Setting Up Metasploitable VM on Kali Linux
Author : Zawad Hossain
Dated : 19th June 2025
My Host Device : HP Elitebook Folio 9470m

Introduction:
Metasploitable is a virtual machine (VM) used for testing and penetration-testing purposes. It has been intentionally designed to be vulnerable, making it an ideal tool for security professionals working in controlled environments like VMs. This report outlines the step-by-step process of setting up **Metasploitable on Kali Linux using VirtualBox software.**

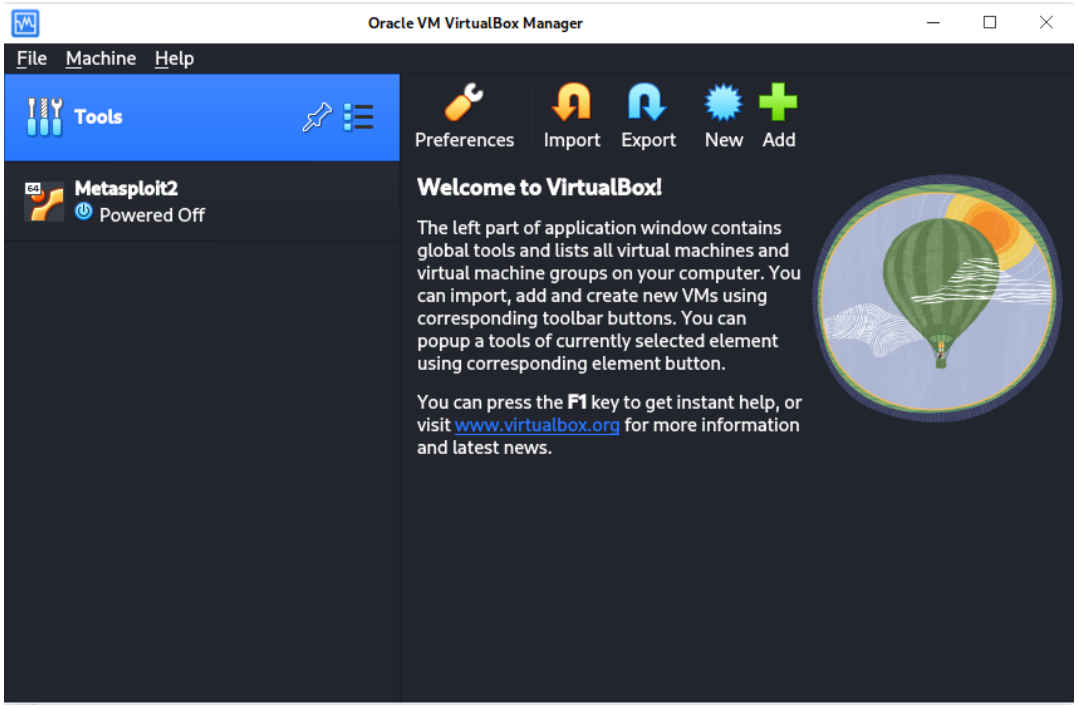
If there is an efficient/updated way of performing these or any mistakes in the document, please let me know @ hossazaw@sheridancollege.ca

1. Checking if Virtio is Enabled:
Before installing any virtualization tools, it's essential to verify whether your host laptop has virtio (VTx) enabled in the BIOS settings for optimal performance and resource utilization of VMs. Reboot after making changes to these configurations.

2. Installing VirtualBox on Kali Linux:
To set up **Metasploitable**, we'll need a virtual machine environment provided by **VirtualBox** software installed on our host system (Kali). Follow the steps below for installation and configuration of VirtualBox in your Kali laptop:
- Open terminal using Ctrl + Alt + T.
- Update package lists with
    sudo apt update
- Install VirtualBox packages along with its extension packs to support hardware features (e.g., USB, video cards)
    sudo apt install virtualbox virtualbox-ext-pack
- Add the user to the 'vboxusers' group for proper access rights and privileges in VirtualBox settings.
    sudo usermod -aG vboxusers $USER
- Reboot your Kali machine so that changes take effect
    sudo reboot

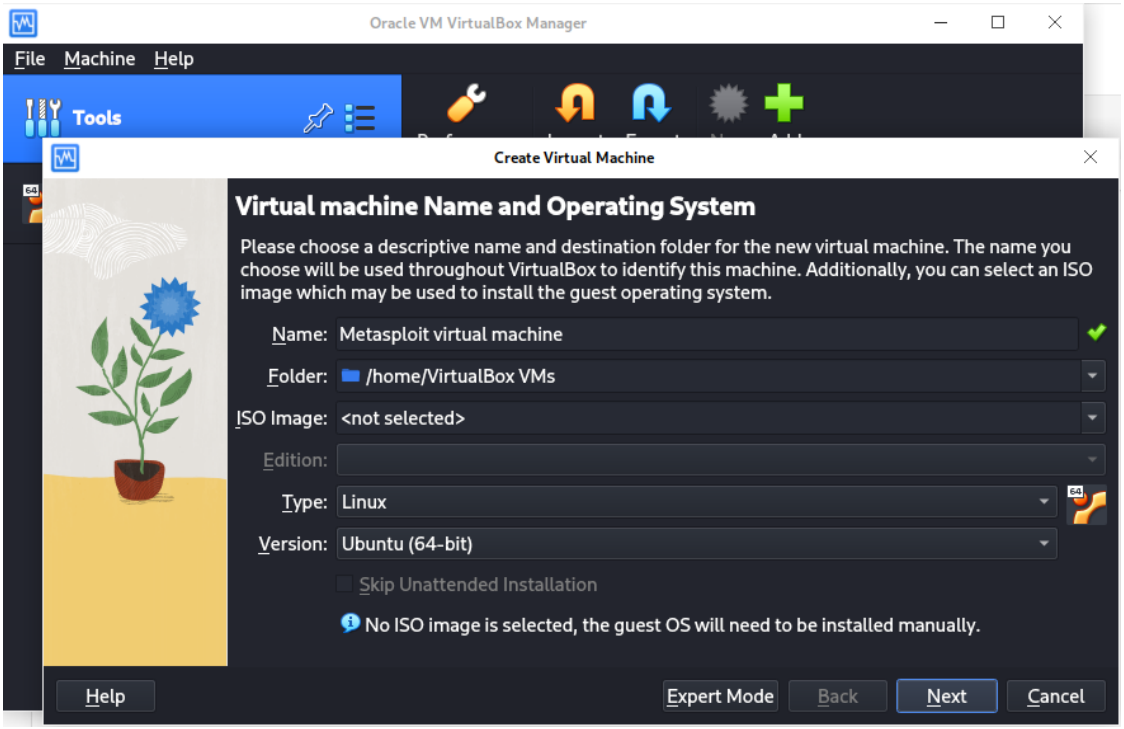
3. Downloading Metasploitable Image:
Metasploitable is available as a zip file on the official website https://download.vulnhub.com/metasploitable/metasploitable-linux-2.0.0.zip or SourceForge (http://sourceforge.net/projects/metasploit/.
Download and extract this archive to a designated folder on your Kali machine for easy access during the setup process.

4. Creating Metasploitable VM in VirtualBox:

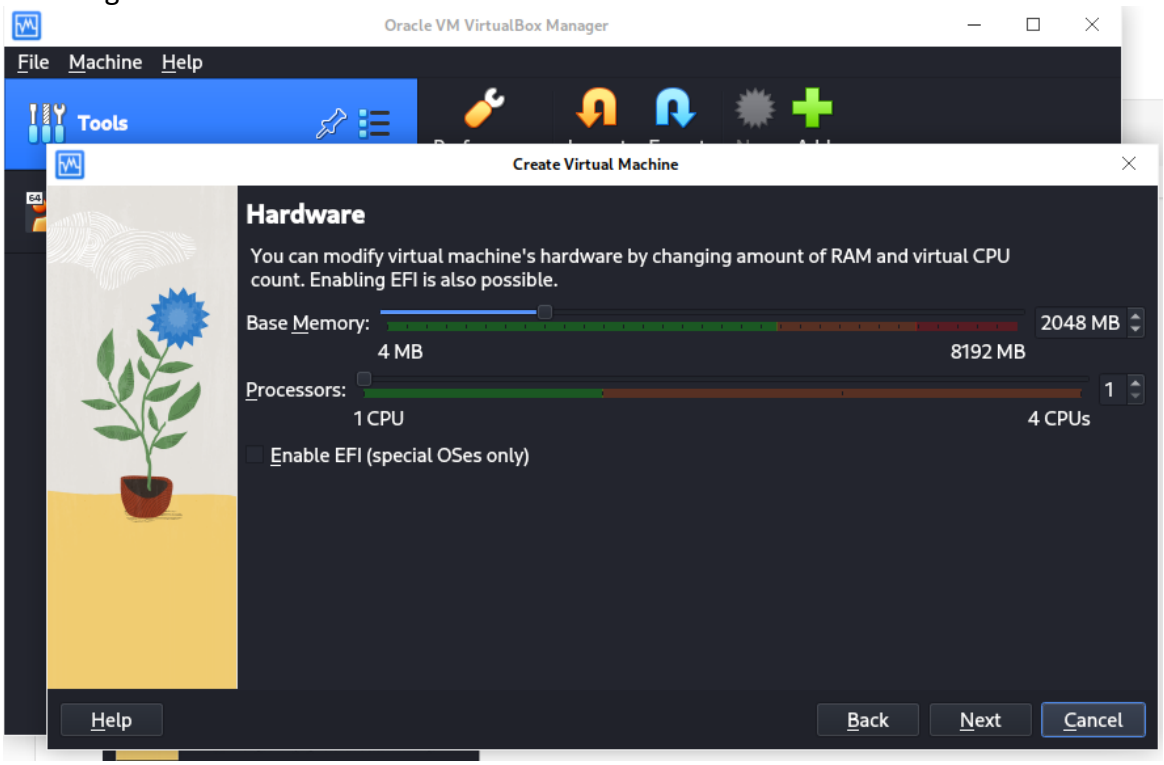


Launching VirtualBox application, create a new virtual machine with Linux as its operating system type (Ubuntu) by following these steps:

- Select "New" from the menu bar

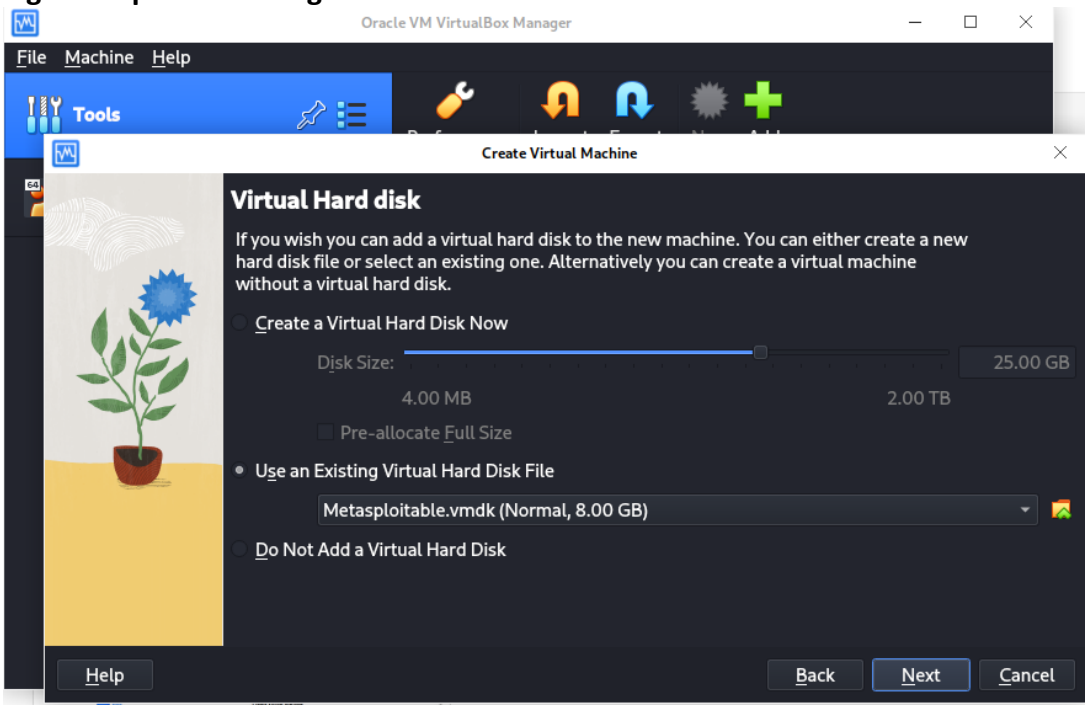


- Name your newly created VM 'Metasploitable' or it can be anything to distinguish from other VMs.
- Leave **ISO** tab empty
- Select the **Type** as ***Linux*** and
- Finally **Version** as ***Ubuntu 64bit***
- Click Next to go to the next screen to allocate resources



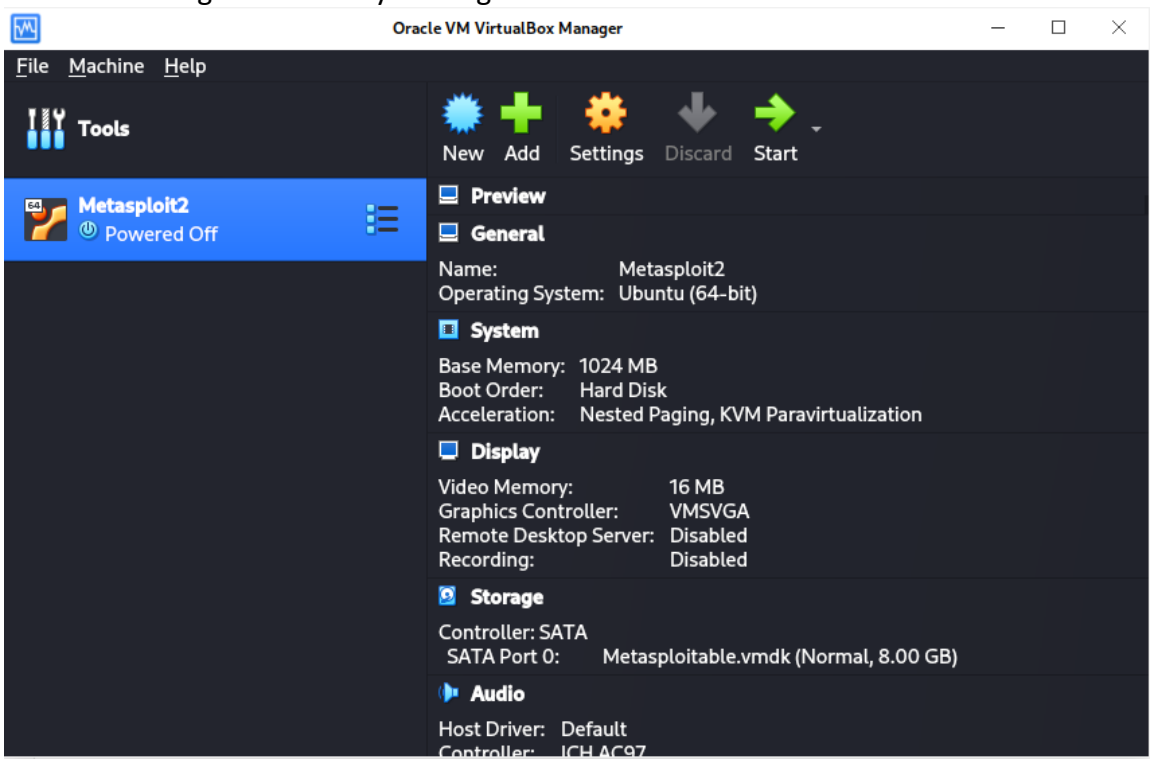
- Set memory allocation to at least 1GB. (Increase this value if you have more resources available, but be mindful of host machine resource usage)
- Allocate one CPU core for optimal performance (you can increase it as per availability)

5. Mounting Metasploitable Image:



In this step we need to locate the extracted 'Metasploitable' folder (extracted from step #3) on Kali machine and select the .vmdk image file for mounting as follows:
- Choose "Use an existing virtual hard disk file" option.
- Use the folder icon to locate the extracted 'Metasploitable' folder and select the **.vmdk image file**.
- Click **Next** once file is located and selected to go to the **Summary** page.

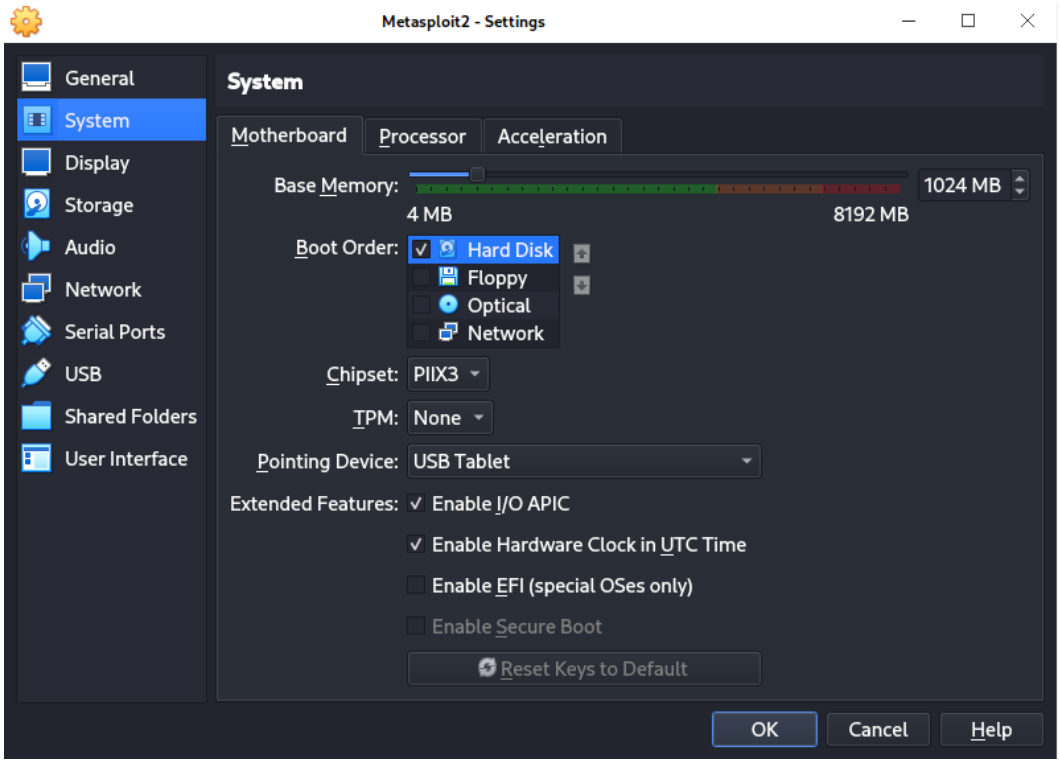
- Proceed with creating a new VM by clicking **Finish**.



- After the step, the virtual machine will show up on the dashboard with name that you had set earlier.

6. Changing the Boot Order of the VM and disable EFI UEFI:

By default the Boot Order is set to Floppy Disk followed by Optical and Hard Disk. We need to change the priority for Hard Disk to be at the top.



- Select the Virtual Machine, click on **Settings > System > Motherboard**

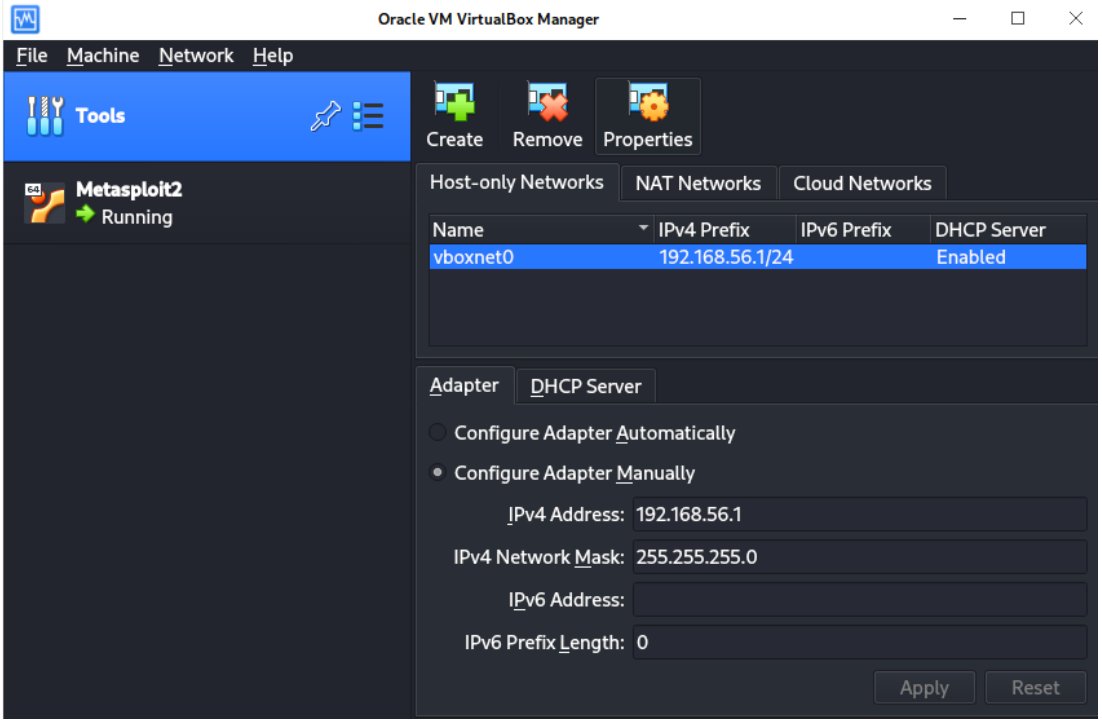
  Under **Boot Order** Either change the order or remove(uncheck) both **Floppy Disk** and **Optical Drive** to keep **Hard Disk** at the top of the list

As ***Metasploitable 2*** is an older version it runs on ***BIOS*** and does not support ***UEFI or EFI*** . So if it is enabled/checked please uncheck them and launch the vm

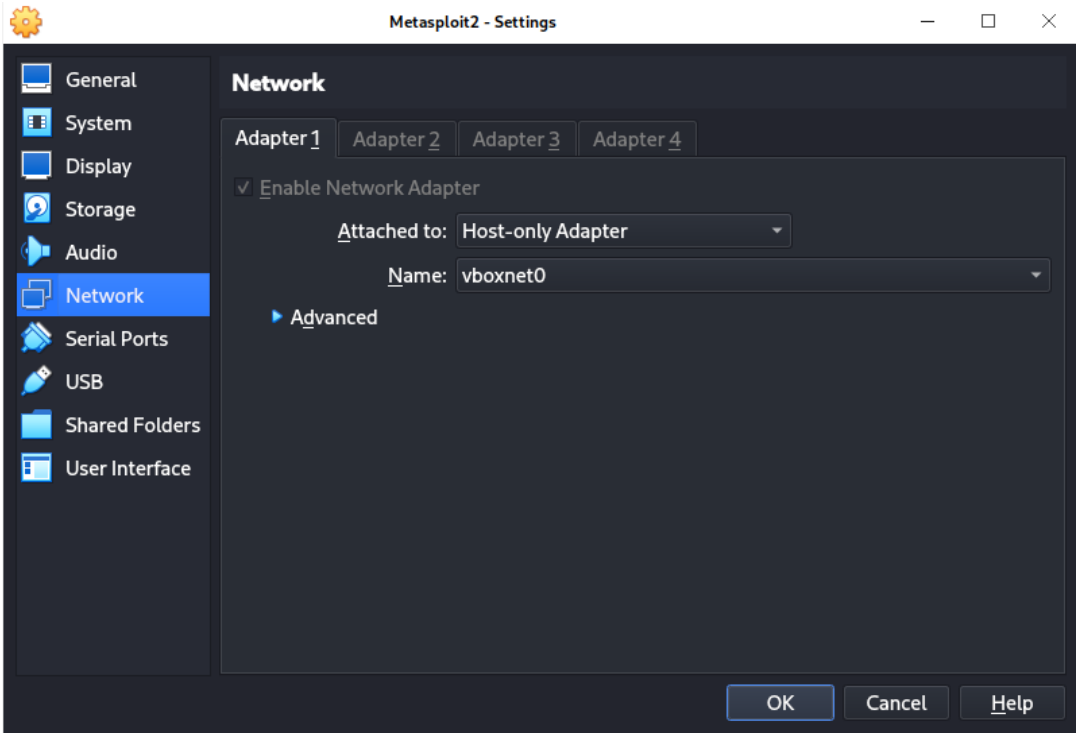
- Under the **Extended Features** confirm **Enable EFI** is unchecked

7. Configuring Network Settings:

Before starting your Metasploitable VM, ensure that it has network connectivity to communicate with host Kali machine for testing purposes. Follow these steps under the settings of a newly created virtual adapter in VirtualBox interface:



- On the Virtual Box dashboard, **File > Tools > Network Manager** or press **Ctrl + H** , this will open the network configuration tab
- An adapter named "vboxnet0" should be listed. If not already present, then click **Create** to add it.



- To confirm this you can check on the Metasploit vm settings by going to **Settings > Network**
  Change the **"Attached To"** from **NAT** to **Host-only Adapter**
  it should show the adapter ***vboxnet0***

Enabling Host only option for added security during testing purposes and adjust other network configurations accordingly (e.g., bridged or promiscuous mode).

8. Launching and Testing Connectivity:

After configuring your Metasploitable VM, start it using the Start button in VirtualBox interface. Upon login prompts with default credentials ('msfadmin' for both username/password), verify connectivity between host Kali machine and 'Metasploitable':

- Verify the IP address of your 'Metasploitable' VM using **ifconfig** command in its terminal session (e.g., "eth0"). Take note of this IP, as you'll need it to ping from host Kali machine later on.
- Open terminal on host Kali machine (Ctrl + Alt + T) and run `**ping <*IP address of Metasploitable VM*>**`.

If successful, you should receive a response from the target. This confirms that your network settings are correctly configured for testing purposes. *For security reasons did not add any screenshot on this step*

9. Scaling VirtualBox Window:

To improve readability while working with 'Metasploitable' in virtualized environment, hold down **Right Ctrl** and **press C** to scale up or down the window size as needed. This allows for better visualization of Metasploitable within VirtualBox interface.

In conclusion, this report has provided a detailed step-by-step guide to setting up Metasploitable in Kali Linux using VirtualBox software while ensuring optimal performance and network connectivity between host machine (Kali) and target VM ('Metasploitable'). Proper configuration of Virtio settings on the host system, correct installation of required packages for virtualization tools like VirtualBox, as well as appropriate adjustments to networking configurations are essential factors in achieving a successful setup.