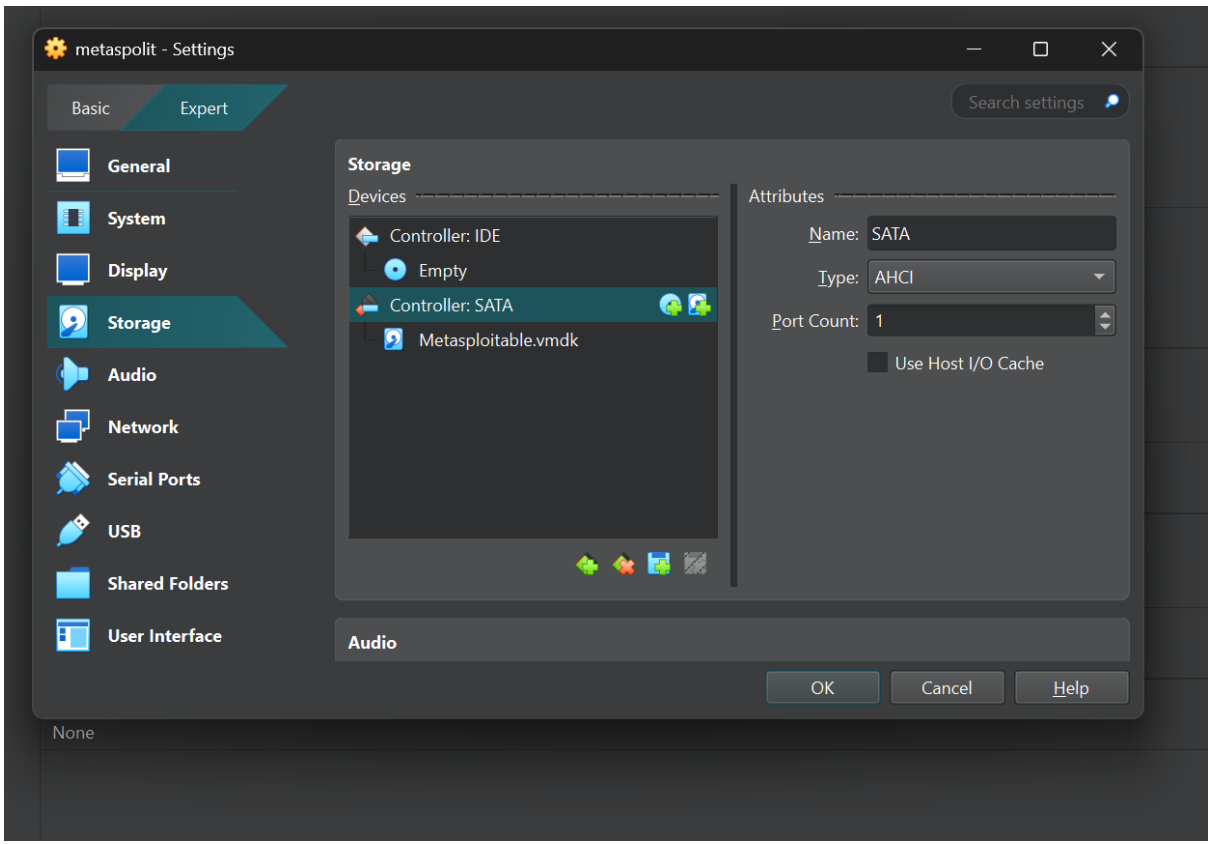
Steps to Install Metasploitable 2:

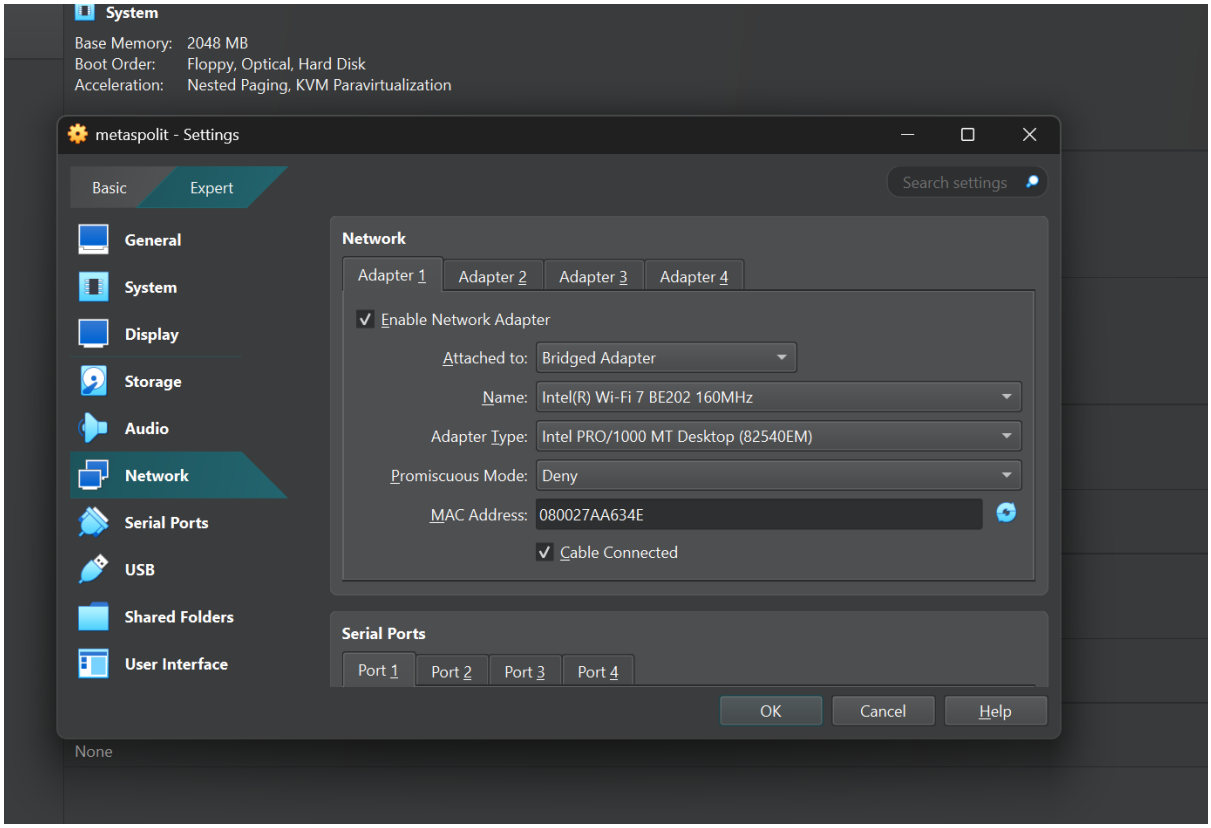
1. **Download SourceForge: https://sourceforge.net/projects/metasploitable/.**
2. **Open VirtualBox and create a new virtual machine.**
3. **Set the following VM configurations:**
    - **Name: Metasploitable 2**
    - **Type: Linux**
    - **Version: Ubuntu (64-bit)**
    - **RAM: 512MB**
    - **Storage: 8GB (Dynamically Allocated)**
4. **Attach the Metasploitable 2 VMDK file to the virtual machine.**
5. **Start the VM and log in using the default credentials:**
    - **Username: msfadmin**
    - **Password: msfadmin**
6. **Verify the installation and check network settings.**
7. **Metasploitable ip is 192.168.198.138**

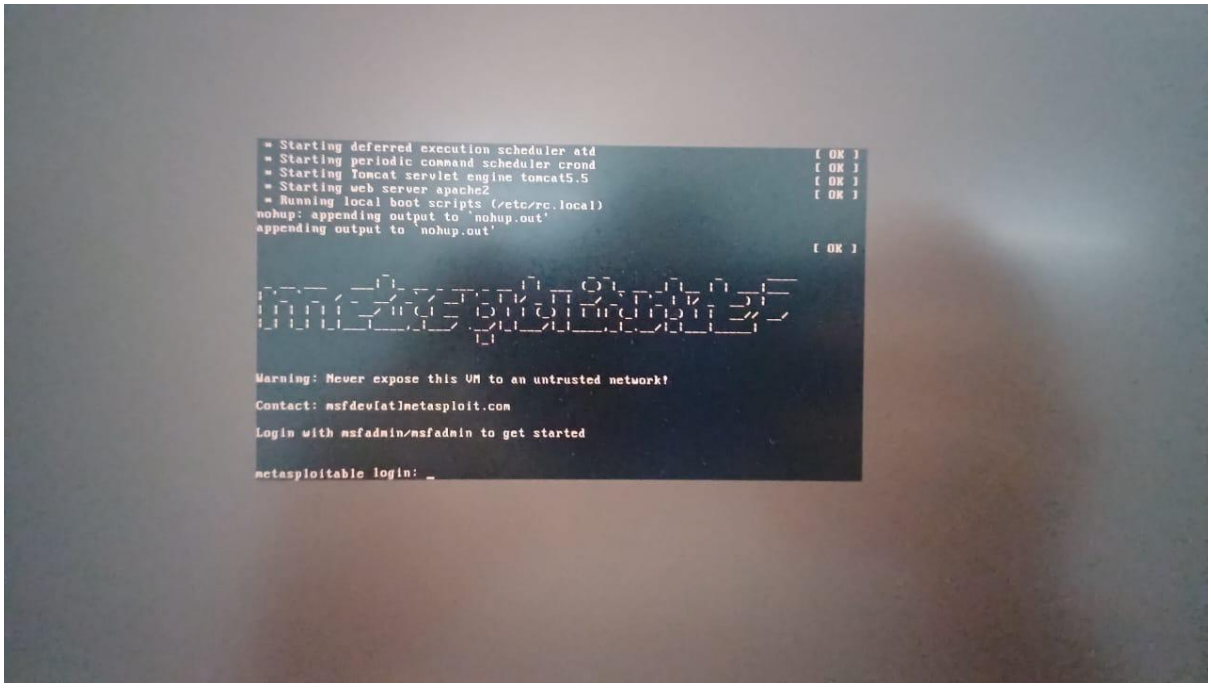

Oracle VirtualBox Manager
File Machine Help
Tools
metaspolit
Powered Off
kali-linux-2024.4-virtualbox-amd64
Powered Off
New Add Settings Discard Start
General
Name: metaspolit
Operating System: Ubuntu (64-bit)
System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)
Audio
Host Driver: Default
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Wi-Fi 7 BE202 160MHz)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None

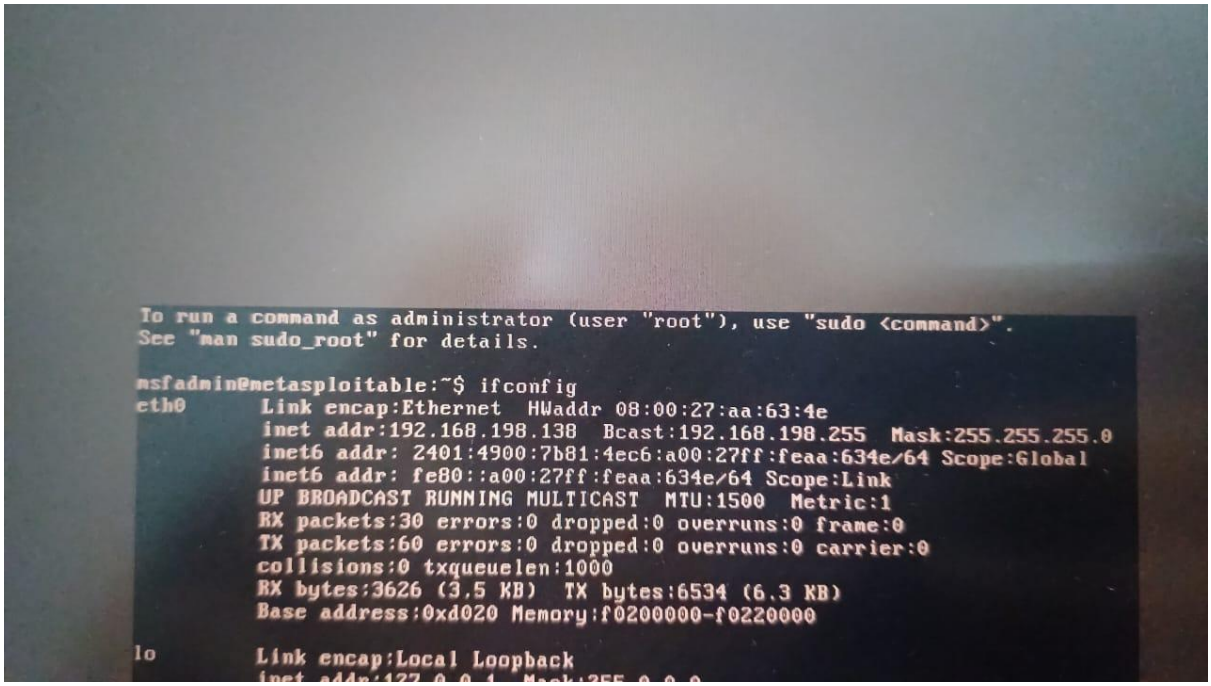

metaspolit - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
General
Basic
Advanced
Description
Disk Encryption
Name: metaspolit
Type: Linux
Subtype: Ubuntu
Version: Ubuntu (64-bit)
System
Motherboard
Processor
Acceleration
Base Memory:
2048 MB
4 MB
16384 MB
Boot Order:
Floppy
OK
Cancel
Help


System
Motherboard
Processor
Acceleration
Base Memory:
2048 MB
4 MB
16384 MB
Boot Order:
Floppy
Optical
Hard Disk
Network
Chipset:
PIIX3
TPM:
None
Pointing Device:
USB Tablet
Extended Features:
Enable I/O APIC
Enable Hardware Clock in UTC Time
Enable EFI (special OSes only)
OK
Cancel
Help


metaspolit - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Devices
Controller: IDE
Empty
Controller: SATA
Metasploitable.vmdk
Attributes
Name:
SATA
Type:
AHCI
Port Count:
1
Use Host I/O Cache
Audio
OK
Cancel
Help
None


System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization
metaspolit - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: Intel(R) Wi-Fi 7 BE202 160MHz
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027AA634E
Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
OK
Cancel
Help
None


* 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'
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: _



4. Initial Reconnaissance

Nmap Scan Summary

Command Used:

1. Service Version Detection Scan (SV Scan)

nmap -sV 44.228.249.3

Purpose

1.Identifies versions of services running on open ports.

2. Helps in detecting vulnerabilities based on software versions.

2. Aggressive Scan

nmap -A 44.228.249.3

Purpose

1. Combines multiple scans, including OS detection, version detection, script scanning, and traceroute.

2. Provides detailed information about the target.

3. Ping Scan on Port 80

nmap -sn -p 80 44.228.249.3

Purpose

1. Checks if the target is up by scanning only port 80.

2. Useful for verifying web server availability.

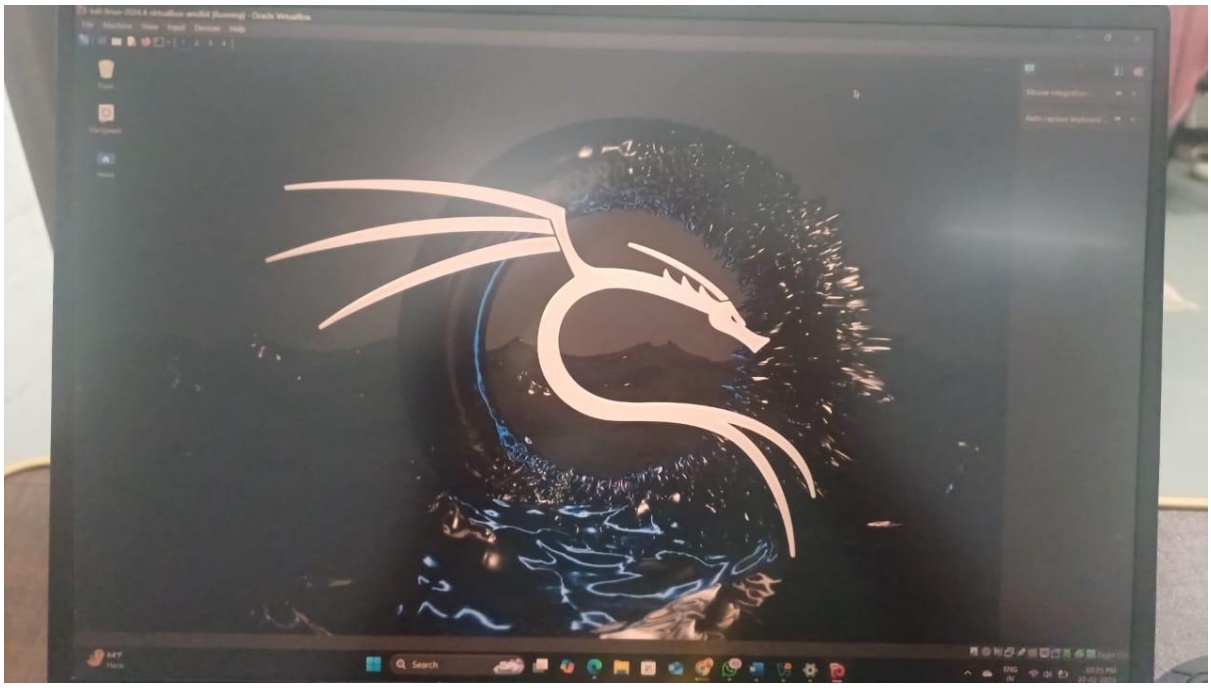
4. Fast Scan (F Scan)

nmap -F 44.228.249.3

Purpose

1. Scans only the top 100 most common ports instead of all 65,535 ports.

2. Provides a quick overview of open services without a full deep scan.

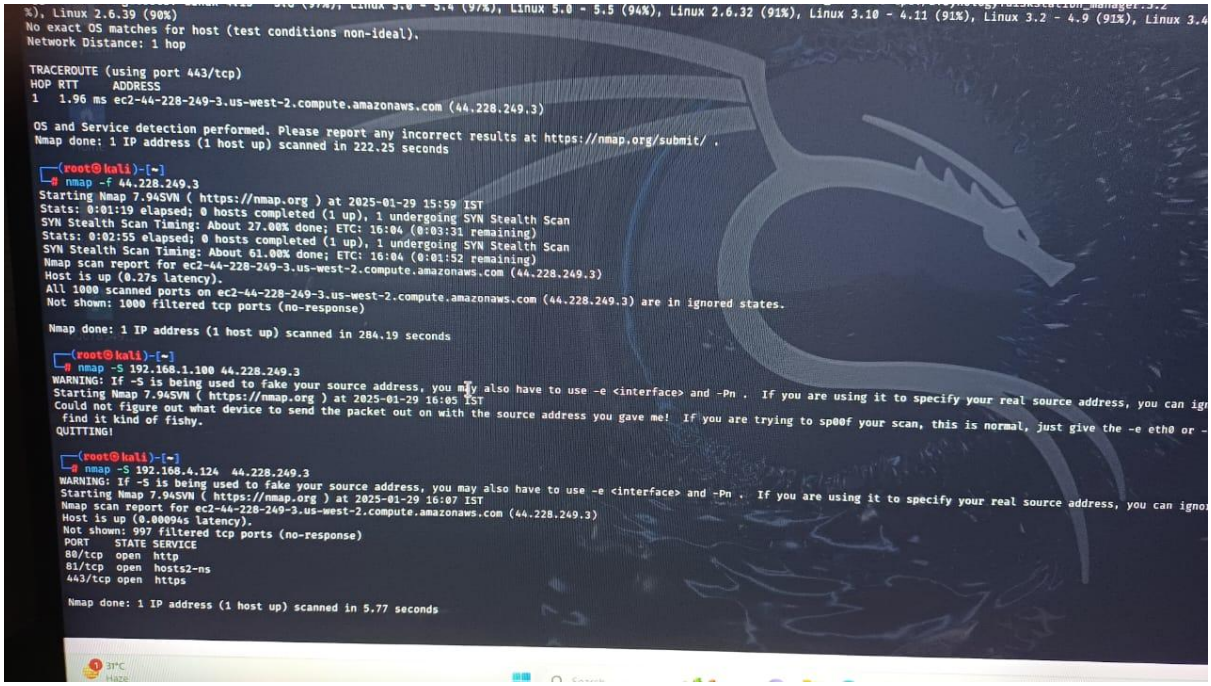


```
File Actions Edit View Help                                  root@kali: ~

┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.4.124  netmask 255.255.255.0  broadcast 192.168.4.255
        inet6 fe80::8aa4:f2df:7f24:5261  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d2:26:79  txqueuelen 1000  (Ethernet)
        RX packets 2341  bytes 236274 (230.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10185  bytes 638529 (623.5 KiB)
        TX errors 0  dropped 0 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 133078  bytes 5589420 (5.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 133078  bytes 5589420 (5.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kali)-[~]
└─# nmap -sn 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:28 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00057s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

┌──(root㉿kali)-[~]
└─# nmap -p 80, 443 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:28 IST
Nmap scan report for 443 (0.0.1.187)
Host is up (0.00094s latency).
```

```
File Actions Edit View Help                                  root@kali: ~

┌──(root㉿kali)-[~]
└─# nmap -sn 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:28 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00057s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

┌──(root㉿kali)-[~]
└─# nmap -p 80, 443 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:28 IST
Nmap scan report for 443 (0.0.1.187)
Host is up (0.00094s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0011s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.36 seconds

┌──(root㉿kali)-[~]
└─# nmap -p 443 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:29 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00057s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(root㉿kali)-[~]
└─# nmap -p- 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:29 IST
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.93% done; ETC: 15:32 (0:02:38 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0011s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
81/tcp   open  hosts2-ns
443/tcp open  https
```

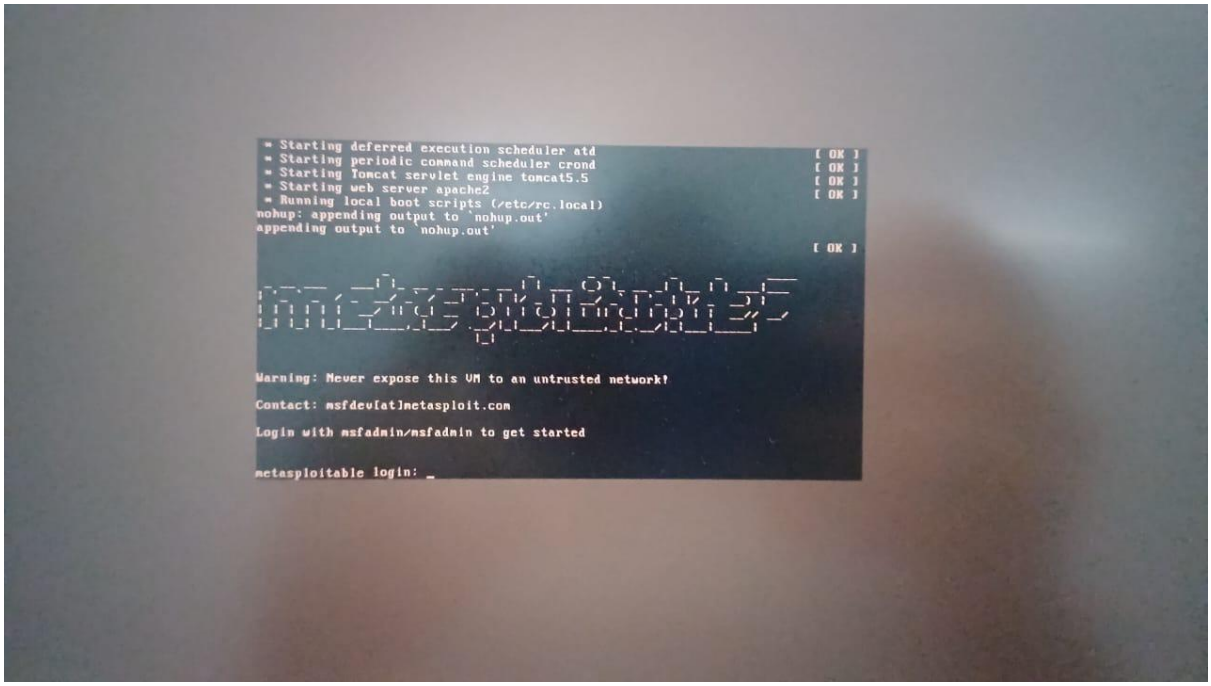
```
80/tcp  open  http
81/tcp  open  hosts2-ns
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 135.05 seconds

┌──(root㉿kali)-[~]
└─# nmap -sV 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:32 IST
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.24% done; ETC: 15:33 (0:00:00 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00096s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy DansGuardian HTTP proxy
81/tcp  open  http-proxy DansGuardian HTTP proxy
443/tcp open  https?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.22 seconds
```

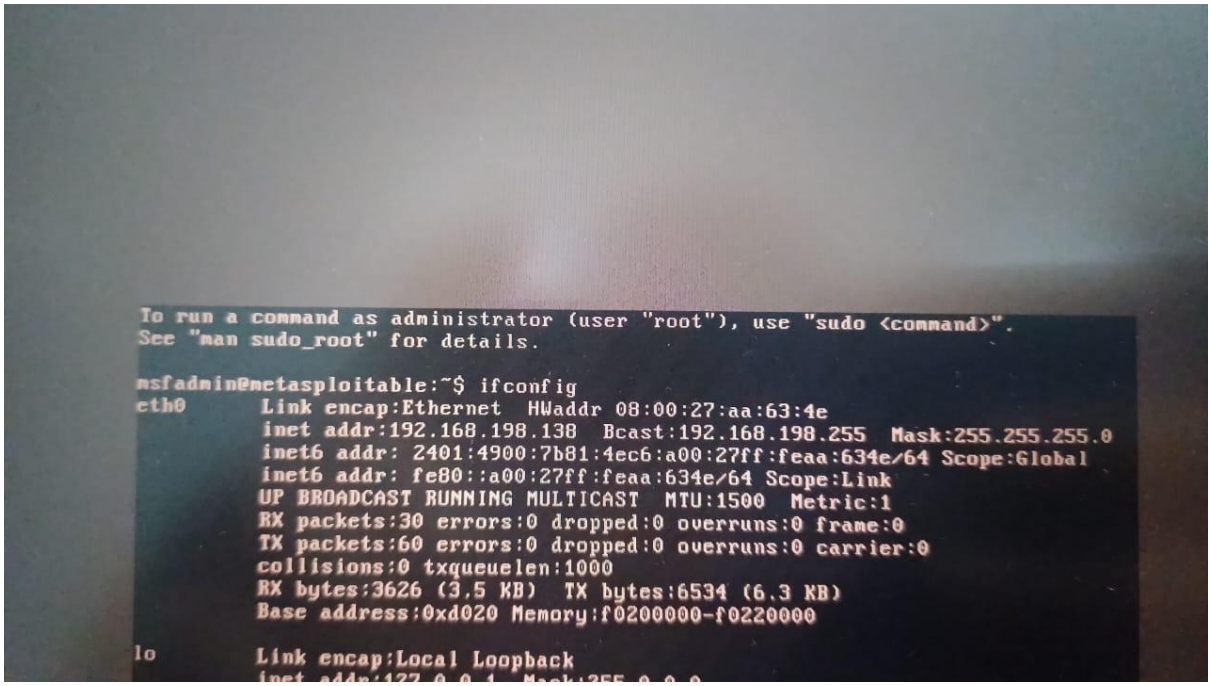
```
File  Actions  Edit  View  Help                                  root@kali: ~

┌──(root㉿kali)-[~]
└─# nmap -A 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:55 IST
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.53% done; ETC: 15:56 (0:00:00 remaining)
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.53% done; ETC: 15:56 (0:00:00 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy DansGuardian HTTP proxy
|_http-server-header: squid/5.9
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported: HEAD CONNECTION
|_http-title: Problem loading page
81/tcp  open  http-proxy DansGuardian HTTP proxy
|_http-server-header: squid/5.9
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported: HEAD CONNECTION
443/tcp open  https?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), Synology DiskStation Manager 5.X (89%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/a:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.0 - 5.5 (94%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91%), Linux 3.4 - 3.
%), Linux 2.6.39 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   1.96 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 222.25 seconds

┌──(root㉿kali)-[~]
└─# nmap -f 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:59 IST
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.00% done; ETC: 16:04 (0:03:31 remaining)
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.00% done; ETC: 16:04 (0:01:52 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.27s latency).
```



5.Finding Metaspolitable Ip address

Metasploitable ip is 192.168.198.138

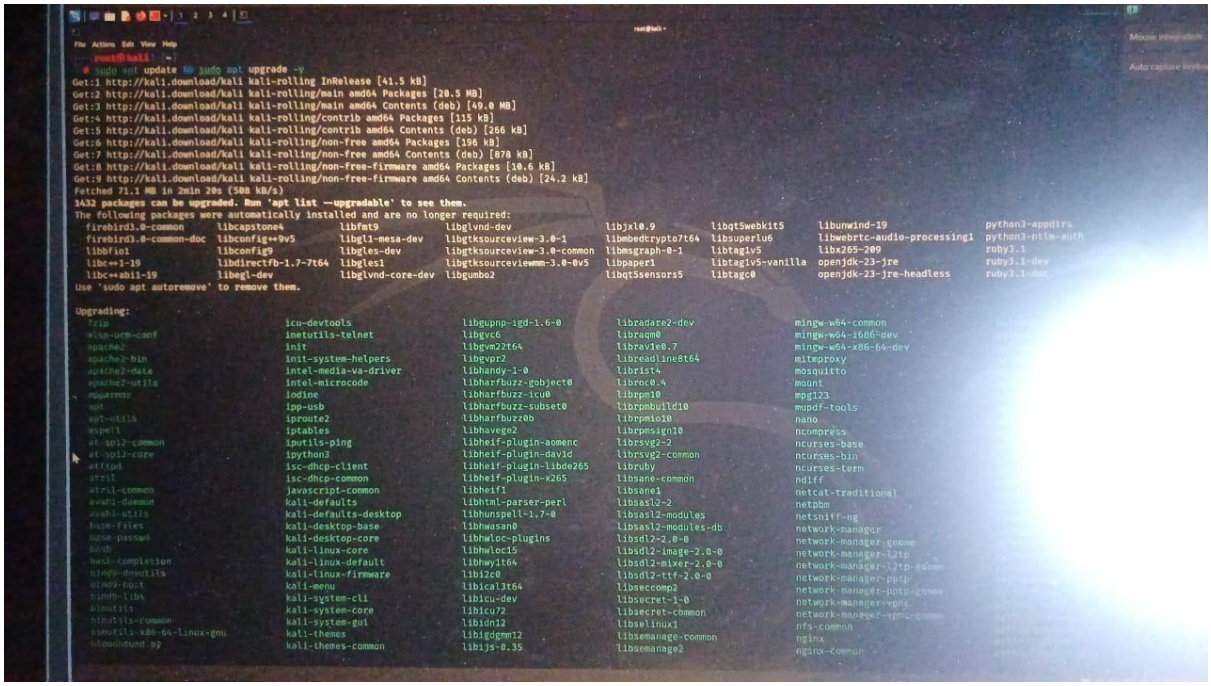


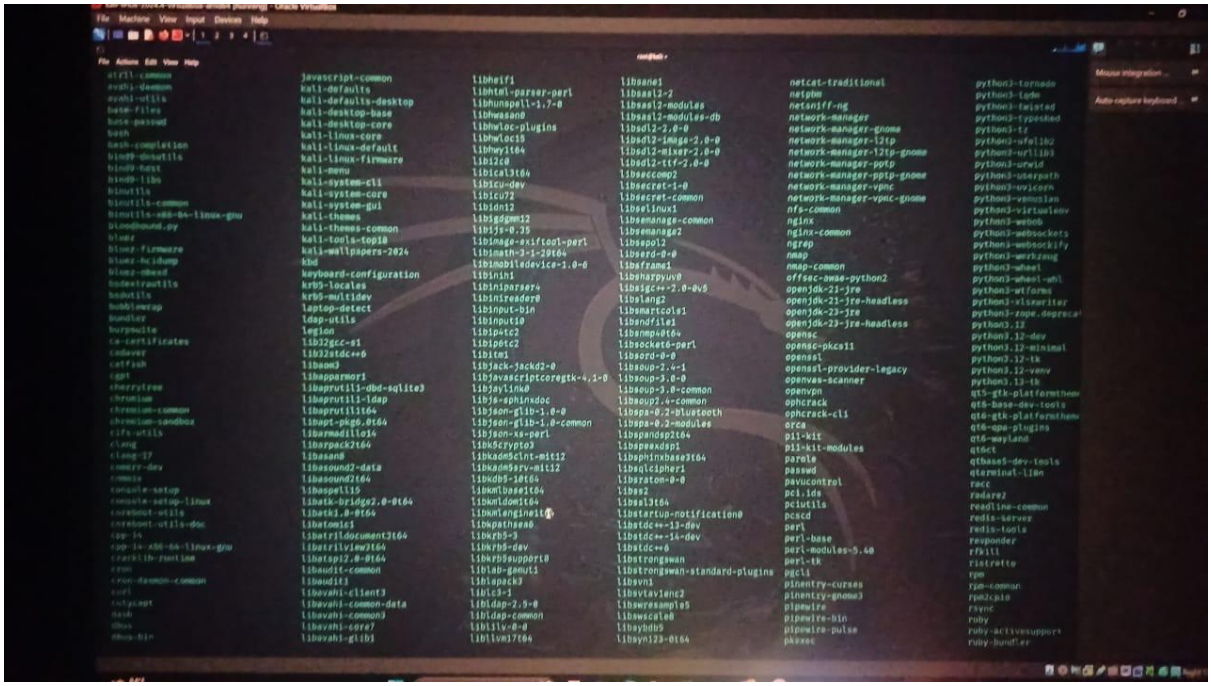


6: Updating and Configuring Kali Linux

Updated Kali Linux using:

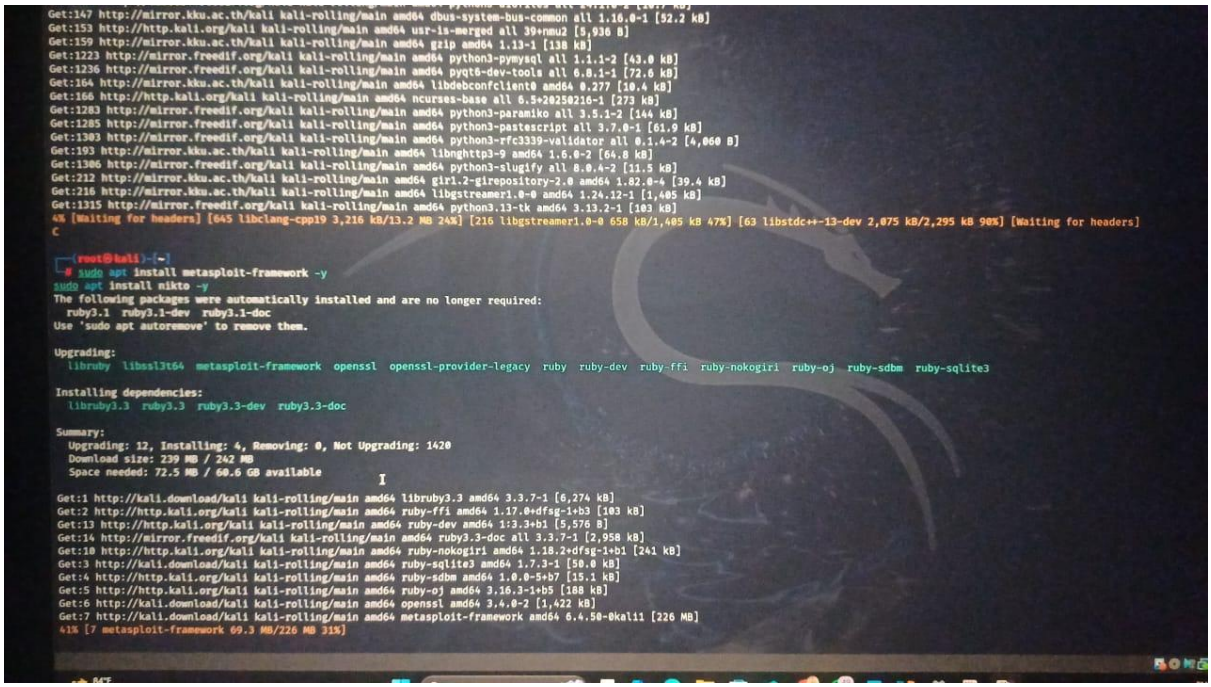
sudo apt update && sudo apt upgrade -y



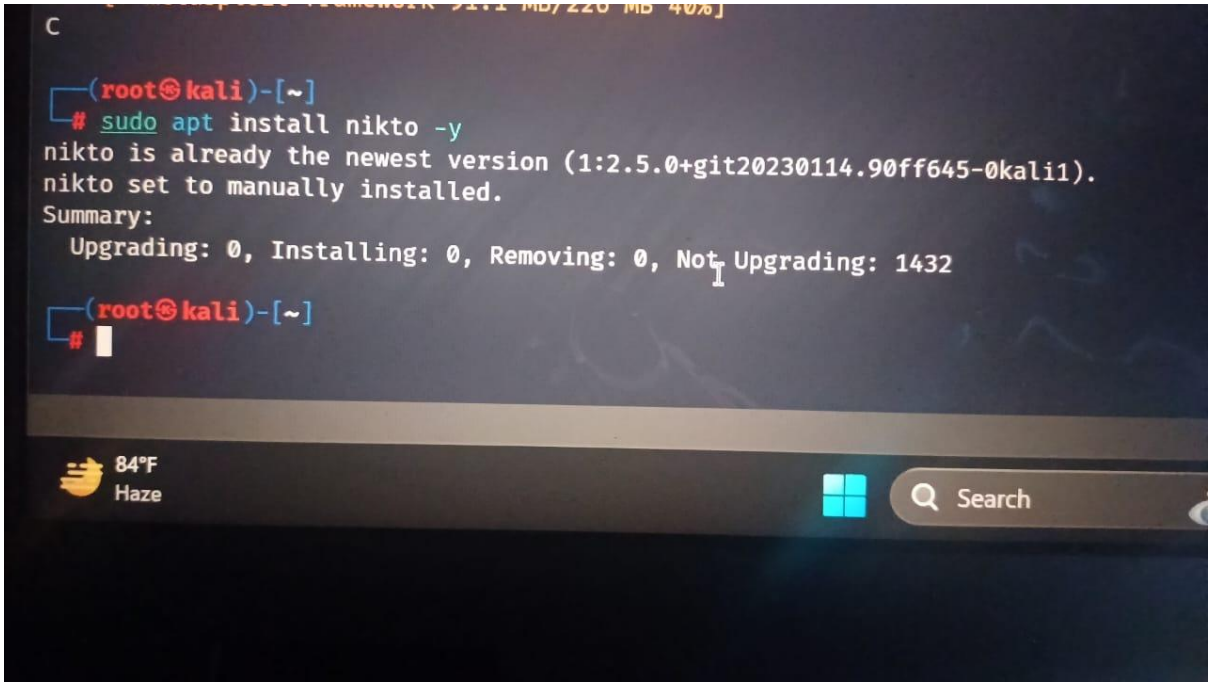


Installed additional tools for penetration testing:

sudo apt install metasploit-framework -y



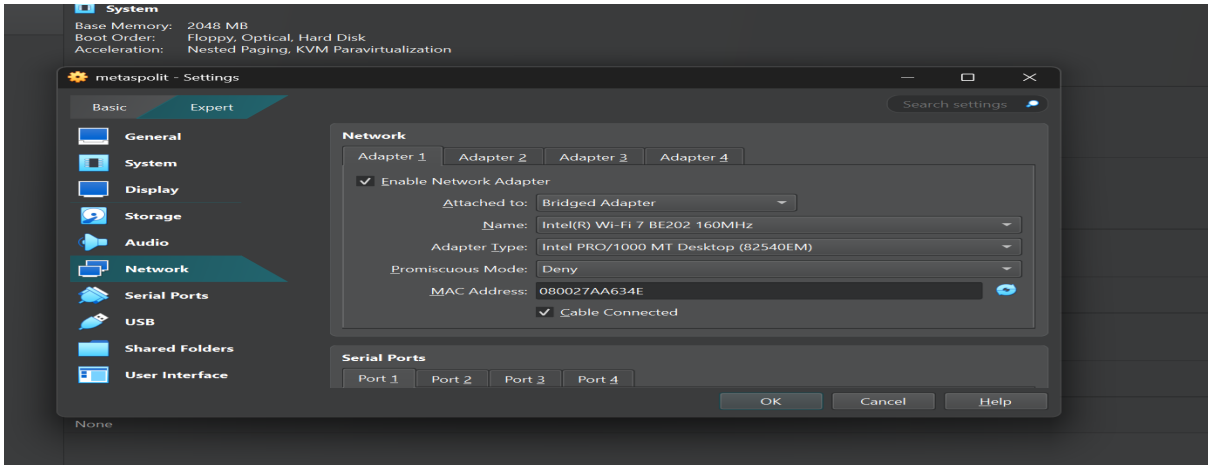
sudo apt install nikto -y



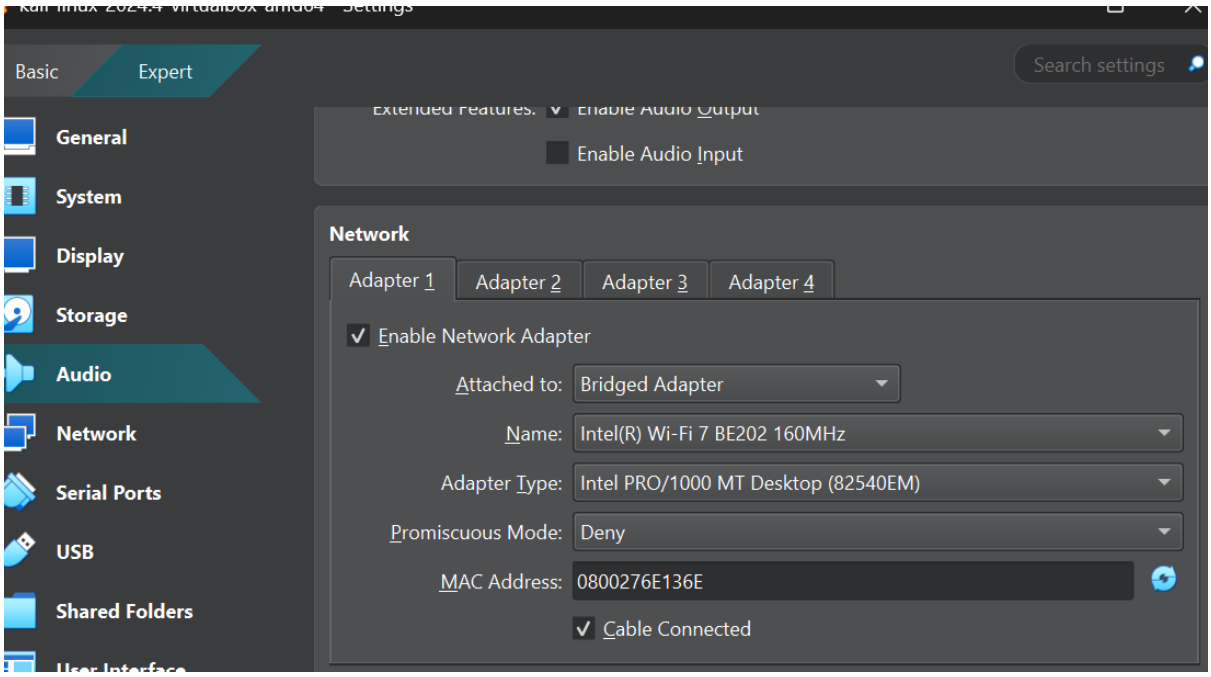
7. Configure Networking

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

For Metasploitable2

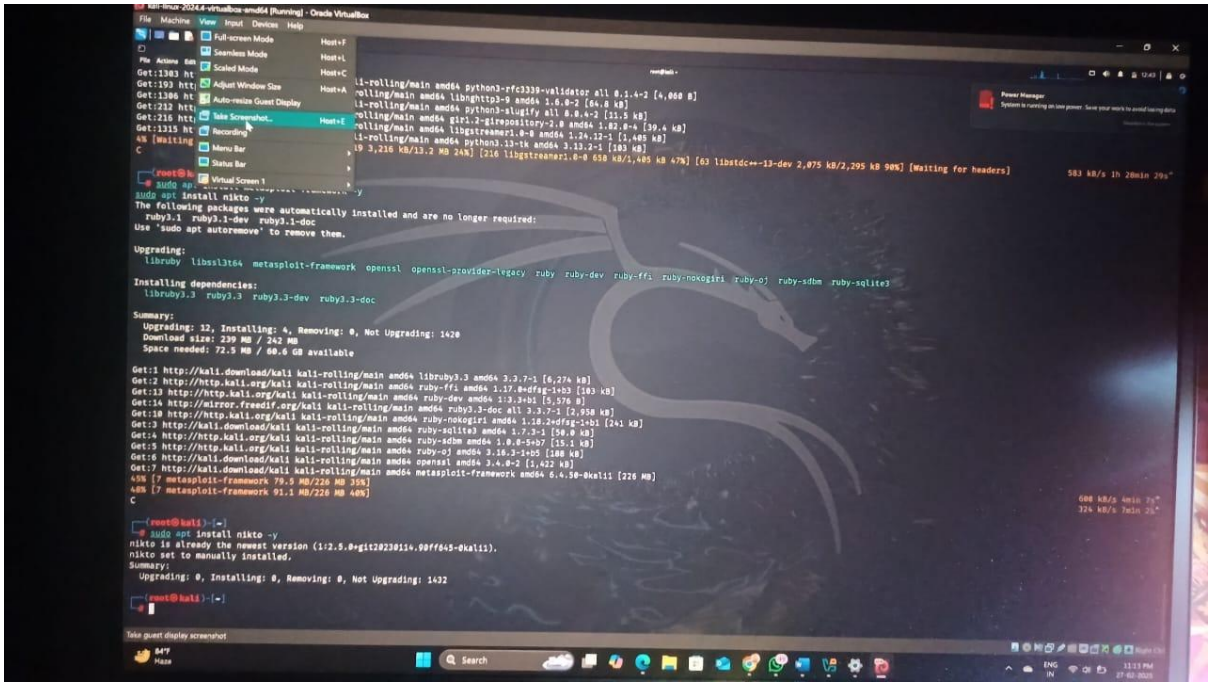


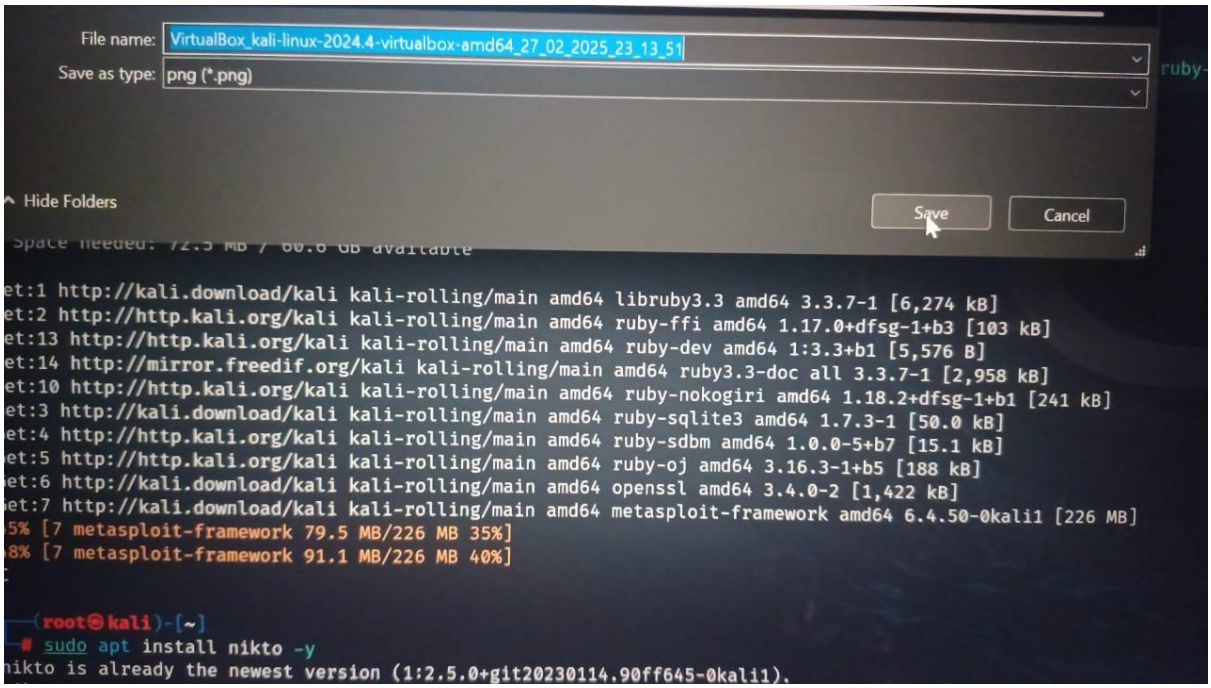
For Kali Linux



9. Snapshots and Cleanup Process

After performing the Nmap scans and security assessments, it is essential to take snapshots of the virtual machines and clean up unnecessary files to maintain an organized and stable lab environment.





sudo apt autoremove && sudo apt autoclean

```
┌──(root㉿kali)-[~]
└─# sudo apt autoremove && sudo apt autoclean

REMOVING:
  imagemagick-6.q16

Summary:
  Upgrading: 0, Installing: 0, Removing: 1, Not Upgrading: 1426
  Freed space: 581 kB
```

Final Takeaways and Findings

- **Virtualization Setup:** Successfully installed and configured **Kali Linux and Metasploitable**.
- **Networking:** Configured a **Bridged Network Adapter** for communication between VMs.
- **Reconnaissance:** Conducted scans using **Nmap and fscan**, identifying vulnerabilities.
- **Exploitation:** Successfully exploited **vsFTPd 2.3.4** using **Metasploit**.
- **System Maintenance:** Performed cleanup and took snapshots to preserve the lab state.

Conclusion

The successful setup of a virtual cybersecurity lab with Kali Linux and Metasploitable provides a safe environment for penetration testing and security assessments. By configuring networking properly, we enabled effective communication between the virtual machines. Initial reconnaissance using Nmap and fscan helped identify open ports and vulnerabilities, such as vsFTPd 2.3.4.

Exploitation using Metasploit demonstrated real-world attack scenarios. Regular snapshots and cleanup processes ensured a stable and organized lab environment. This hands-on experience enhanced our understanding of cybersecurity tools and techniques. Moving forward, further security assessments and advanced exploitation techniques can be explored to strengthen ethical hacking skills.