SOC Lab: To Investigate and Simulate Attacks

Lab Setup:

1. **Network Topology**

2. **Installation Steps**

- I downloaded and installed VirtualBox to create a virtual environment for my attack simulation, within the VirtualBox I set the operating systems using their ISO and image file.

Kali Linux – It's Linux distribution designed for penetration testing. In this setup it will be used to simulate the attacker machine.

Windows 10 – It's A widely-used operating system. In the setup it will serve as the target machine to mimic a real-world user environment.

Metasploitable – It's a tool designed for testing and practicing exploitation techniques.

Below are the officially download links for each component mentioned above:

- VirtualBox: https://www.virtualbox.org/wiki/Downloads
- Kali Linux and ISO: https://www.kali.org/get-kali/
- Windows 10 and ISO: https://www.microsoft.com/software-download/windows10
- Metasploitable 2 VM Image: https://sourceforge.net/projects/metasploitable/

3. VM Configuration

After installing the virtual machines, I configured the network settings for each VM by enabling and adjusting the network adapters. The configuration details are illustrated in the image below.

VM Name	Adapter 1	Adapter 2	Purpose
Kali Linux	NAT Network	Host-Only Adapter	Internet access + communicate with Windows
Windows 10	Host-Only Adapter	Bridged Adapter	Communicate with Kali + Internet access
Metasploitable	NAT Network	—	Communicate with Kali (via NAT network)

For my vulnerable machine (Metasploitable), I needed to ensure that Kali Linux and Metasploitable could communication effectively within the virtual environment. And to achieve this, I created a custom NAT network using the VirtualBox Network Manager.

I named the network "meta-lab", set the ipv4 prefix to 10.0.2.0/24 and enabled DHCP to allow automatic Ip addressing. Next, I attached the "meta-lab" network to Adapter 1 of

both Kali Linux and Metasploitable, enabling a communication between the two machines. The final configuration is shown in the image below.

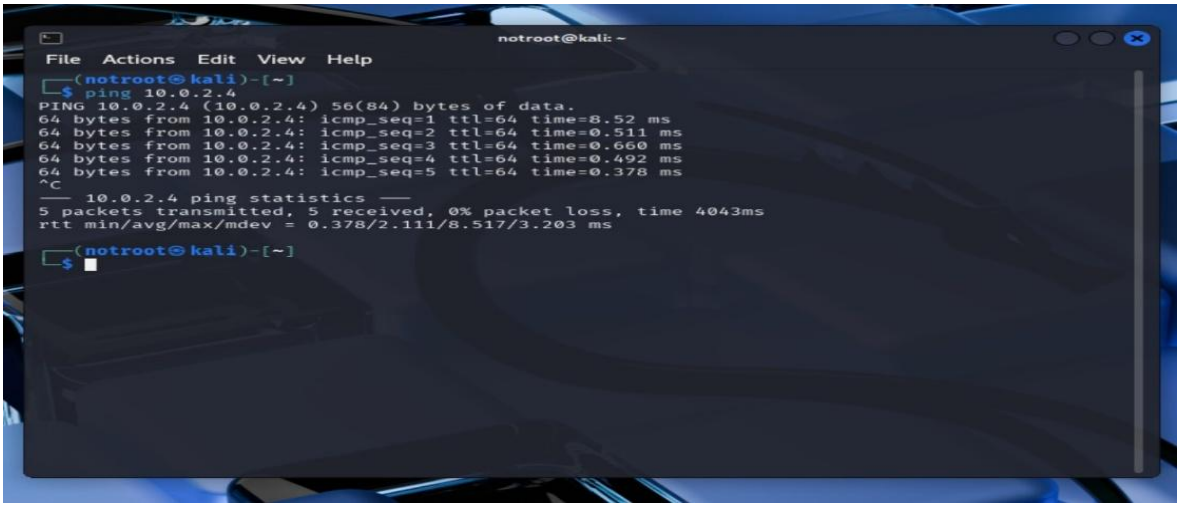
VM Name	Adapter	Attached To	Network Name	IP Range	Promiscuous Mode	DHCP
Kali Linux	Adapter 1	NAT Network	meta-lab	10.0.2.0/24	Allow VMs	✅
	Adapter 2	Host-Only Adapter	vboxnet	192.168.x.x	—	—
Metasploitable	Adapter 1	NAT Network	meta-lab	10.0.2.0/24	Allow VMs	✅
Windows 10	Adapter 1	Host-Only Adapter	vboxnet	192.168.x.x	—	—
	Adapter 2	Bridged Adapter	—	192.168.1.x	—	—

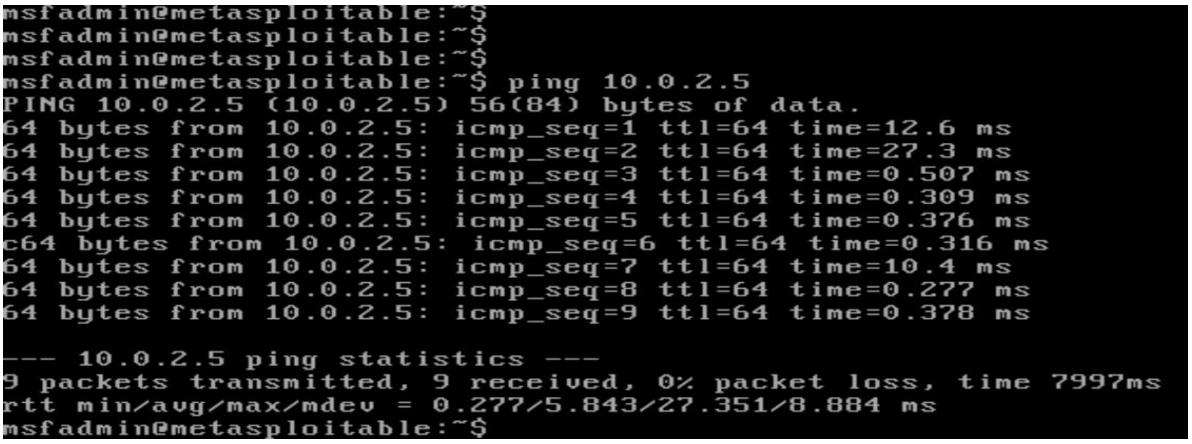
The image below shows the network interfaces of each virtual machine, including their adapter settings and assigned networks.

VM Name	Adapter	Attached To	IP Address	Interface
Kali Linux	Adapter 1	NAT Network	10.0.2.5	eth0
	Adapter 2	Host-Only Adapter	192.168.56.102	eth1
Metasploitable	Adapter 1	NAT Network	10.0.2.4	eth0
Windows 10	Adapter 1	Host-Only Adapter	192.168.56.103	eth0
	Adapter 2	Bridged Adapter	192.168.1.5	eth2

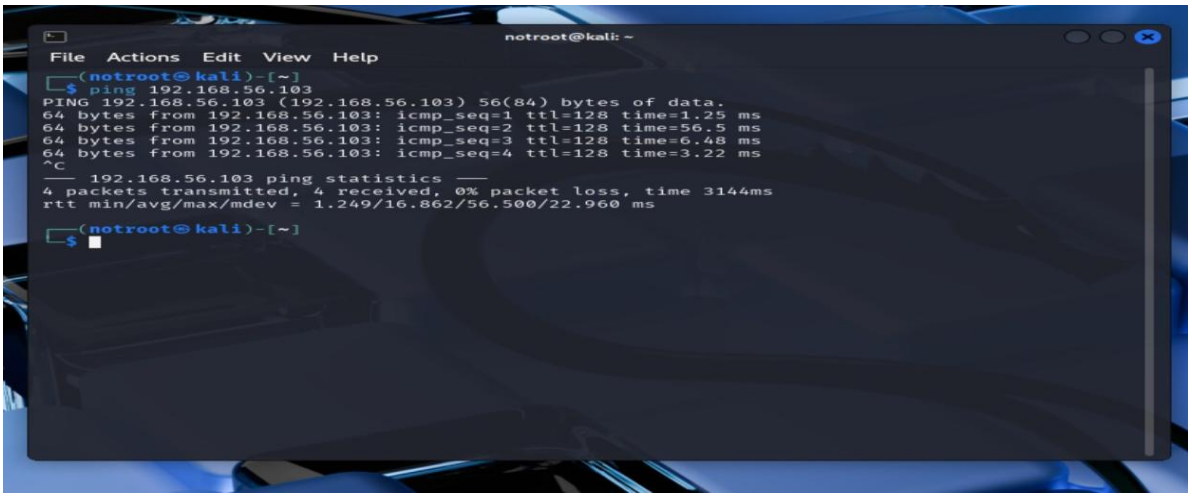
The next step was to verify network connectivity between the virtual machines. I ensured that:

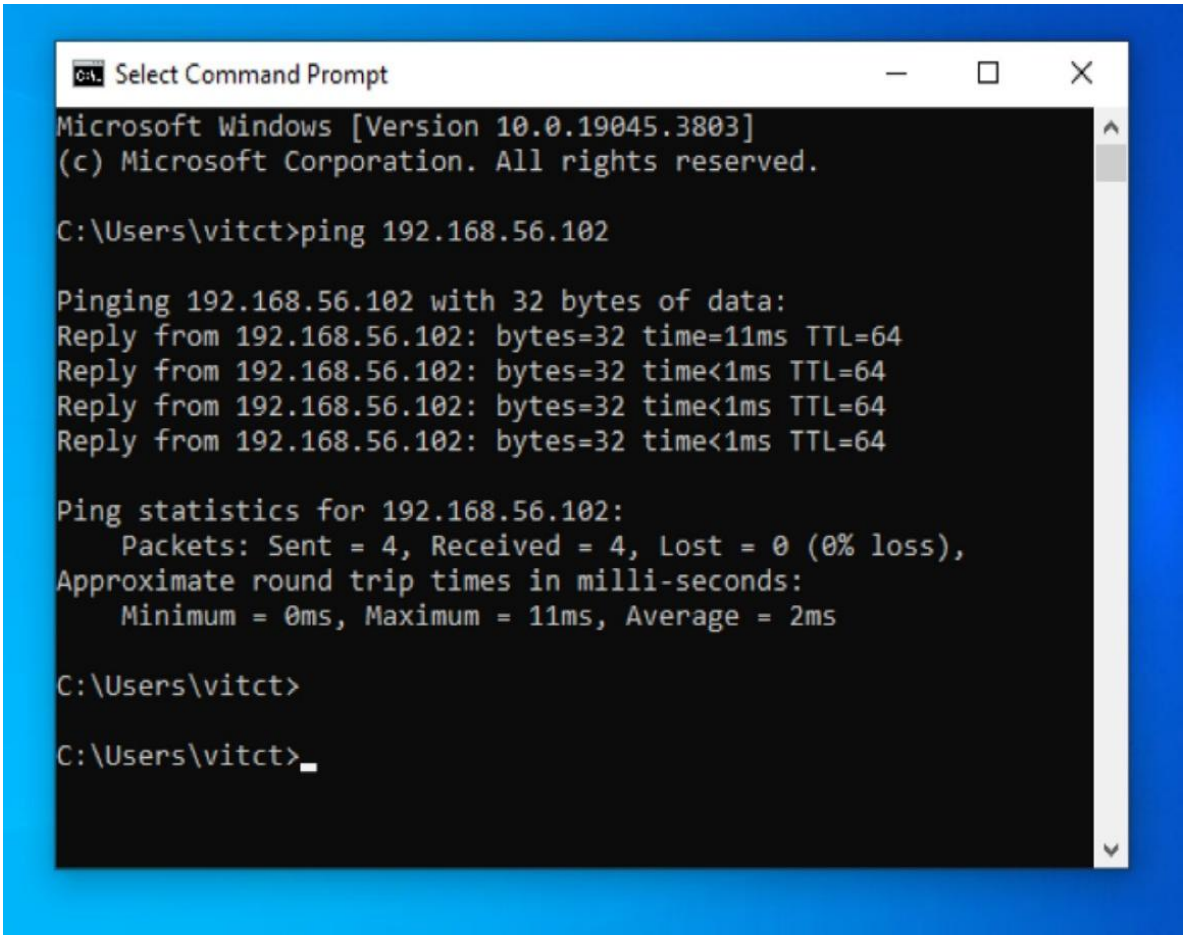
- Kali Linux can ping Metaspoloitable, and Metaspoloitable can also ping Kali Linux successfully.





- Kali Linux can ping Windows 10, and Windows 10 can also ping Kali Linux successfully.





The screenshots are taken from VirtualBox, to show the successful communication between the virtual machines.