

Cybersecurity & Ethical Hacking

Internship at ApexPlanet Soft. Pvt. Ltd.

Task-1 Report: Screenshot of Kali Linux-Metasploitable, Lab Setup & Tool Familiarization

Student Name: Jatin Prajapat

Date: 01/09/2025

1. Kali Linux Setup

- Installed VirtualBox on host system.
- Imported and configured two VMs:
- Kali Linux (Attacker) – IP: 192.168.56.4



```

jatin@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.56.4 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::400:27ff:fe0d:495a prefixlen 64 scopeid 0x20<link>
    ether 00:0c:27:00:00:15 txqueuelen 1000 (Ethernet)
    RX packets 2106 bytes 364647 (375.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2895 bytes 304681 (309.6 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 2254 bytes 160070 (162.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2254 bytes 160070 (162.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

jatin@kali:~$
```

2. Metasploitable 2 Setup

- Metasploitable 2 (Target) – IP: 192.168.56.5

Both set to **Host-Only Adapter** for communication.

- Verified connection using ping.

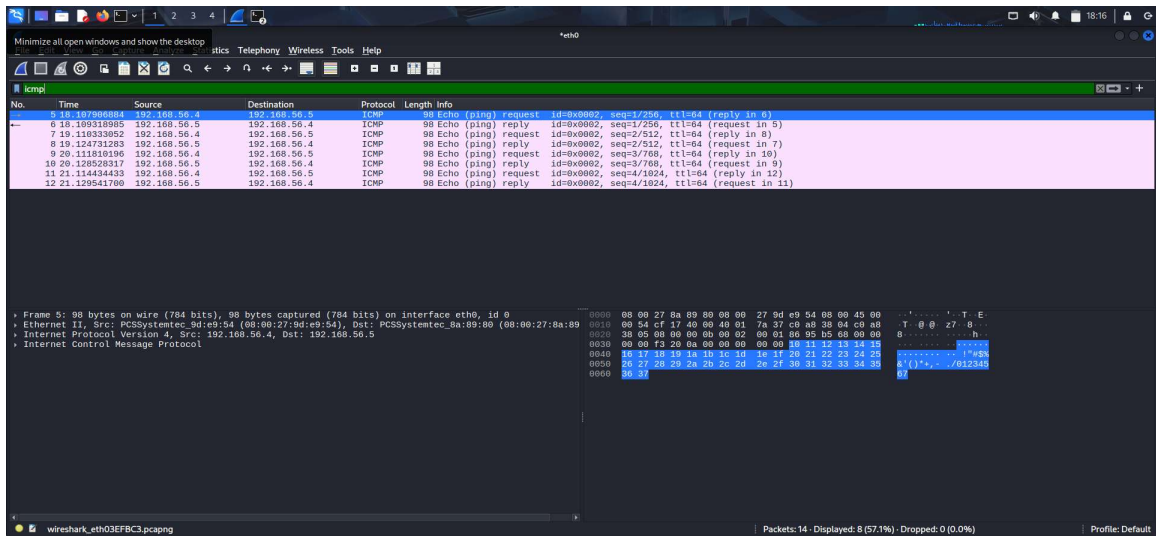
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8a:89:80
          inet addr:192.168.56.5  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8a:8980/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1252 (1.2 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:~$ c_
```

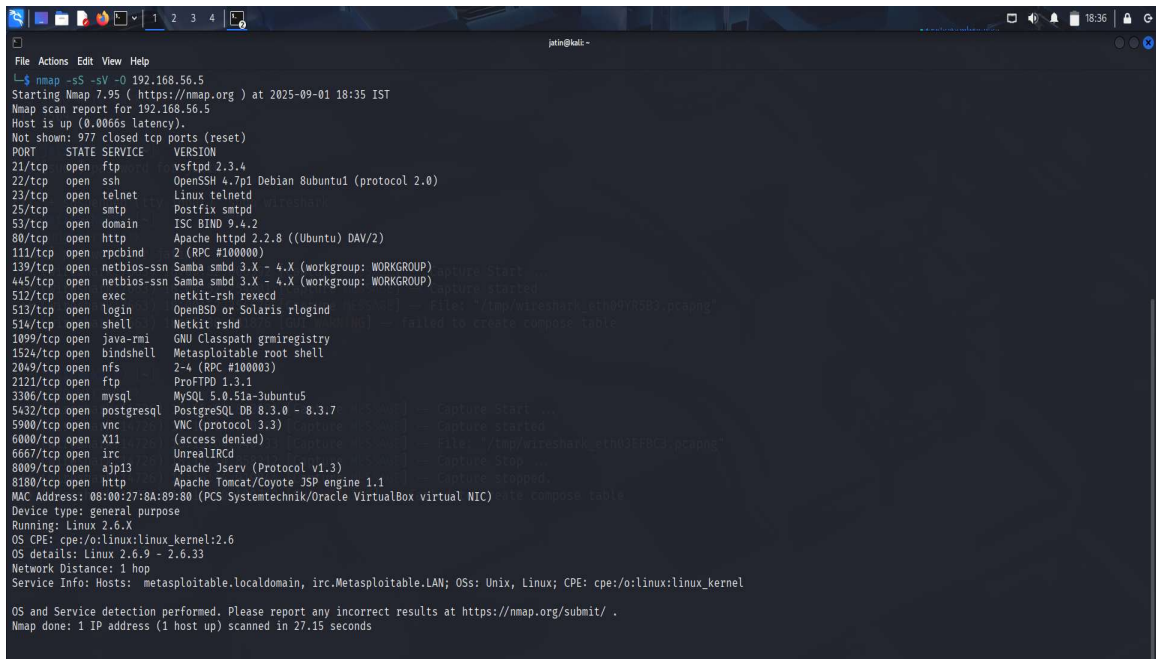
3. Wireshark Test Capture

- Ran a ping from Kali to Metasploitable.
- Captured traffic in Wireshark and applied icmp filter.
- Observed Echo Request and Echo Reply.



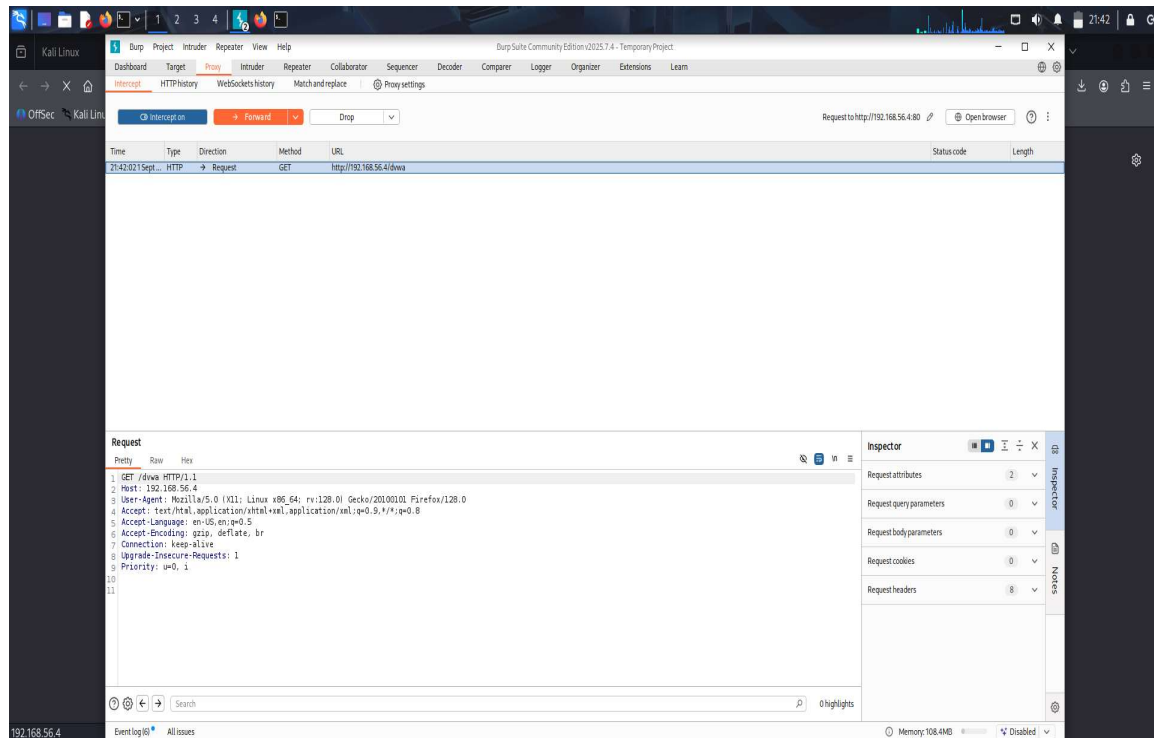
4. Nmap Scan

- Performed scan on Metasploitable using Nmap.
- Command: `nmap -sS -sV -O 192.168.56.5`
- Found open ports, detected services and OS fingerprint.



5. Burp Suite Proxy

- Configured Burp as proxy (127.0.0.1:8080).
- Set Firefox to use Burp proxy.
- Opened DVWA login page.
- Successfully intercepted HTTP request in Burp.



6. Netcat Debugging

- ❑ Started listener on Metasploitable: nc -lvp 4444.
- ❑ Connected from Kali: nc 192.168.56.5 4444.
- ❑ Sent messages between both machines.

```
msfadmin@metasploitable:~$ nc -lvp 4444
listening on [any] 4444 ...
192.168.56.4: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.5] from (UNKNOWN) [192.168.56.4] 60910
netcat has been successfully tested
```

Conclusion

In Task-1, the lab environment was successfully set up with Kali Linux and Metasploitable 2 in a Host-Only network configuration. Tools like Wireshark, Nmap, Burp Suite, and Netcat were tested and verified. The captured screenshots provide proof of functionality.