

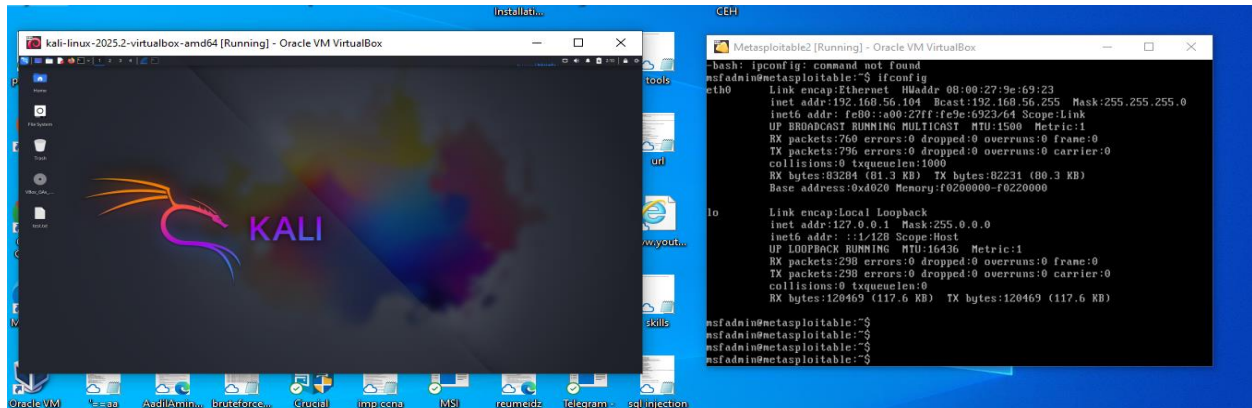
Linux Essentials Lab Setup Report
Aman Jiwani
Date: 10-9-2025

Introduction

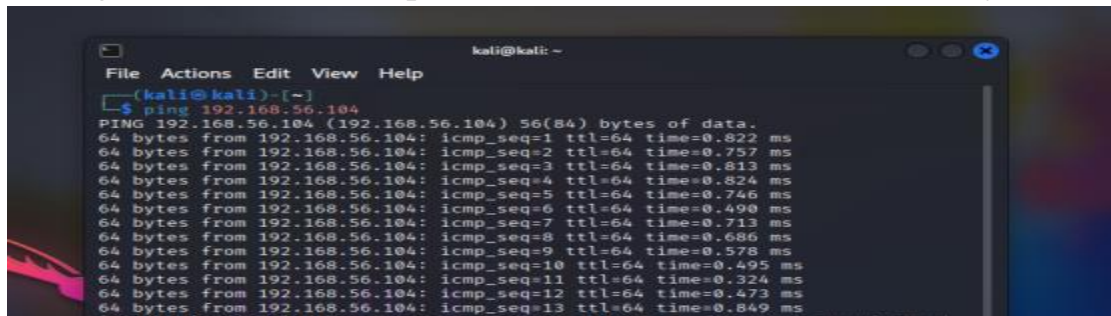
- This lab focuses on setting up a secure Linux virtual environment for cybersecurity practice using VirtualBox.
- Kali Linux is used as the attacker machine and Metasploitable2 as the target machine to simulate real-world scenarios.
- The lab covers Linux fundamentals, networking commands, user and file permissions, package management, and basic network monitoring with Wireshark.
- It provides hands-on experience in verifying connectivity, capturing network traffic, and understanding system processes and services.

Environment Setup

1. Kali Linux (192.168.56.105) and Metasploitable2 (192.168.56.104) running in Host-Only Network.



2. Ping from Kali to Metasploitable2 verifies network connectivity.

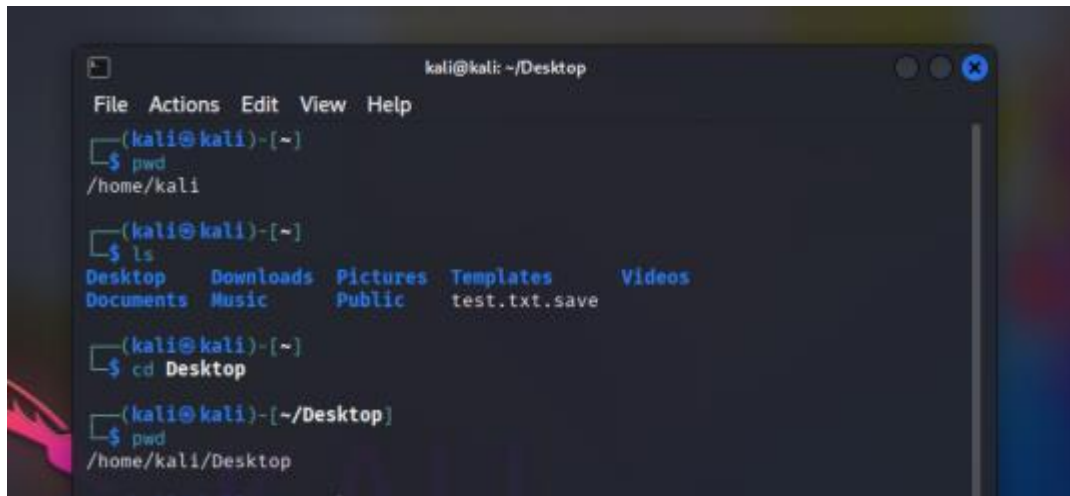


3. Wireshark capture showing ICMP ping traffic between Kali and Metasploitable2.

No.	Time	Source	Destination	Protocol	Length	Info
3	44.646096972	192.168.56.105	192.168.56.104	ICMP	98	Echo (ping) request id=0x0002, seq=1/256, ttl=64 (reply in 6)
6	44.656627006	192.168.56.104	192.168.56.105	ICMP	98	Echo (ping) reply id=0x0002, seq=1/256, ttl=64 (request in 3)
7	45.647766748	192.168.56.105	192.168.56.104	ICMP	98	Echo (ping) request id=0x0002, seq=2/512, ttl=64 (reply in 8)
8	45.648427819	192.168.56.104	192.168.56.105	ICMP	98	Echo (ping) reply id=0x0002, seq=2/512, ttl=64 (request in 7)
9	46.691315914	192.168.56.105	192.168.56.104	ICMP	98	Echo (ping) request id=0x0002, seq=3/768, ttl=64 (reply in 10)
10	46.692037892	192.168.56.104	192.168.56.105	ICMP	98	Echo (ping) reply id=0x0002, seq=3/768, ttl=64 (request in 9)
11	47.702253470	192.168.56.105	192.168.56.104	ICMP	98	Echo (ping) request id=0x0002, seq=4/1024, ttl=64 (reply in 12)
12	47.702698073	192.168.56.104	192.168.56.105	ICMP	98	Echo (ping) reply id=0x0002, seq=4/1024, ttl=64 (request in 11)

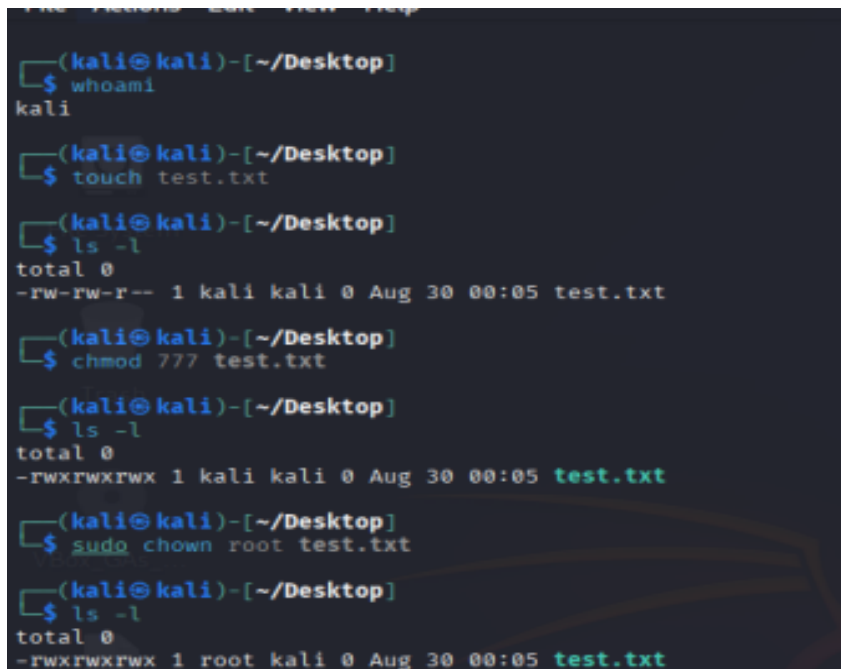
Linux Key Commands & Outputs

1. Linux file system navigation commands.

A terminal window titled 'kali@kali: ~/Desktop' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the following sequence of commands and outputs:

```
(kali@kali)-[~]  
$ pwd  
/home/kali  
  
(kali@kali)-[~]  
$ ls  
Desktop  Downloads  Pictures  Templates  Videos  
Documents Music      Public    test.txt.save  
  
(kali@kali)-[~]  
$ cd Desktop  
  
(kali@kali)-[~/Desktop]  
$ pwd  
/home/kali/Desktop
```

2. File permissions and ownership changes.

A terminal window showing the following sequence of commands and outputs:

```
(kali@kali)-[~/Desktop]  
$ whoami  
kali  
  
(kali@kali)-[~/Desktop]  
$ touch test.txt  
  
(kali@kali)-[~/Desktop]  
$ ls -l  
total 0  
-rw-rw-r-- 1 kali kali 0 Aug 30 00:05 test.txt  
  
(kali@kali)-[~/Desktop]  
$ chmod 777 test.txt  
  
(kali@kali)-[~/Desktop]  
$ ls -l  
total 0  
-rwxrwxrwx 1 kali kali 0 Aug 30 00:05 test.txt  
  
(kali@kali)-[~/Desktop]  
$ sudo chown root test.txt  
  
(kali@kali)-[~/Desktop]  
$ ls -l  
total 0  
-rwxrwxrwx 1 root kali 0 Aug 30 00:05 test.txt
```

3.Package Management

```
(kali@kali)-[~/Desktop]
$ sudo apt update
[sudo] password for kali:
Get:1 http://mirror.aktkn.sg/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Packages [21.3 MB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Contents (deb) [51.8 MB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Packages [118 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Contents (deb) [325 kB]
Get:6 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Packages [200 kB]
Get:7 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Contents (deb) [911 kB]
Get:8 http://mirror.aktkn.sg/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:9 http://mirror.aktkn.sg/kali kali-rolling/non-free-firmware amd64 Contents (deb) [27.1 kB]
Fetched 74.7 MB in 31s (2,393 kB/s)
877 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

4.Network interfaces, connectivity, and hops.

A)Ip

```
(kali@kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.105 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::7f7e:bd1b:8045:1808 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:dl:f8:5d txqueuelen 1000 (Ethernet)
    RX packets 13 bytes 7478 (7.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 9062 (8.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

B)Ping

```
(kali@kali)-[~/Desktop]
$ ping -c 4 google.com
PING google.com (142.250.70.46) 56(84) bytes of data:
64 bytes from pnbomb-aa-in-f14.1e100.net (142.250.70.46): icmp_seq=1 ttl=116 time=9.52 ms
64 bytes from pnbomb-aa-in-f14.1e100.net (142.250.70.46): icmp_seq=2 ttl=116 time=8.49 ms
64 bytes from pnbomb-aa-in-f14.1e100.net (142.250.70.46): icmp_seq=3 ttl=116 time=8.17 ms
64 bytes from pnbomb-aa-in-f14.1e100.net (142.250.70.46): icmp_seq=4 ttl=116 time=8.08 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 8.079/8.564/9.520/0.572 ms
```

C)Traceroute

```
(kali@kali)-[~/Desktop]
$ traceroute 192.168.56.104
traceroute to 192.168.56.104 (192.168.56.104), 30 hops max, 60 byte packets
1 192.168.56.104 (192.168.56.104) 1.719 ms 1.638 ms 1.609 ms
```

Conclusion

- The lab environment with **Kali Linux and Metasploitable2** was successfully set up.
- **Network connectivity** was verified using ping and traceroute commands.
- **Wireshark captured ICMP traffic**, and Linux commands were executed to validate file permissions, package management, and running processes.
- Overall, the lab provides a solid foundation for practicing Linux essentials and cybersecurity fundamentals.