Sapience Edu Connect Pvt Ltd

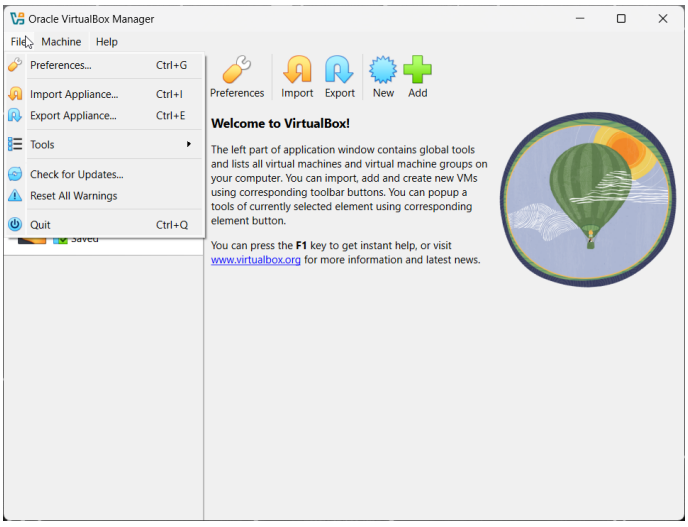
NAME: DEVALLA JWALA NARSIMHA
DOMAIN: CYBER SECURITY

Week 1: Introduction to Cybersecurity and Virtualization

Task 1

Step1: Set Up Virtualization Software

1. **Choose a Platform**: Decide on a virtualization tool (e.g., VMware Workstation, VirtualBox, Hyper-V).
2. **Download Installer**: Go to the official website and download the installer.
3. **Run Installer**: Open the downloaded file and start the installation process.
4. **Follow Prompts**: Accept the license agreement and choose the installation directory.
5. **Initial Configuration**: Open the software and set up basic settings like network configuration.
6. **Create Test VM**: Make a new virtual machine and install an operating system to test the setup.
7. **Install Tools**: Add guest additions or tools for better performance and integration.
8. **Update Software**: Check for and install any available updates or patches.



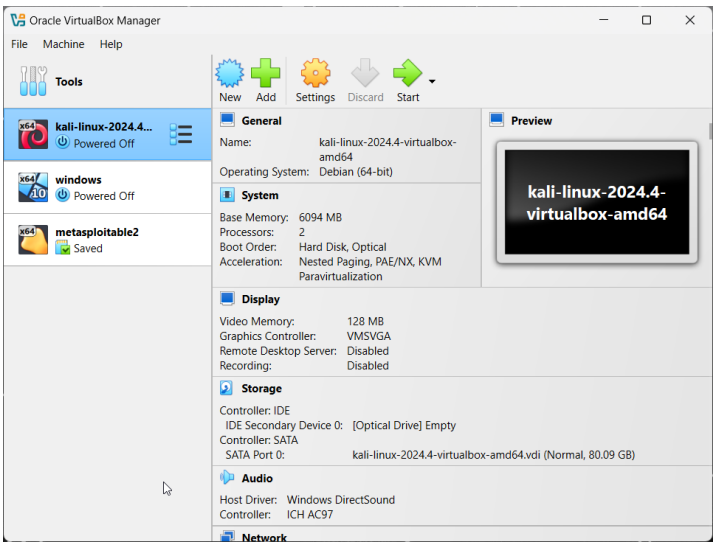
Step2: Download Kali Linux and Metasploitable

Download Kali Linux:

1. **Visit the Official Website**: Go to the Kali Linux Downloads page.
2. **Choose the Version**: Select the appropriate version for your needs (e.g., 64-bit, 32-bit, ARM).
3. **Download the ISO**: Click on the download link to get the ISO image of Kali Linux.
4. **Verify the Download**: Optionally, verify the integrity of the downloaded file using the provided checksums.

Download Metasploitable:

1. **Visit the Official Repository**: Go to the Metasploitable Downloads page.
2. **Download the Image**: Click on the download link to get the Metasploitable image.
3. **Extract the File**: If the file is compressed, extract it to get the virtual machine image.



Step3: Create a Virtual Machine for Kali Linux

Open Virtualization Software

1. Launch your virtualization software (VMware, VirtualBox, Hyper-V).
2. Create a new virtual machine.

Allocate Resources

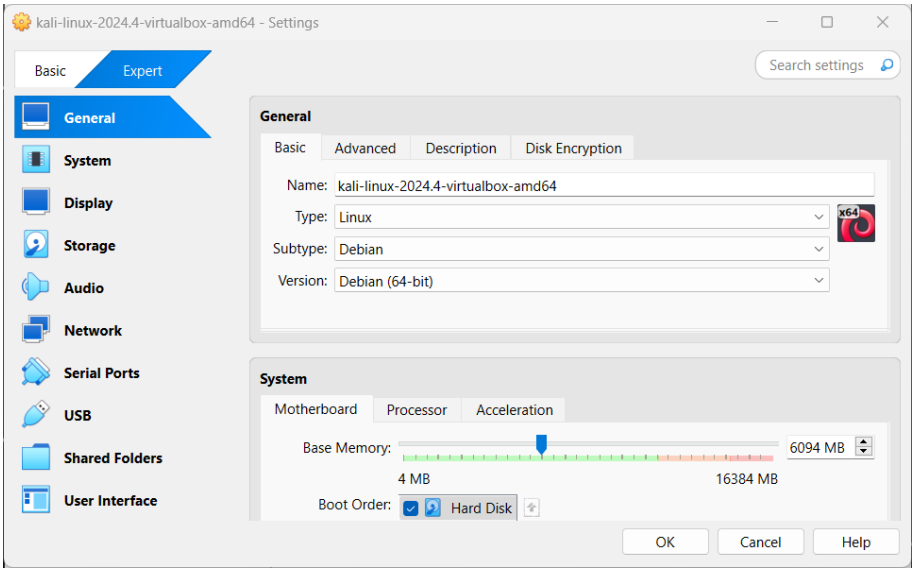
1. Name and Location: Name your VM (Kali Linux VM).
2. Guest OS: Select Linux > Debian.
3. RAM: Allocate at least 4 GB.
4. Disk Space: Allocate at least 50 GB.

Attach Kali Linux ISO

1. Configure VM: Go to VM settings.
2. Optical Drive: Attach the Kali Linux ISO to the virtual CD/DVD drive.

Install Kali Linux

1. Start VM: Boot from the Kali Linux ISO.
2. Follow Installer: Complete the installation via the graphical or text-based installer.



Step4: Create a Virtual Machine for Metasploitable

Open Virtualization Software

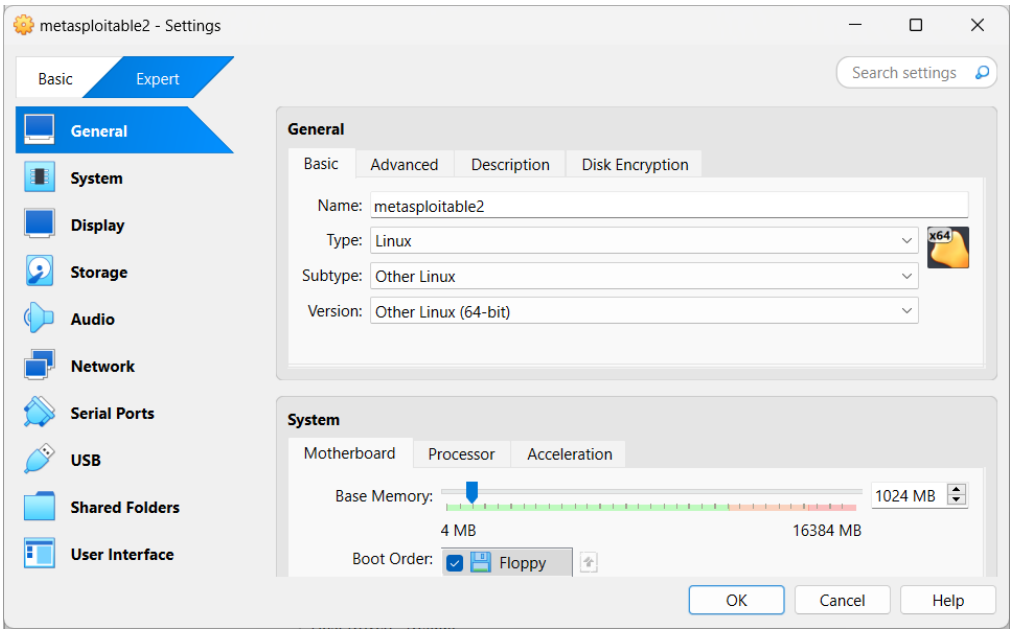
1. Launch your virtualization software (e.g., VMware, VirtualBox, Hyper-V).
2. Create a new virtual machine.

Allocate Resources

1. **Name and Location**: Name your VM (e.g., "Metasploitable VM").
2. **Guest OS**: Select **Linux** > **Ubuntu**.
3. **RAM**: Allocate at least 512 MB.
4. **Disk Space**: Allocate at least 8 GB.

Attach Metasploitable ISO

1. **Configure VM**: Go to VM settings.
2. **Optical Drive**: Attach the Metasploitable ISO to the virtual CD/DVD drive.



Step5: Configure Networking

Bridged Network Adapter

1: Access VM Network Settings

1. **Open Virtualization Software**: Launch your virtualization software
2. **Select VM**: Choose the virtual machine you want to configure (**Step 2: Configure Network Adapter**
1. **Go to Network Settings**:
   - In VirtualBox: Go to **Settings** > **Network**.
2. **Set Adapter Type to Bridged**:
   - In VirtualBox: Select **Bridged Adapter** and choose the

2: Repeat for kali linux

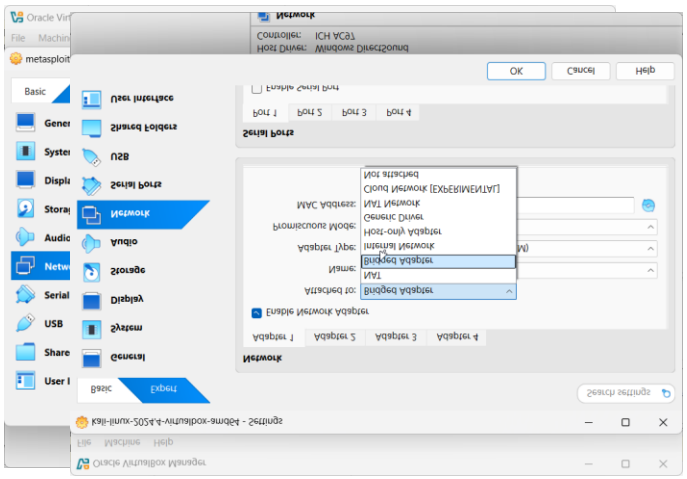
1. **Repeat Steps 1 and 2** for the other virtual machine .

1: Access VM Network Settings

1. **Open Virtualization Software**: Launch your virtualization software
2. **Select VM**: Choose the virtual machine you want to configure

Configure Network Adapter

1. **Go to Network Settings**:
   - In VirtualBox: Go to **Settings** > **Network**.
2. **Set Adapter Type to Bridged**:
   - In VirtualBox: Select **Bridged Adapter** and choose the appropriate network interface from the dropdown.



Step6: Update and Configure Kali Linux:

Step 1: Open Kali Linux

1. **Boot into Kali Linux**: Start your Kali Linux machine

Step 2: Update the System

1. **Open a Terminal**: You can do this by pressing **Ctrl + Alt + T** or by searching for "Terminal" in the application menu.
2. **Update the Package List**: Run the following command to update the package list:

sudo apt update

This command fetches the latest information on the newest versions of packages and their dependencies.

3. **Upgrade Installed Packages**: Run the following command to upgrade all installed packages to their latest versions:

sudo apt upgrade -y

This command installs the newest versions of all packages currently installed on the system.

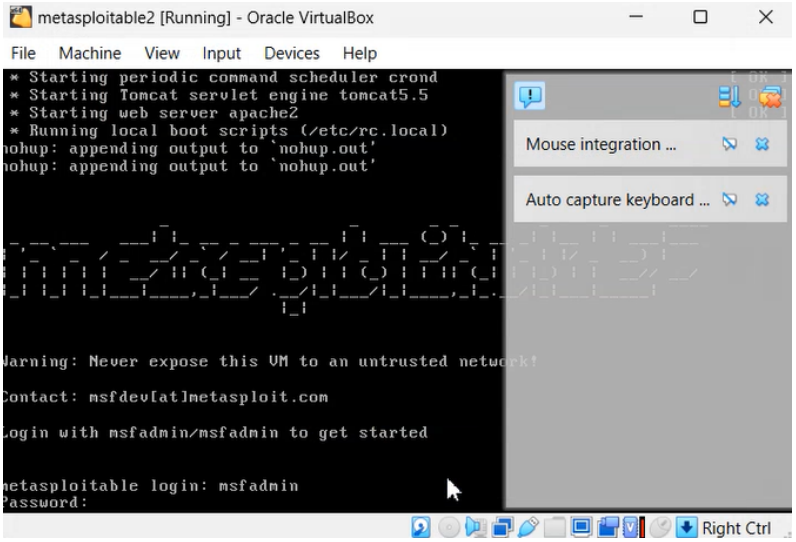
4. **Dist-Upgrade**: Run the following command to handle changing dependencies with new versions of packages:

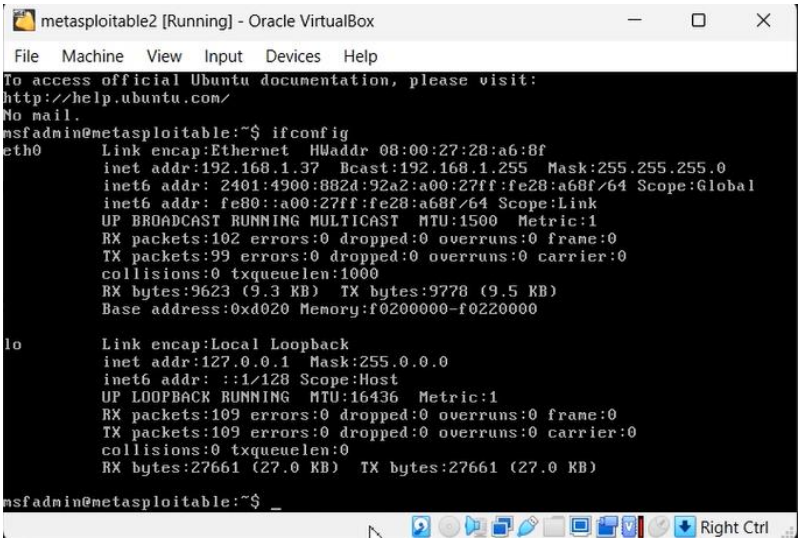
sudo apt dist-upgrade -y

This command performs the function of **upgrade** but also intelligently handles changing dependencies with new versions of packages.

Step7: Identify Metasploitable's IP Address

1. **Start Metasploitable**: Boot up your Metasploitable virtual machine using VirtualBox, VMware, or any other virtualization software.
2. **Log In**: Use the default credentials to log in. The default username and password are typically **msfadmin** for both.
3. **Find the IP Address**:
    - Open a terminal in Metasploitable.
    - Run the following command to display network interfaces and their IP addresses:
      - ifconfig
    - Look for the **eth0** interface





Step8: Perform Initial Reconnaissance

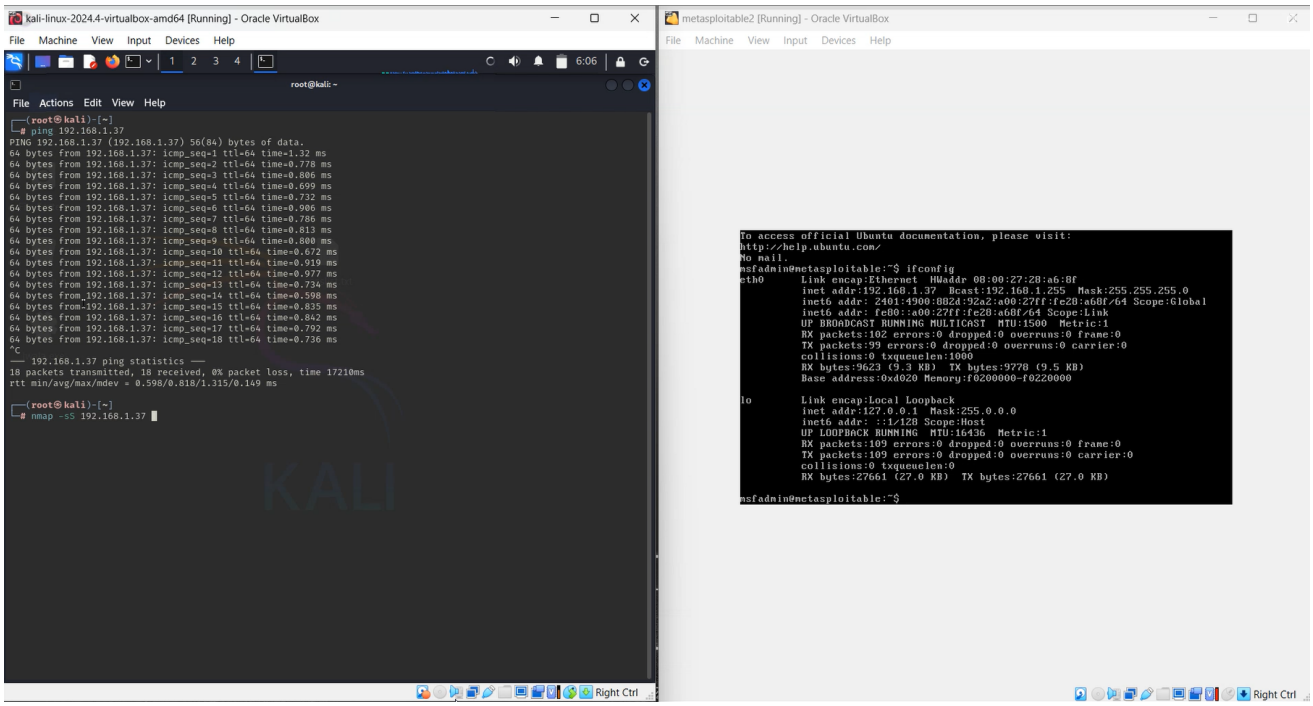
1. **Open Kali Linux:**
   - Start your Kali Linux virtual machine or open a terminal if you are already running Kali Linux**.**
2. **Use Nmap to Scan Metasploitable:**
   - Open a terminal in Kali Linux.
   - Use the nmap command to scan the Metasploitable machine. Replace with the IP address **.**

nmap -sS 192.168.1.37

- -sS performs a SYN scan to identify open ports.
- -sV attempts to determine the version of the services running on the open ports**.**

Example Commands and Output

1. Finding the IP Address in Metasploitable:



nmap -sS 192.168.1.37

```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.1.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 06:06 EDT
Nmap scan report for 192.168.1.37
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:28:A6:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

nmap -sV 192.168.1.37

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.1.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 06:06 EDT
Nmap scan report for 192.168.1.37
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:28:A6:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.88 seconds
```

Step8: Perform Initial Reconnaissance

Step 1: Take Snapshots

1. **Open Virtualization Software:**
   - Open VirtualBox
2. **Take a Snapshot:**
   - Select the VM, go to the snapshot menu, and take a snapshot. Name it for easy identification.

Step 2: Clean Up Unnecessary Files

1. **Delete Temporary Files:**
   - Remove files in /tmp and /var/tmp.

rm /tmp/* /var/tmp/*

2. **Clean Log Files:**
   - Delete old log files in /var/log.

sudo rm /var/log/old-log-file.log

3. **Remove Unused Software:**
   - Uninstall unnecessary packages.

sudo apt-get remove --purge package-name

4. **Clean Package Cache:**
   - Free up space by cleaning the package cache.

sudo apt-get clean

Step 3: Organize Your Lab

1. **Create Directories:**
   - Make directories for reports, scripts, and tools.

mkdir -p ~/lab/{reports,scripts,tools}

2. **Move Files:**
   - Organize files into the new directories.

mv /path/to/file ~/lab/reports/

THANK YOU!