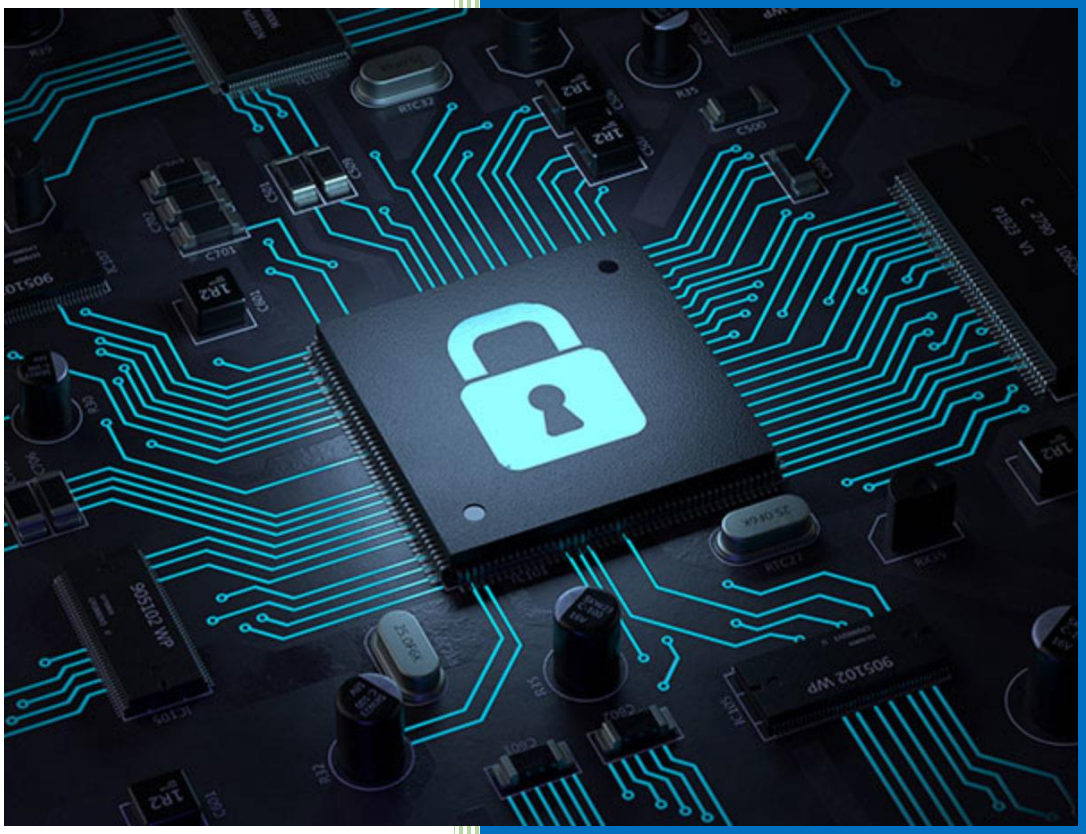
FAKULTI TEKNOLOGI
KEJURUTERAAN KELAUTAN
DAN INFORMATIK

2020/2021

CYBER SECURITY



Lab 1: Setting Up A Cyber Security Lab Basic of Linux Operating System

VERSION 1

`

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
30/03/2021		First Issue	Fakhrul Adli Mohd Zaki Dr Farizah Yunus

`

CONTENTS

`

INSTRUCTIONS

Manual makmal ini adalah untuk kegunaan pelajar-pelajar Fakulti Teknologi Kejuruteraan Kelautan dan Informatik (FTKKI), Universiti Malaysia Terengganu (UMT) sahaja. Tidak dibenarkan mencetak dan mengedar manual ini tanpa kebenaran rasmi daripada penulis.

Sila ikuti langkah demi langkah sebagaimana yang dinyatakan di dalam manual.

Arahan laporan makmal:

a) Pelajar perlu menyediakan laporan makmal untuk aktiviti makmal.
b) Kandungan laporan makmal mesti terdiri daripada beberapa tangkapan skrin untuk semua tetapan makmal keselamatan maya yang berjaya dengan beberapa penjelasan.
c) Jawab semua soalan refleksi untuk setiap sesi makmal.
d) Pelajar dapat memberikan senarai rujukan untuk rujukan tambahan.
e) Laporan makmal mesti dihantar dalam masa yang diberikan menggunakan pautan yang disediakan di platform eLearning.

This laboratory manual is for use by the students of the Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu (UMT) only. It is not permissible to print and distribute this manual without the official authorisation of the author.

Please follow step by step as described in the manual.

Lab report instructions:

a) Students need to prepare lab report for lab activities.
b) The contents of the lab report must consist of several screenshots for all successful setting of virtual security lab with some explanation.
c) Answer all the reflection questions for every lab sessions.
d) Student can provide the list of references for extra references.
e) *Lab report must be submitted within the time given using the provided link in the eLearning platform.*

`

TASK 1: DOWNLOADING REQUIRED SOFTWARE & IMAGES

OBJECTIVE

To download images that later will be used in setting up a virtual security lab.

TASK DESCRIPTION

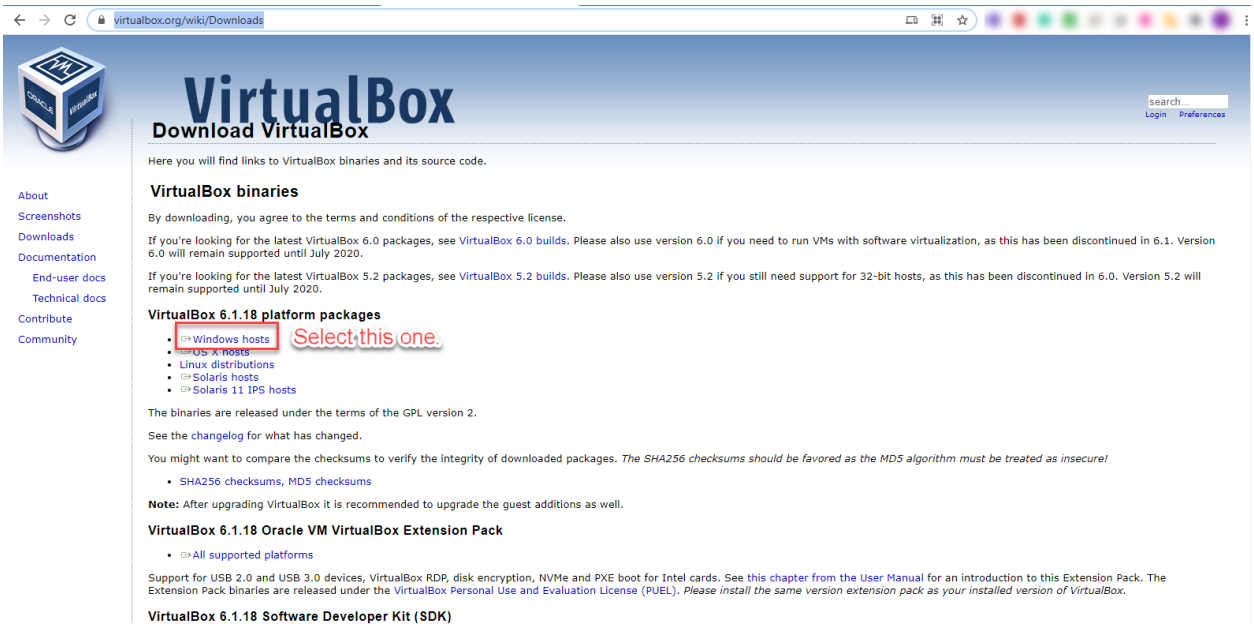
Student is required to download a Virtual Box software and images from different sources. Those images will be used to setup a virtual lab.

ESTIMATED TIME

60 Minutes

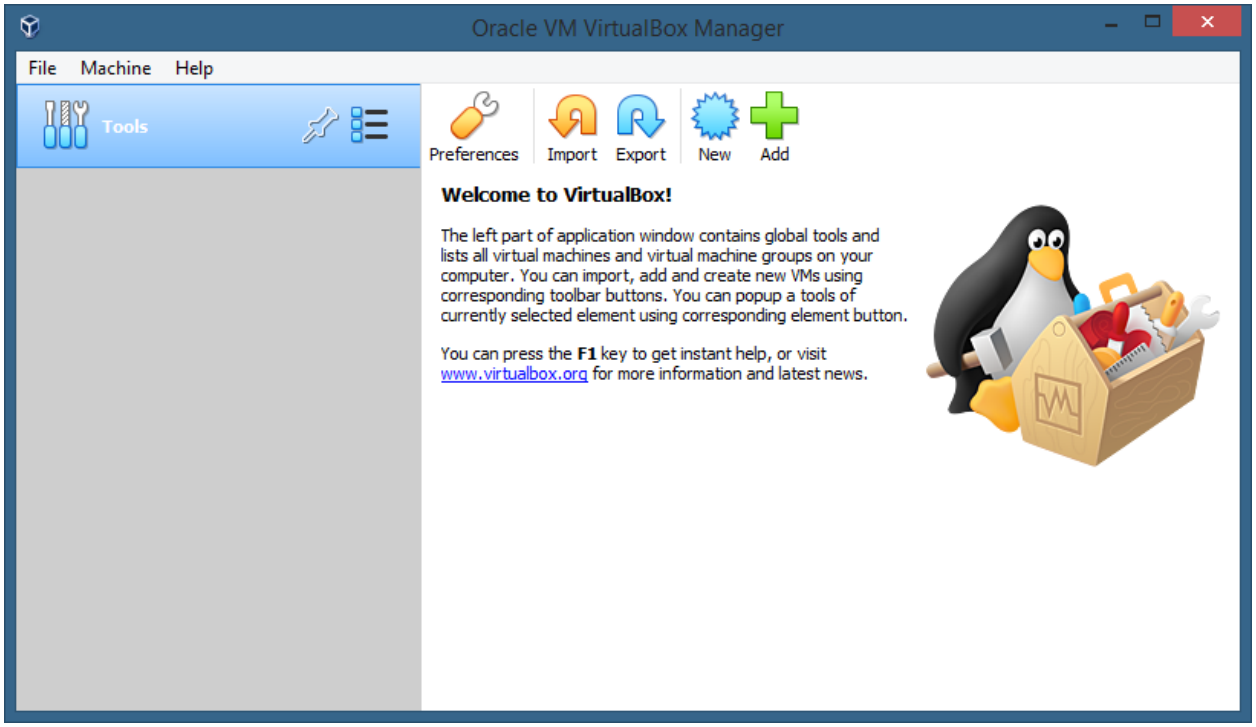
STEPS:

1. Download a Virtual Box software from https://www.virtualbox.org/wiki/Downloads

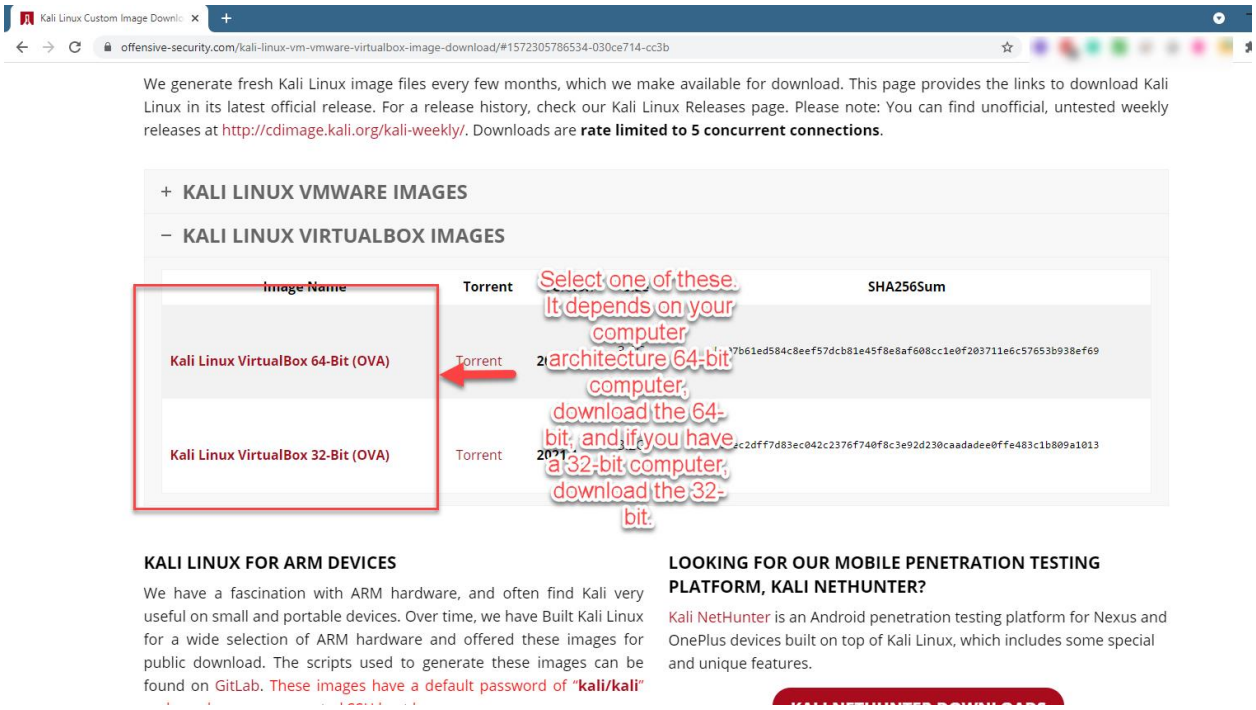


2. After the download finish, double click on the installer and follow the installation steps until the end.
3. Once finish, run the Virtual Box and you will see a screen like below:

`



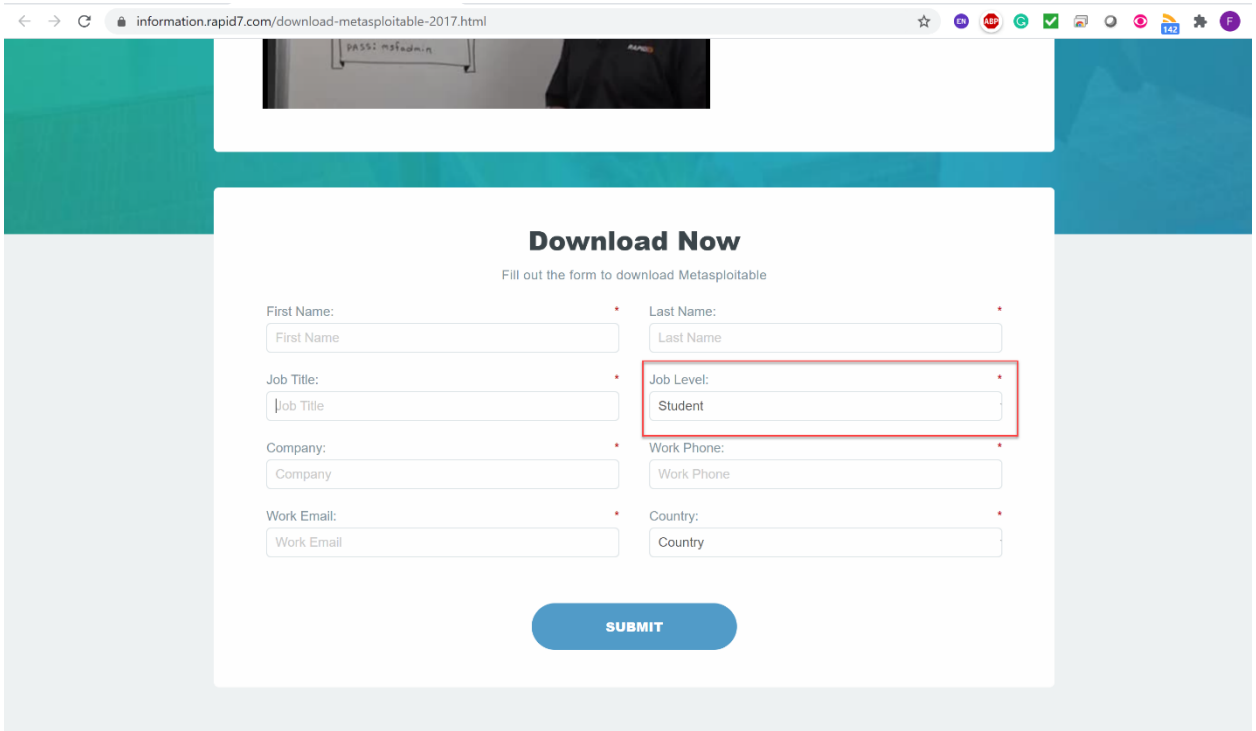
4. Next, we are going to download the Kali Linux image that will be ran on Virtual Box.
5. Kali Linux can be downloaded from https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786534-030ce714-cc3b. Scroll download until you see this screen:



6. It will take a while for the download to finish. Remember to take note the location that you save Kali Linux image in your computer. We will run the image using virtual box after this.

`

7. Next, we will download metasploitable image from the following links. This image will act as a victim for our virtual lab.
    - https://information.rapid7.com/metasploitable-download.html.
8. Before you can download the image, you have to fill in your personal details. Put "Student" as the Job Title and Job Level. Use you student email for the Work Email.



9. Next, you redirected to the download page, again remember the location of the downloaded file as we going to execute it later.
10. All the downloaded files will be used in the incoming tasks.

REFLECTION QUESTIONS

1. What is Virtual Box and what are their benefits?
2. What are the types of virtualization available?
3. Give four reasons for using Virtual Box.

`

TASK 2: SETTING AND RUNNING KALI LINUX FOR THE FIRST TIME

OBJECTIVE

To run and explore the features available in Kali Linux

TASK DESCRIPTION

Student need to run and test the Kali Linux image on the virtual box that had been downloaded earlier.

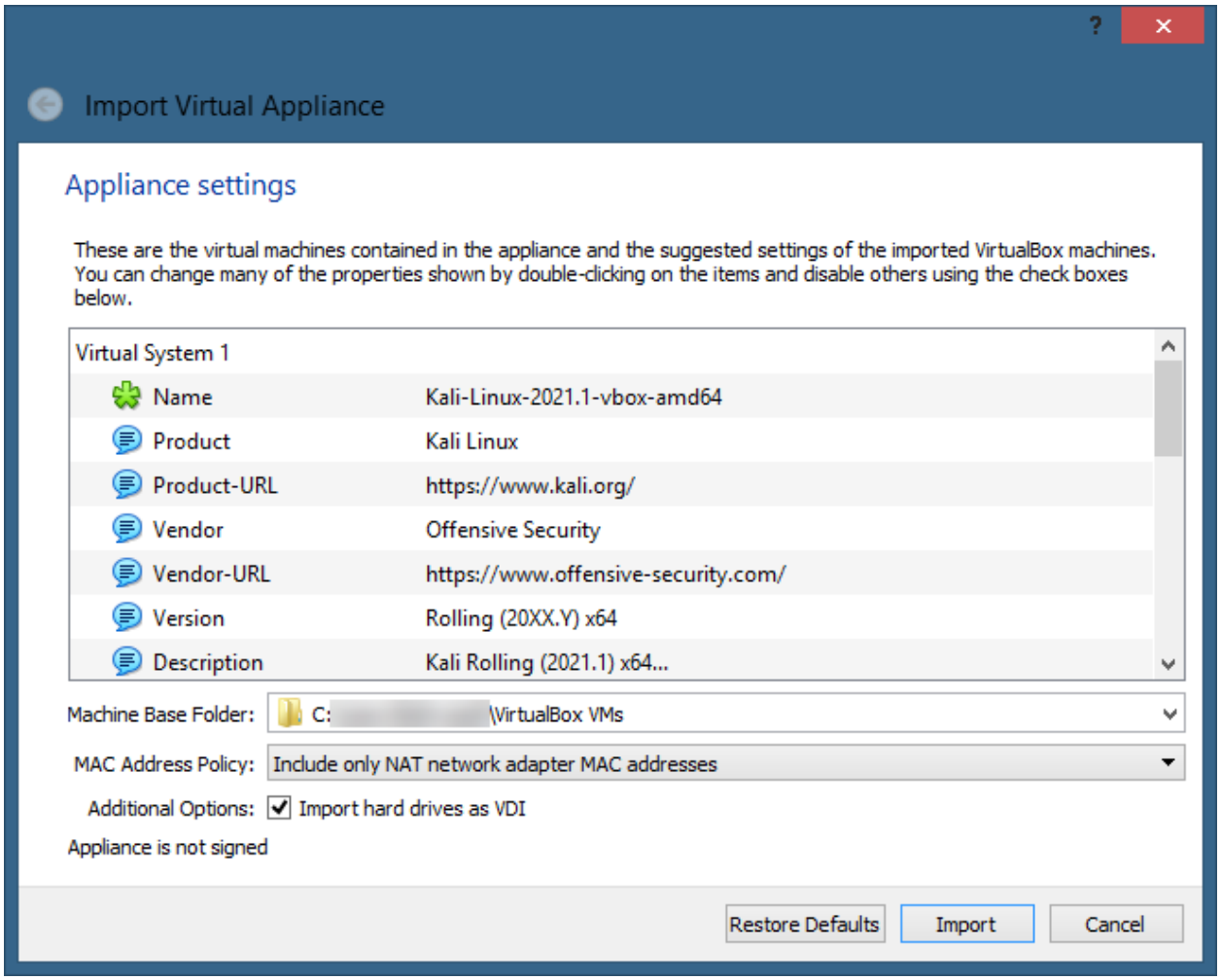
ESTIMATED TIME

60 Minutes

STEPS:

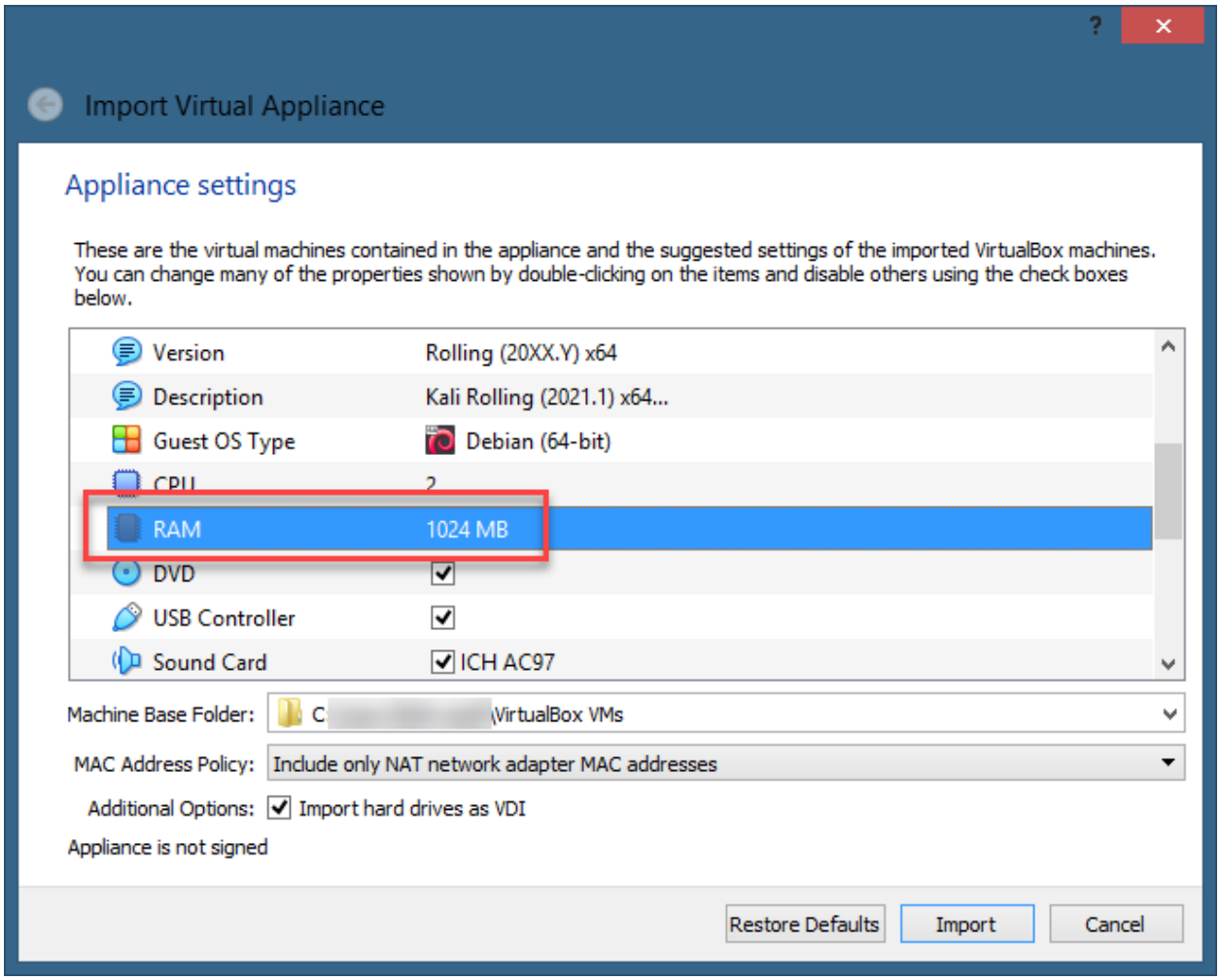
1. Go to the location where you save the Kali Linux image on your computer. Double click on it.
2. This screen will appear after you do so.

`



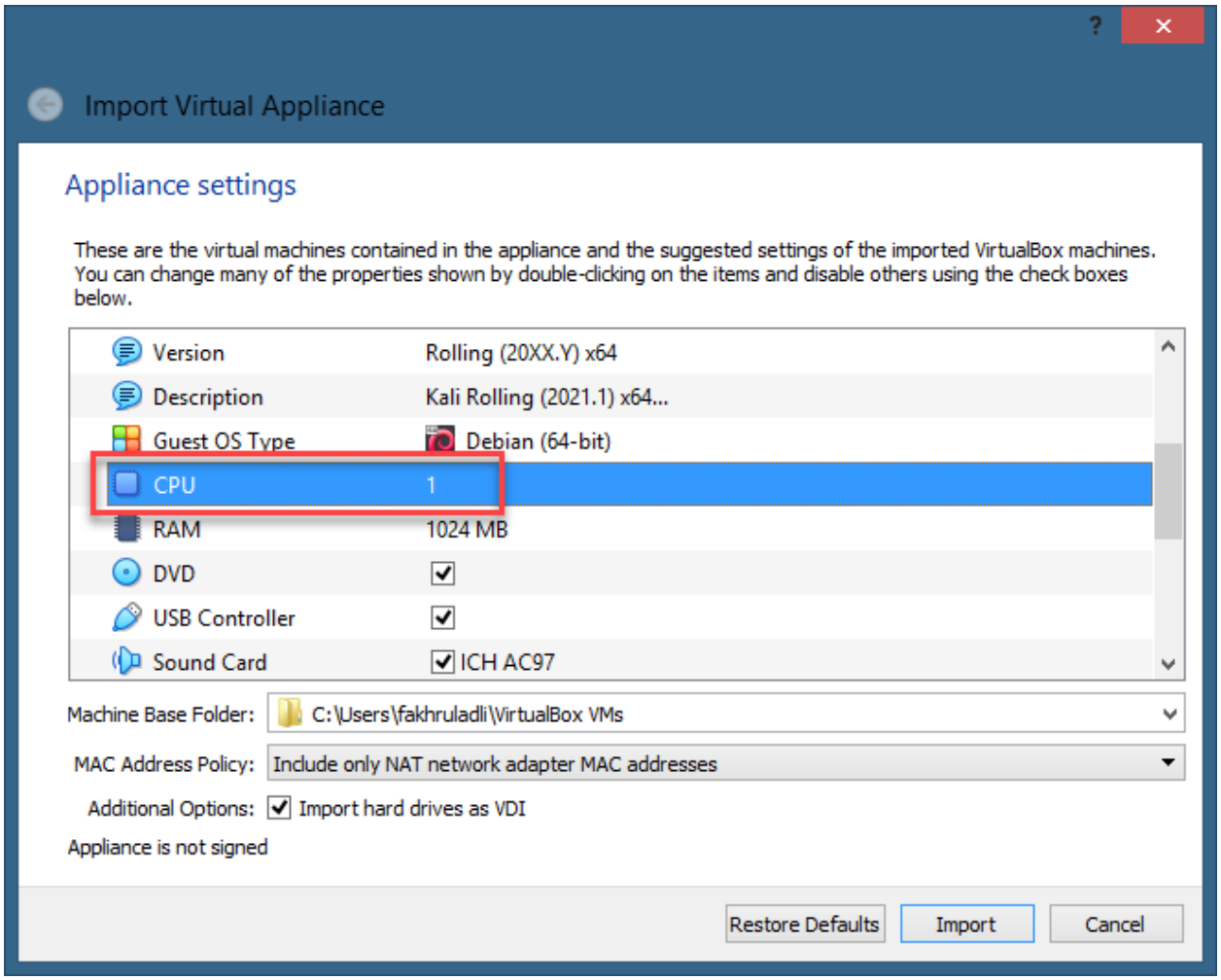
3. Next, we are going to specify the RAM size for Kali Linux. Scroll down the "Appliance settings" screen until you find the location for setting the RAM value.

`



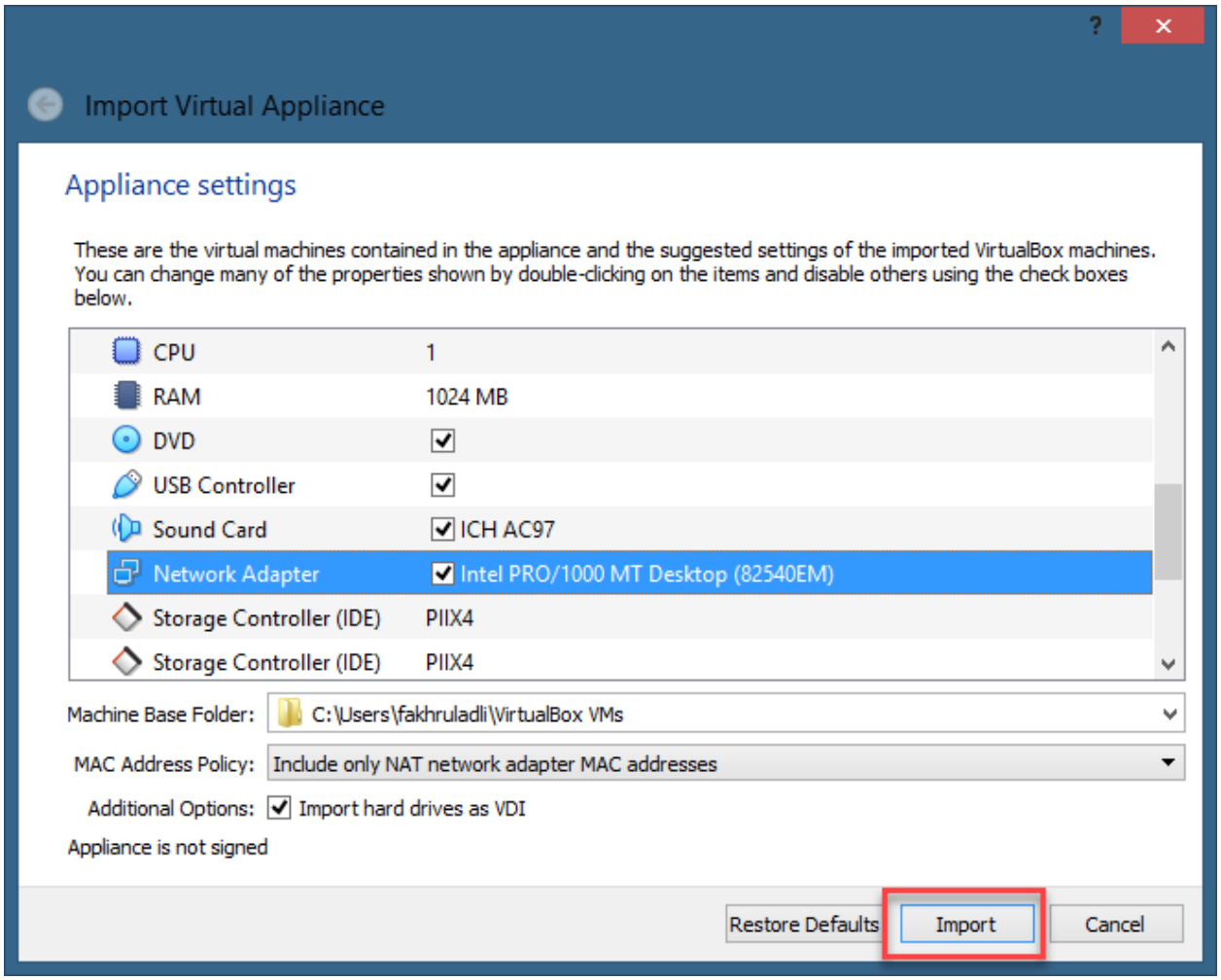
4. Adjust the RAM accordingly by double clicking the value. 1024MB is enough for running Kali Linux. However, if your computer has more than 4GB RAM, then you may set it to a higher value.
5. The second parameter that you may want to adjust is the CPU. 1 CPU is considered enough to run a Kali Linux. Again, if your computer is powerful enough, then you can change it to a higher number of CPU.

`



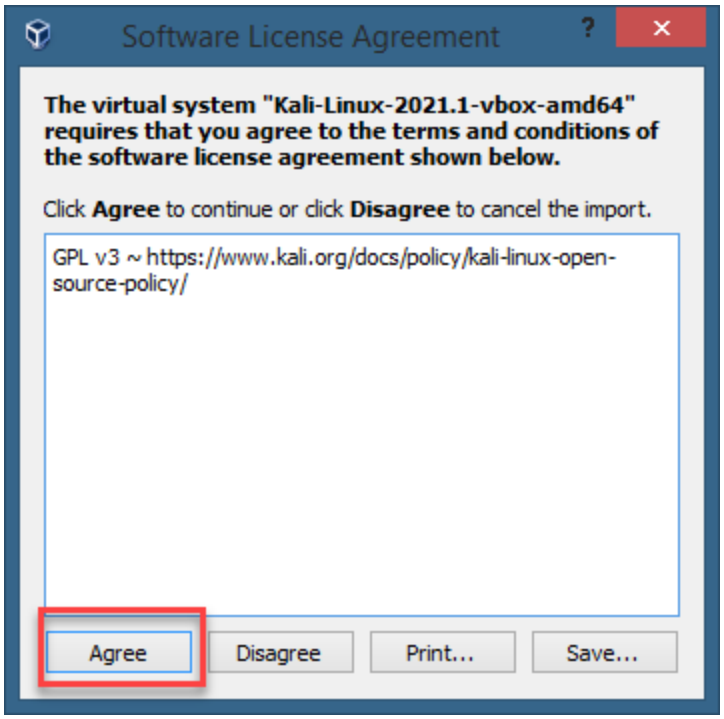
6. Finally, click **Import**.

`

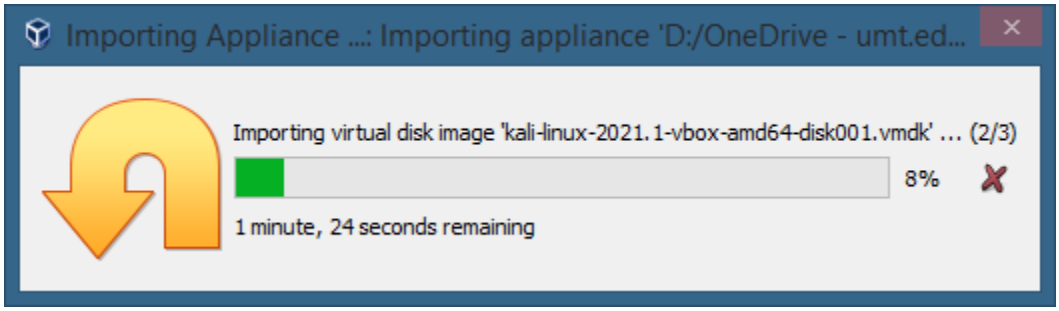


7. If you see a pop-up screen as below, just click **Agree**.

`

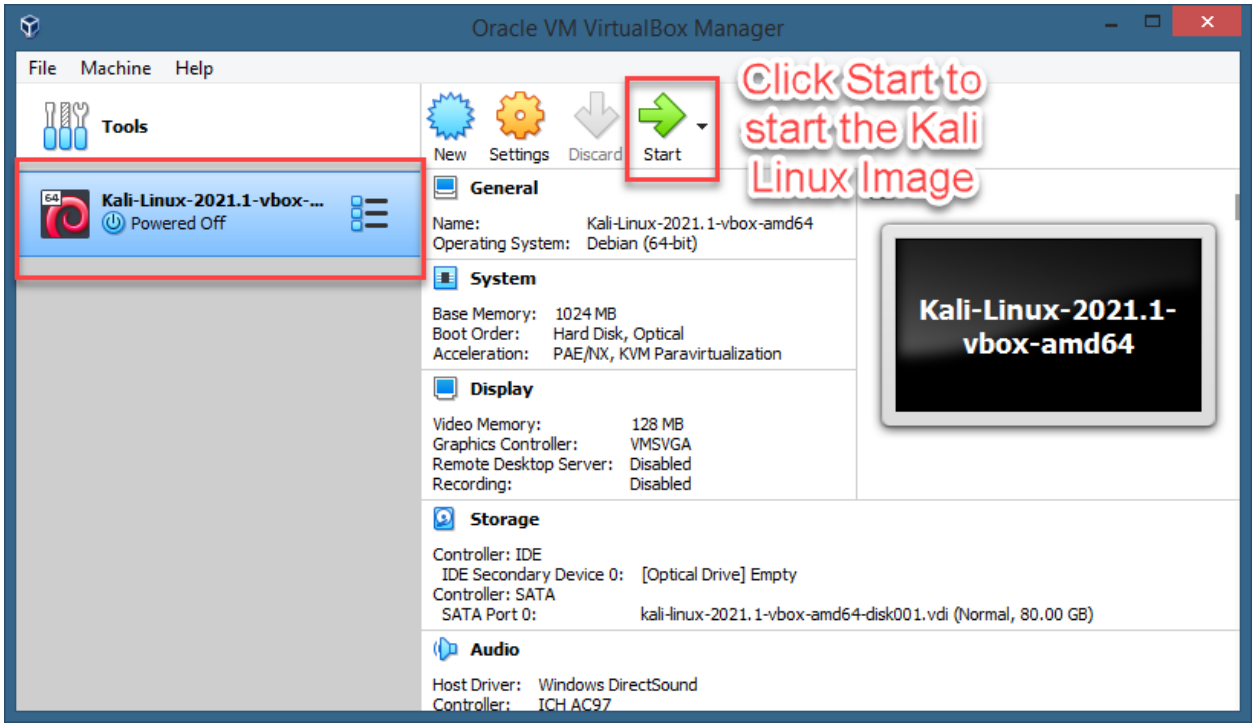


8. Wait until the importing process finish.

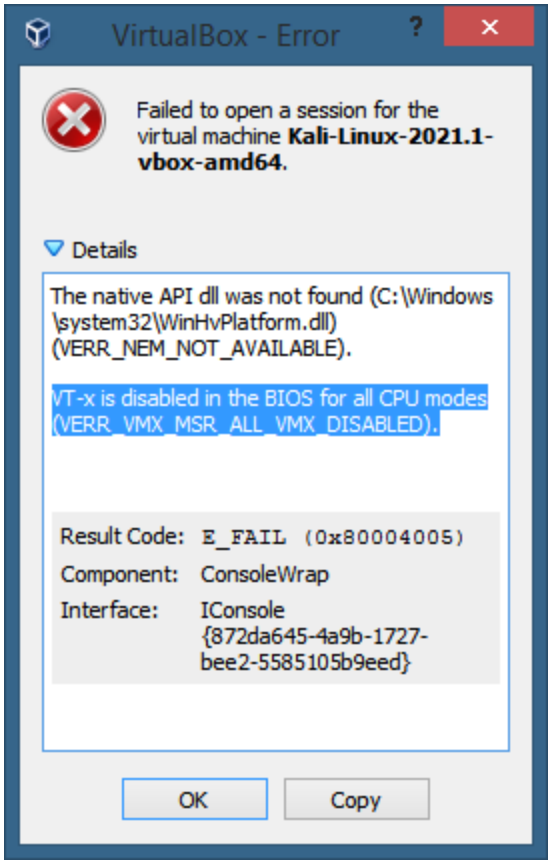


9. Now, to start the Kali Linux on Virtual Box, just click on the **Start** button on the Virtual Box screen.

`

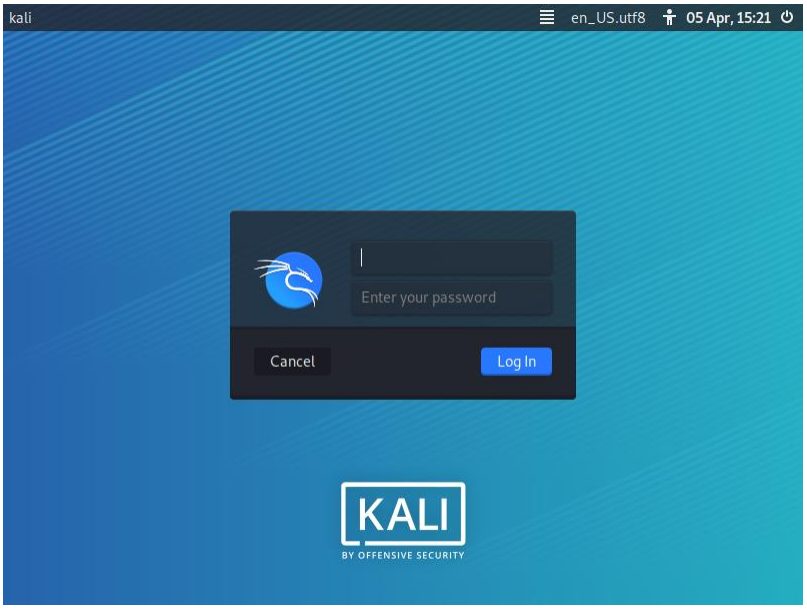


10. If you see an error as shown in the screenshots below, go to Step 11. Otherwise, please proceed to Step 13.

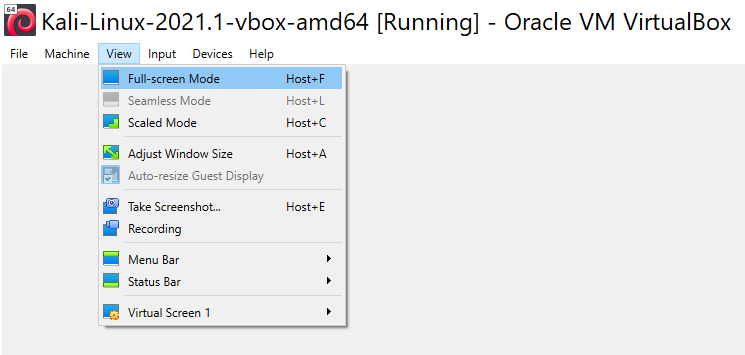


`

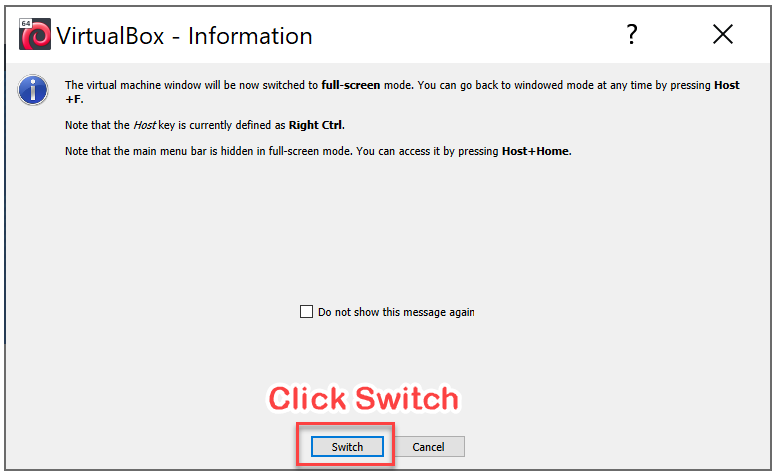
11. The error most probably occurred because your computer BIOS has not been setup yet to run a virtual machine. The following links might be able to help you troubleshoot the error:
    a. https://bce.berkeley.edu/enabling-virtualization-in-your-pc-bios.html
    b. https://youtu.be/KxYaDQvJizU
    c. Alternatively, you can search the troubleshooting guides from the Google search engine by using the term "enabling virtualization in bios".
12. After clicked the Start button, click inside the virtual machine and hit **Enter**. Now, you can see the Kali Linux welcome screen similar as follows:



13. Now it's asking for the username, which is **kali**, and then it's asking for the password, which is also **kali**. Both with small letters.
14. To view the screen in full screen mode, on the Virtual Box screen follow this screenshot:



`

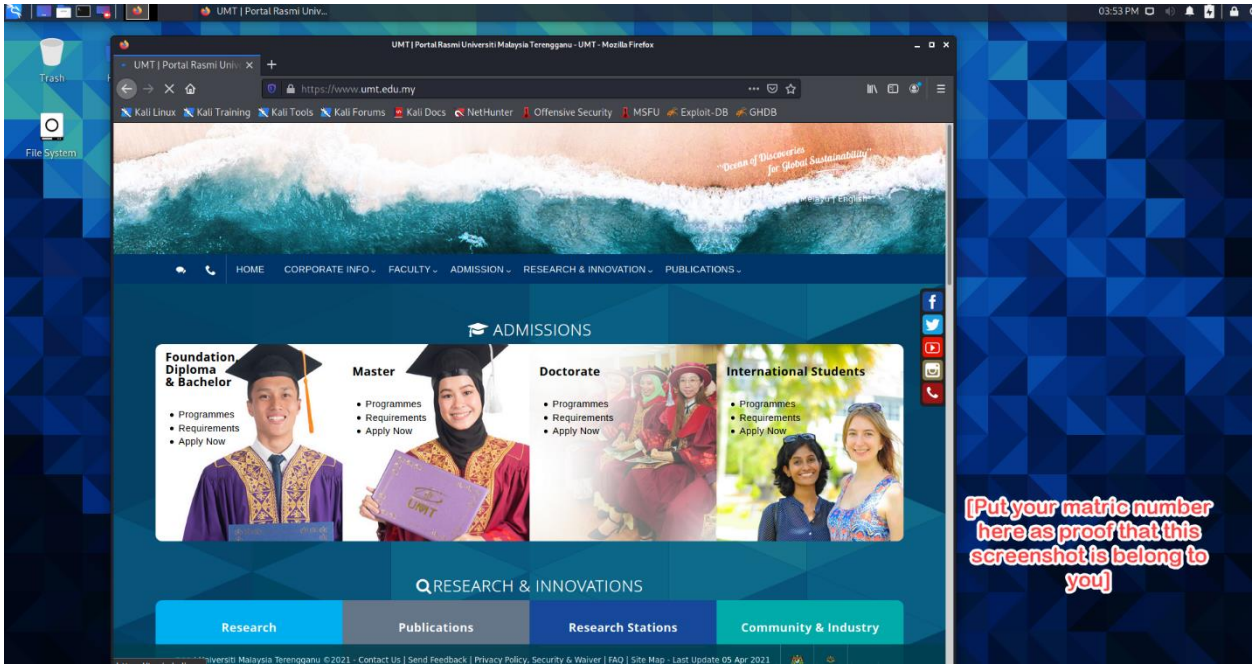


15. If you did the above steps correctly, now you will see the desktop of Kali Linux

16. Congratulations! You have successfully setup your Kali Linux.
17. Next, we are going to test the internet connection of the Kali Linux virtual machine. As we know, Kali Linux uses the network provided by the host computer. To do this, we simply need to open the browser and go to UMT website, www.umt.edu.my.

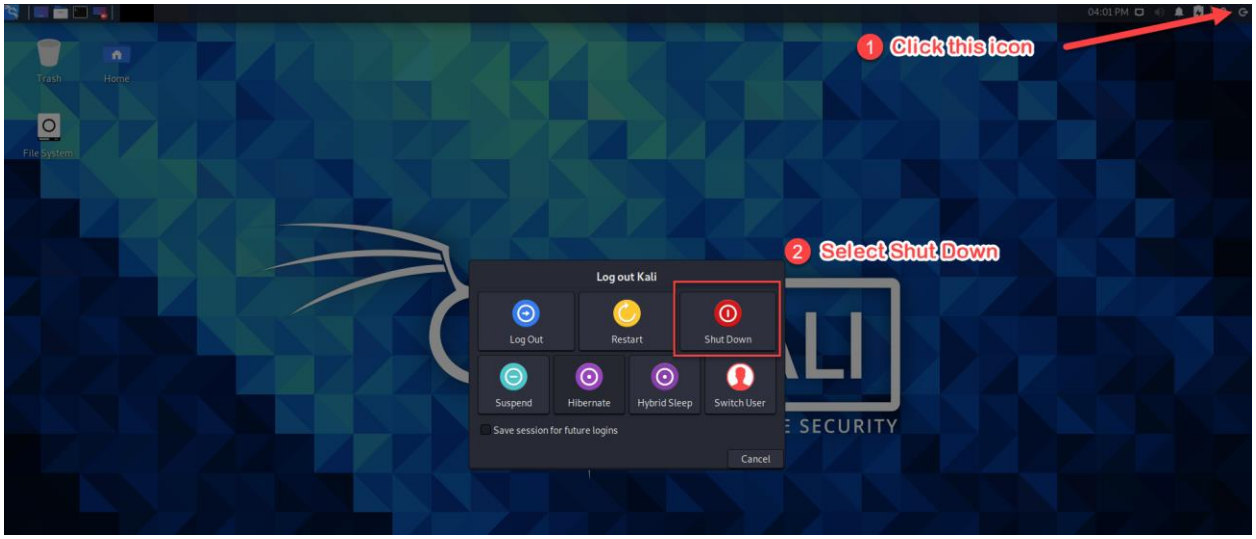
`

18. If the network and internet connection is OK, then you will see the screen as below. You have to take the screenshots and put your matric number on top of it. Save the screenshot in a Word document and submit it as lab work report to epembelajaran.



`

19. It's now time for shutting down the Kali Linux virtual machine. Just go to the top right corner of the Kali Linux screen, then select **Shut Down**.



20. Until then, we have finished with the setup and testing the network for Kali Linux virtual machine, ready for the next task.

REFLECTION QUESTIONS

1. **Based on your understanding, what is Kali Linux?**
2. **What is Kali Linux used for?**
3. **Give five reasons for using Kali Linux.**

`

TASK 3: SETTING AND RUNNING METASPLOITABLE IMAGE

OBJECTIVE

To run and explore the Metasploitable as a virtual machine

TASK DESCRIPTION

Student need to run and test the Metasploitable image on the virtual box that had been downloaded earlier.

ESTIMATED TIME

60 Minutes

STEPS:

1. In the previous tasks, you have downloaded the image for Metasploitable. It is compressed in a zip format.

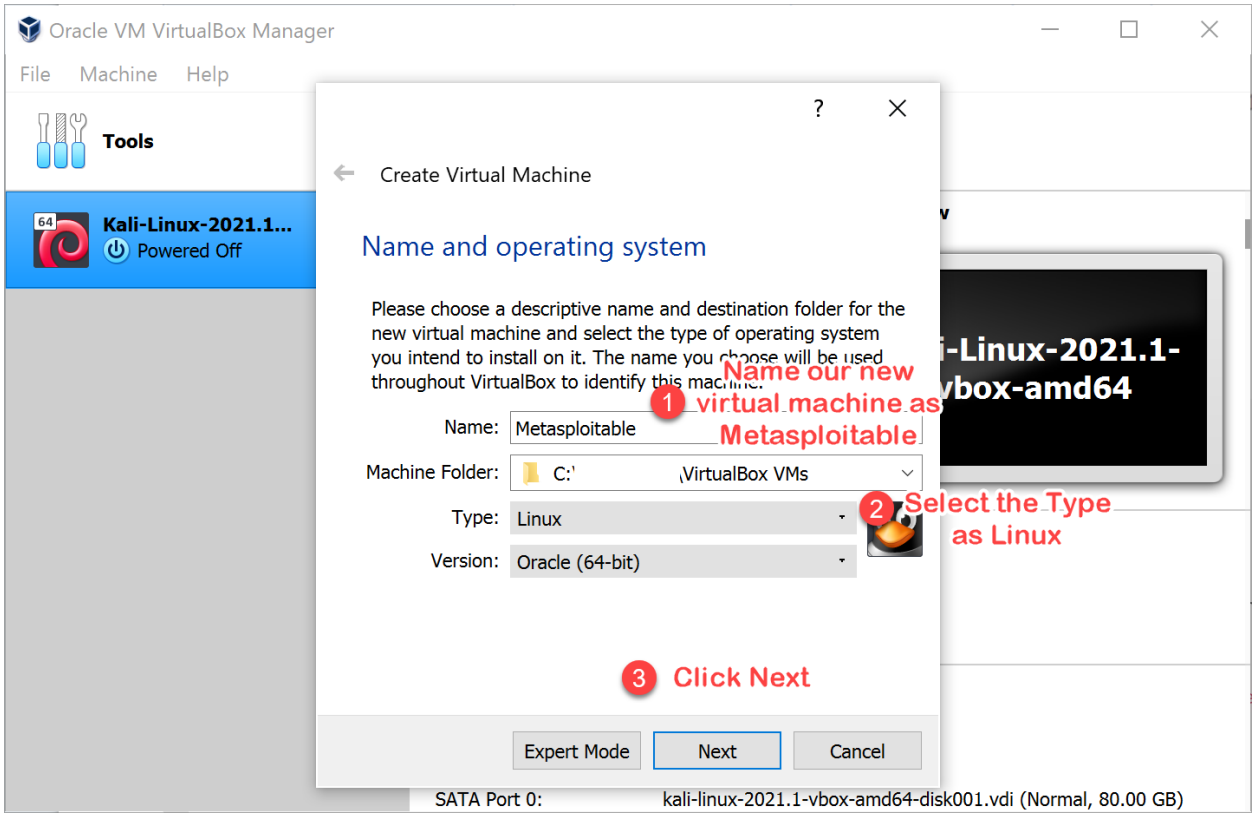
   metasploitable-linux-2.0.0.zip

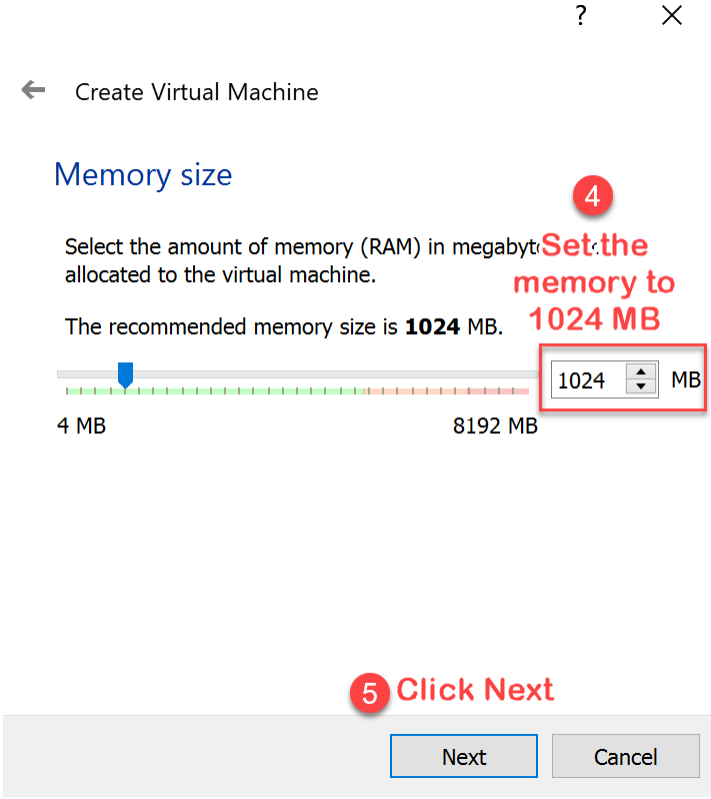
2. Now, decompress the zip file in any suitable location on your computer. You should see list of files similar to this:

   Metasploitable2-Linux

Name	Status	Type	Size
Metasploitable.nvram		NVRAM File	9 KB
Metasploitable.vmdk		Virtual Machine Disk ...	1,880,512 KB
Metasploitable.vmsd		VMSD File	0 KB
Metasploitable.vmx		VMX File	3 KB
Metasploitable.vmxf		VMXF File	1 KB

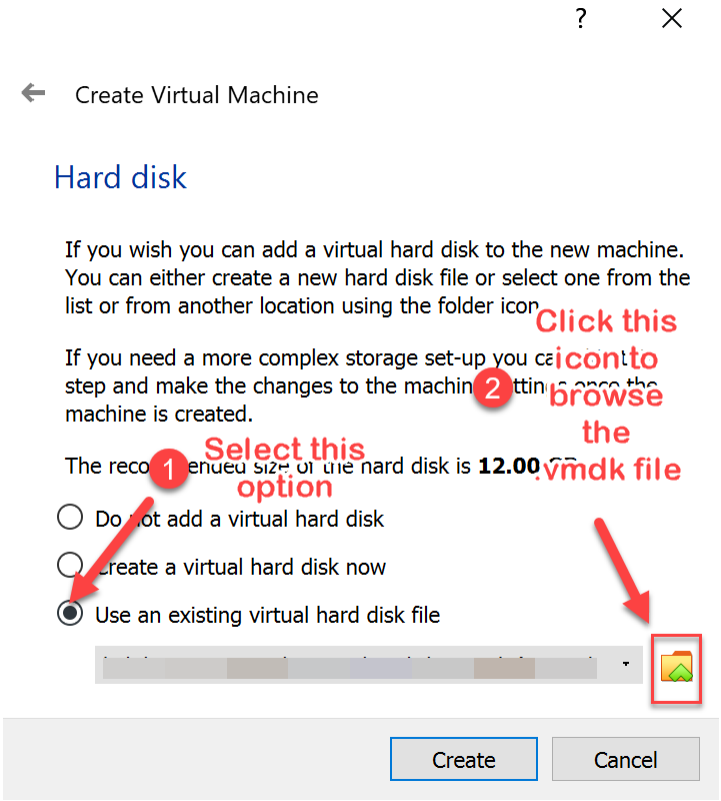
3. Next, follow these steps:

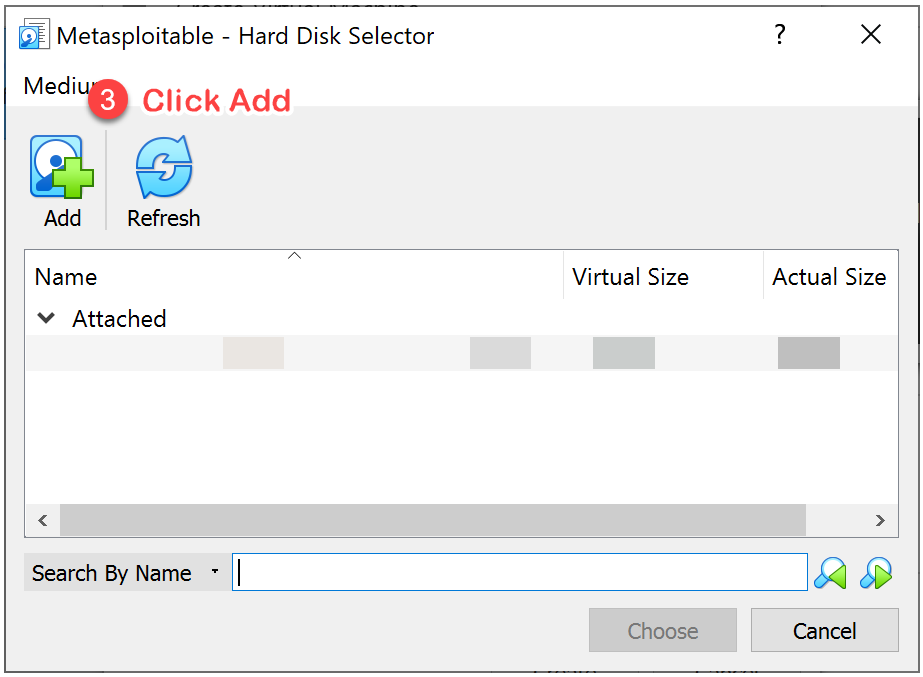

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Kali-Linux-2021.1...
Powered Off
Create Virtual Machine
Name and operating system
Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
Name: Metasploitable
Machine Folder: C:\ \VirtualBox VMs
Type: Linux
Version: Oracle (64-bit)
1 Name our new virtual machine as Metasploitable
2 Select the Type as Linux
3 Click Next
Expert Mode
Next
Cancle
SATA Port 0:
kali-linux-2021.1-vbox-amd64-disk001.vdi (Normal, 80.00 GB)

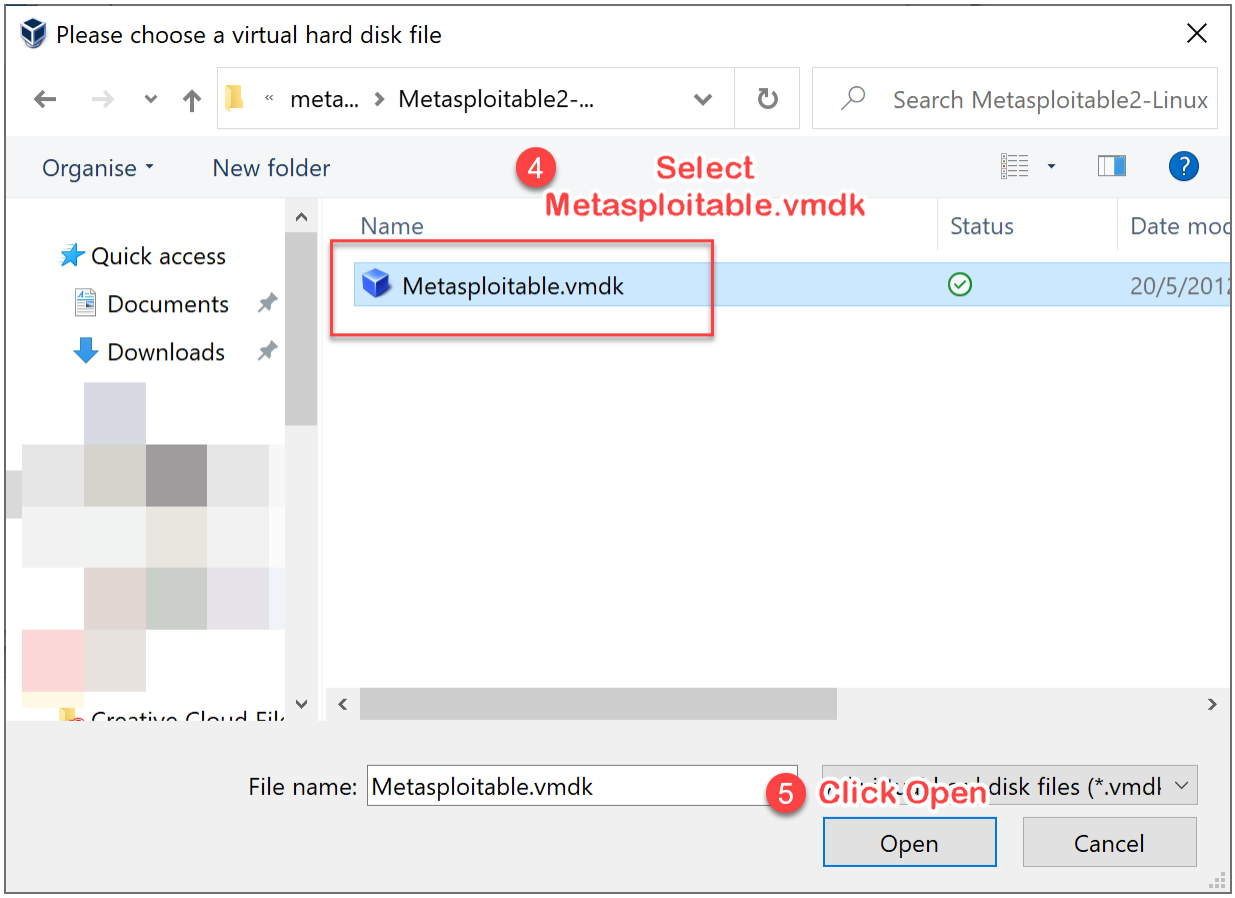

Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes allocated to the virtual machine.
The recommended memory size is 1024 MB.
4 Set the memory to 1024 MB
1024
MB
4 MB
8192 MB
5 Click Next
Next
Cancel

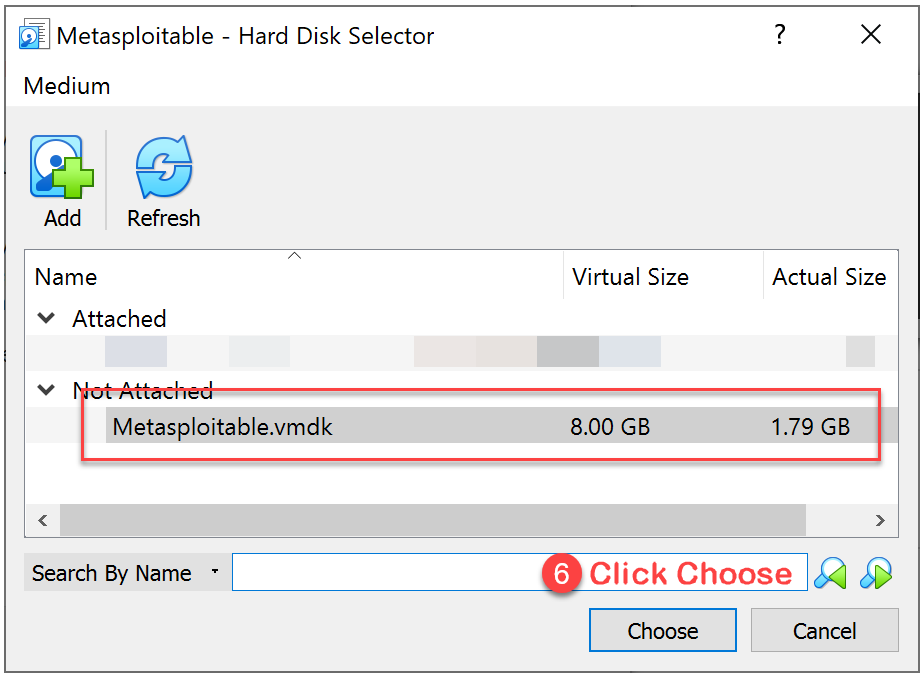
`

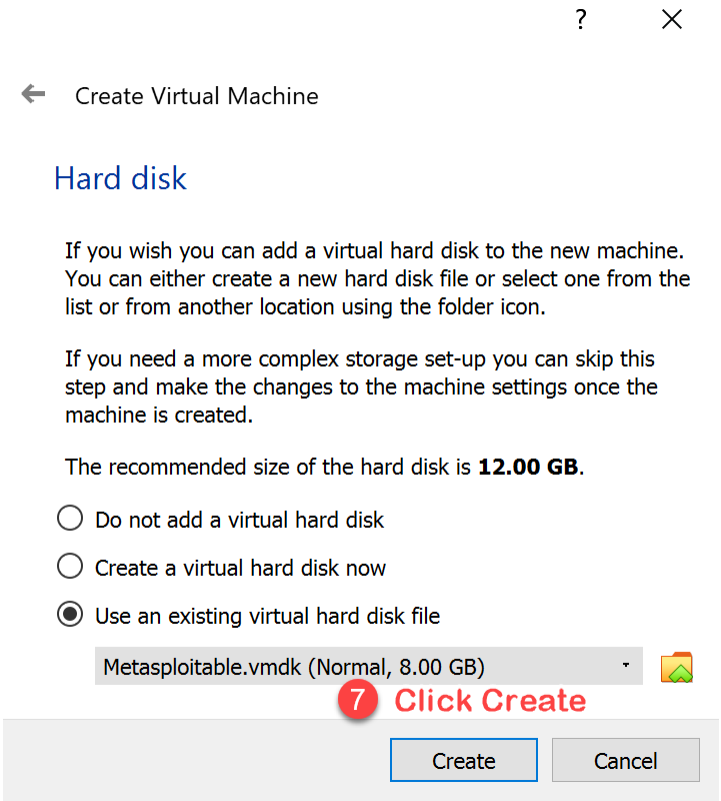
4. Then, unlike when creating Kali Linux in the previous task, we will use the existing virtual file option (that is, when we created a new virtual hard disk). The explanation for this is that the downloaded Metasploitable image is actually was created for VMware Player. So, we are going to import the hard disc file, or hard disc image, to have an installation ready to go without having to install it. We will only use a hard disc file that already exists. To do, this pick the **.vmdk** file from the Metasploitable directory (location where have extracted the zip file in Step 2).




Metasploitable - Hard Disk Selector
3 Click Add
Add
Refresh
Name
Virtual Size
Actual Size
Attached
Search By Name
Choose
Cancel

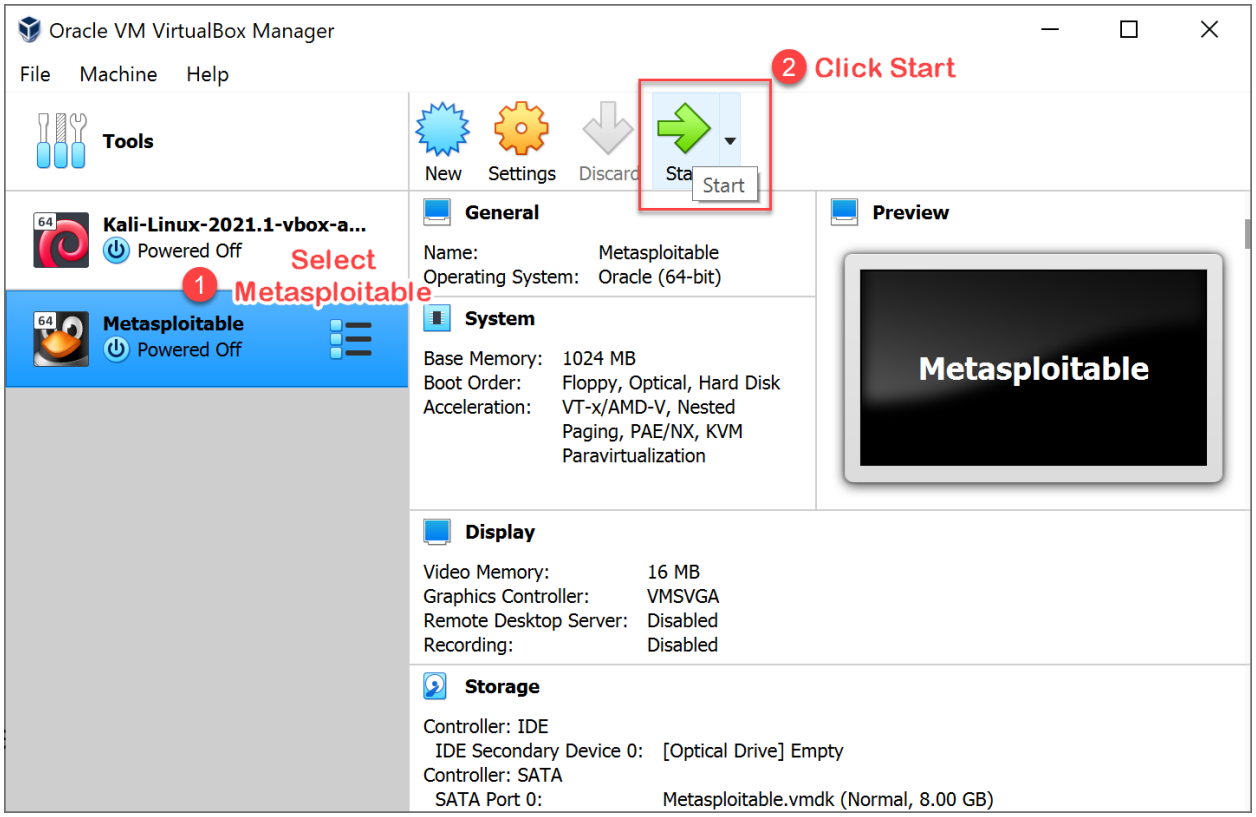

Please choose a virtual hard disk file
meta... > Metasploitable2-...
Search Metasploitable2-Linux
Organise
New folder
4 Select Metasploitable.vmdk
Name
Status
Quick access
Documents
Downloads
Metasploitable.vmdk
File name: Metasploitable.vmdk
5 Click Open
Open
Cancel



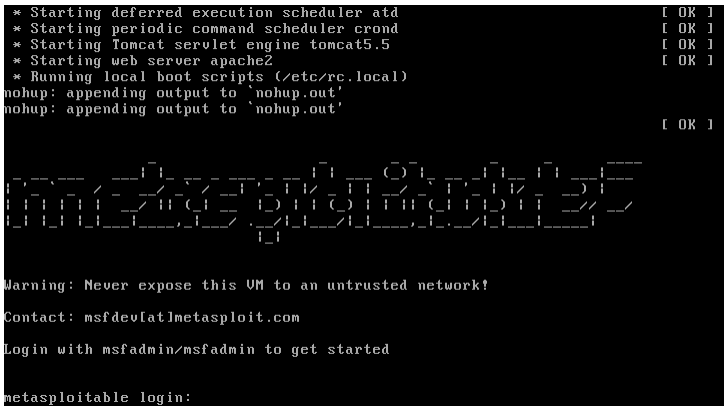


5. Now we have successfully created the virtual machine for Metasploitable.
6. Next, start the Metaspolitable virtual machine.

`



7. Wait until the loading is complete. If you want to view the screen in Full Screen mode, repeat the steps as been done during setting the Kali Linux previously. As you can see below, Metasploitable does not has a graphical user interface as Kali Linux, everything is on the terminal.



8. To login, use **msfadmin** as username and password.
9. If the login successful, you will see the screen below:

`

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

10. Then, type **clear** on the terminal and press **Enter** to clear out everything from the console.

```
msfadmin@metasploitable:~$ clear_
```

11. If you need to go back to host environment (your real computer), just click on **right ctrl** button on the keyboard.
12. Next, we are going to explore a few Linux commands.
13. Type, **ls** command to view list of directories in the Metasplotable virtual machine. You will see some output as below:

```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ _
```

You will see a folder name **vulnerable**.

14. Next, you are going to create a directory with your matric number as the name. Type this command on the console **mkdir [your matric number]**, then hit **Enter.**
15. Type dir command again to see the director you just created.

```
msfadmin@metasploitable:~$ mkdir CS12345
msfadmin@metasploitable:~$ dir
CS12345  vulnerable
msfadmin@metasploitable:~$
```

Change this to your matric number

16. Take a screenshoot of the output and put it into your lab work report.
17. Next, lets go into the directory we just created and create a file in it.
18. Type **cd [name of your directory]**, then hit **Enter**.
19. In the directory we are going to create a new file, type **vi [Your matric number].txt**.

```
msfadmin@metasploitable:~$ cd CS12345
msfadmin@metasploitable:~/CS12345$ vi CS12345.txt
```

Change this to your matric number

`

20. You will see a blinking cursor, waiting for you to type something inside the file. To do that, hit letter **a** on your keyboard. This will allow you to enter some input to the file. Type "My name is [your name]" and "My Matric number is [matric number into]" the file (see the example input in the screenshot below). Take a screenshot of your work and put it in the lab work report.
21. If finish, hit **esc** button and type **:wq** to save and exit.

22. For learn more about vi editor, you can visit https://www.guru99.com/the-vi-editor.html
23. To view your current location in the console, type **pwd** command.

24. Again, get the screenshot of the output and put it into the lab work report.
25. You may explore other Linux commands by searching the list of command sat Google. Try to play around with three different commands. Make sure you screenshots every output and put it in the lab report.
26. Finally, we are going to shutdown our Metasploitable virtual machine. This can be done by typing **sudo poweroff** on the console and hit **enter**. Put in the password **msfadmin** and **enter**.
27. Well done, you have successfully run and explore the Metasploitable virtual machine!