Lab Setup Report

Objective: To successfully configure a virtual lab environment for practicing network penetration testing. This setup includes an attacker machine (Kali Linux), a vulnerable target machine (Metasploitable 2), and network traffic analysis using Wireshark.

---

1. Lab Components

- **Virtualization Software:** Oracle VM VirtualBox
- **Attacker Machine:** Kali Linux
- **Target Machine:** Metasploitable 2
- **Network Analyzer:** Wireshark
- **Network Configuration:** NAT

---

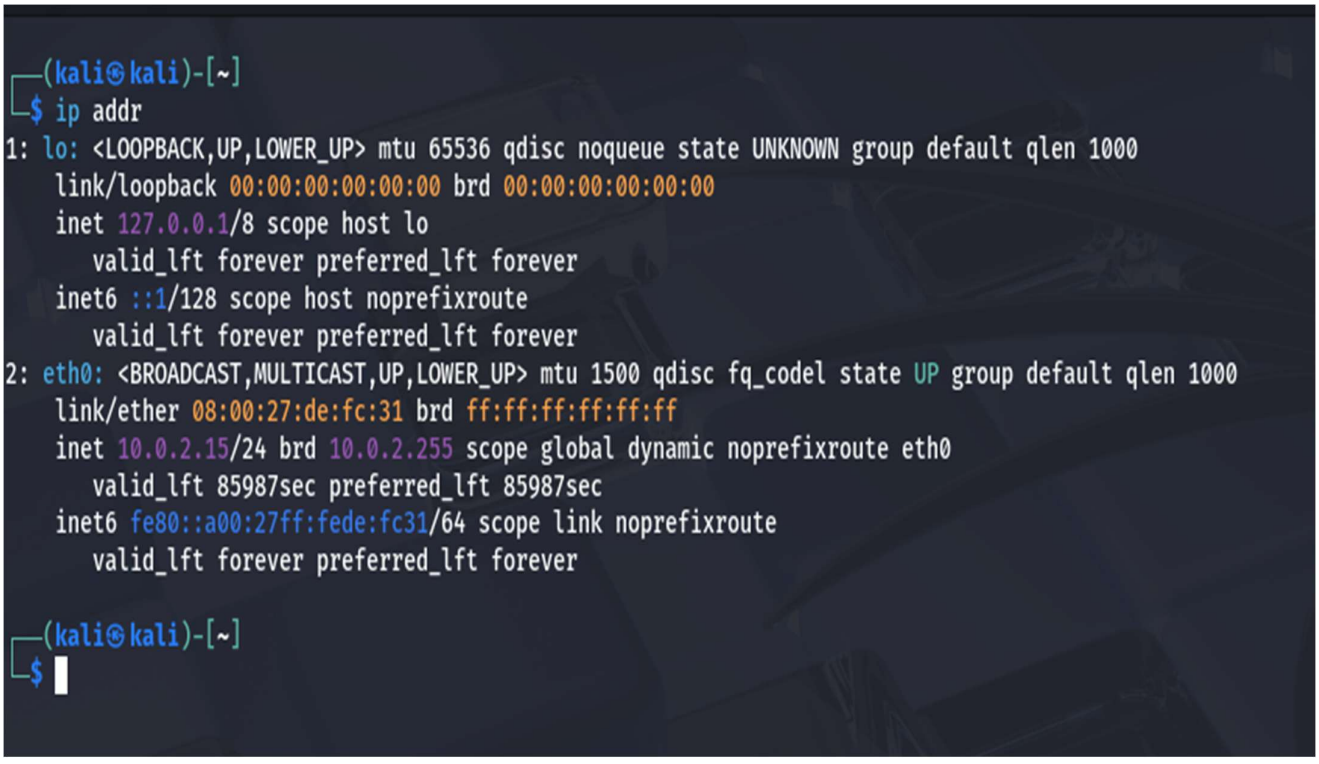
2. Configuration & Verification

The primary goal is to ensure the attacker and target machines can communicate with each other on an isolated virtual network.

2.1. Kali Linux Setup

The Kali Linux virtual machine was configured and booted. Network connectivity was verified using the ip addr command to identify its assigned IP address.

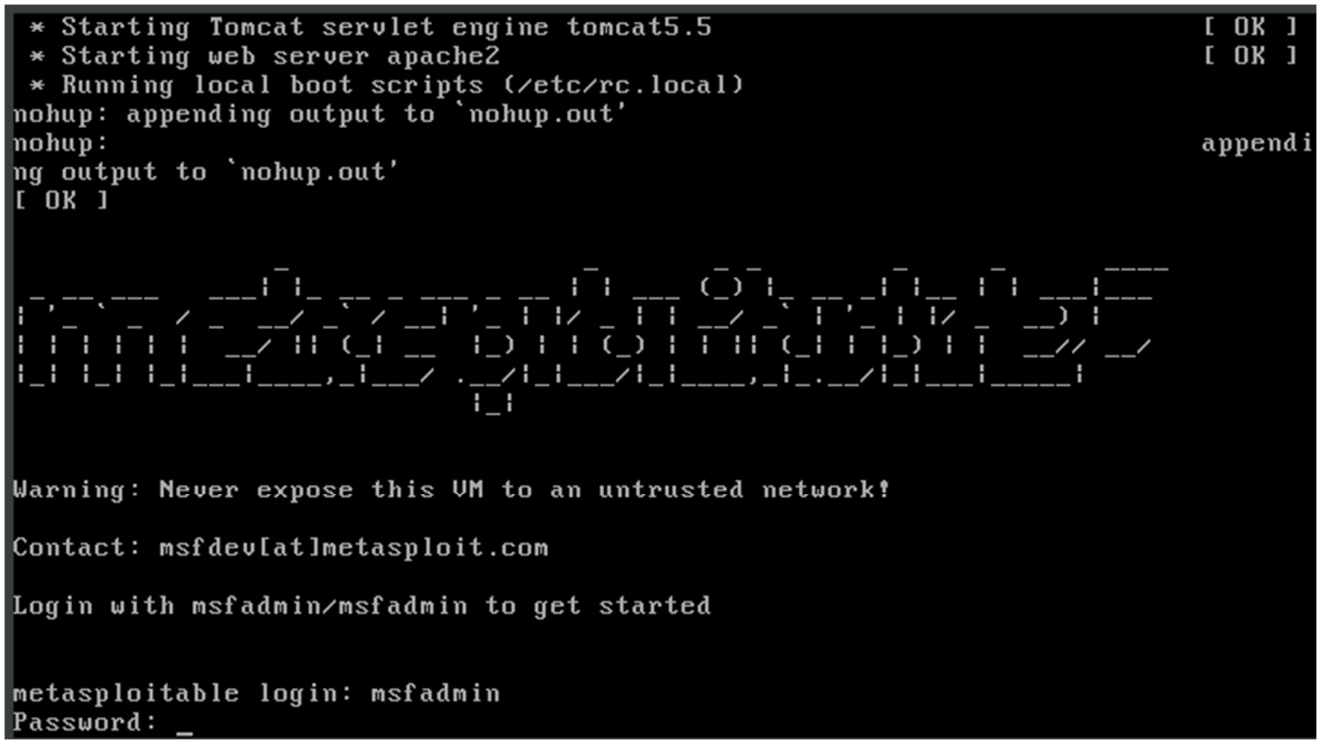
- **Assigned IP Address:** 10.0.2.15

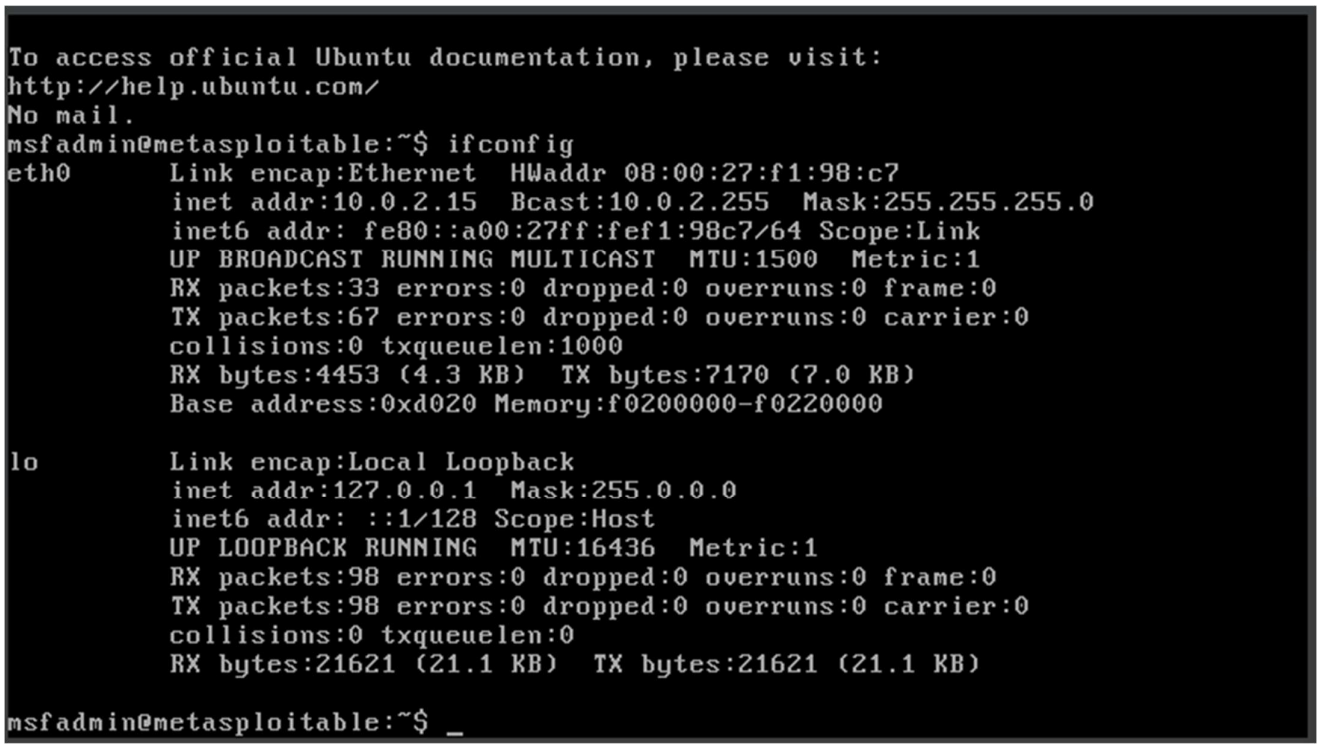


2.2. Metasploitable 2 Setup

The Metasploitable 2 virtual machine was imported and started. Upon booting, the login screen displays the IP address assigned to it by the virtual network's DHCP server.

- **Assigned IP Address:** 10.0.2.15





2.3. Connectivity Test

A network connectivity test was performed by pinging the Metasploitable 2 machine from the Kali Linux machine to confirm that they are on the same network and can communicate. The test was successful, with ICMP echo replies received.

- **Command:** ping -c 4 10.0.2.15

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.323 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.040 ms

--- 10.0.2.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3049ms
rtt min/avg/max/mdev = 0.033/0.109/0.323/0.123 ms

┌──(kali㉿kali)-[~]
└─$
```

---

3. Wireshark Test Capture

To verify that network traffic can be monitored, Wireshark was launched on the Kali Linux machine to capture the ICMP traffic generated by the ping test. The capture successfully recorded the ICMP echo request and echo reply packets between the two virtual machines.