Experiment No. 1a(b)
Title : Setting Up the Environment

Roll No.:16010423076 **Experiments No.:1a(b)**

Aim : Setting Up the Environment (b) Installation of Metasploit

---

Resources : A computer with Oracle Virtual box, Kali-Linux installed, Metasploitable 2 zip file

Theory:

What is Metasploitable?
Metasploitable is a purposely vulnerable virtual machine designed for use in penetration testing and ethical hacking exercises. It provides a safe environment where security professionals and learners can practice exploiting real-world vulnerabilities without causing harm to actual systems. It contains a variety of vulnerabilities in different services, protocols, and applications, making it an ideal tool for learning how to discover and exploit security weaknesses.

Why is Metasploitable Used?
Metasploitable is used by security professionals, ethical hackers, and penetration testers to practice and improve their skills. It allows them to simulate attacks, exploit known vulnerabilities, and test the effectiveness of various tools and techniques in a controlled environment. It is also widely used in security courses and training programs to provide hands-on experience in vulnerability assessment and exploitation.

How Does Metasploitable Help in Learning Security?
Metasploitable provides a safe and controlled environment for learning and practicing penetration testing. Users can scan the system with tools like Nmap or Nessus to identify vulnerabilities, attempt to exploit them using frameworks like Metasploit, and analyze the results to understand how attacks work. It teaches important concepts such as vulnerability identification, exploitation, privilege escalation, and post-exploitation techniques.

What Are the Key Features of Metasploitable?
Metasploitable comes pre-configured with a wide range of outdated and vulnerable services, including:

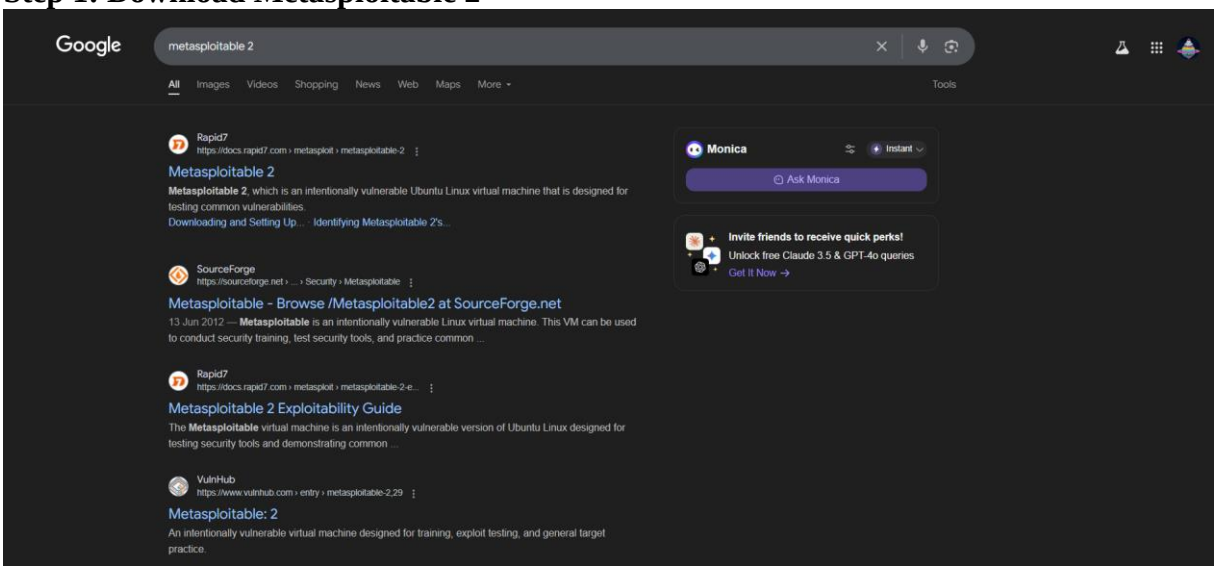
- Insecure web applications (e.g. vulnerable to SQL injection, cross-site scripting)
- Unpatched software with known exploits
- Misconfigured servers and services (e.g. open ports, weak passwords)
- Legacy protocols with known weaknesses

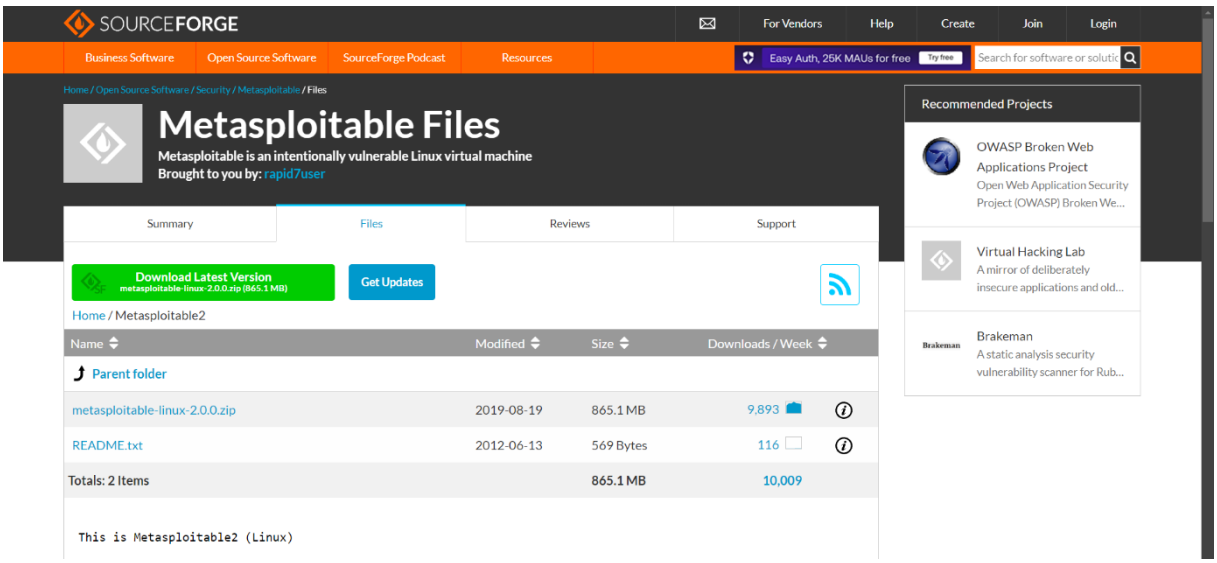
These vulnerabilities help users practice exploiting real-world security flaws without the risk of affecting live systems.

IMPLEMENTATION AND RESULTS:

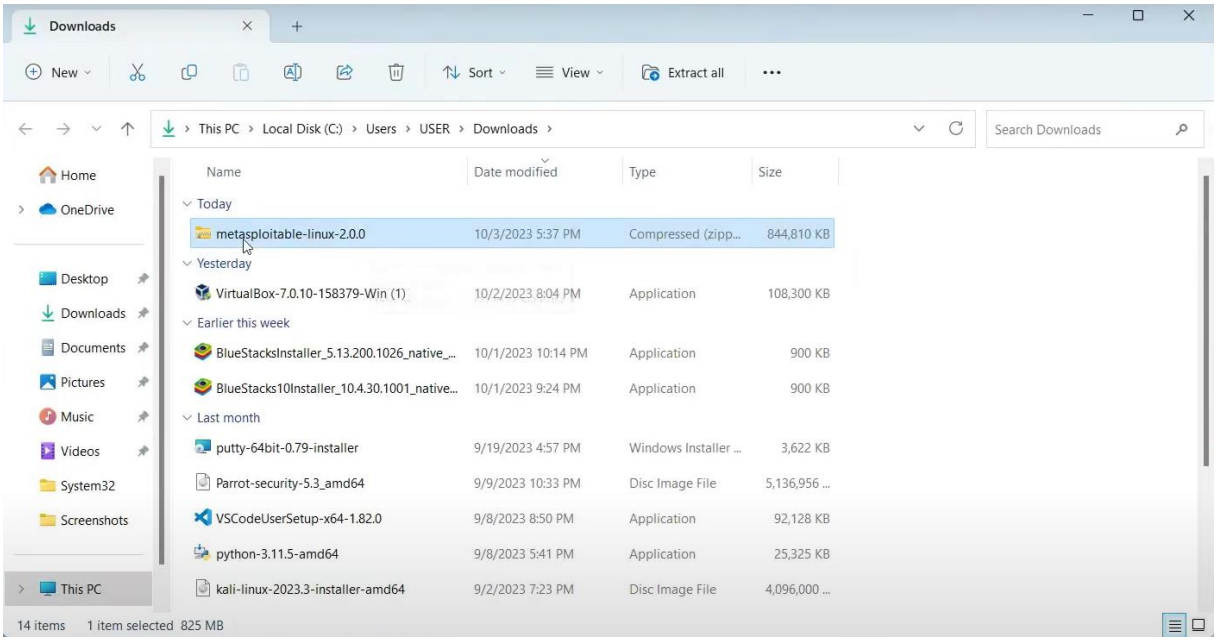
Installing Metasploitable 2 Using SourceForge

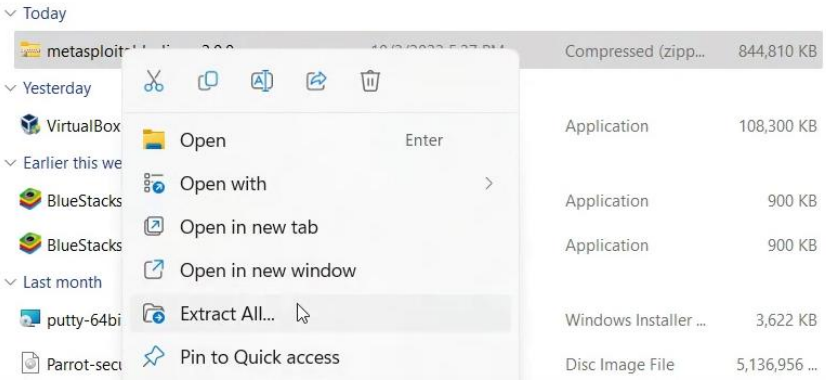
Step 1: Download Metasploitable 2

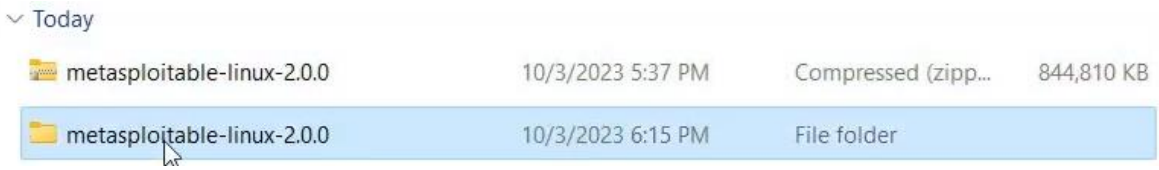




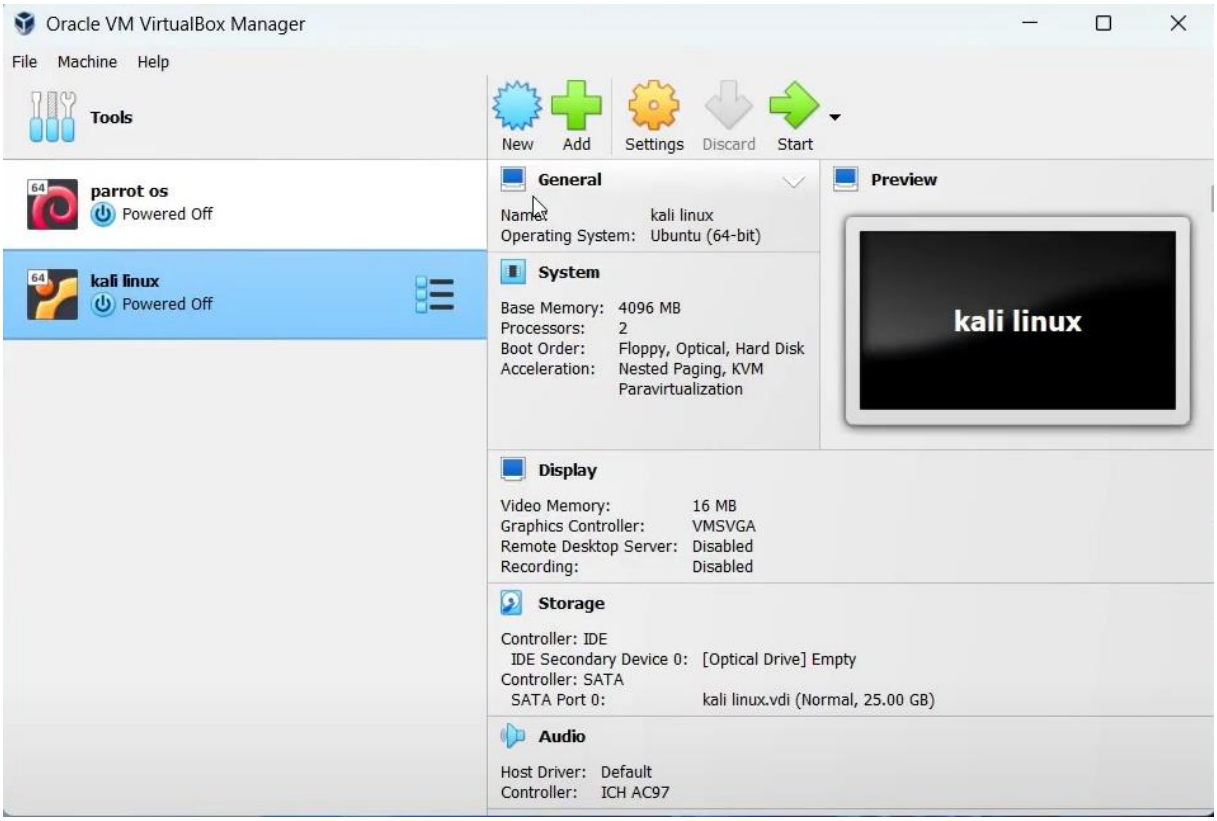
Step 2: Extract the ZIP Archive



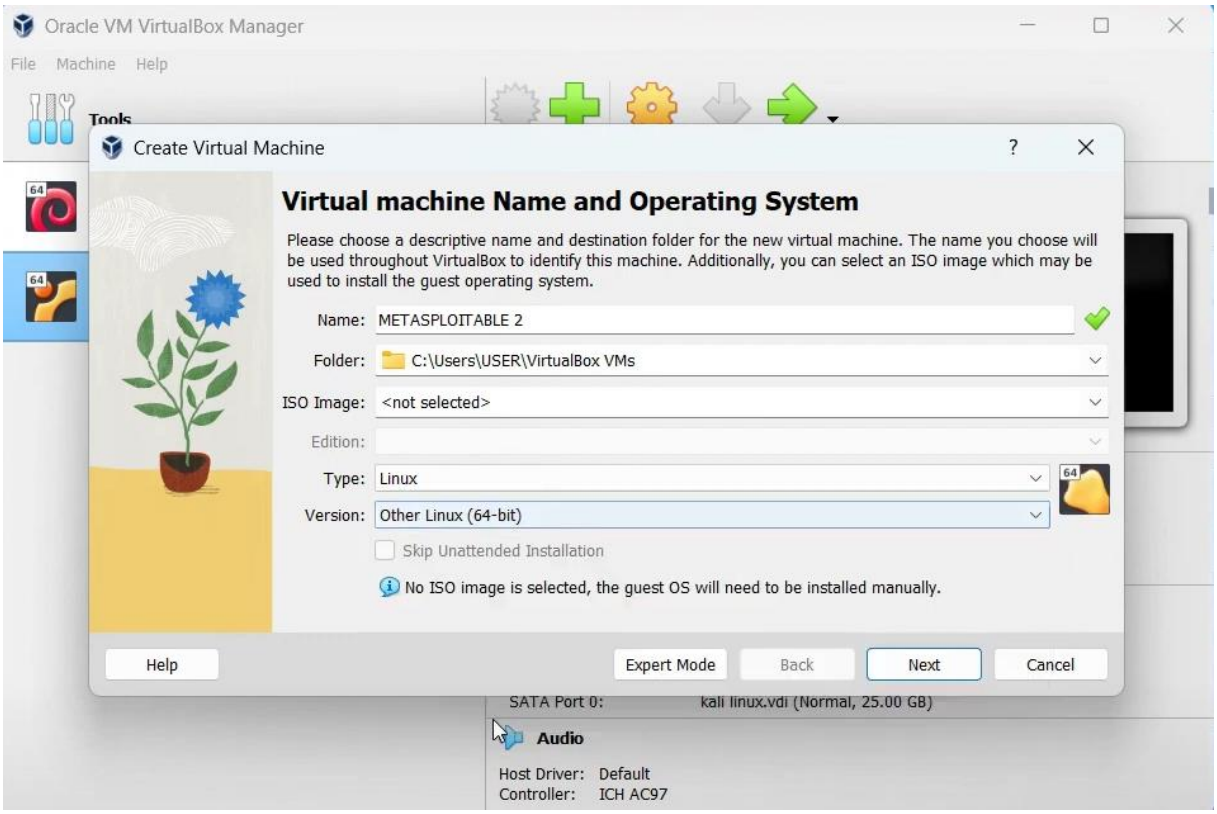


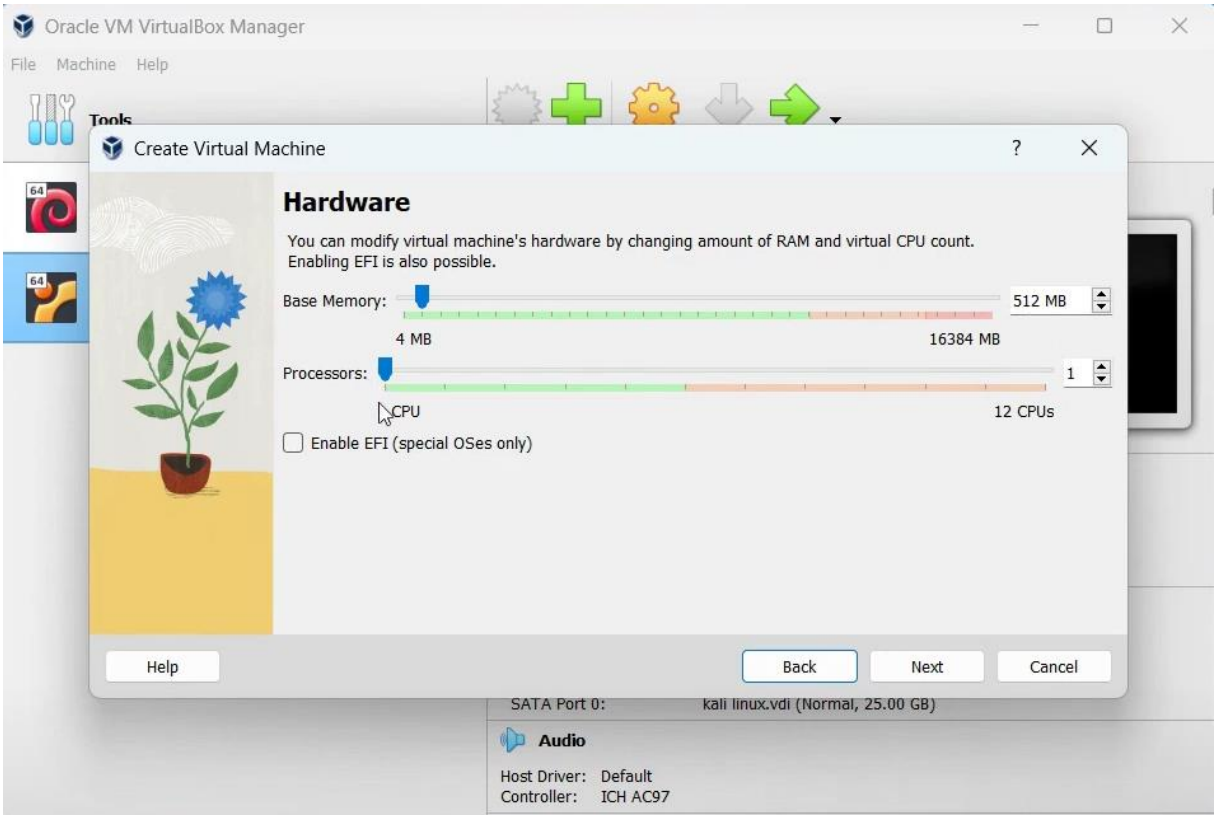


Step 3: Open Oracle VirtualBox

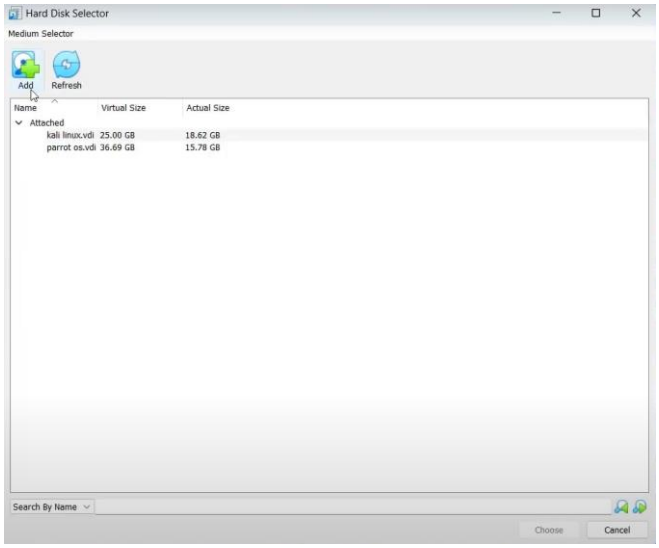


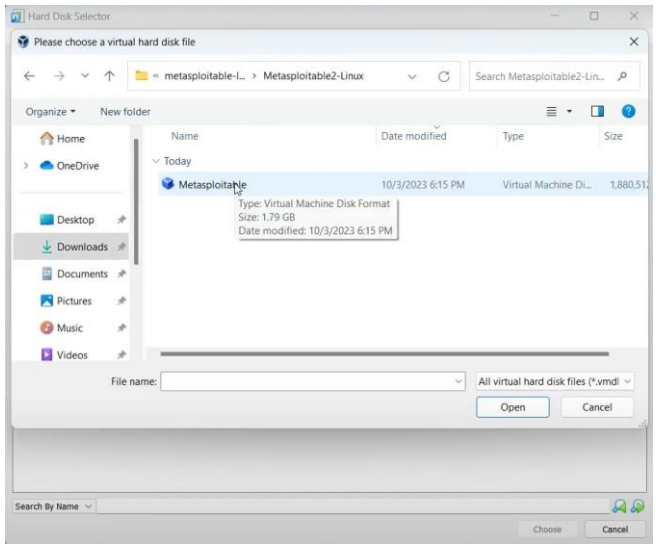
Step 4: Configure the Virtual Machine

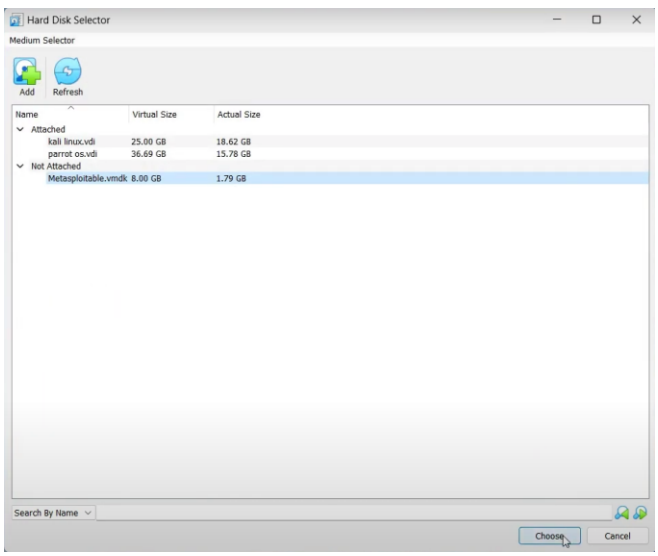


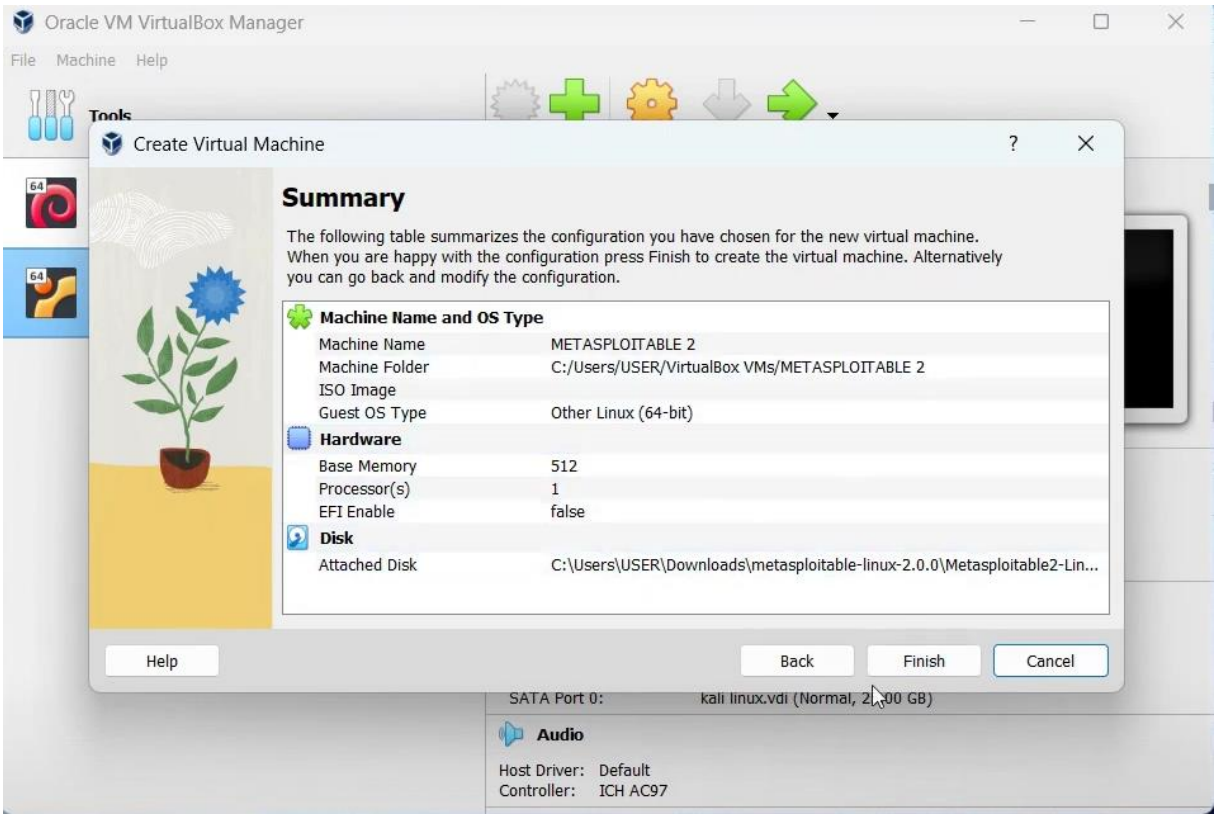


Change the virtual hard disk to Metasploitable

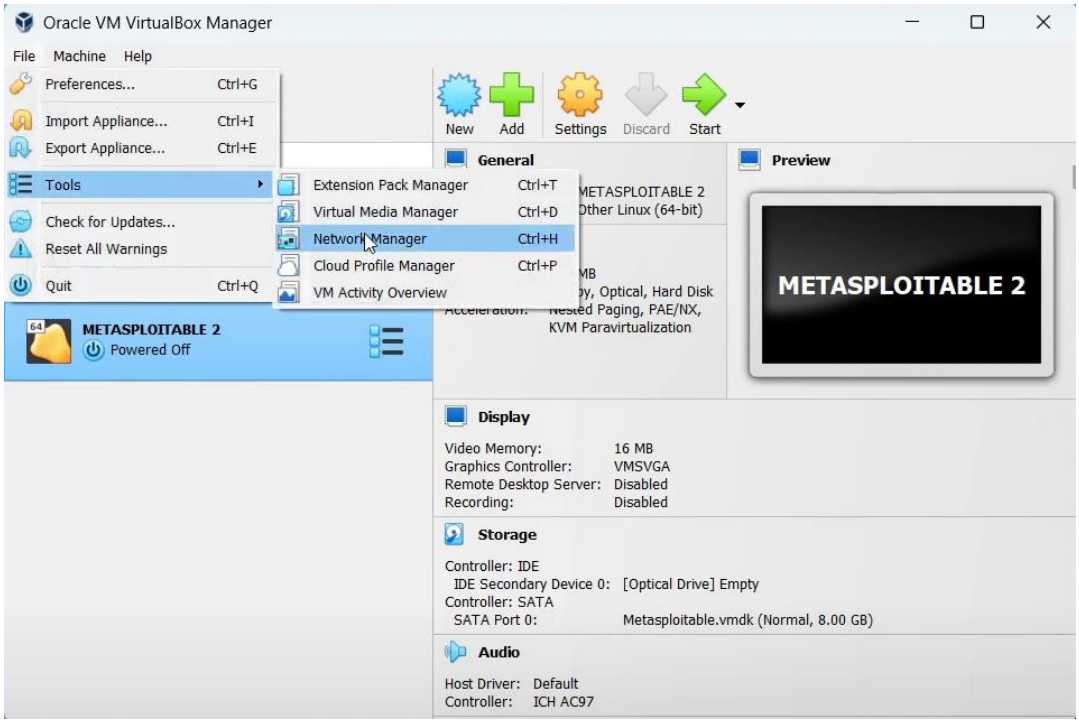

Hard Disk Selector
Medium Selector
Add
Refresh
Name
Virtual Size
Actual Size
Attached
kali linux.vdi 25.00 GB 18.62 GB
parrot os.vdi 36.69 GB 15.78 GB
Search By Name
Choose
Cancel

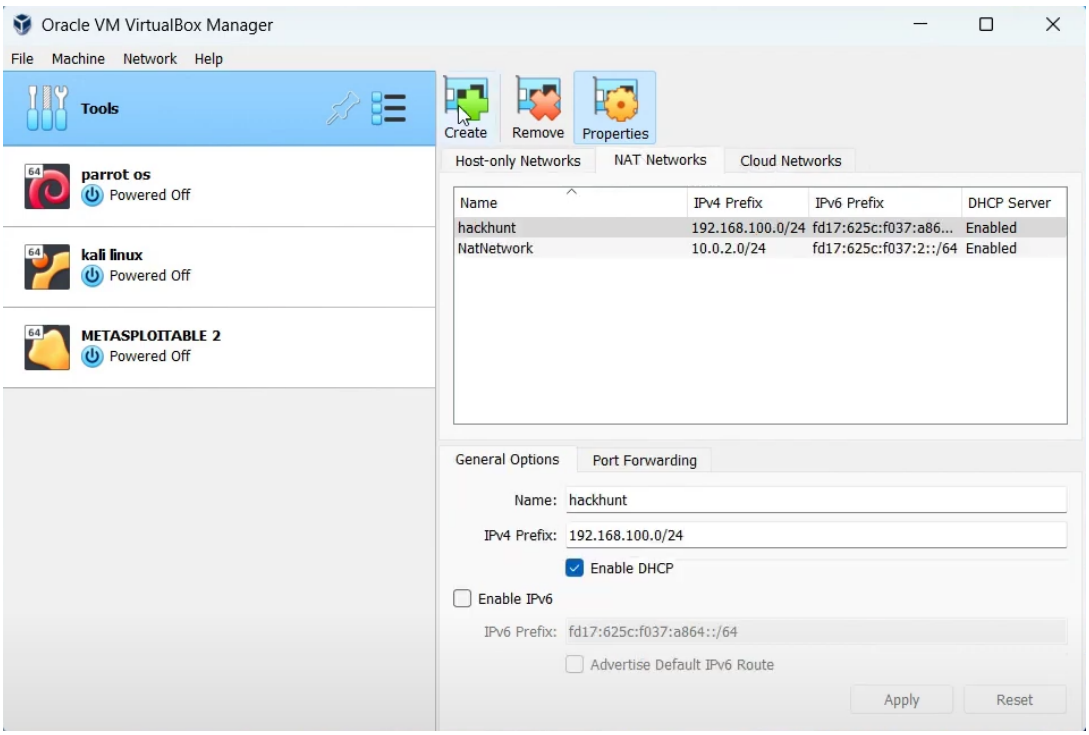

Hard Disk Selector
Please choose a virtual hard disk file
metasploitable-l... › Metasploitable2-Linux
Search Metasploitable2-Lin...
Organize
New folder
Home
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
Name
Date modified
Type
Size
Today
Metasploitable
10/3/2023 6:15 PM
Virtual Machine Di...
Type: Virtual Machine Disk Format
Size: 1.79 GB
Date modified: 10/3/2023 6:15 PM
File name:
All virtual hard disk files (*.vmdi
Open
Cancel
Search By Name
Choose
Cancel

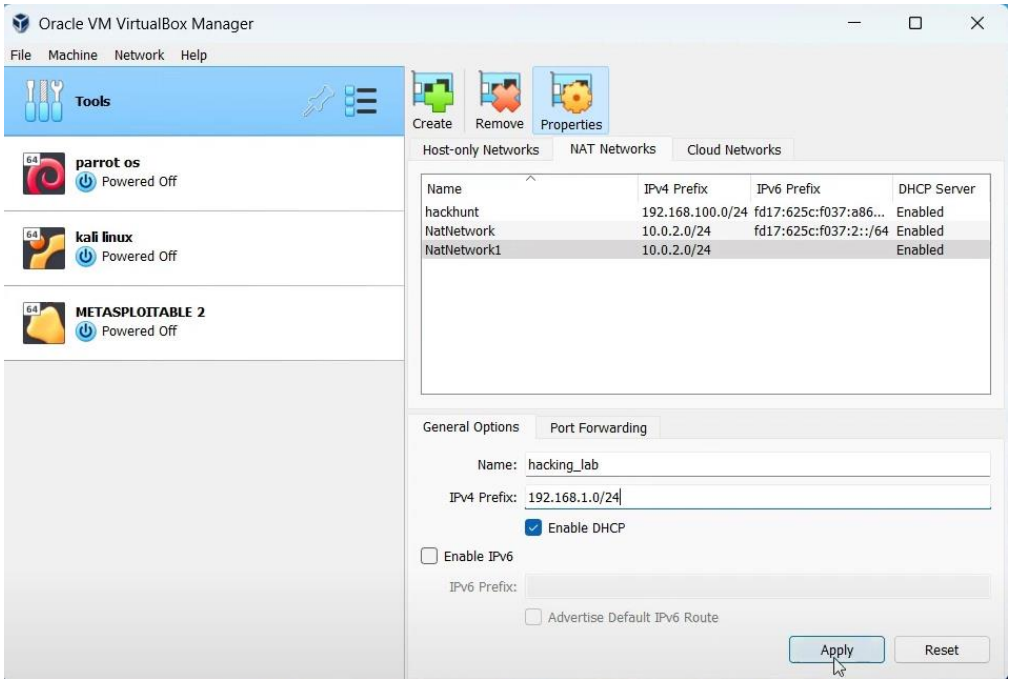

Hard Disk Selector
Medium Selector
Add
Refresh
Name
Virtual Size
Actual Size
Attached
kali linux.vdi 25.00 GB 18.62 GB
parrot os.vdi 36.69 GB 15.78 GB
Not Attached
Metasploitable.vmdk 8.00 GB 1.79 GB
Search By Name
Choose
Cancel



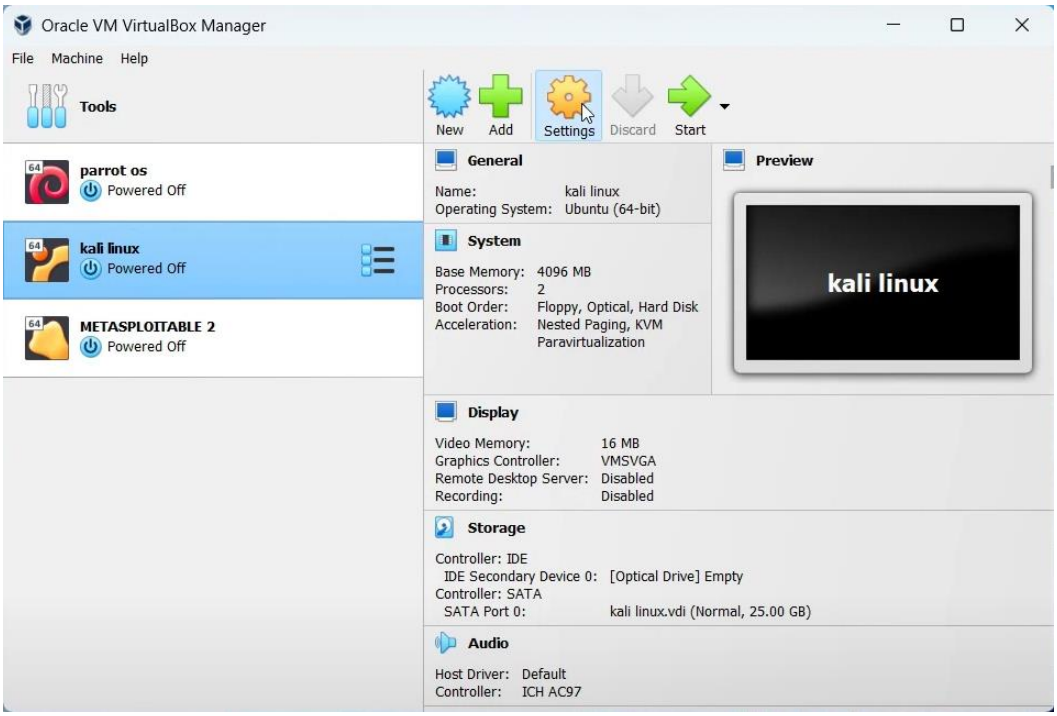
Step 5: Adjust Virtual Machine Settings

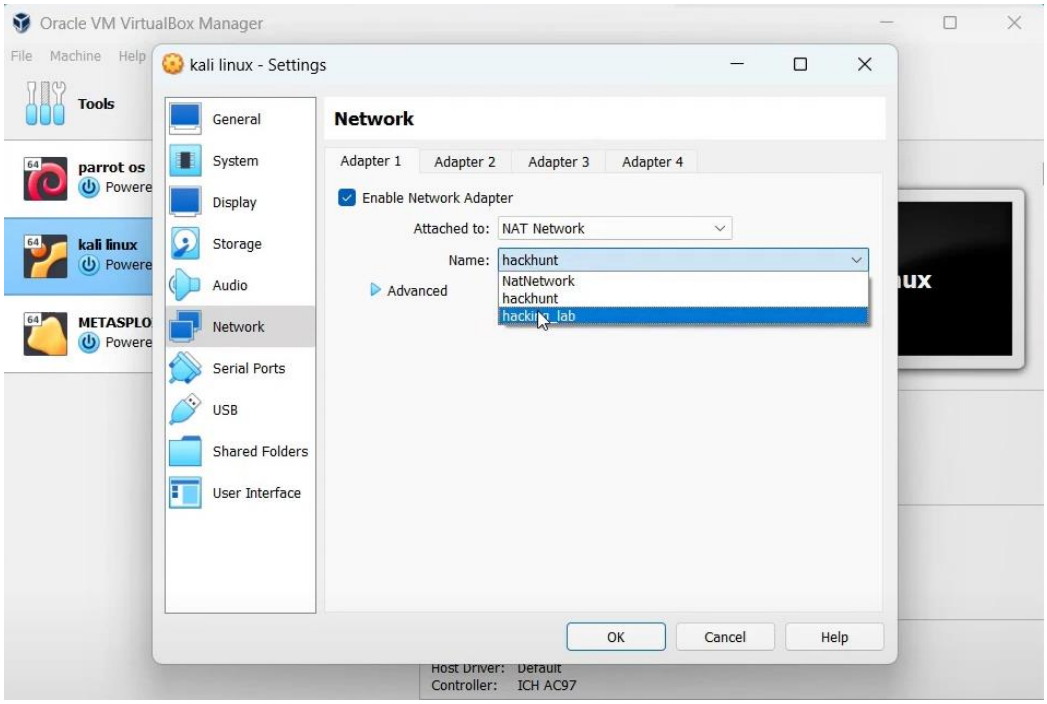

Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Tools
Check for Updates...
Reset All Warnings
Quit Ctrl+Q
Extension Pack Manager Ctrl+T
Virtual Media Manager Ctrl+D
Network Manager Ctrl+H
Cloud Profile Manager Ctrl+P
VM Activity Overview
New
Add
Settings
Discard
Start
General
Preview
METASPLOITABLE 2
Powered Off
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)
Audio
Host Driver: Default
Controller: ICH AC97

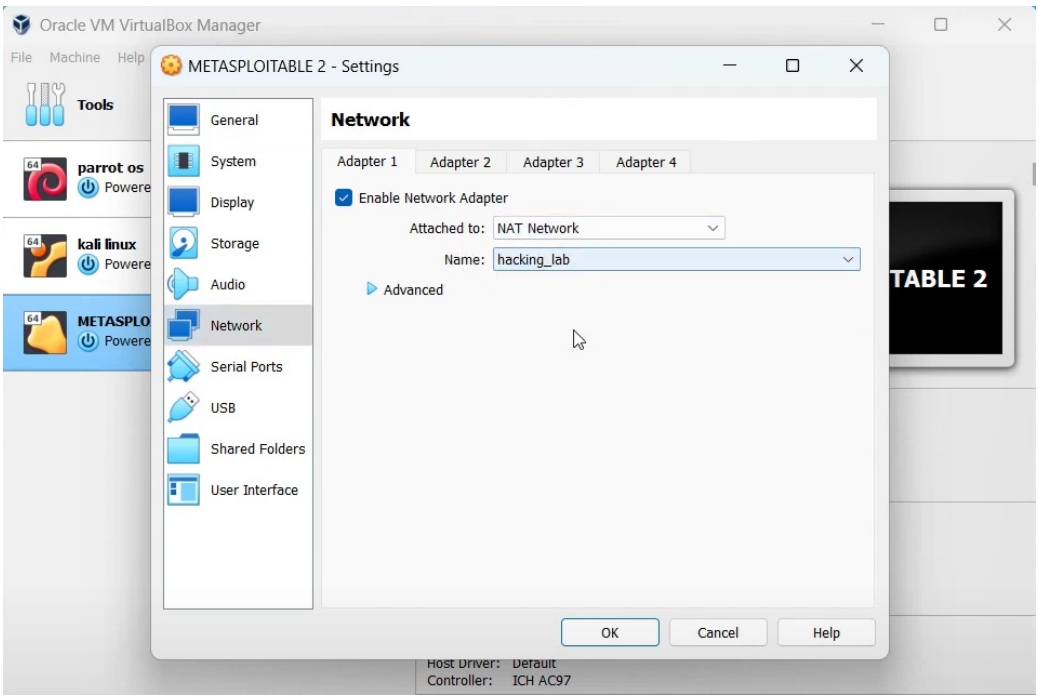

Oracle VM VirtualBox Manager
File
Machine
Network
Help
Tools
parrot os
Powered Off
kali linux
Powered Off
METASPLOITABLE 2
Powered Off
Create
Remove
Properties
Host-only Networks
NAT Networks
Cloud Networks
Name
IPv4 Prefix
IPv6 Prefix
DHCP Server
hackhunt 192.168.100.0/24 fd17:625c:f037:a86... Enabled
NatNetwork 10.0.2.0/24 fd17:625c:f037:2::/64 Enabled
General Options
Port Forwarding
Name: hackhunt
IPv4 Prefix: 192.168.100.0/24
Enable DHCP
Enable IPv6
IPv6 Prefix: fd17:625c:f037:a864::/64
Advertise Default IPv6 Route
Apply
Reset



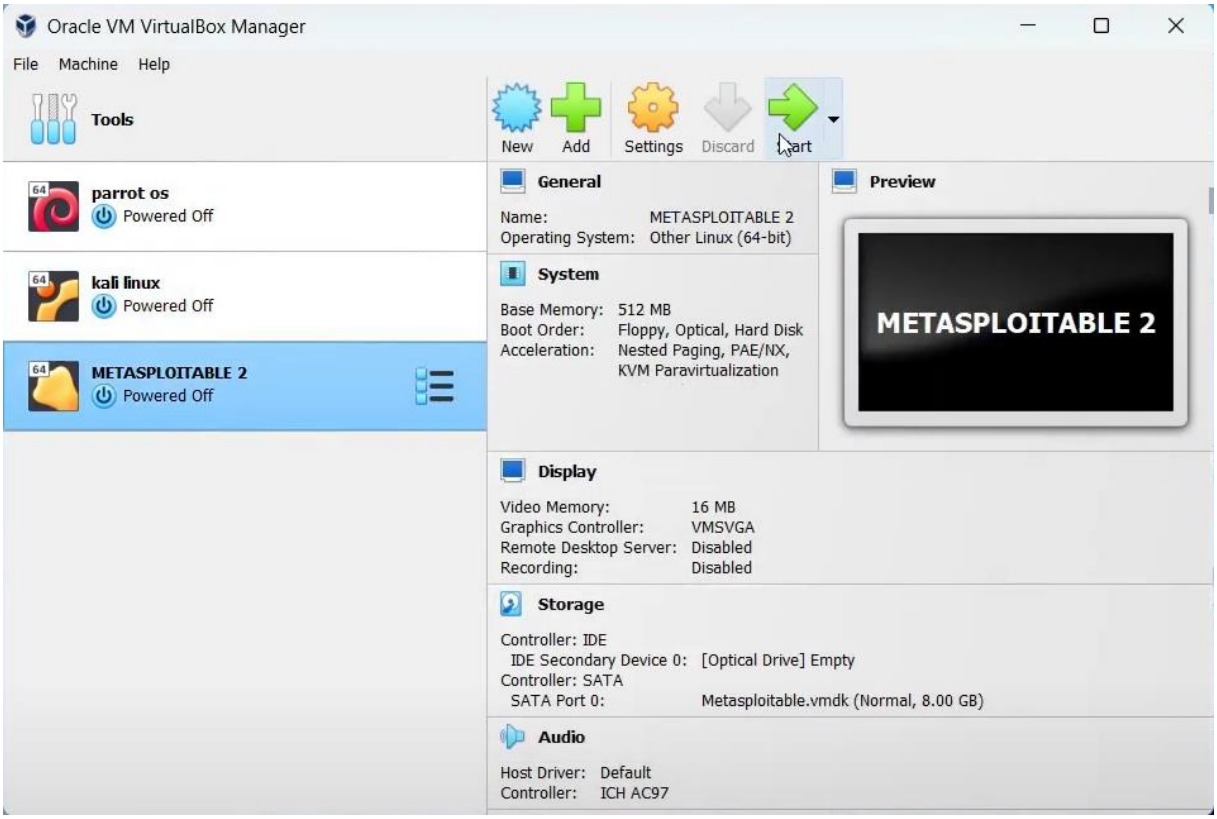
Step 6: Connect Metasploitable and Kali-Linux to hacking_lab





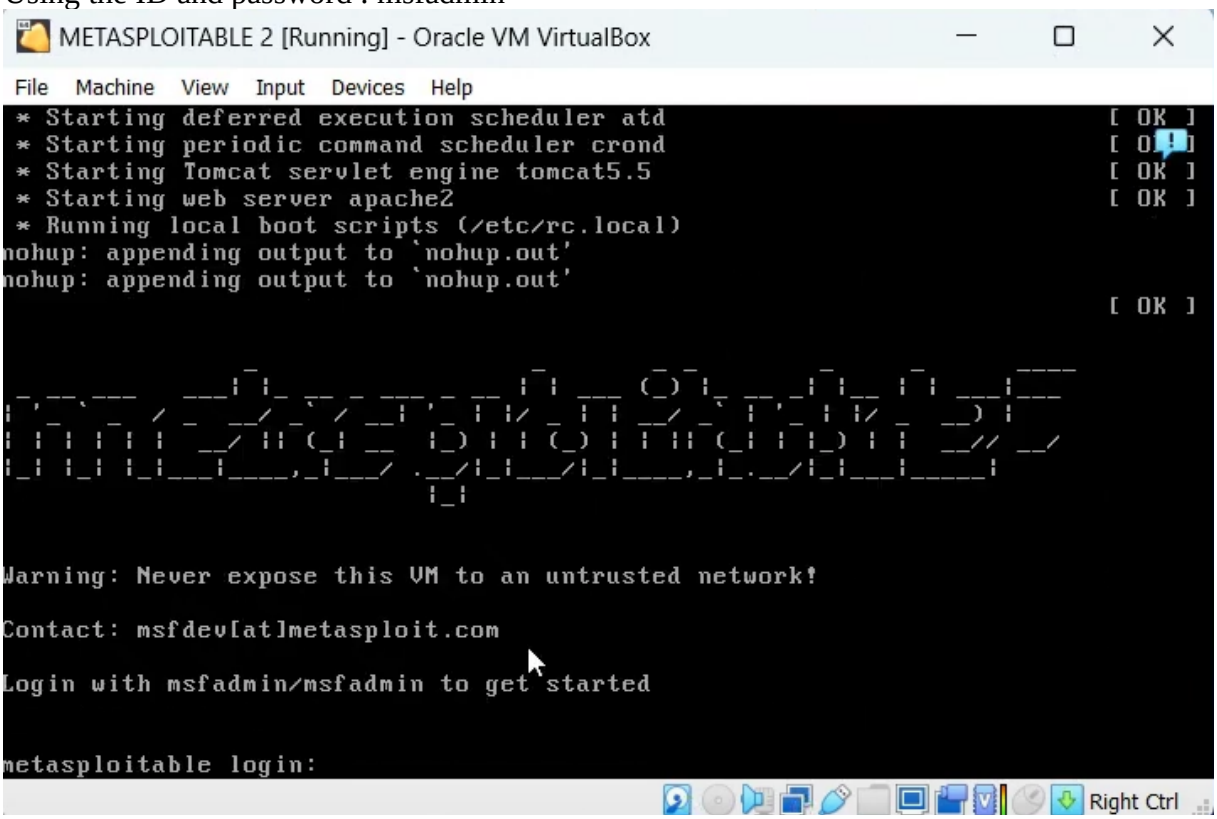


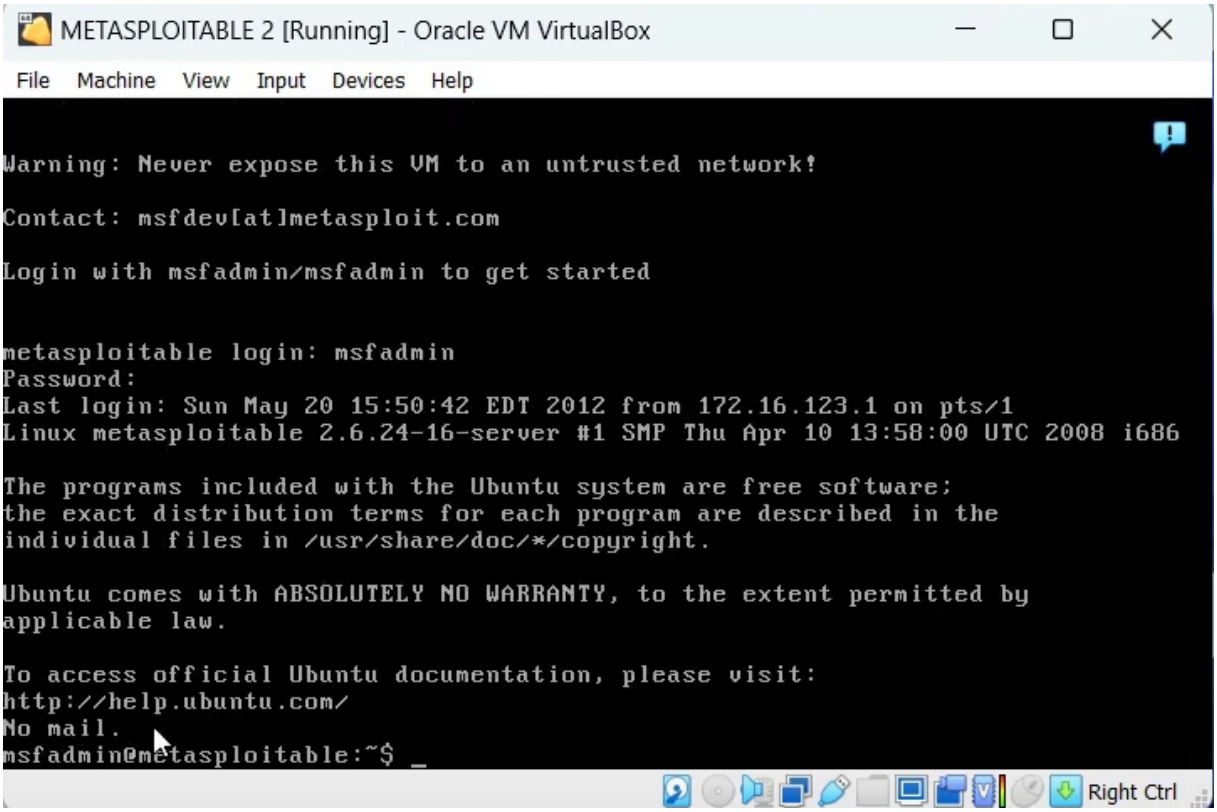
Step 7: Start the Virtual Machine



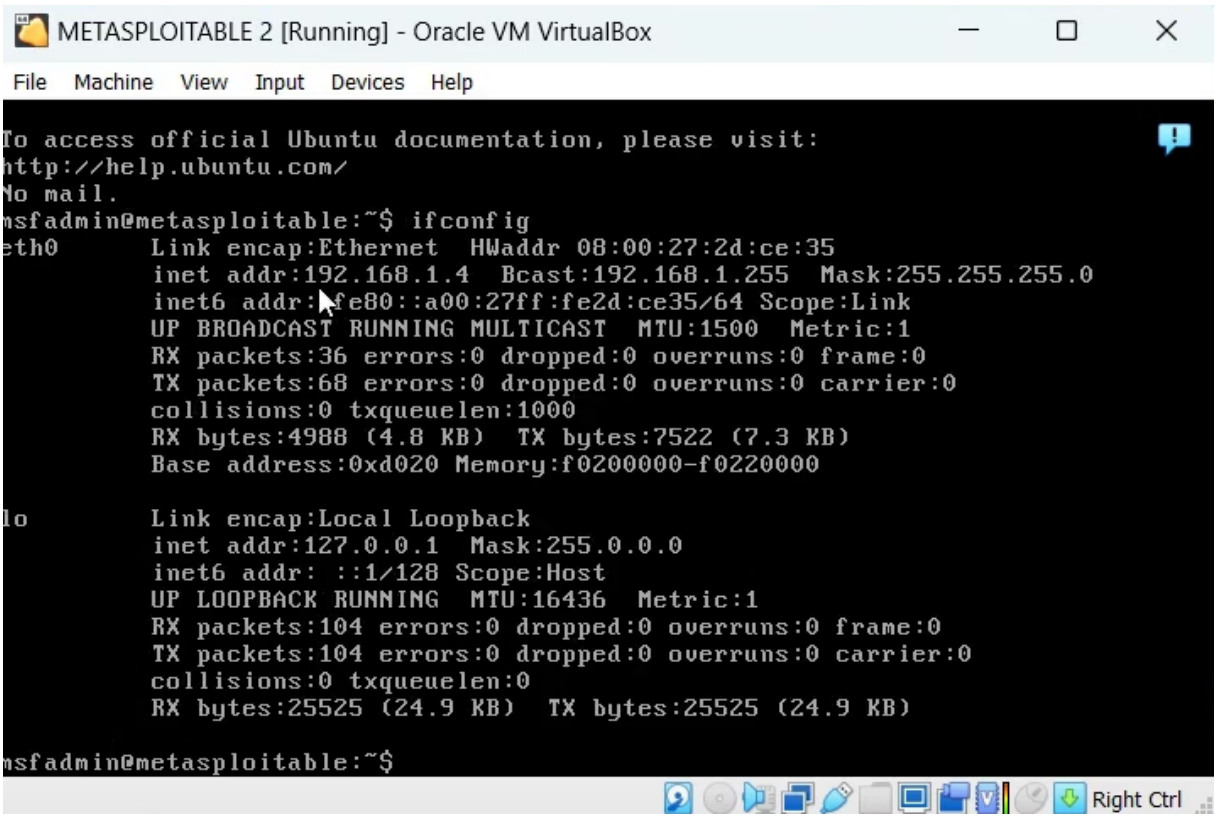
Step 8: Log In to Metasploitable 2

Using the ID and password : msfadmin





Check if everything is running properly using ifconfig command



Outcomes:
CO1 : Realize that premise of vulnerability analysis and penetration testing(VAPT)

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this experiment, I learned how to set up and configure Metasploitable 2 as a vulnerable system within a secure virtual environment using Oracle VirtualBox. This process helped me understand the importance of creating isolated lab setups for penetration testing and how to use pre-configured virtual machines to simulate real-world vulnerabilities for ethical hacking and learning purposes.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
https://www.youtube.com/watch?v=l8v65ePR44k
https://www.kali.org/docs/installation/hard-disk-install/
https://www.youtube.com/watch?v=MPkni85O9JA&t=866s