

Lab Set-Up Report

INTRODUCTION

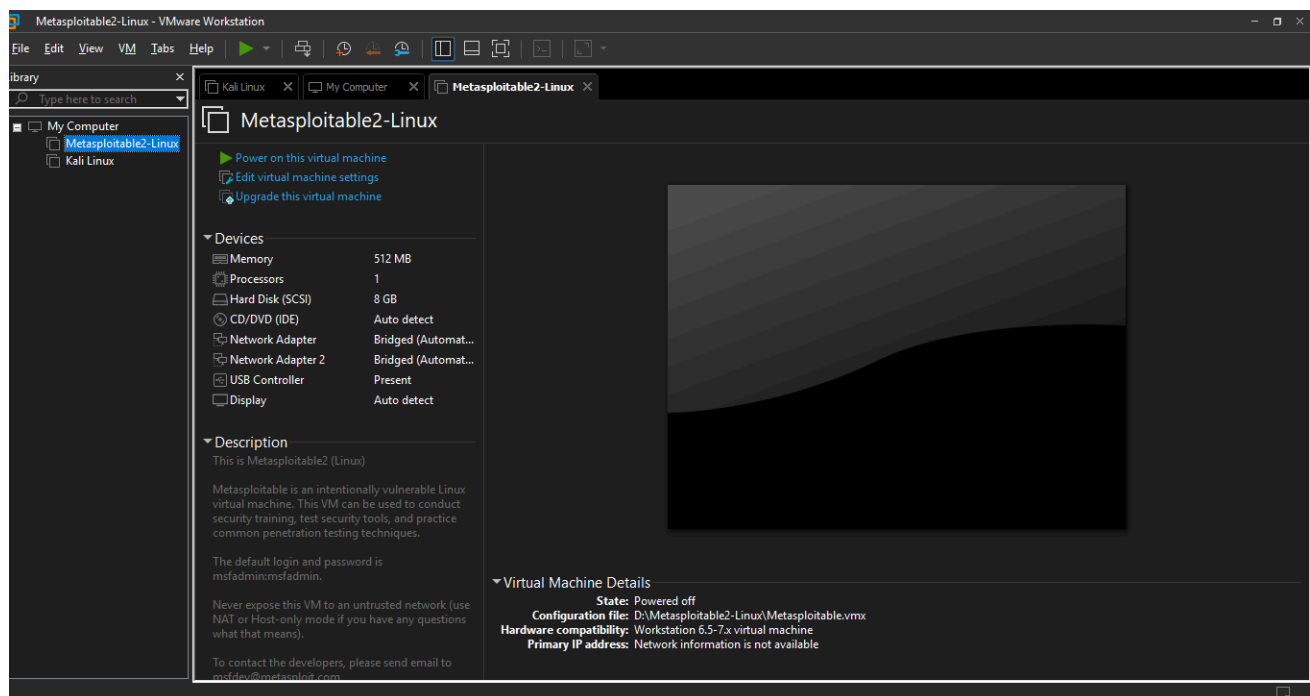
This report describes the setup of a cybersecurity lab environment using Kali Linux as an attacker machine and Metasploitable2 as a vulnerable target system. The lab was created using virtualization technology with a bridged adapter network configuration to allow communication between systems. The environment was used to practice Linux commands, networking concepts, packet analysis using Wireshark, and basic cybersecurity tools in a controlled setup.

OBJECTIVE

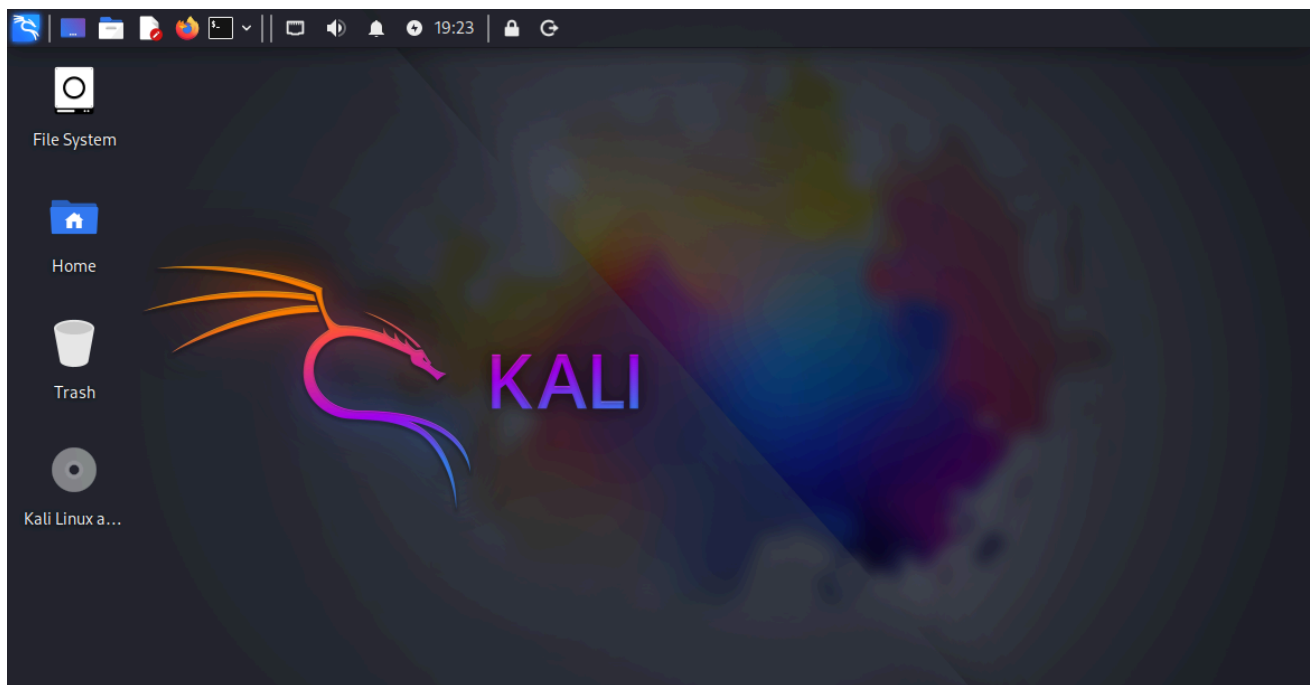
1. Setup cybersecurity lab
2. Install Kali Linux and Metasploitable2 Machine
3. Configure NAT network
4. Practice Linux commands
5. Capture traffic using Wireshark

LAB INVIROMENT SET-UP

- **Virtualization Software: VMware / VirtualBox**



- **Attacker Machine: Kali Linux**



- **Target Machine: Metasploitable2**

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ae:4f:3f
          inet addr:192.168.0.108  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feae:4f3f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 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:4806 (4.6 KB)  TX bytes:6968 (6.8 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:~$
```

- Network Type: NAT Adapter

Network Configuration

- Check IP Using :
`ifconfig`

```
akanksha@kali: ~
Session Actions Edit View Help
zsh: corrupt history file /home/akanksha/.zsh_history
(akanksha@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.109 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::20c:29ff:fec2:d0e5 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:c2:d0:e5 txqueuelen 1000 (Ethernet)
    RX packets 55 bytes 9069 (8.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 61 bytes 7265 (7.0 KiB)
    TX errors 0 dropped 4 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 80 bytes 6312 (6.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 80 bytes 6312 (6.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Devices
(akanksha@kali)-[~]
$
Network
  eth0
```

- Test Connection With Target machine Using :
`ping <target ip>`

```
akanksha@kali: ~
Session Actions Edit View Help
(akanksha@kali)-[~]
$ ping 192.168.0.108
PING 192.168.0.108 (192.168.0.108) 56(84) bytes of data.
64 bytes from 192.168.0.108: icmp_seq=1 ttl=64 time=0.312 ms
64 bytes from 192.168.0.108: icmp_seq=2 ttl=64 time=1.26 ms
64 bytes from 192.168.0.108: icmp_seq=3 ttl=64 time=1.04 ms
64 bytes from 192.168.0.108: icmp_seq=4 ttl=64 time=1.13 ms
64 bytes from 192.168.0.108: icmp_seq=5 ttl=64 time=0.977 ms
64 bytes from 192.168.0.108: icmp_seq=6 ttl=64 time=1.23 ms
^C
--- 192.168.0.108 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5016ms
rtt min/avg/max/mdev = 0.312/0.990/1.255/0.318 ms

(akanksha@kali)-[~]
$
```

BASIC LINUX COMMANDS

During the lab setup, basic Linux commands were practiced to understand file system navigation and system management in Kali Linux.

1. `cd` : Used to Changed directory
2. `ls` : List of files and directories

3. pwd : Print working directory
4. ifconfig : check IP address

Tool Used

During the cybersecurity lab setup, multiple tools were used to perform network analysis, system testing, and security practice in a controlled environment. These tools helped in understanding real-world cybersecurity operations and practical ethical hacking techniques.

1. Kali Linux (Attacker Machine)

Kali Linux was used as the attacker machine in the lab environment. It provides a wide range of pre-installed cybersecurity tools used for penetration testing, vulnerability assessment, and network analysis. All testing activities and command practices were performed inside Kali Linux.

2. Metasploitable2 (Target Machine)

Metasploitable was used as a vulnerable target machine. It is an intentionally insecure operating system designed for practicing ethical hacking and learning how vulnerabilities are exploited in a safe environment.

3. Wireshark

Wireshark was used for capturing and analyzing network traffic. During the lab, it was used to monitor packets generated during communication between Kali Linux and the target machine, especially ICMP packets during ping tests.

4. Nmap

Nmap was used for network scanning and identifying open ports and services running on the target machine. It helped in understanding how attackers gather information about systems before performing security testing.

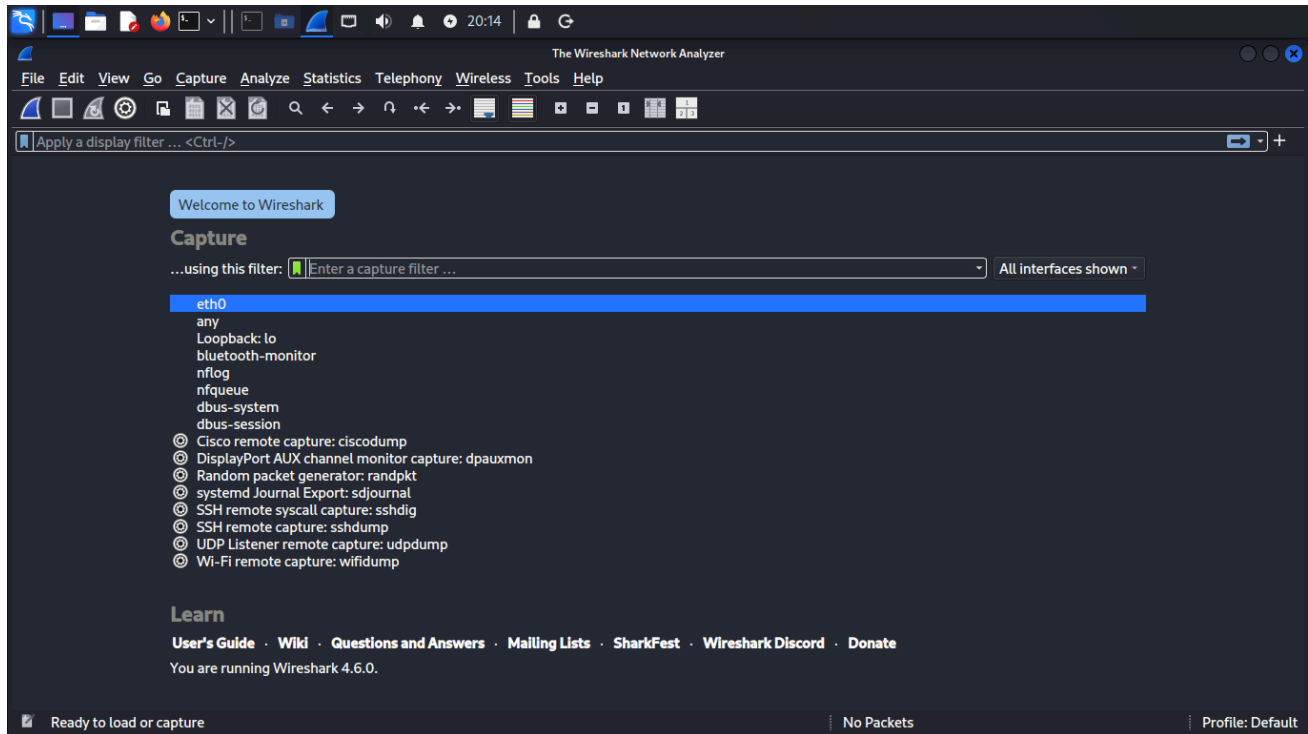
Wireshark Packet Capture

Wireshark is a network packet analysis tool used to capture and monitor data traffic in real time. It helps users analyze communication between systems and understand how network protocols work. In the cybersecurity lab, Wireshark was used to capture packets generated during ping tests between Kali Linux and the Metasploitable machine. It allows detailed inspection of packet information such as source IP, destination IP, and protocol type. Wireshark is widely used by cybersecurity professionals for troubleshooting, network monitoring, and detecting suspicious activity.

How to Used ?

- **Step1 : Opened Wireshark**

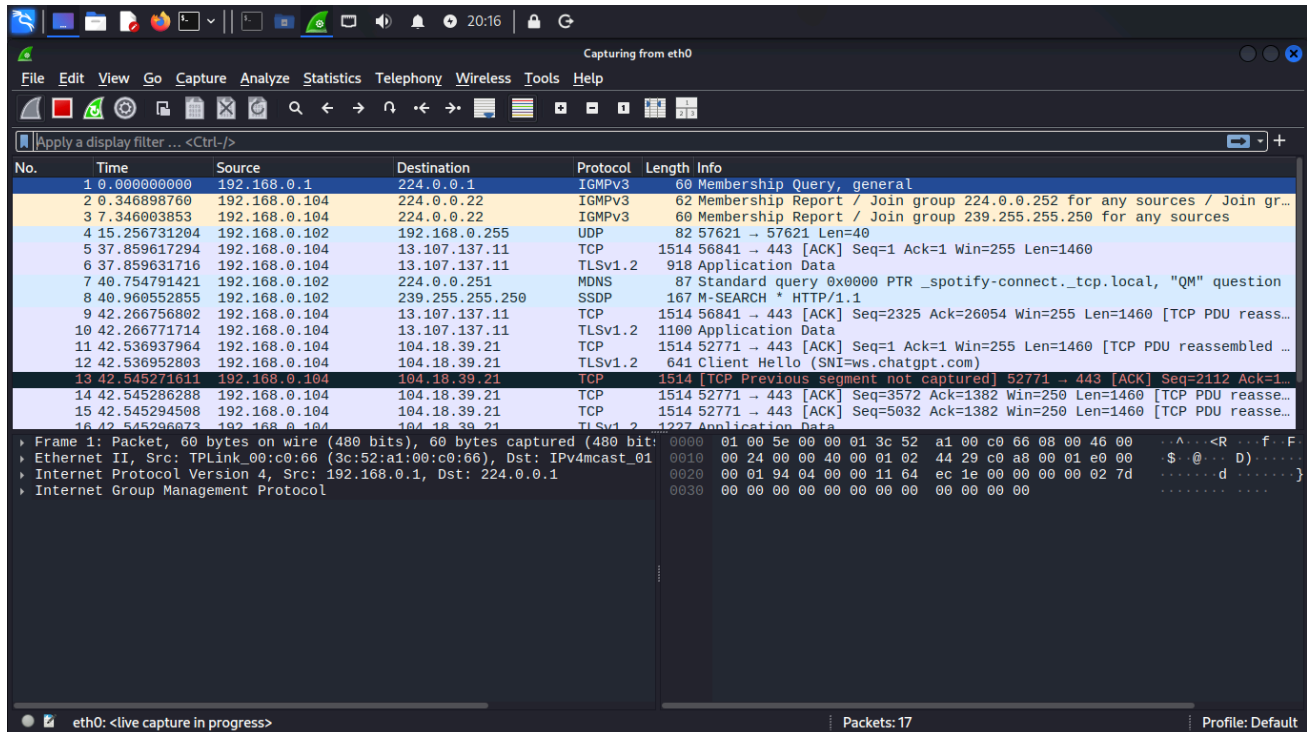
Wireshark was opened in Kali Linux to monitor and analyze network traffic between the attacker and target machines. The active network interface connected to the bridged adapter was selected to begin packet monitoring.



- **Step 2: Started Capture**

The packet capture process was started in Wireshark to record real-time network communication. This allowed all incoming and outgoing packets to be monitored during the

testing process.



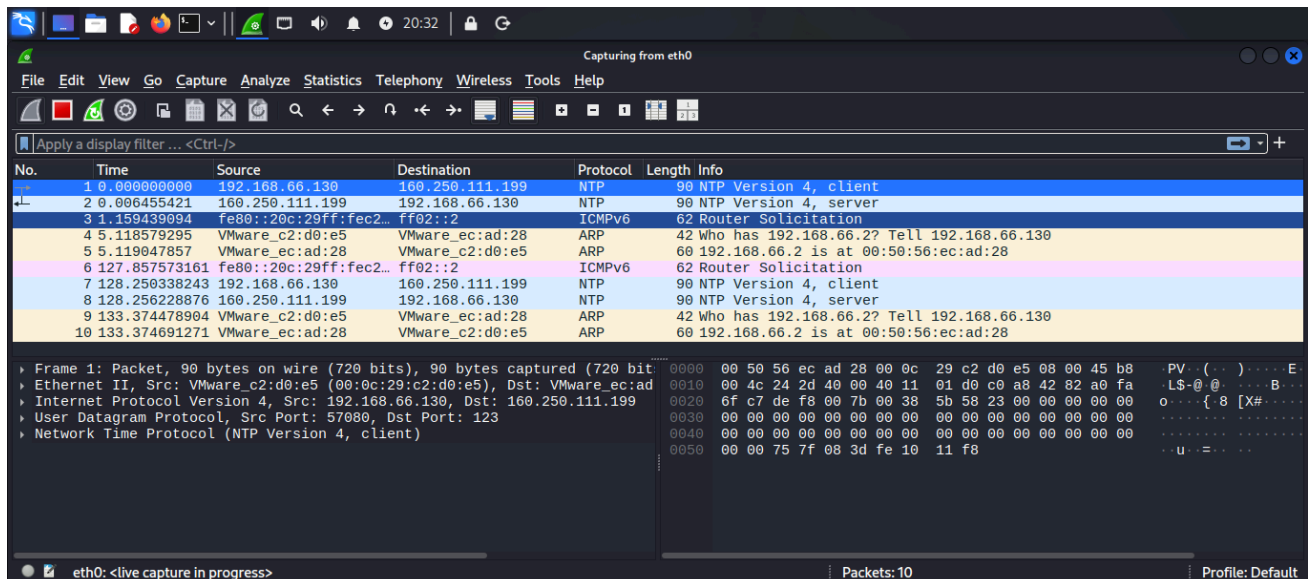
- **Step 3: Ping Target**

A ping command was executed from Kali Linux to the Metasploitable machine to generate network traffic. This helped verify connectivity and create packets for analysis in Wireshark.

- **Step 4: Observed ICMP Packets**

ICMP request and reply packets generated from the ping test were observed in Wireshark. The packet details such as source IP, destination IP, and protocol type were analyzed to

understand communication between systems.



Conclusion:

The configuration of Kali Linux and Metasploitable 2 using Virtual Machine (VM ware) with NAT provides a safe and controlled environment for learning and practicing penetration testing techniques. By leveraging the capabilities of VM ware and the NAT tool, users can explore cybersecurity concepts without compromising the integrity of their host systems or external networks.

Recommendations:

Regularly update the virtual machines and associated tools to ensure the latest security patches and enhancements. Exercise caution while performing penetration tests to avoid unintended consequences and potential legal implications. Continuously expand knowledge and skills in cybersecurity through hands-on experimentation and study.

References

- VM Ware Download : <https://knowledge.broadcom.com/external/article/344595/downloading-and-installing-vmware-workst.html>
- VirtualBox Download : <https://www.virtualbox.org/wiki/Downloads>
- Kali Linux Official Website: <https://www.kali.org/get-kali/#kali-virtual-machines>
- Metasploitable 2 GitHub Repository: Metasploitable - <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>