

# 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

```
(kali@kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:de:fc:31 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 85987sec preferred_lft 85987sec
    inet6 fe80::a00:27ff:fedc:fc31/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

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

---

## 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

```
* Starting Tomcat servlet engine tomcat5.5      [ OK ]
* Starting web server apache2                  [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup:                                          append i
ng output to 'nohup.out'
[ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password: _
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f1:98:c7
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef1:98c7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4453 (4.3 KB)  TX bytes:7170 (7.0 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:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21621 (21.1 KB)  TX bytes:21621 (21.1 KB)

msfadmin@metasploitable:~$ _
```

## 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.

