Cybersecurity Lab Setup

Objective

To set up a basic penetration testing lab using Kali Linux as the attacker machine and Metasploitable2 as the vulnerable target, and to observe network traffic using Wireshark.

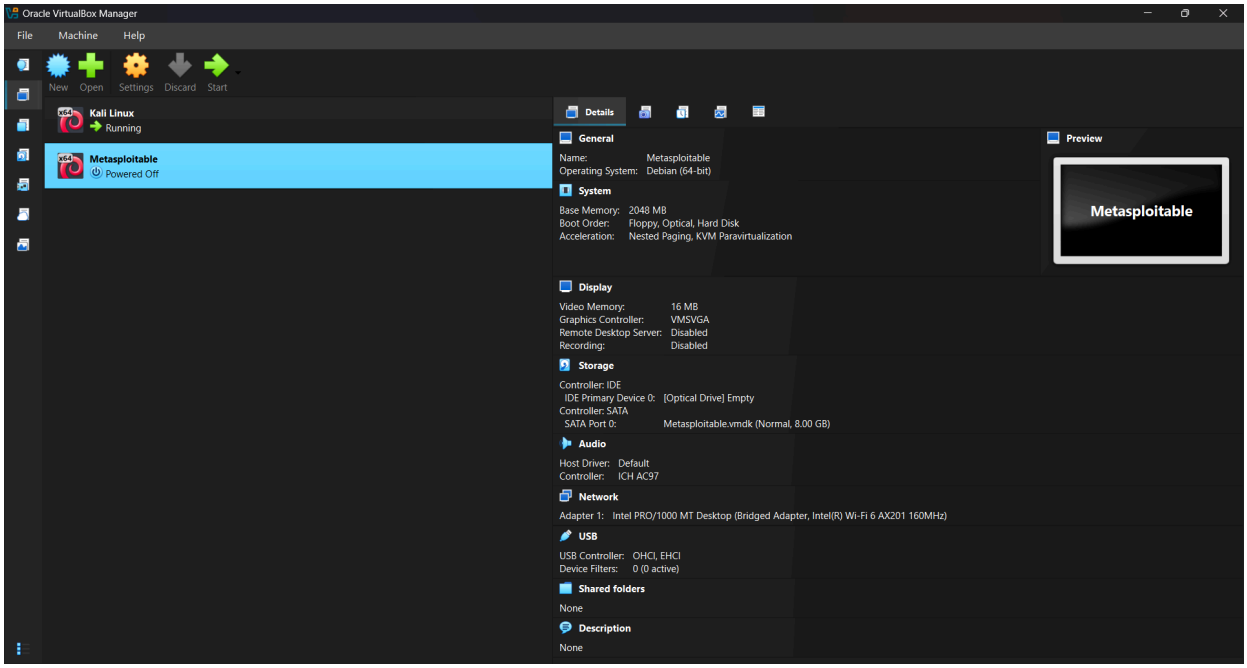
Tools Used

- Oracle VirtualBox
- Kali Linux (Attacker Machine)
- Metasploitable2 (Target Machine)
- Wireshark
- Host System: Windows

Lab Architecture

Host Machine
↳ VirtualBox
    ↳ Kali Linux VM (Attacker)
    ↳ Metasploitable2 VM (Target)

Both VMs are connected using **Internal Network** mode to ensure isolation and secure testing.

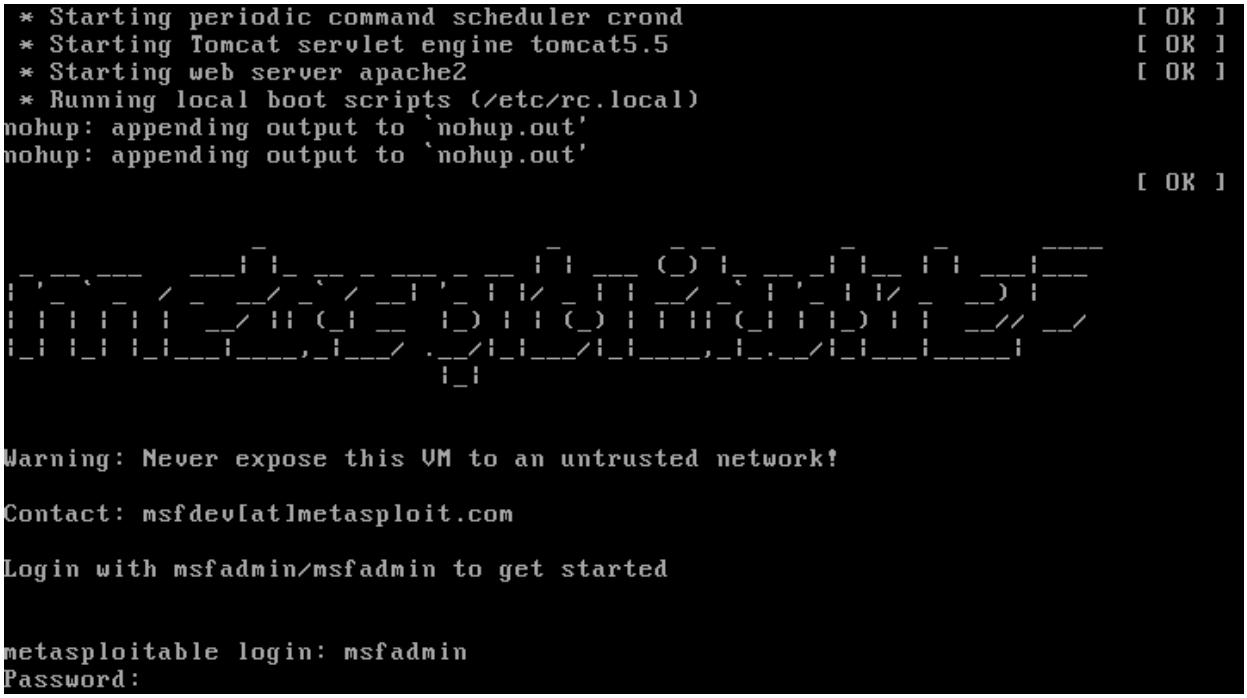


Step 1: Kali Linux Setup

- Installed Kali Linux ISO on VirtualBox
- Allocated minimum 2GB RAM and 2 CPUs
- Network Adapter set to **Internal Network**
- Kali boot verified successfully

Step 2: Metasploitable2 Setup

- Imported Metasploitable2 VM into VirtualBox
- Network Adapter set to **Internal Network** (same as Kali)
- Default credentials used for login



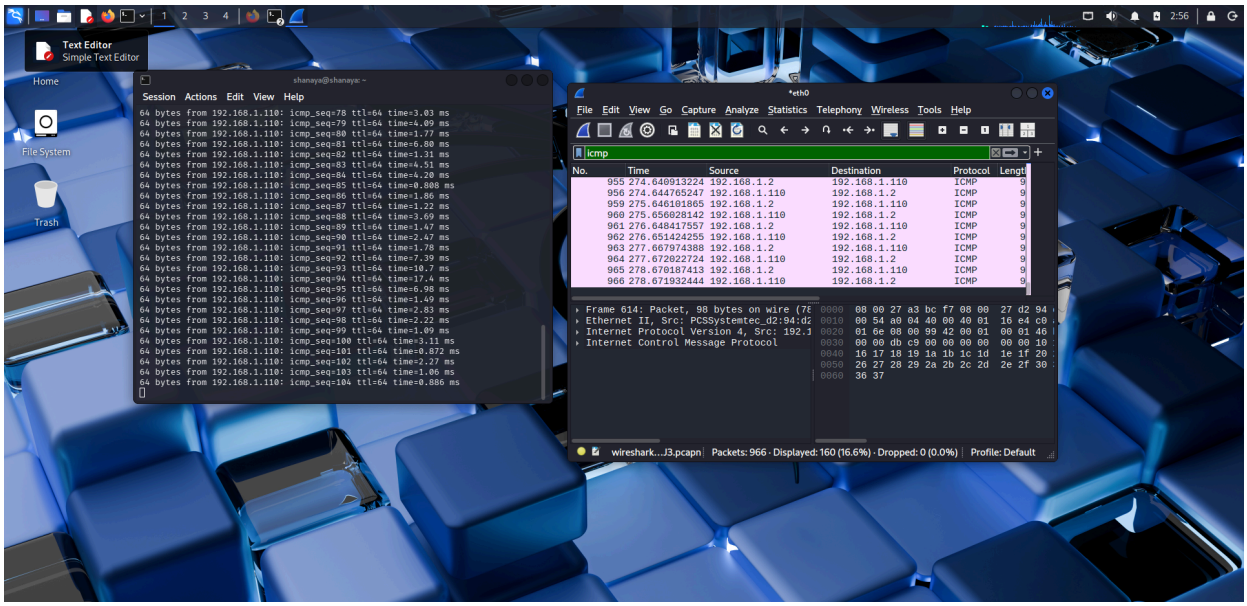
Step 3: Network Verification

- Checked IP address on Kali using:
  `ifconfig`
- Checked IP address on Metasploitable using:
  `ip a`

- Verified connectivity using:
  `ping 192.168.1.110`

Step 4: Wireshark Test Capture

- Opened Wireshark on Kali
- Selected active network interface
- Started capture
- Performed ping scan to generate traffic
- Observed ICMP packets



Result

The lab was successfully set up. Kali Linux and Metasploitable were able to communicate within a secure isolated environment, and network traffic was captured using Wireshark.