|| सिद्धिः भूषयते विद्याम् ||
avantika
UNIVERSITY

Assignment 1

Kali Linux Virtual Machine Setup and Basics

SUBMITTED BY
Mohit Bansal
(AU23E1016)

SUBMITTED TO
Dr. Vaishali Sharma

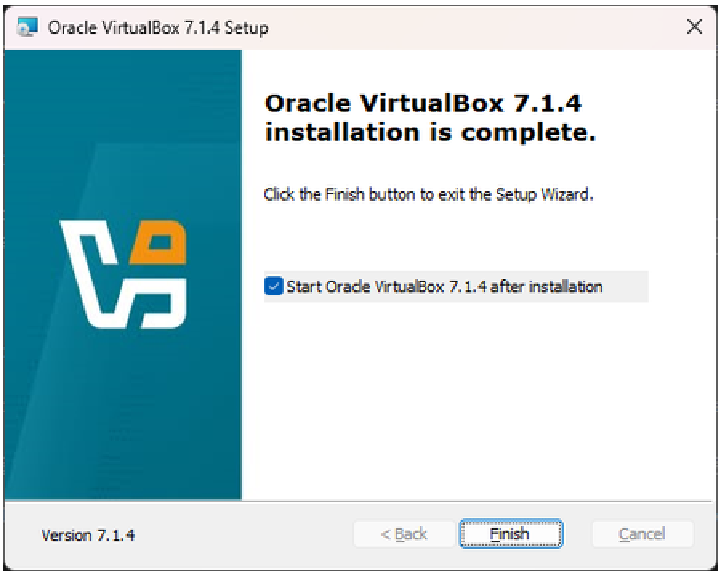
- # Introduction

Kali Linux is a dedicated Linux-based operating system for cybersecurity, penetration testing, and digital forensic fields. It comes with hundreds of security tools loaded up, which are generally used for network scanning, vulnerability assessment, password cracking, and system analysis. Because of its strong focus on security testing, Kali Linux is widely used by ethical hackers, security analysts, and students who want hands-on exposure to real-world cybersecurity techniques.

Running Kali Linux inside a Virtual Machine provides a very safe and controlled environment for learning. A VM isolates Kali from the main operating system, which cannot be accidentally damaged or pose any security risks when trying out tools. It also allows easy snapshots, quick resets, and multiple systems to be up and running at once. Using a VM ensures flexibility, portability, and a secure means with which to practice cybersecurity tasks without affecting the host computer.

- # Installation Steps with Screenshots

VirtualBox Installation Completed Successfully



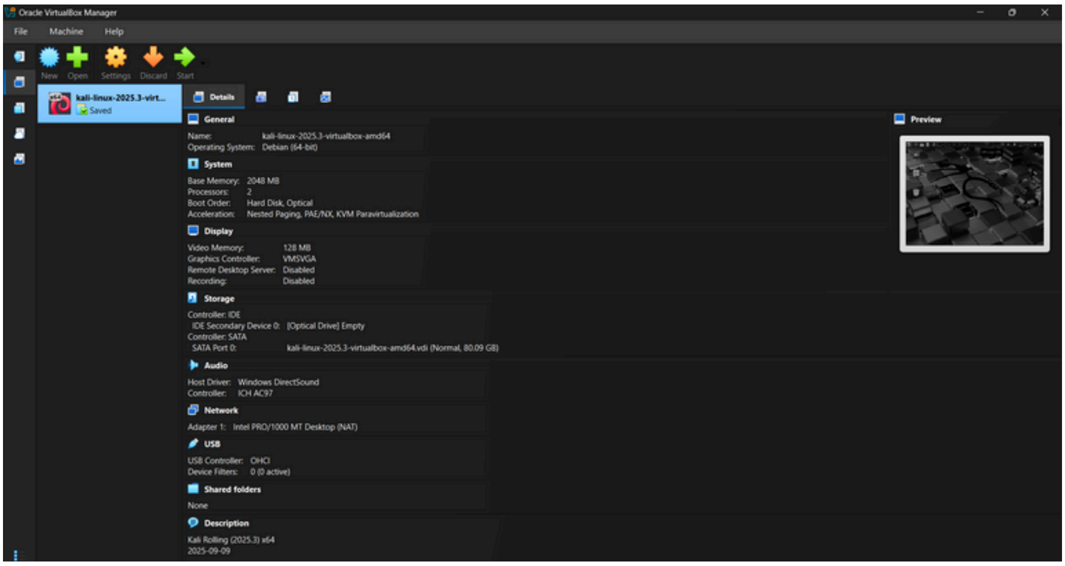
Oracle VirtualBox 7.1.4 installation is complete.

Click the Finish button to exit the Setup Wizard.

☑ Start Oracle VirtualBox 7.1.4 after installation

Version 7.1.4

Virtual Machine Homescreen



General

Name: kali-linux-2025.3-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-2025.3-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

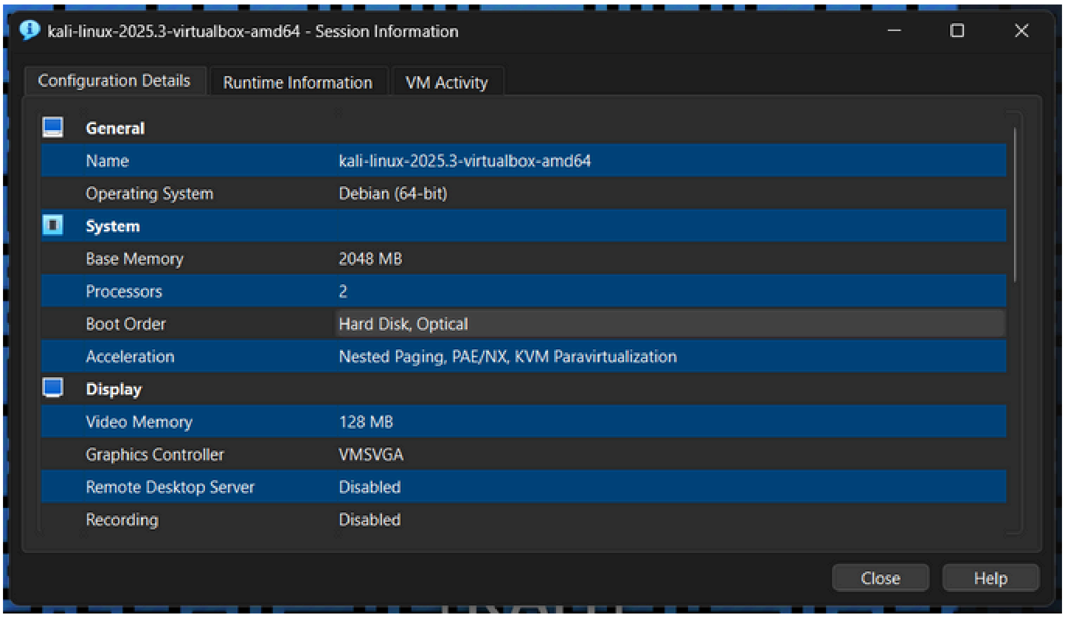
Shared folders

None

Description

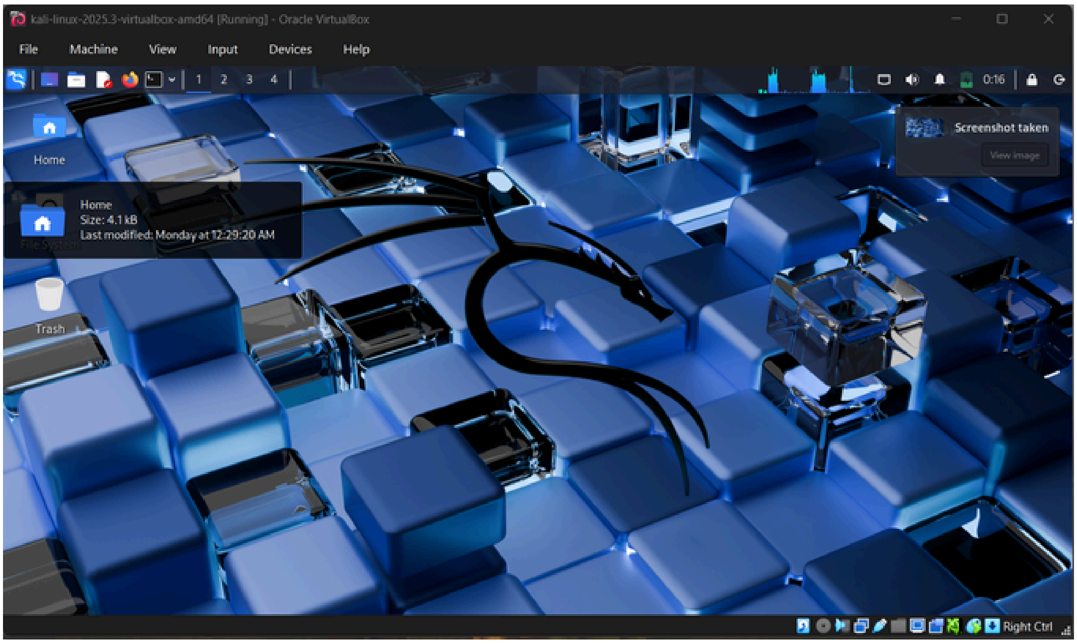
Kali Rolling (2025.3) x64
2025-09-09

Kali Linux Virtual Machine Configuration in VirtualBox



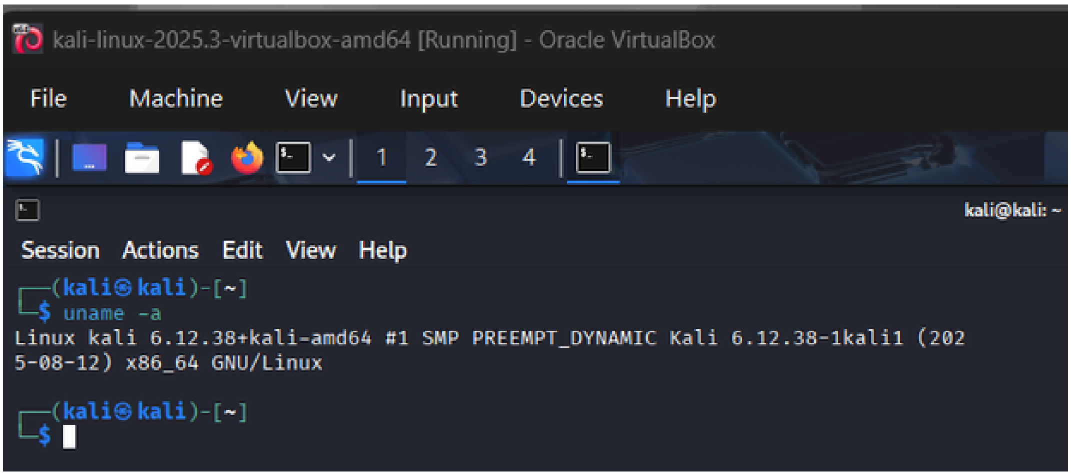
General	
Name	kali-linux-2025.3-virtualbox-amd64
Operating System	Debian (64-bit)
System	
Base Memory	2048 MB
Processors	2
Boot Order	Hard Disk, Optical
Acceleration	Nested Paging, PAE/NX, KVM Paravirtualization
Display	
Video Memory	128 MB
Graphics Controller	VMSVGA
Remote Desktop Server	Disabled
Recording	Disabled

Kali Linux Desktop Home Screen After Installation



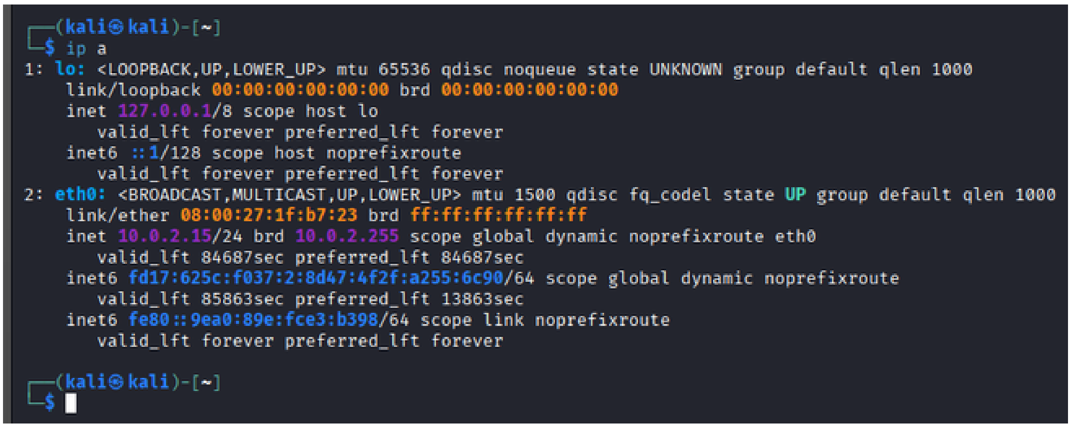
- # Command Execution Output

1. **Command:** uname -a



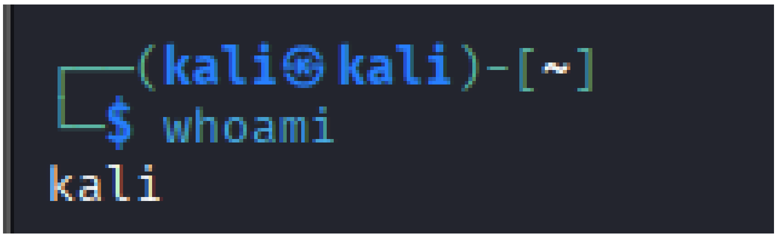
```
┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (202
5-08-12) x86_64 GNU/Linux

┌──(kali㉿kali)-[~]
└─$ 
```

2. **Command:** ip a



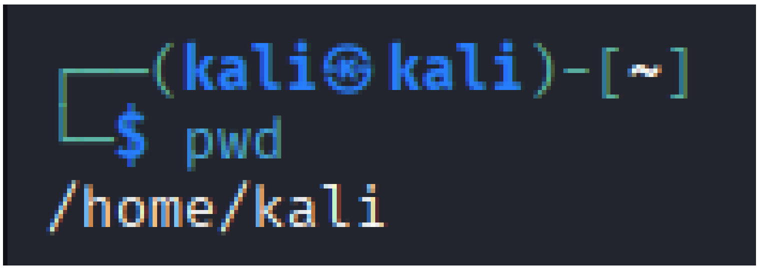
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 84687sec preferred_lft 84687sec
    inet6 fd17:625c:f037:2:8d47:4f2f:a255:6c90/64 scope global dynamic noprefixroute
       valid_lft 85863sec preferred_lft 13863sec
    inet6 fe80::9ea0:89e:fce3:b398/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

3. **Command:** whoami



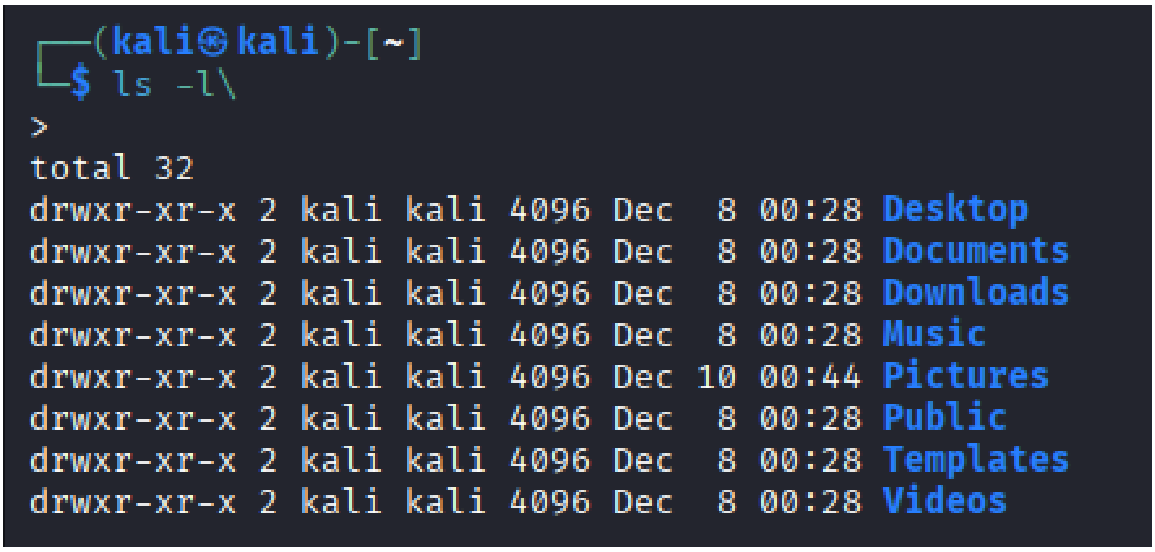
```
┌──(kali㉿kali)-[~]
└─$ whoami
kali
```

4. **Command:** pwd



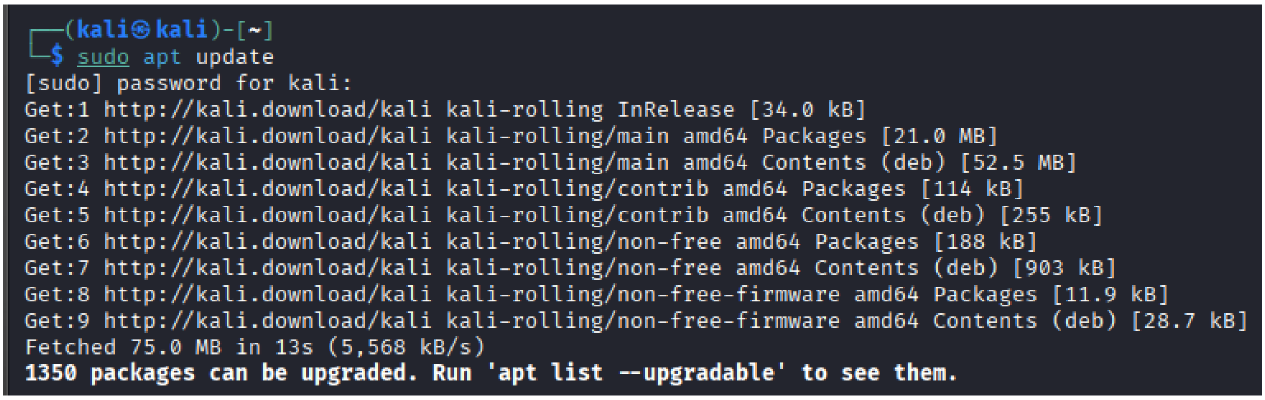
```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali
```

5. **Command:** ls -l



```
┌──(kali㉿kali)-[~]
└─$ ls -l\
>
total 32
drwxr-xr-x 2 kali kali 4096 Dec  8 00:28 Desktop
drwxr-xr-x 2 kali kali 4096 Dec  8 00:28 Documents
drwxr-xr-x 2 kali kali 4096 Dec  8 00:28 Downloads
drwxr-xr-x 2 kali kali 4096 Dec  8 00:28 Music
drwxr-xr-x 2 kali kali 4096 Dec 10 00:44 Pictures
drwxr-xr-x 2 kali kali 4096 Dec  8 00:28 Public
drwxr-xr-x 2 kali kali 4096 Dec  8 00:28 Templates
drwxr-xr-x 2 kali kali 4096 Dec  8 00:28 Videos
```

6. **Command:** sudo apt update



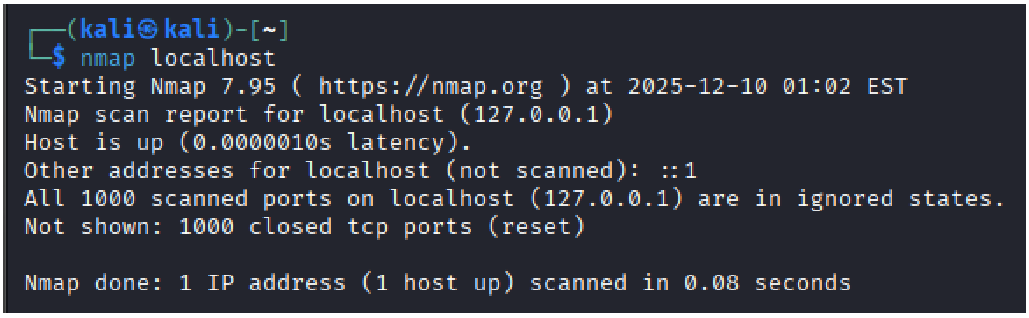
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.5 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [255 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [188 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [903 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.9 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [28.7 kB]
Fetched 75.0 MB in 13s (5,568 kB/s)
1350 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

- # Tool Exploration Screenshots

1. Nmap

Purpose:

Nmap is used to scan networks, detect active hosts, identify open ports, and map network topology.



```
┌──(kali㉿kali)-[~]
└─$ nmap localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 01:02 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

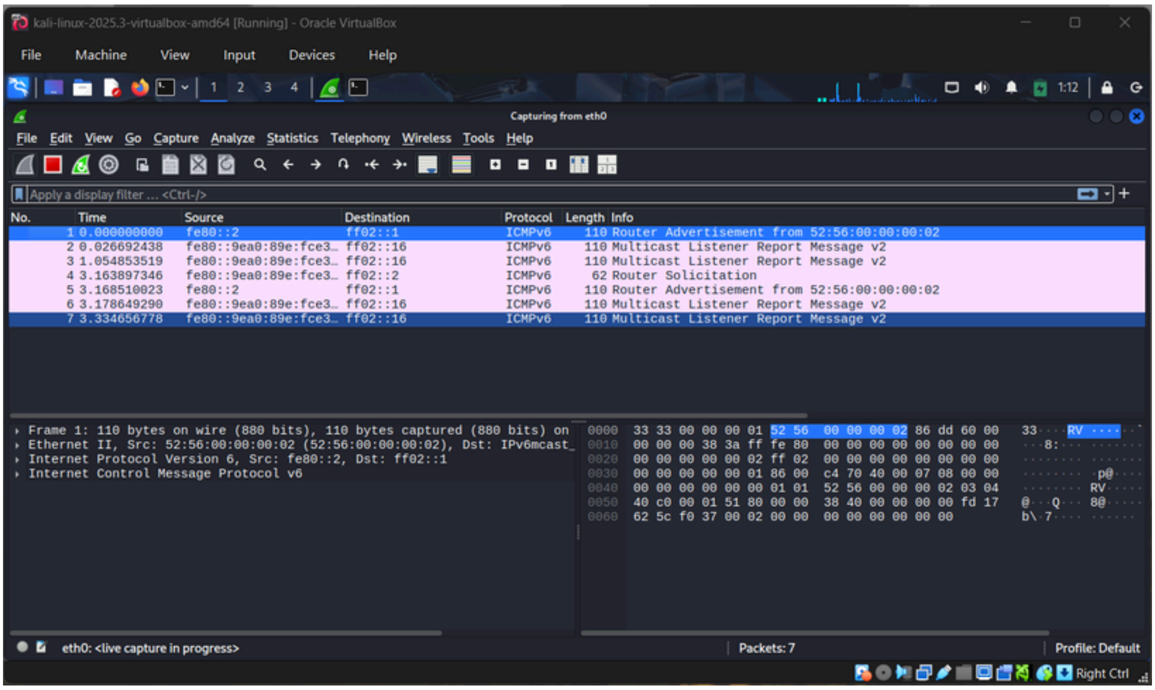
Practical Use Case:

Used by security analysts to discover devices and services running on a network.

2. Wireshark

Purpose:

Wireshark captures and analyzes network packets in real-time. It helps understand network behavior and troubleshoot communication issues.



```
No.     Time         Source                Destination  Protocol  Length Info
      1 0.000000000  fe80::2               ff02::1      ICMPv6    110 Router Advertisement from 52:56:00:00:00:02
      2 0.026692438  fe80::9ea0:89e:fce3…  ff02::16     ICMPv6    110 Multicast Listener Report Message v2
      3 1.054853519  fe80::9ea0:89e:fce3…  ff02::16     ICMPv6    110 Multicast Listener Report Message v2
      4 3.163897346  fe80::9ea0:89e:fce3…  ff02::2      ICMPv6     62 Router Solicitation
      5 3.168510023  fe80::2               ff02::1      ICMPv6    110 Router Advertisement from 52:56:00:00:00:02
      6 3.178649290  fe80::9ea0:89e:fce3…  ff02::16     ICMPv6    110 Multicast Listener Report Message v2
      7 3.334656778  fe80::9ea0:89e:fce3…  ff02::16     ICMPv6    110 Multicast Listener Report Message v2
```

```
› Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on
› Ethernet II, Src: 52:56:00:00:00:02 (52:56:00:00:00:02), Dst: IPv6mcast_
› Internet Protocol Version 6, Src: fe80::2, Dst: ff02::1
› Internet Control Message Protocol v6
```

```
0000  33 33 00 00 00 01 52 56  00 00 00 02 86 dd 60 00   33····RV ······`·
0010  00 00 00 38 3a ff fe 80  00 00 00 00 00 00 00 00   ···8:··· ········
0020  00 00 00 00 00 02 ff 02  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 01 86 00  c4 70 40 00 07 08 00 00   ········ ·p@·····
0040  00 00 00 00 00 00 01 01  52 56 00 00 00 02 03 04   ········ RV······
0050  40 c0 00 01 51 80 00 00  38 40 00 00 00 00 fd 17   @···Q··· 8@······
0060  62 5c f0 37 00 02 00 00  00 00 00 00 00 00         b\·7···· ······
```

eth0: <live capture in progress>
Packets: 7
Profile: Default

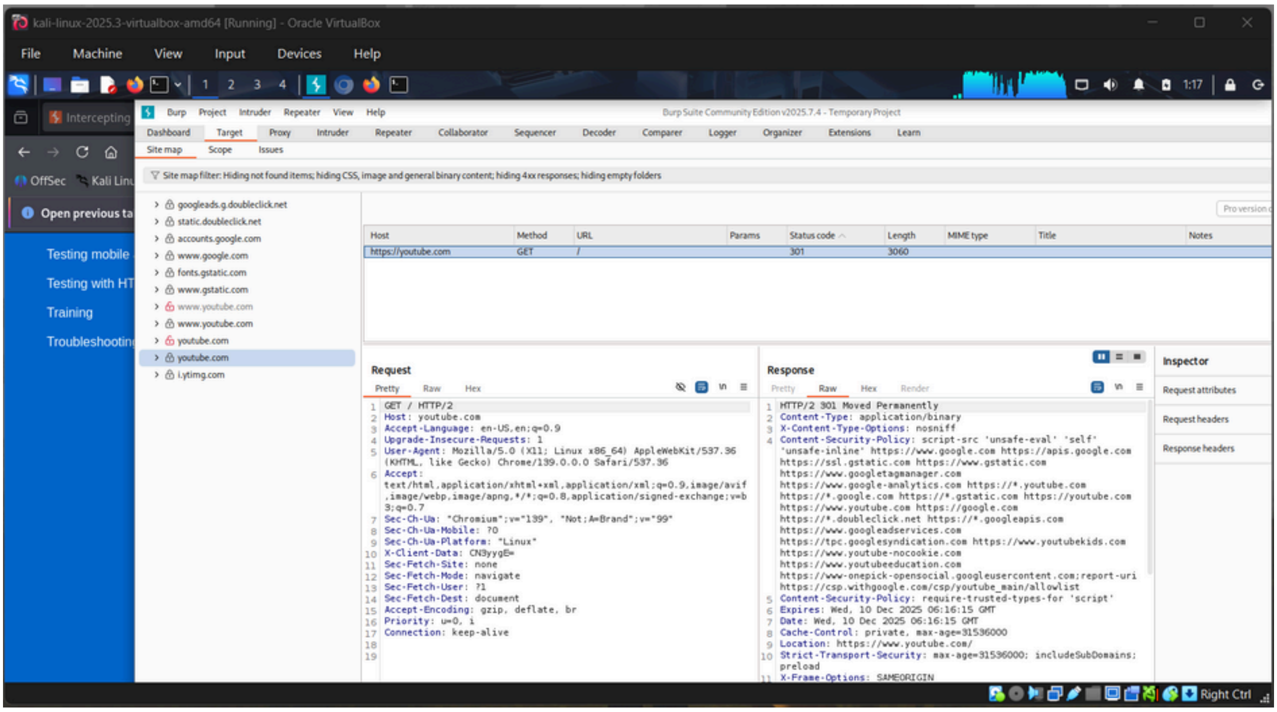
Practical Use Case:

Used to inspect suspicious network activity or debug network issues.

3. Burpsuite

Purpose:

BurpSuite is a web vulnerability testing suite used to intercept, analyze, and manipulate web traffic.



Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes
https://youtube.com	GET	/		301	3060			

Request

```
GET / HTTP/2
Host: youtube.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
X-Client-Data: CN3yygE=
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Response

```
HTTP/2 301 Moved Permanently
Content-Type: application/binary
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'unsafe-eval' 'self'
'unsafe-inline' https://www.google.com https://apis.google.com
https://ssl.gstatic.com https://www.gstatic.com
https://www.googletagmanager.com
https://www.google-analytics.com https://*.youtube.com
https://*.google.com https://*.gstatic.com https://youtube.com
https://www.youtube.com https://google.com
https://*.doubleclick.net https://*.googleapis.com
https://www.googleadservices.com
https://tpc.googlesyndication.com https://www.youtubekids.com
https://www.youtube-nocookie.com
https://www.youtubeeducation.com
https://www-onepick-opensocial.googleusercontent.com;report-uri
https://csp.withgoogle.com/csp/youtube_main/allowlist
Content-Security-Policy: require-trusted-types-for 'script'
Expires: Wed, 10 Dec 2025 06:16:15 GMT
Date: Wed, 10 Dec 2025 06:16:15 GMT
Cache-Control: private, max-age=31536000
Location: https://www.youtube.com/
Strict-Transport-Security: max-age=31536000; includeSubDomains;
preload
X-Frame-Options: SAMEORIGIN
```

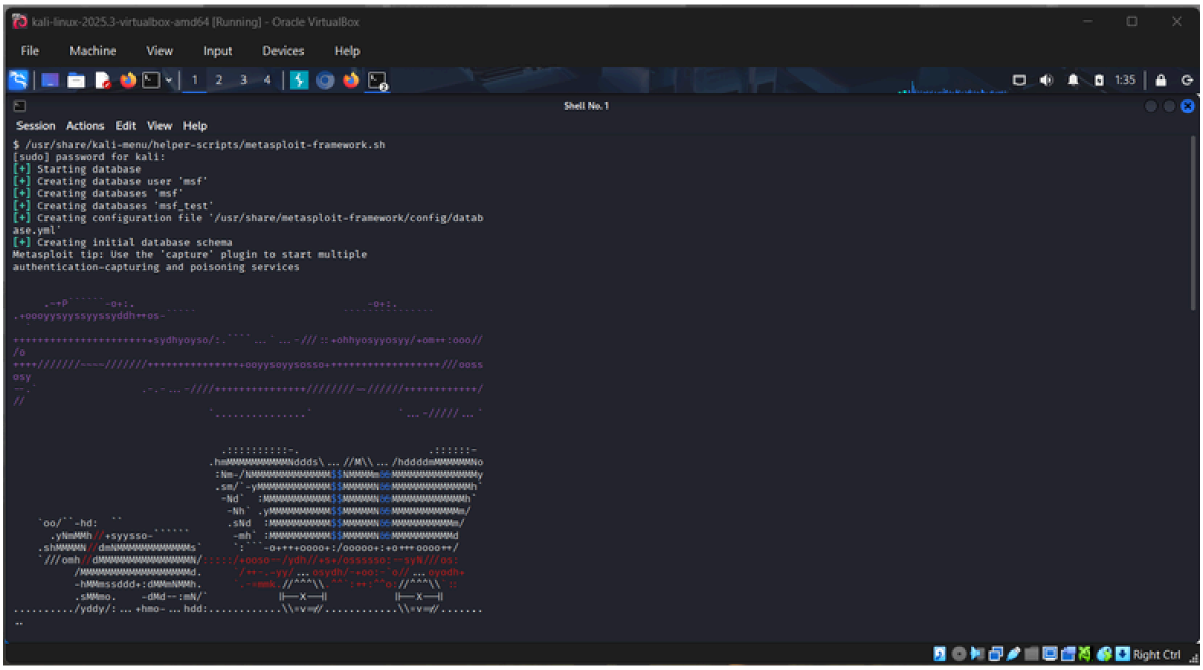
Practical Use Case:

Used for identifying security flaws in websites during penetration testing.

4. Metasploit

Purpose:

Metasploit is one of the most powerful penetration testing frameworks used to identify vulnerabilities, develop exploits, and test the security of systems. It provides a command-line interface and modules for scanning, payload generation, and launching controlled exploits in ethical hacking environments.



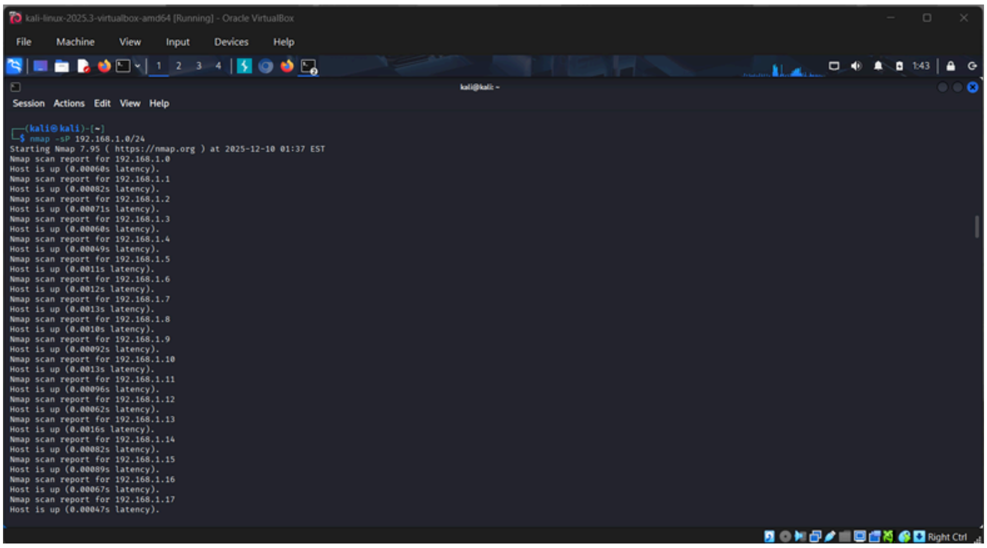
```
$ /usr/share/kali-menu/helper-scripts/metasploit-framework.sh
[sudo] password for kali:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab
ase.yml'
[+] Creating initial database schema
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services
```

Practical Use Case:

Used by ethical hackers to simulate attacks and evaluate the security posture of networks and applications.

- # Bonus Task

1. Run a basic network scan of your local network:
2. nmap -sP 192.168.1.0/24



```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 01:37 EST
Nmap scan report for 192.168.1.0
Host is up (0.00060s latency).
Nmap scan report for 192.168.1.1
Host is up (0.00082s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00071s latency).
Nmap scan report for 192.168.1.3
Host is up (0.00060s latency).
Nmap scan report for 192.168.1.4
Host is up (0.00049s latency).
Nmap scan report for 192.168.1.5
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.6
Host is up (0.0012s latency).
Nmap scan report for 192.168.1.7
Host is up (0.0013s latency).
Nmap scan report for 192.168.1.8
Host is up (0.0010s latency).
Nmap scan report for 192.168.1.9
Host is up (0.00092s latency).
Nmap scan report for 192.168.1.10
Host is up (0.0013s latency).
Nmap scan report for 192.168.1.11
Host is up (0.00096s latency).
Nmap scan report for 192.168.1.12
Host is up (0.00062s latency).
Nmap scan report for 192.168.1.13
Host is up (0.0016s latency).
Nmap scan report for 192.168.1.14
Host is up (0.00082s latency).
Nmap scan report for 192.168.1.15
Host is up (0.00089s latency).
Nmap scan report for 192.168.1.16
Host is up (0.00067s latency).
Nmap scan report for 192.168.1.17
Host is up (0.00047s latency).
```

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
Session Actions Edit View Help
Right Ctrl

Parameter	**Details**
Subnet Scanned	192.168.1.0/24
Total Hosts Scanned	256
Hosts Reported Up	256
Reason	VirtualBox virtual network responds for the entire range
Notes	Not all 256 are real devices — virtual NAT makes the entire range appear active

- # Observations Table

Task	Observation
Kali Linux Installation	Installation completed successfully. VirtualBox handled the OS smoothly with allocated resources.
VM Configuration	2–4 GB RAM and 2 CPU cores were sufficient for running Kali and its tools.
Basic Commands	All terminal commands executed correctly and helped understand system information and user environment.
Security Tools	Nmap and Wireshark were easy to operate, BurpSuite required more system resources, and Hydra has strong password-testing capabilities.
Overall Experience	Kali Linux provided a powerful environment for learning cybersecurity tools and Linux fundamentals.

- # Conclusion

The completion of this assignment really introduced me to Kali Linux, virtual machines, and basic cybersecurity tools. Installing Kali inside VirtualBox provided a secure and isolated environment in which to experiment without affecting the host system. Performing simple terminal commands built confidence with Linux operations, while the use of tools such as Nmap, Wireshark, BurpSuite, and Hydra showed ways in which cybersecurity professionals analyze networks and test system security. In all, this assignment consolidated practical skills, enhanced my awareness of the penetration-testing tool kit, and underscored benefits that come with virtual environments for safe experimentation in cybersecurity.

Thank you!