Cybersecurity & Ethical Hacking Internship at ApexPlanet Soft. Pvt. Ltd.

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

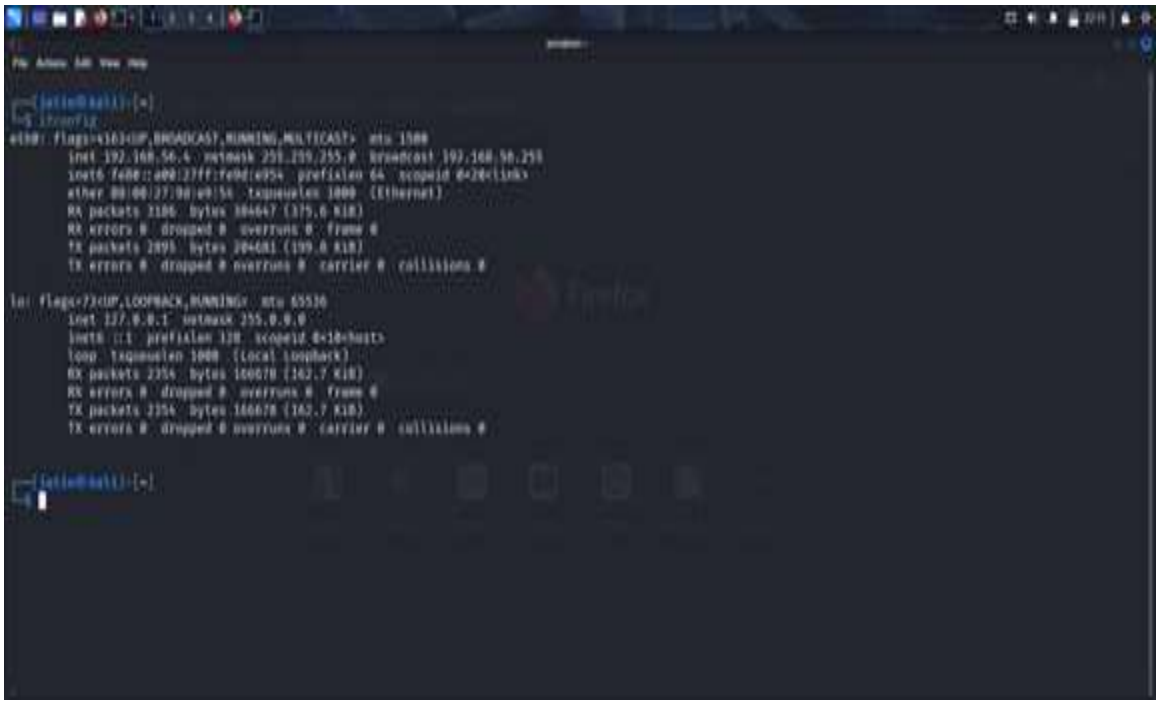
Student Name: Jatin Prajapat

Date: 01/09/2025

1. Kali Linux Setup

- Installed VirtualBox on host system.
- Imported and configured two VMs:

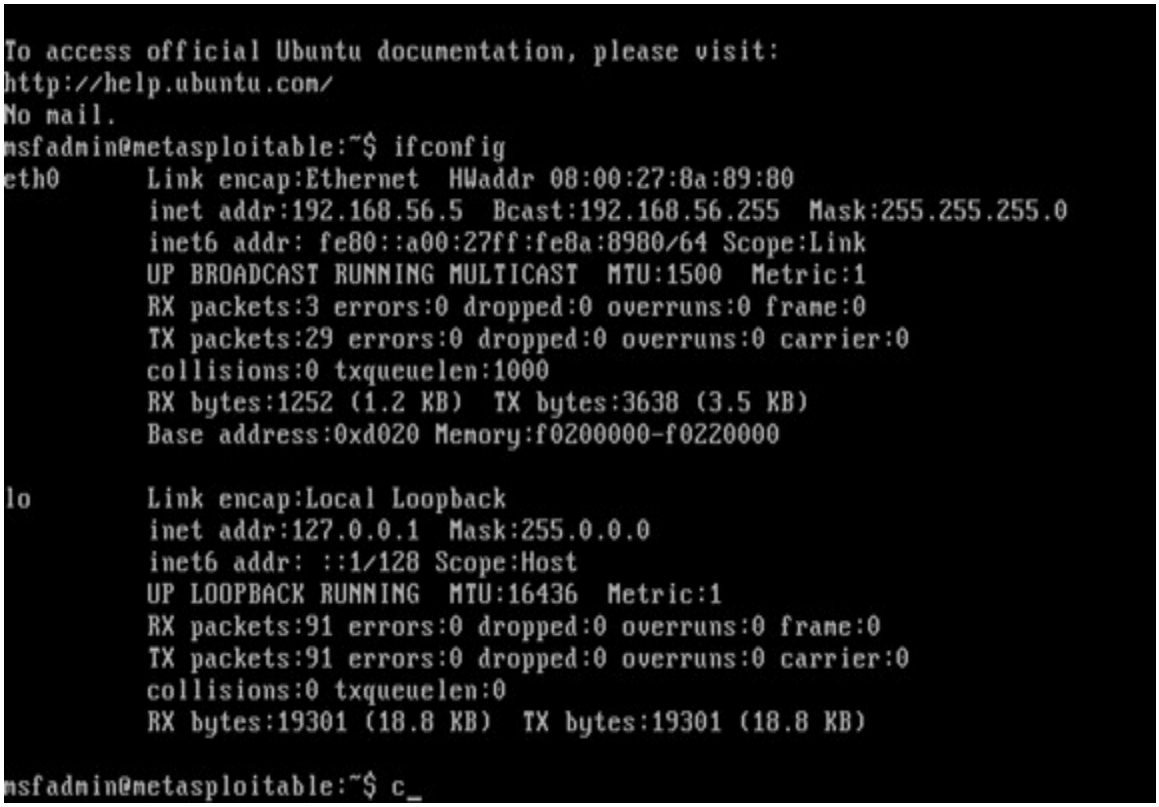
- Kali Linux (Attacker) – IP: 192.168.56.4



2. Metasploitable 2 Setup

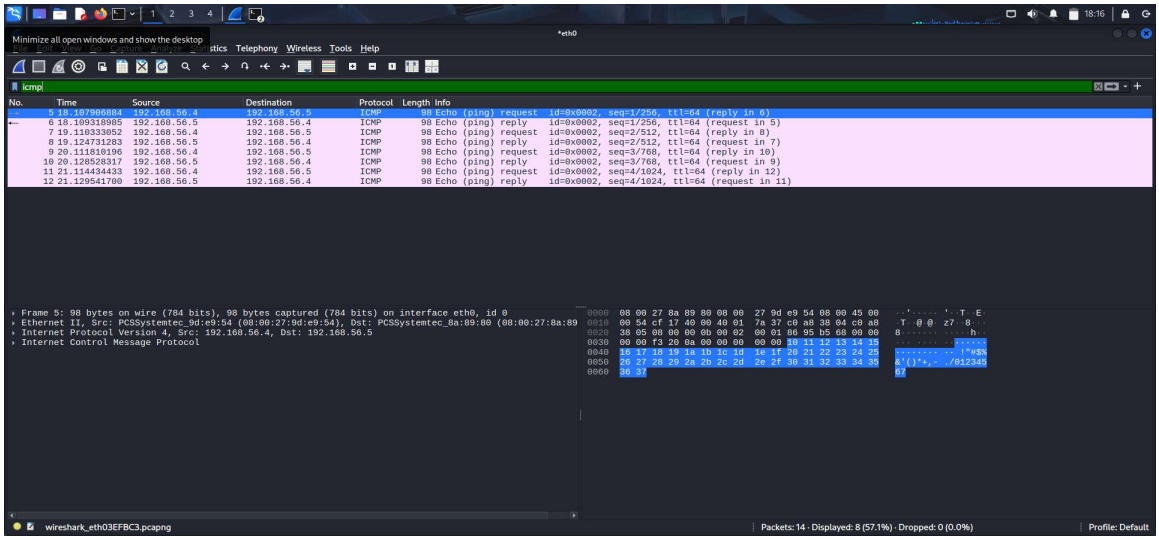
- Metasploitable 2 (Target) – IP: 192.168.56.5

  Both set to **Host-Only Adapter** for communication.
- Verified connection using ping.



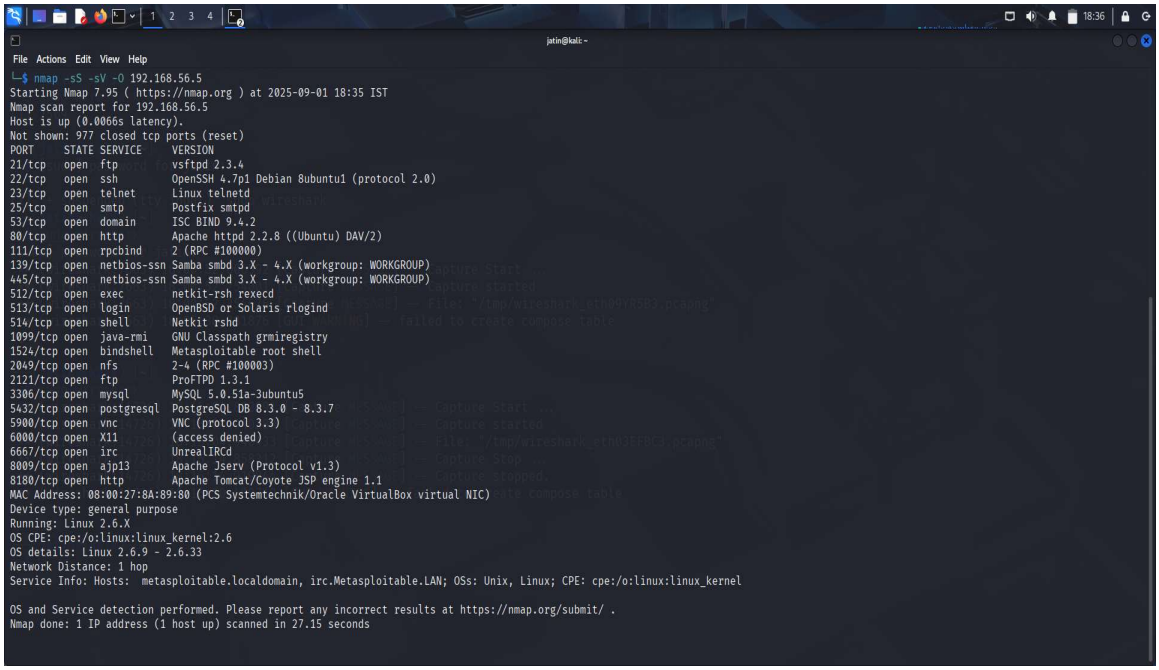
3. Wireshark Test Capture

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



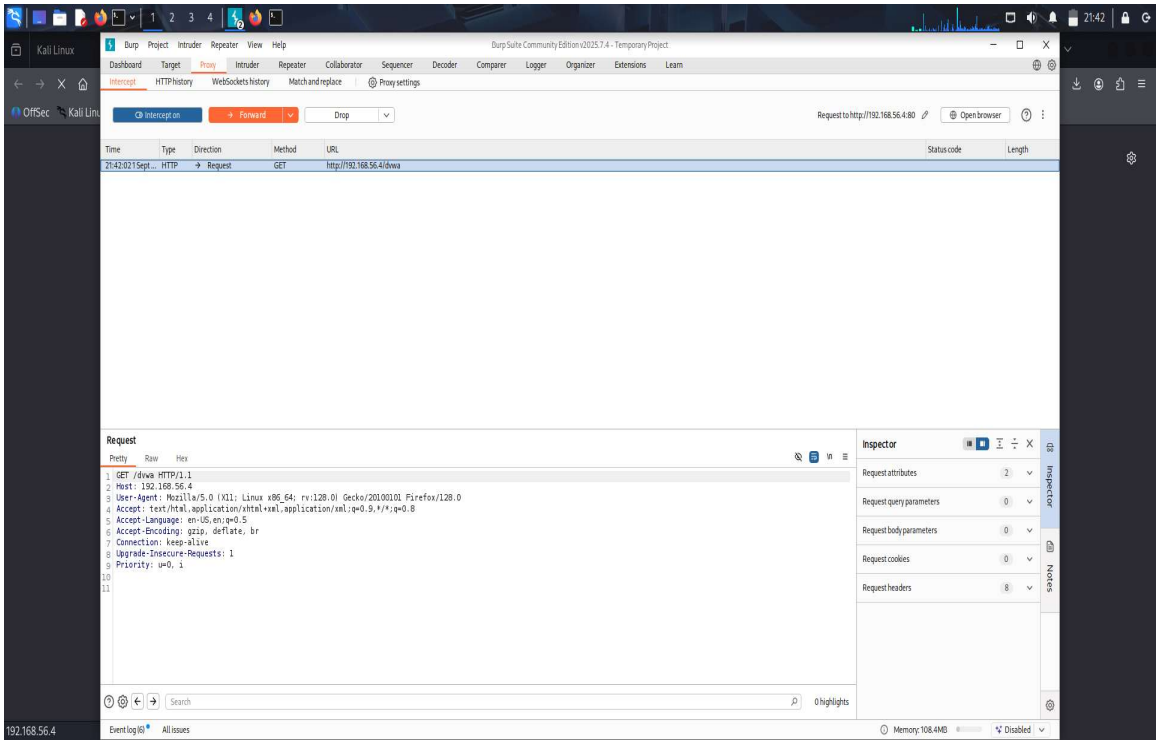
4. Nmap Scan

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



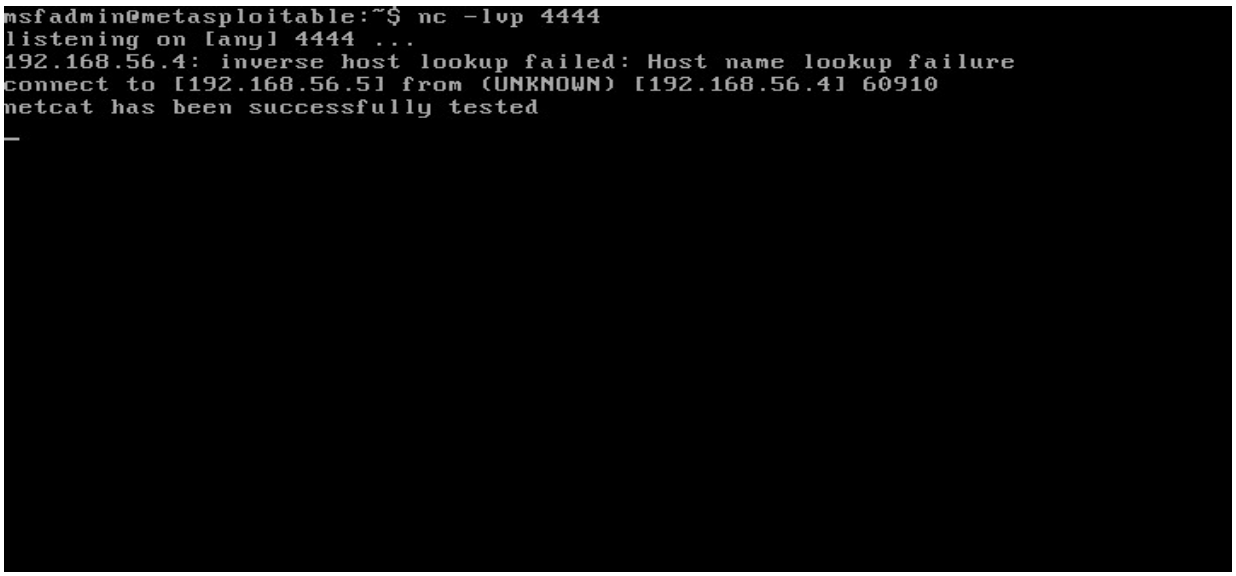
5. Burp Suite Proxy

- 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.



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.