Lab 2: Target Virtual Machine

Part 1: Metasploitable 3:

Virtualization is a powerful tool that allows ethical hackers to safely test different attacks, malware, and exploits on a multitude of different systems. The objective of this lab is to create two different Metasploitable 3 virtual machines (one running Windows 2008, the other running Ubuntu 14.04) for this purpose, and to establish a connection between them. The results are shown below.

Figure 1: Windows 2008 Metasploitable 3 VM

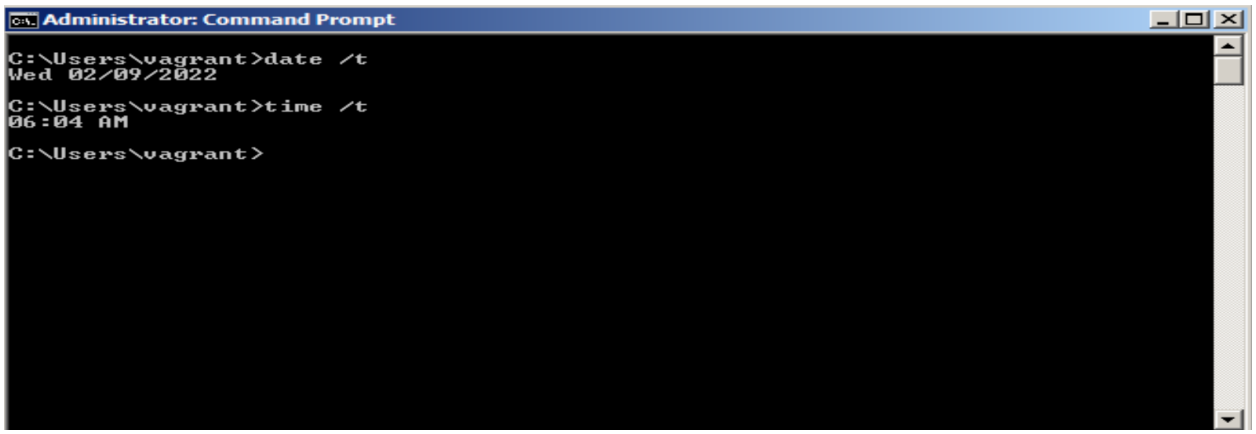
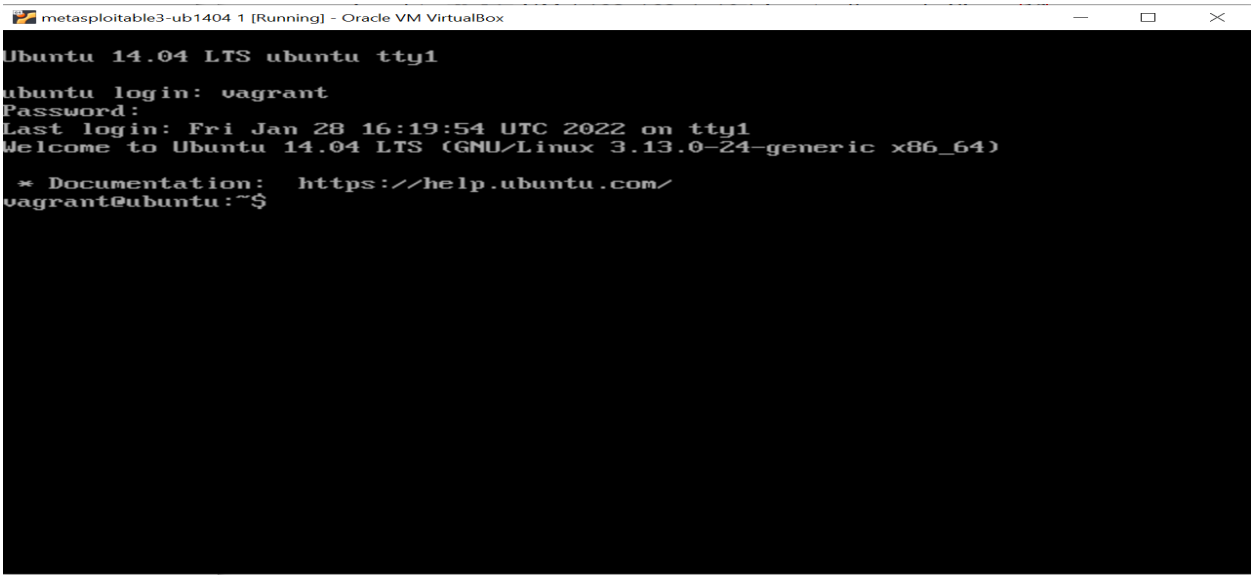


Figure 2: Ubuntu 14.04 Metasploitable VM

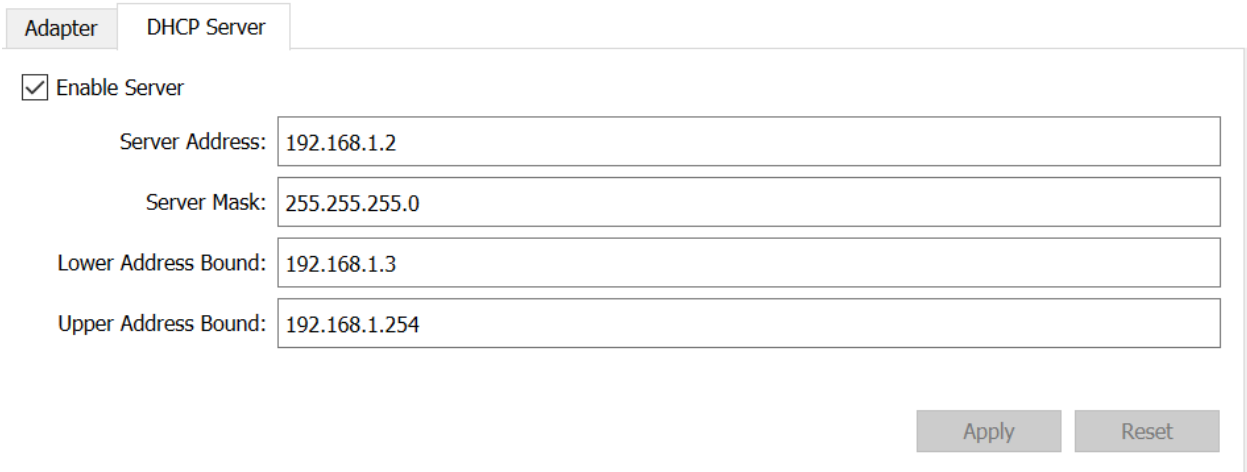


Part 2: Network Settings

VirtualBox supports many different methods of network virtualization, each with their own use cases. Host only networking is employed to connect all three virtual machines used in this lab, as shown below.

Figure 3: Network Adapter Configuration

Figure 4: DHCP Server Configuration



Part 3: Configure Kali to Use a Static IP Address

In order to communicate with the two Metasploitable 3 virtual machines, the Kali virtual machine must manually be assigned a static IP address, subnet mask, default gateway, and DNS server. Thankfully, these changes were made and verified quite easily with Kali's built in networking GUI and the command line.

Figure 5: Manually Editing the Network

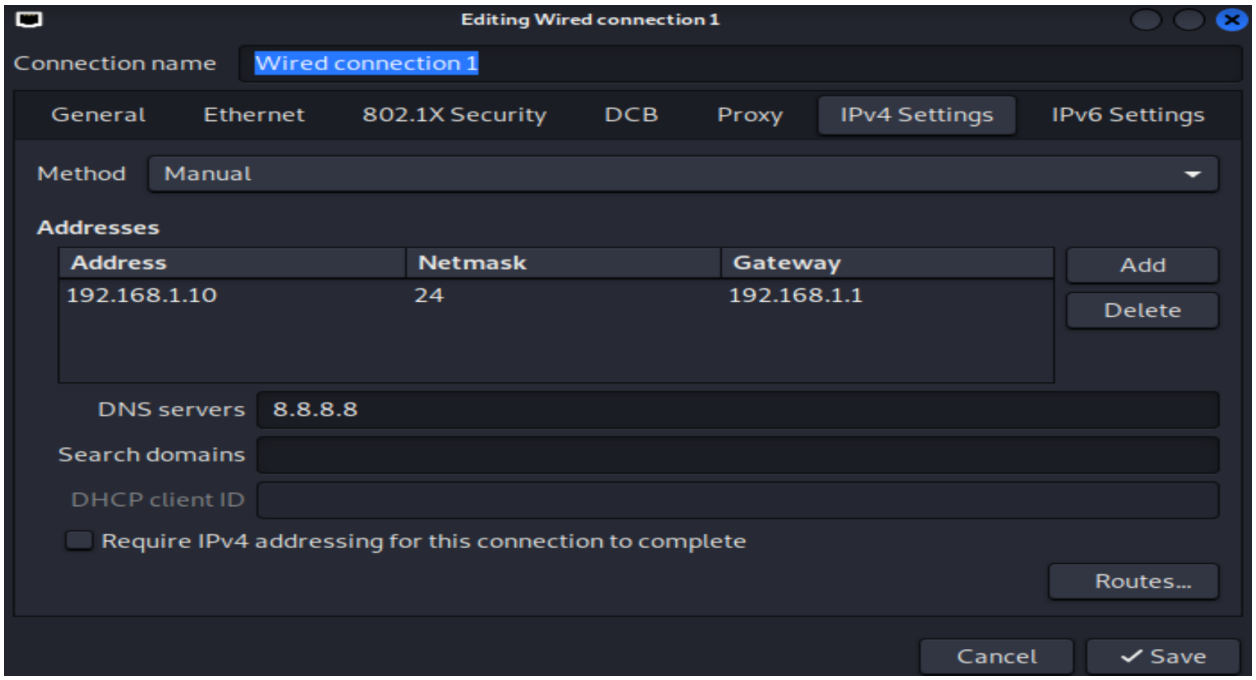
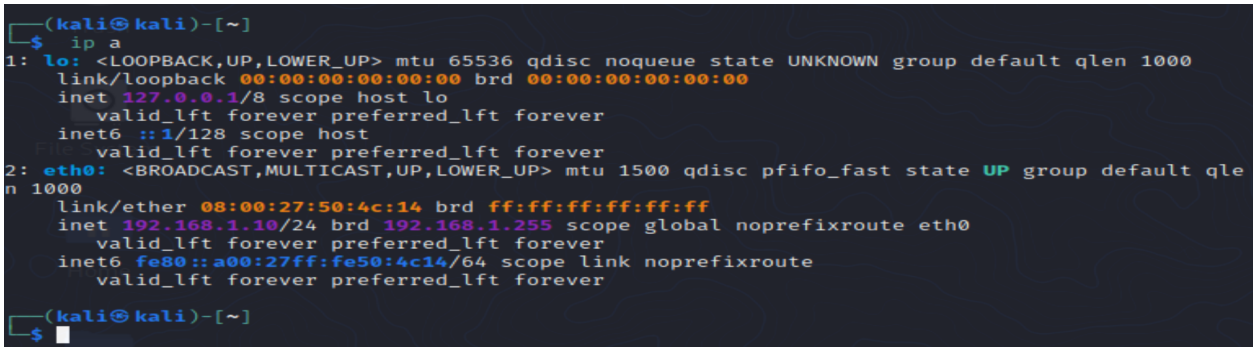


Figure 6: Verification of Network Changes



The two Metasploitable guest machines are now accessible to Kali over the host-only network, as demonstrated below using the ping command.

Figure 7: Pinging Metasploitable Guest Machines

```
┌──(kali㉿kali)-[~]
└─$ ping -c 2 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=128 time=0.652 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=128 time=0.354 ms

--- 192.168.1.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1034ms
rtt min/avg/max/mdev = 0.354/0.503/0.652/0.149 ms

┌──(kali㉿kali)-[~]
└─$ ping -c 2 192.168.1.30
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.
64 bytes from 192.168.1.30: icmp_seq=1 ttl=64 time=0.272 ms
64 bytes from 192.168.1.30: icmp_seq=2 ttl=64 time=0.362 ms

--- 192.168.1.30 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1025ms
rtt min/avg/max/mdev = 0.272/0.317/0.362/0.045 ms

┌──(kali㉿kali)-[~]
└─$
```

<u>Part 4: Shell Scripts</u>

Shell scripts are yet another tool in the ethical hacker's toolkit, and are widely used throughout the industry to automate various tasks. One such example is the problem of scanning for active hosts on a network, which can become quite tedious as the size of the network grows. Thankfully, this process can be easily automated using a few common UNIX commands embedded in a shell script. The source code of such a script is shown below in figure 8, and the results of running it are shown in figures 9 and 10. When the two metasploitable virtual machines are running, the script picks up each of their IP addresses, and when they are not, only the DHCP server and the Kali VM itself are detected.

Figure 8: pingScan.sh

```
#! /usr/bin/bash
if [ -z "$1" ]
then
        echo "Usage: ./pingScan [network]"
        echo "Ex: ./pingScan.sh 192.168.0"
else
        for i in {1..254}
        do
                (ping -c 1 $1.$i | grep "bytes from" | cut -d " " -f 4 | tr -d ":" &)
        done
fi
```

Figure 9: Detection of Metasploitable VMs

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern/Lab/Lab 2]
└─$ ./pingScan.sh 192.168.1
192.168.1.2
192.168.1.10
192.168.1.20
192.168.1.30
```

Figure 10: Detection of DHCP Server

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern/Lab/Lab 2]
└─$ ./pingScan.sh 192.168.1
192.168.1.2
192.168.1.10
```