COURSE

SETTING UP A HACK LAB

R4IM4NN

Table of Contents

I. [Course aim]....3
II. [Course Prerequisites]....3
III. [Enable virtualization]....3
IV. [Hypervisor type 2(Hosted hypervisor)]....3
V. [Hack Lab - Setting up virtual machines]....4
VI. [Hack Lab - Network isolation]....10
VII. [Hack Lab - virtual machines snapshots]....13
VIII. [Thanks]....14

I. [Course aim]

Set up a Hacklab, a virtual environment totally isolated from the external network, in which you can run tests in complete security.

II. [Course Prerequisites]

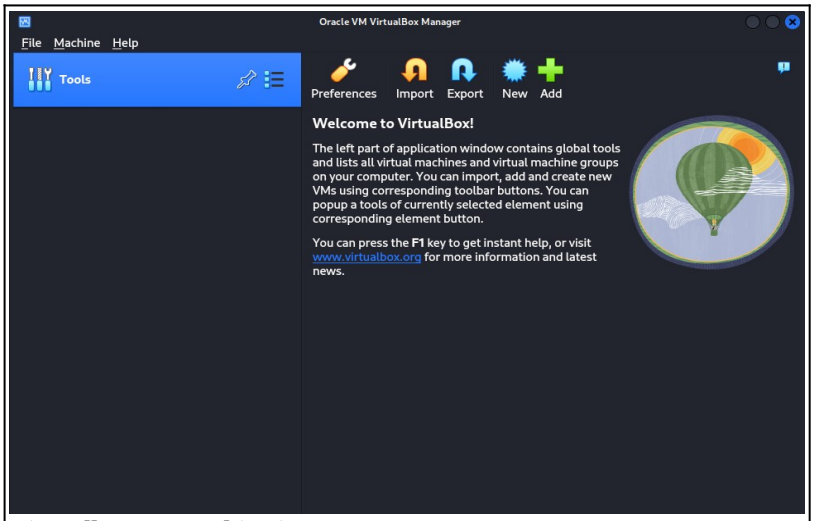
- Computer with at least 8GB ram
- Enable virtualization on your computer to create virtual machines
- Have storage to install 2 virtual machines
- Very little networking knowledge

III. [Enable virtualization]

To activate virtualization, you need to go to your computer's BIOS, to go to the BIOS you need to switch off your computer, then you need to press a specific key on your keyboard, which is different depending on your computer model. The most common keys are F2, F10, F12, DEL, ESC or F1 and F9. This key is often indicated when you switch on your computer. When you're in the BIOS, you need to find the virtualization option and enable it.

IV. [Hypervisor type 2(Hosted hypervisor)]

The type 2 hypervisor runs as an application on our host machine, interacting with your hardware. In our case, the type 2 hypervisor we'll be using is **VIRTUALBOX**

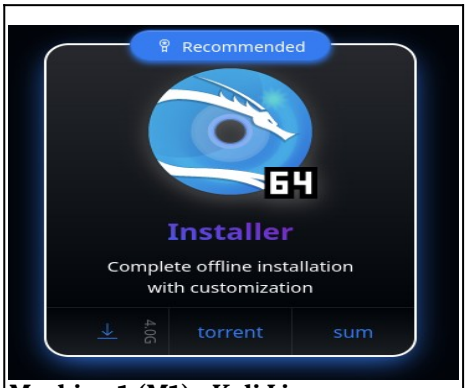


Virtualbox 7.0 on this picture.

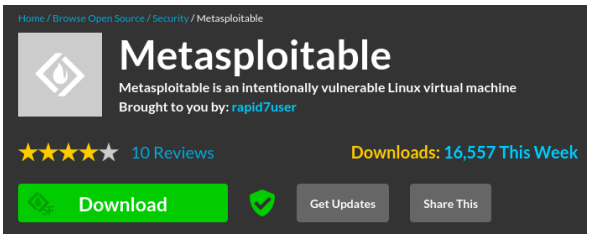
V. [Hack Lab - Setting up virtual machines]

We've installed our type 2 hypervisor (Virtualbox). Now we need to set up our 2 virtual machines, which will represent our hacklab. The two operating systems we'll be installing are :

M1 | [ATTACKER] Kali Linux by OffSec : Debian-based Linux distribution for advanced penetration testing and security auditing.
M2 | [TARGET] Metasploitable 2 by Rapid7 : Ubuntu Linux intentionally vulnerable to test common vulnerabilities.

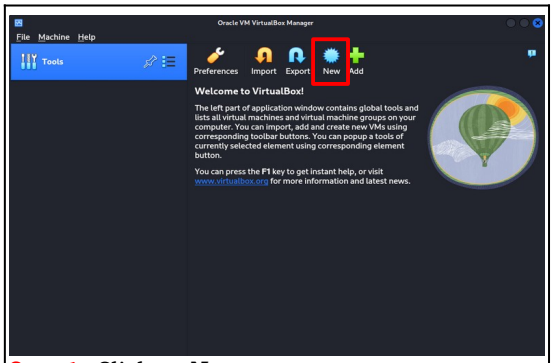


Machine 1 (M1) - Kali Linux installation.

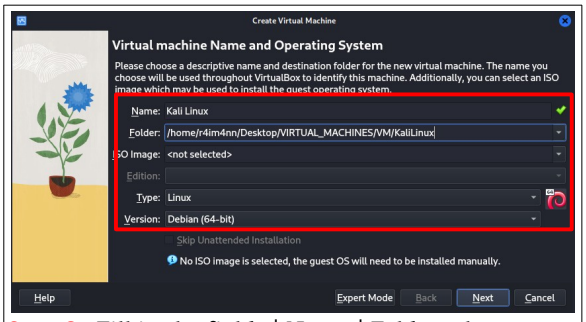


Machine 2 (M2) - Metasploitable 2 installation.

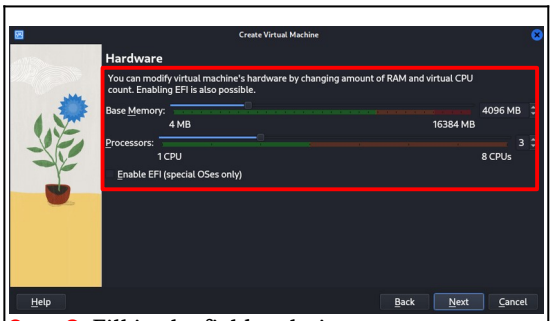
Now we can start setting up our 2 virtual machines, Let's start with Kali Linux (M1).



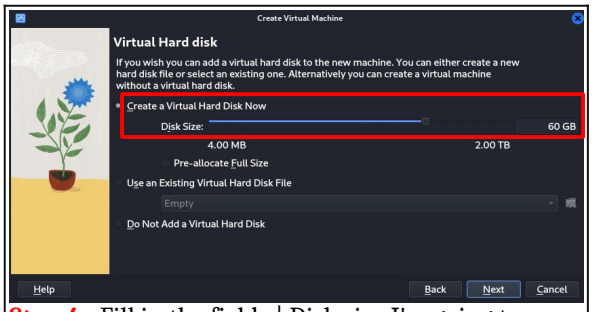
Step 1 : Click on New.



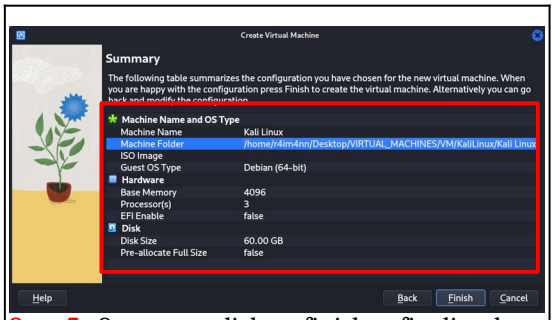
Step 2 : Fill in the fields | Name | Folder where you want to create it | Type | Version.



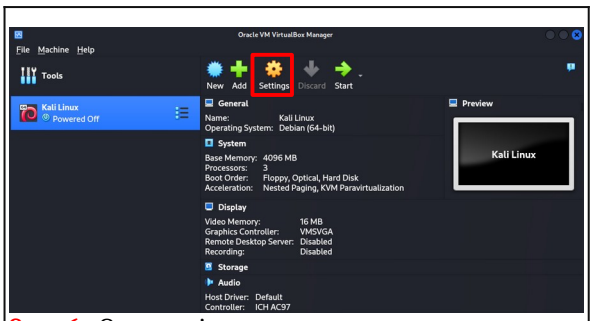
Step 3 :Fill in the fields relative to your computer | RAM | CPU CORE.



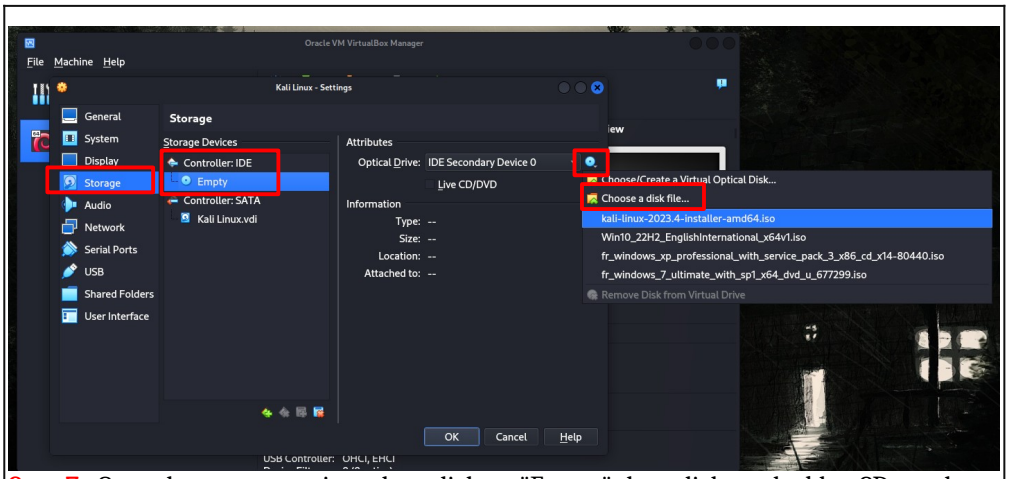
Step 4 : Fill in the fields | Disk size I'm going to use 60GB to install all the tools (30GB of tools).



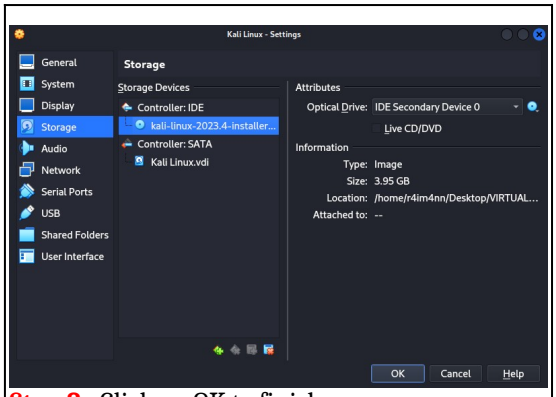
Step 5 : Summary, click on finish to finalise the creation of our virtual machine.



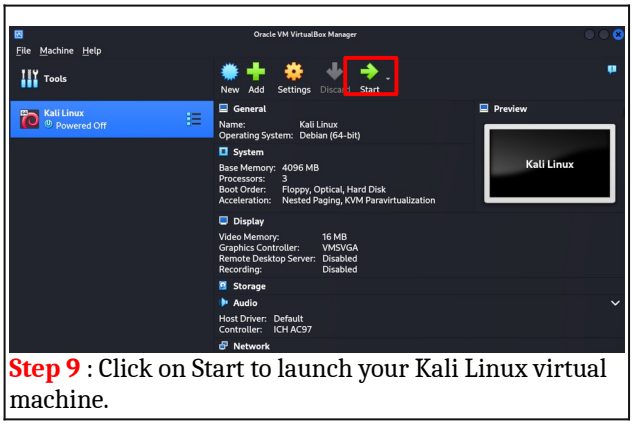
Step 6 : Go to settings



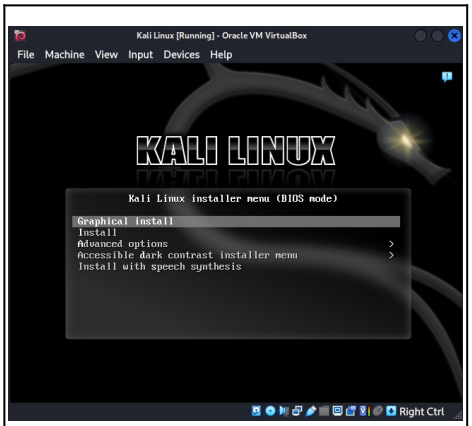
Step 7 : Go to the storage settings then click on "Empty" then click on the blue CD to select the ISO file of your Kali Linux operating system that you downloaded before.



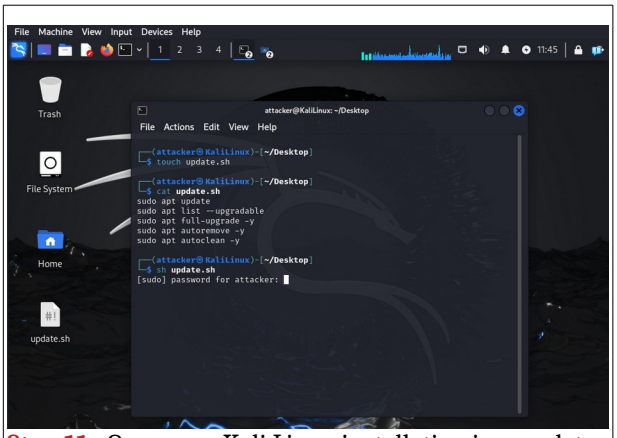
Step 8 : Click on OK to finish.



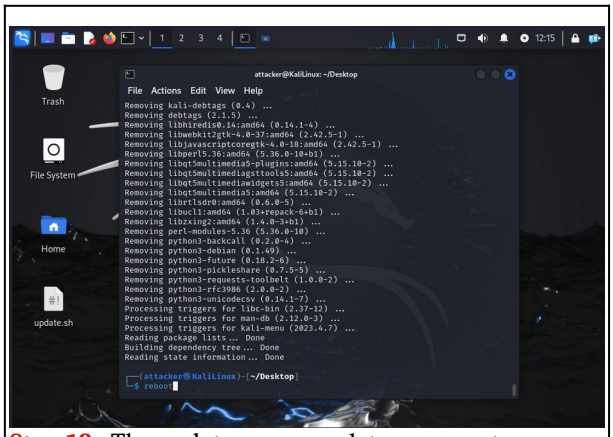
Step 9 : Click on Start to launch your Kali Linux virtual machine.



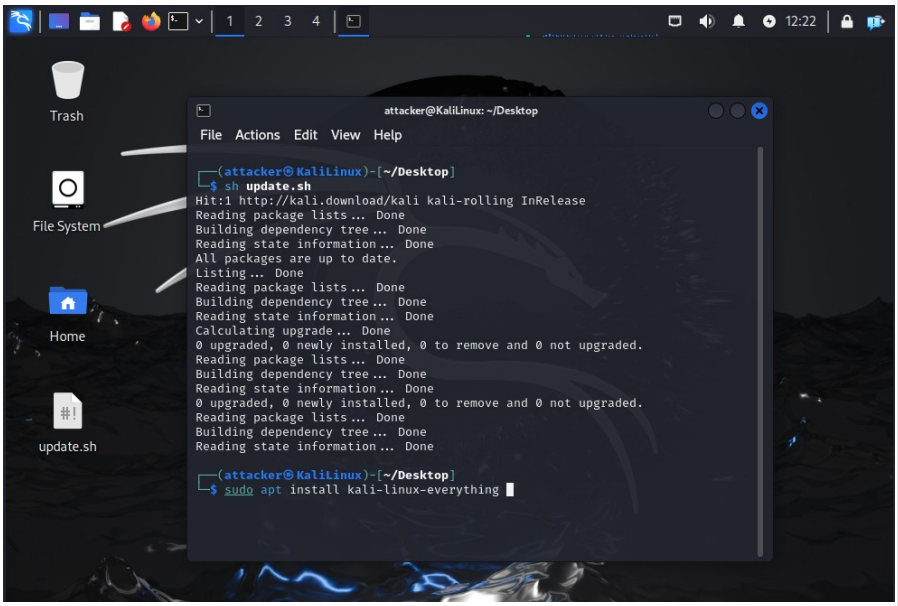
Step 10 : Choose the graphical installation to make it easier to install, then follow the standard installation steps.



Step 11 : Once your Kali Linux installation is complete, you'll need to update it. To do this, I've created a small shell script that will execute the various update commands. To start with, you need to create an "update.sh" file (you can name it anything you like, with a ".sh" extension at the end). To create this file, you can use the "touch" command. Then you add each command (sudo apt update, sudo apt list --upgradable ....) to the file you've created, save it, and finally run the script with the following command "sh update.sh".

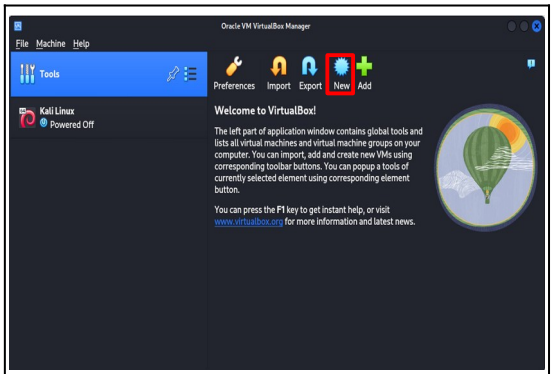


Step 12 : The updates are complete, you must now reboot your Kali Linux machine to do this you can use the "reboot" command.

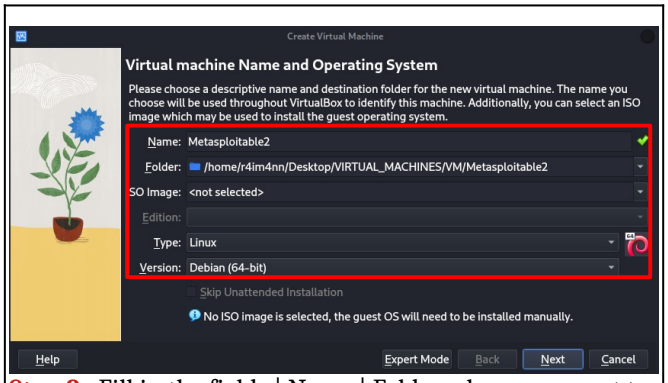


Step 13 : You can re-run the shell script "update.sh", created just before, to see that there are no more updates to be made. Now, if you want to install all tools, you can do so with the following command: "**sudo apt install kali-linux-everything**".

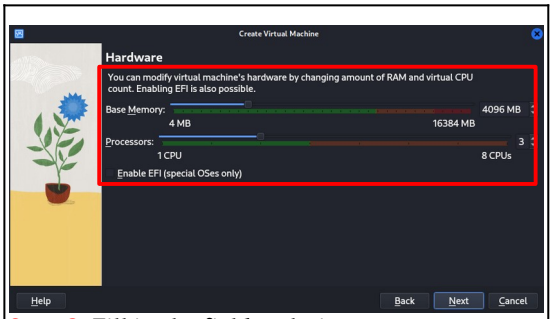
Now switch off your Kali Linux machine (M1) and set up the Metasploitable 2 machine (M2).



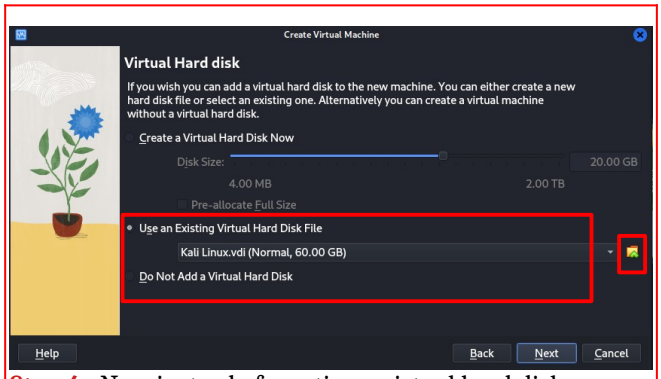
Step 1 : Click on New.



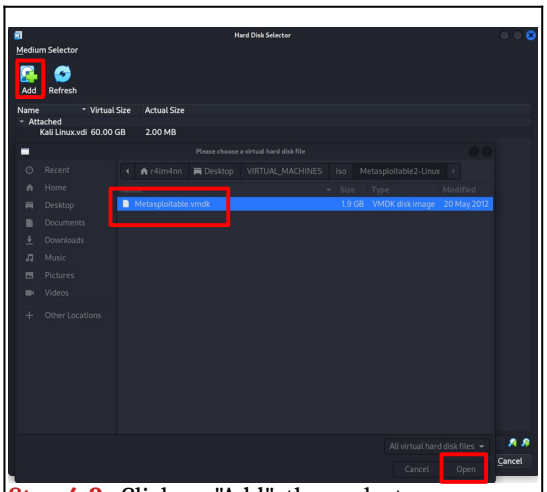
Step 2 : Fill in the fields | Name | Folder where you want to create it | Type | Version.



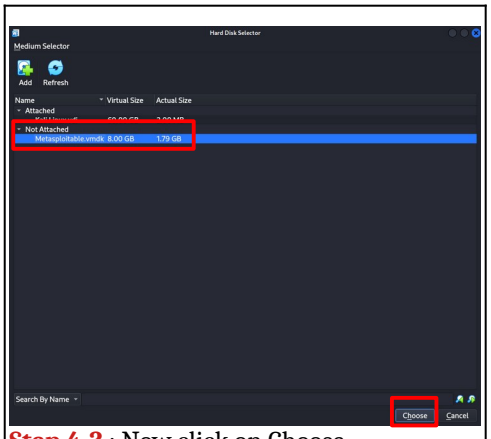
Step 3 :Fill in the fields relative to your computer | RAM | CPU CORE.



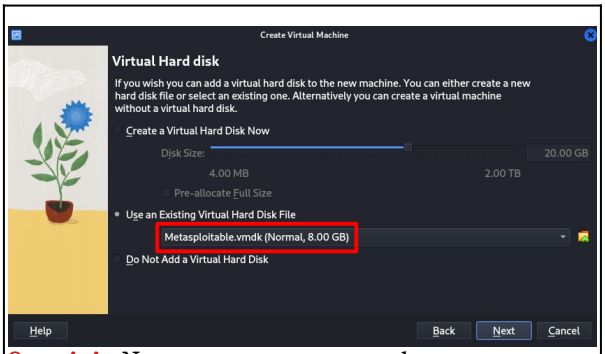
Step 4 : Now instead of creating a virtual hard disk we are going to get the virtual hard disk from metaspoitable 2 that we downloaded before (you have to unzip the zip file of course) to use the virtual hard disk you have to select "**Use an Existing Virtual Hard Disk File**" and then click on the little folder.



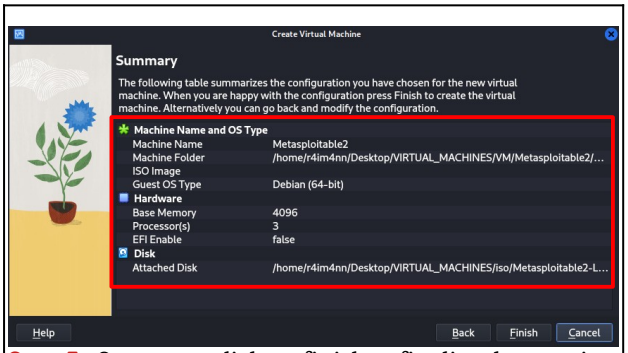
Step 4-2 : Click on "Add", then select your "Metasploitable.vmdk" file and click open.



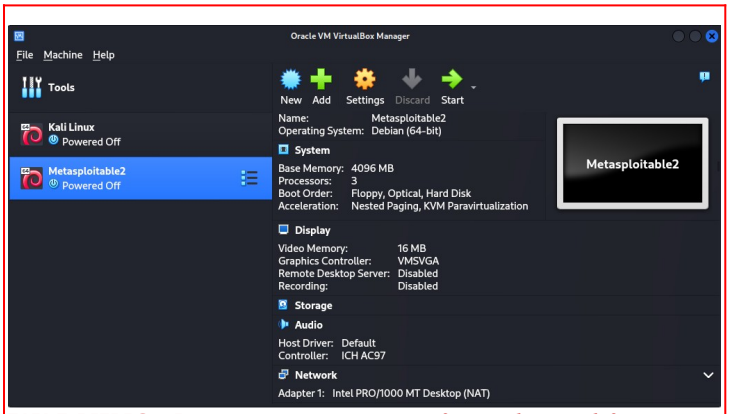
Step 4-3 : Now click on Choose



Step 4-4 : Now you can move on to the next step.



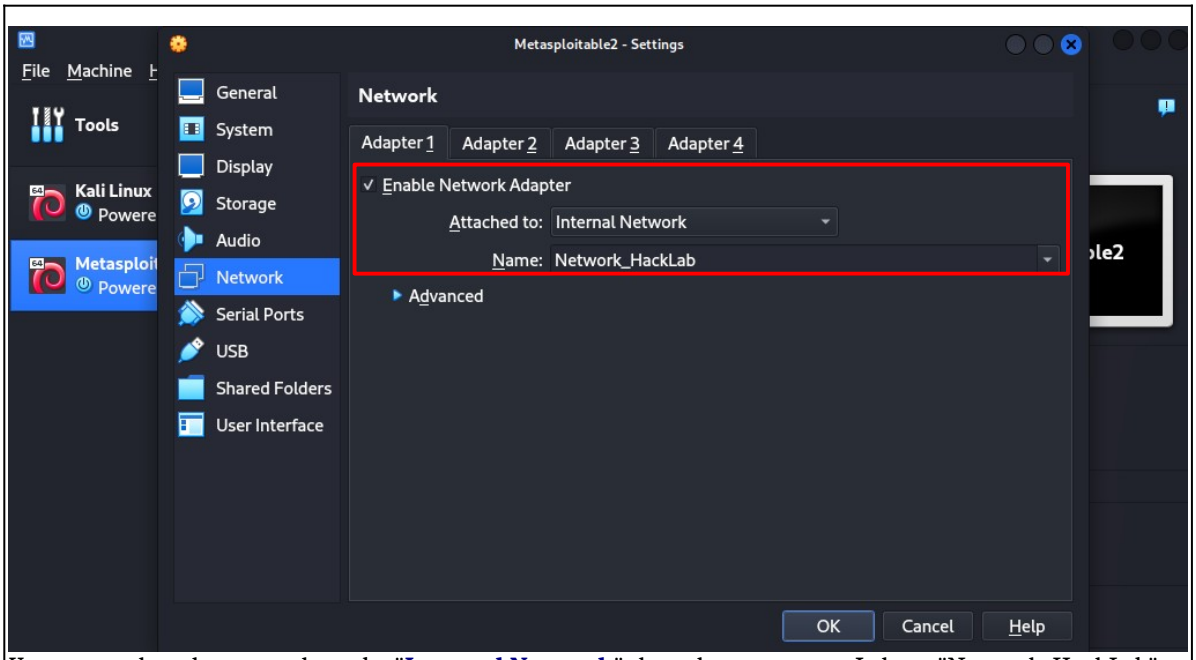
Step 5 : Summary, click on finish to finalise the creation of our virtual machine



WARNING : Do not start your virtual machine metasploitable 2. You must isolate this virtual machine from the Internet.

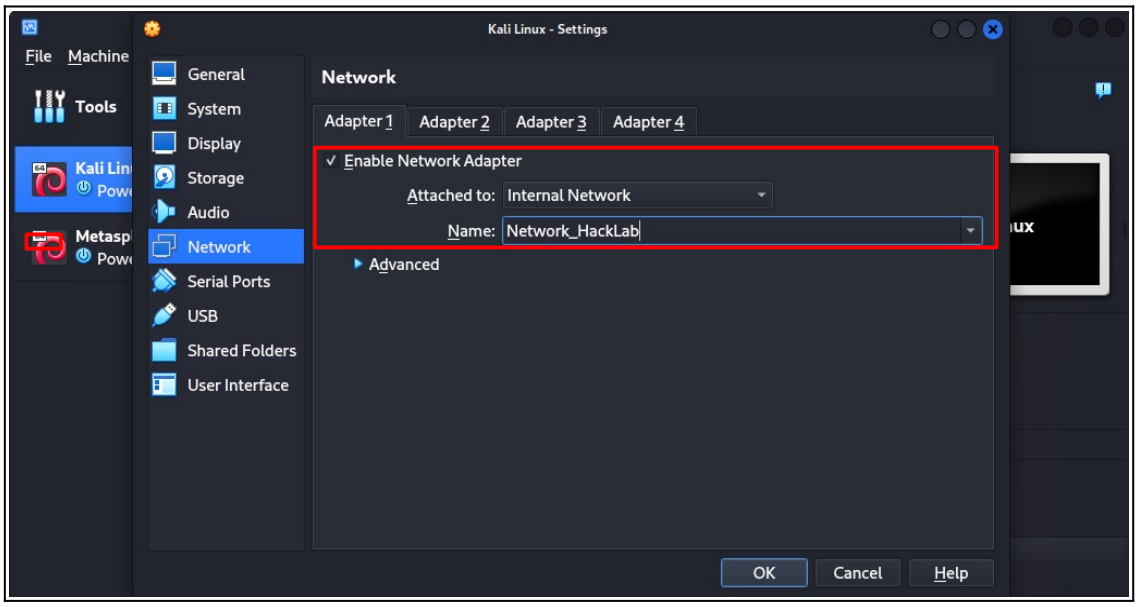
VI. [Hack Lab - Network isolation]

To isolate your HackLab, you need to configure the network of the 2 virtual machines (Kali Linux and Metasploitable 2). Let's start with the Metasploitable 2 virtual machine.

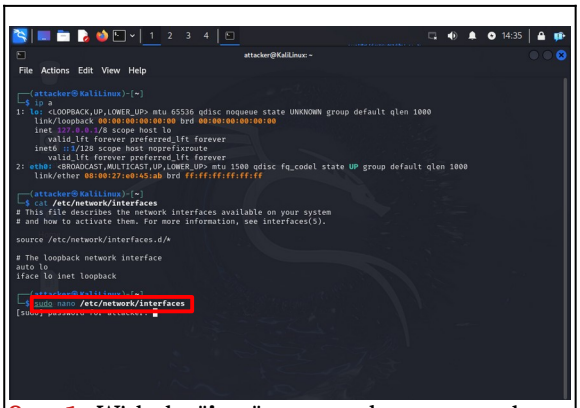


You must select the network mode: "**Internal Network**" then choose a name, I chose "Network_HackLab" then click on "**OK**" to finish.

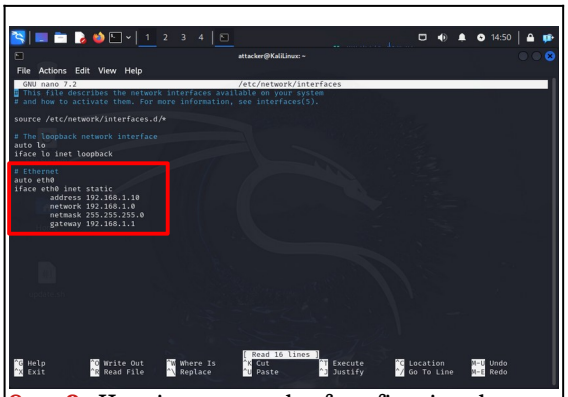
Now we'll do the same thing with the Kali Linux virtual machine.



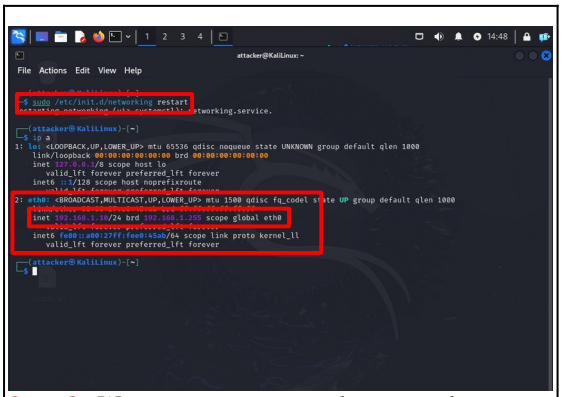
We are now going to configure the network with a static IP address on the 2 virtual machines (Kali Linux and Metasploitable 2) so that these 2 virtual machines can communicate. Let's start with the Kali Linux.



Step 1 : With the "**ip a**" command we can see that we do not have an IP address on our network interface (Ethernet in my case) eth0, in your case it may be different but it remains the same process.We must assign an IP address to this network interface and for this we must modify the "**interfaces**" file which is located at "**/etc/network/interfaces**". To modify this file you must have root rights, in my case I used nano (text editor in the terminal).

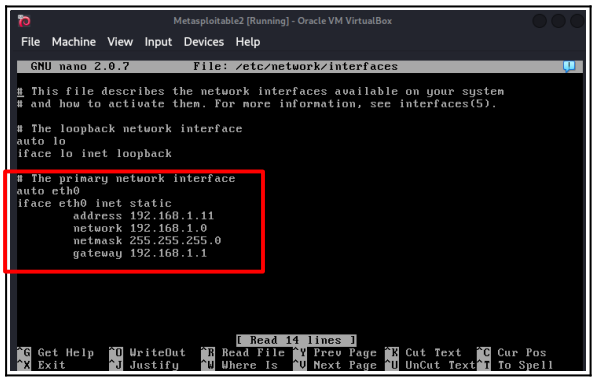


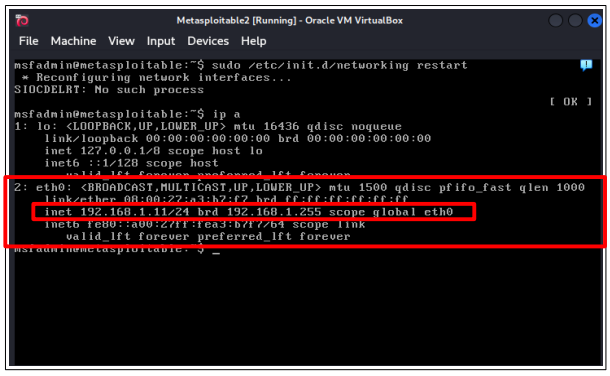
Step 2 : Here is an example of configuring the eth0 interface.

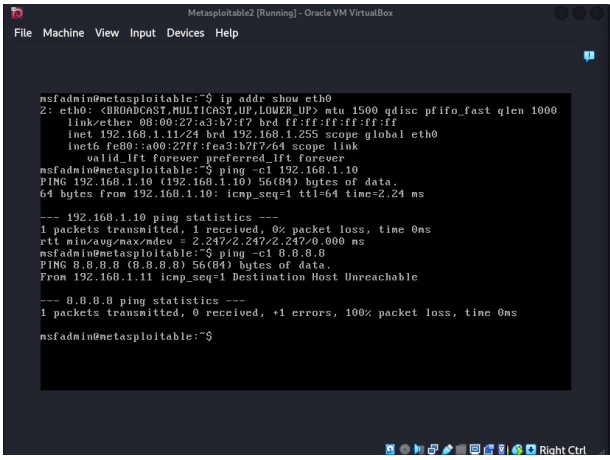


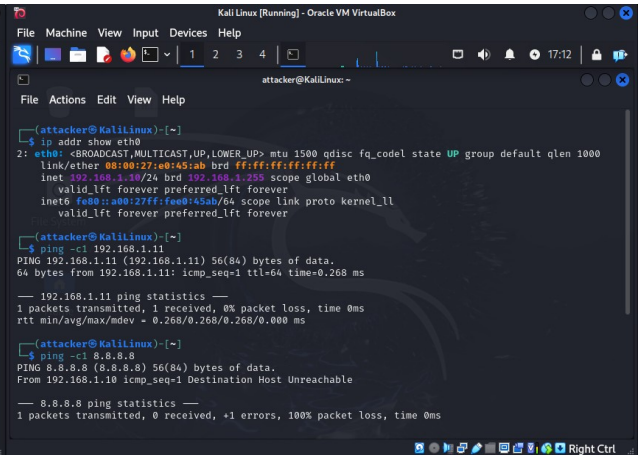
Step 3 : We must now restart the network services and then we can see that our eth0 network interface has the IP address that we have fixed.

Now we'll do the same thing with the Metasploitable 2. The login credentials are msfadmin for login and password.





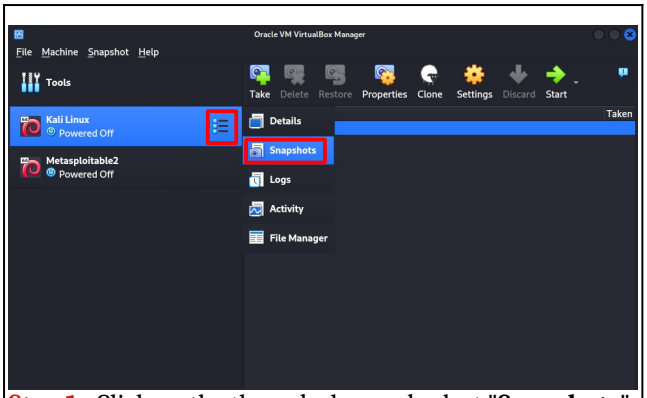




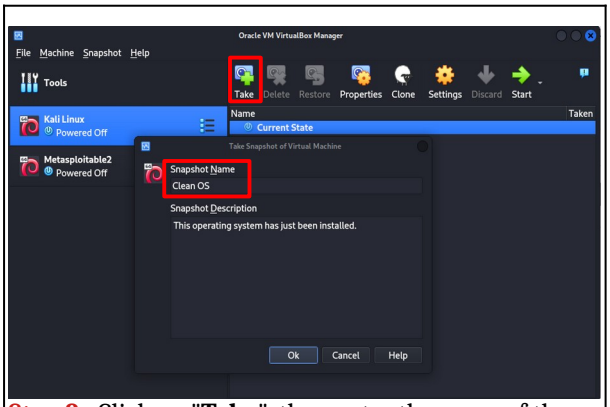
Now you can try to ping the machines between each other. VOILA ! You can see that the two machines communicate with each other and do not communicate with external networks.

VII. [Hack Lab - virtual machines snapshots]

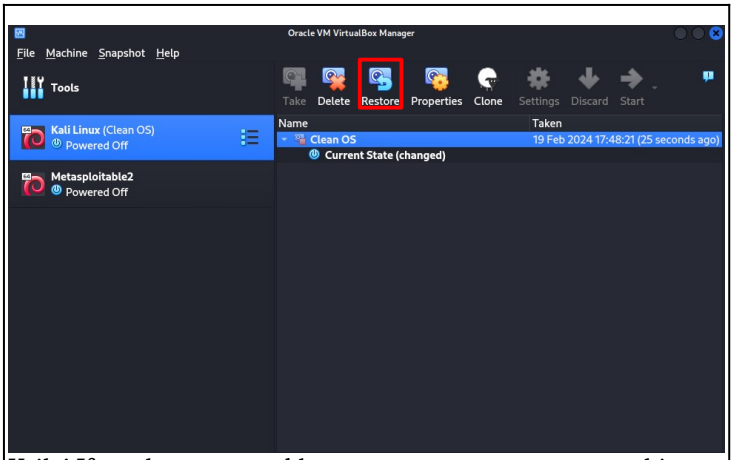
Now that your Hack Lab is ready for use, you'll probably be doing a lot of tests on it, and breaking things on operating systems. If there's a problem, so that you don't have to reinstall everything, there's a thing on virtualbox called a "snapshot", which is simply a capture of your system at a given moment, allowing you to go back in time in the event of problems on your machines.



Step 1 : Click on the three dashes and select "**Snapshots**".



Step 2 : Click on "**Take**", then enter the name of the snapshot and a description if you wish, and finally press "Ok".



Voila! If you have any problems, you can **restore** your machine at any time.

Now do the same with the Metasploitable 2 virtual machine. After that, you'll be able to use both machines safely and without any problems.

VIII. [Thanks]

This course is over, I hope I was clear and that this course was not difficult to understand. Thank you for reading this course and there are many more coming soon.

See you soon.

R4IM4NN