## **Lab Walkthrough**

### Table of Contents

#### [Step 1 - Installation Instructions for VirtualBox](#_rymwqqtto4rj)

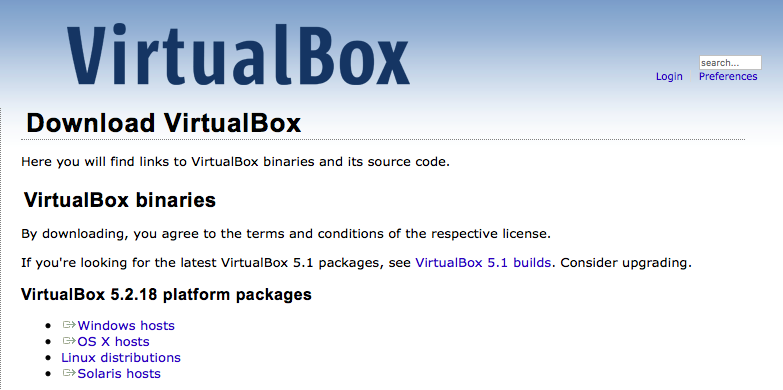
#### [Step 2 - Setting up Metasploit 2](#_9srbv2f1ynyc)

#### [Step 3 - Setting up Kali Linux for VirtualBox](#_nlmfm4pbmfl3)

#### 

#### **Step 1 - Setting Up VirtualBox**

* First, we will install **VirtualBox** from <https://www.virtualbox.org/wiki/Downloads>. The remainder of these instructions will be geared toward VirtualBox, but other VMs such as **VMWare Hypervisor** will have a similar setup.
* Select a platform package. You can choose “**Windows hosts**” or “**OS X Hosts**”, depending on your operating system. This tutorial will focus on setting up on a MAC OS..

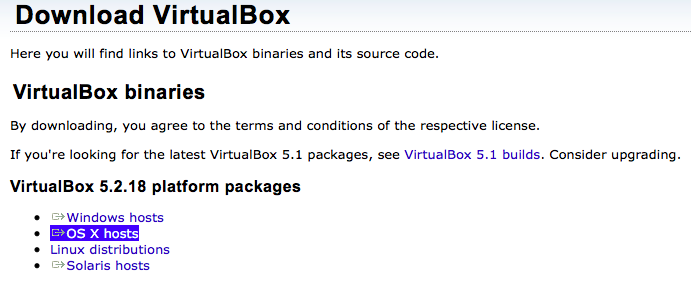


**INSTALLATION INSTRUCTIONS FOR WINDOWS:**

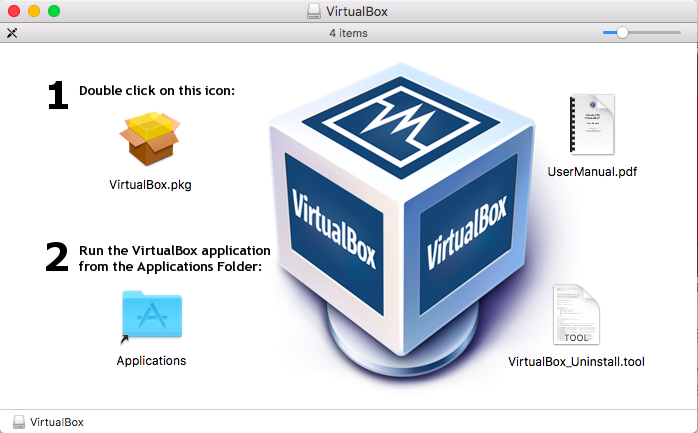
* Here is a video [walkthrough](https://www.youtube.com/watch?v=61GhP8DsQMw&list=PLZOToVAK85MpnjpcVtNMwmCxMZRFaY6mT) for further assistance.

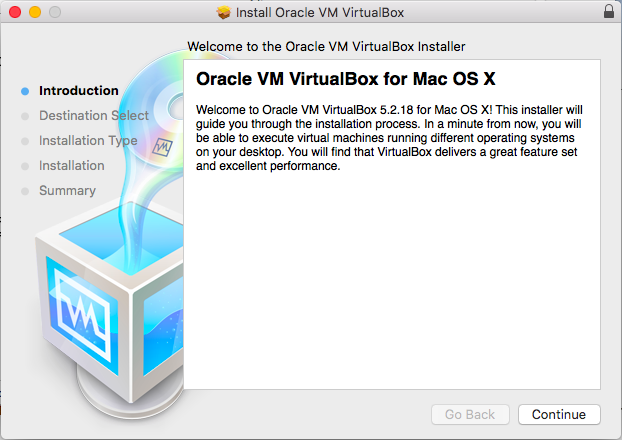
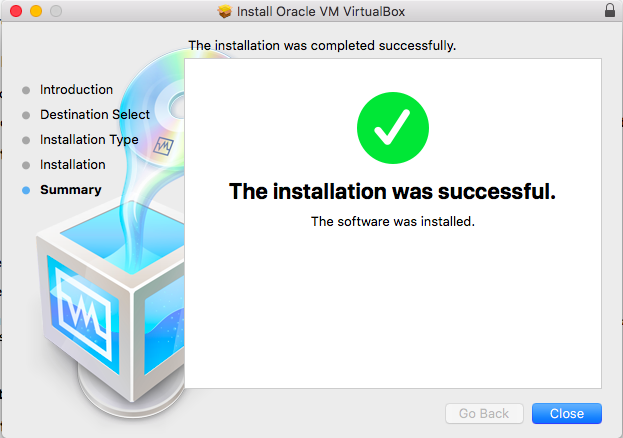
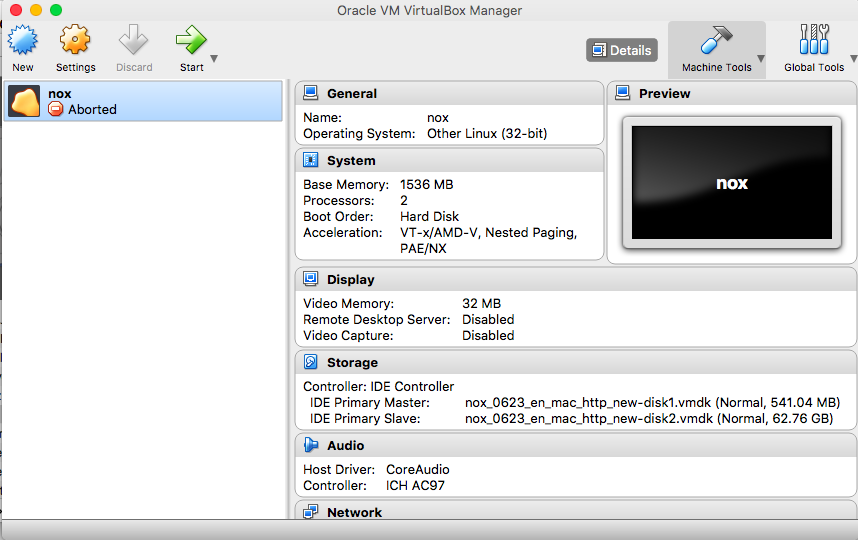
**INSTALLATION INSTRUCTIONS FOR MAC OS:**

* Select “**OS X Hosts**” and to download a .dmg file.

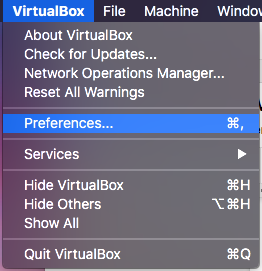
****

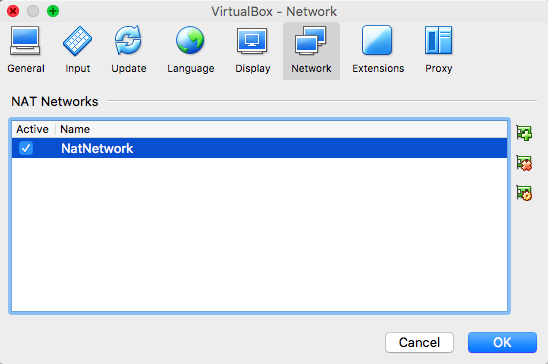
* Once you have installed the .dmg file, this screen should appear:

****

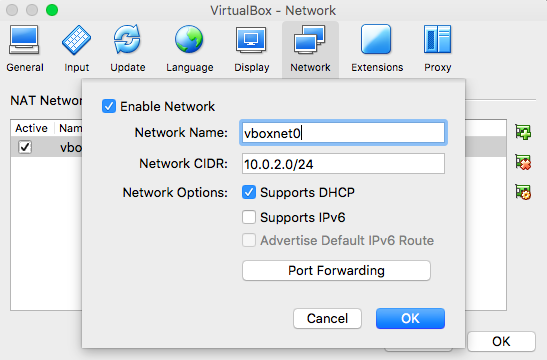
* Double-click “**VirtualBox.pkg**”, which will lead you through an installation process. 
* Congratulations, you now have **VirtualBox** installed! Go back to the first screen and run **VirtualBox** from your **Applications** folder.
* On the top pane, select **VirtualBox** -> **Preferences** -> **Network**  -> **green “+” icon**

to set up a virtual network adapter. This will automatically be named “*NatNetwork*”.

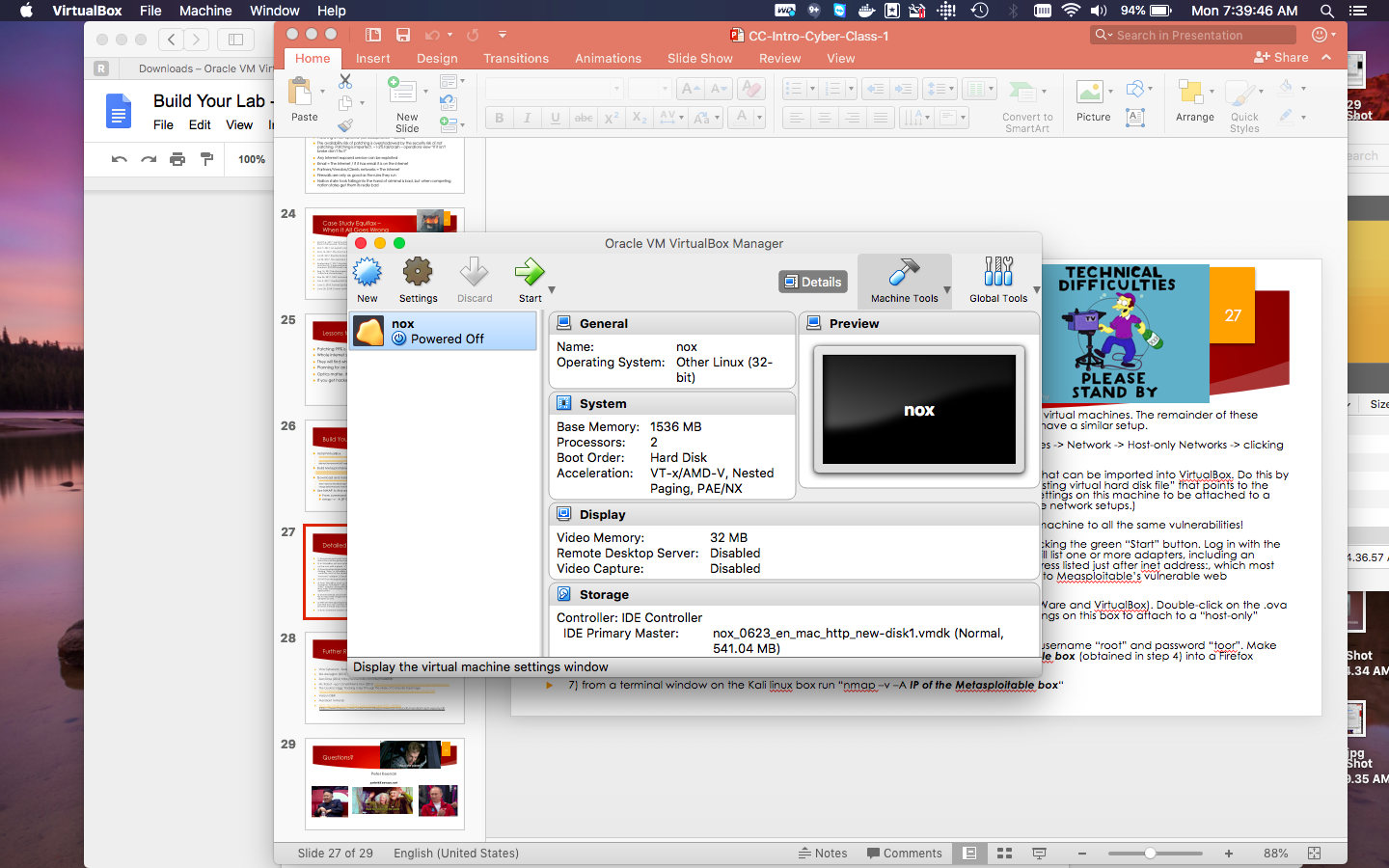
****

****

* In order to change the name, **click on the orange “gear” icon** and change it to “*vboxnet0*”. **Make sure that DHCP is enabled!** Click “OK” to save the settings.

****

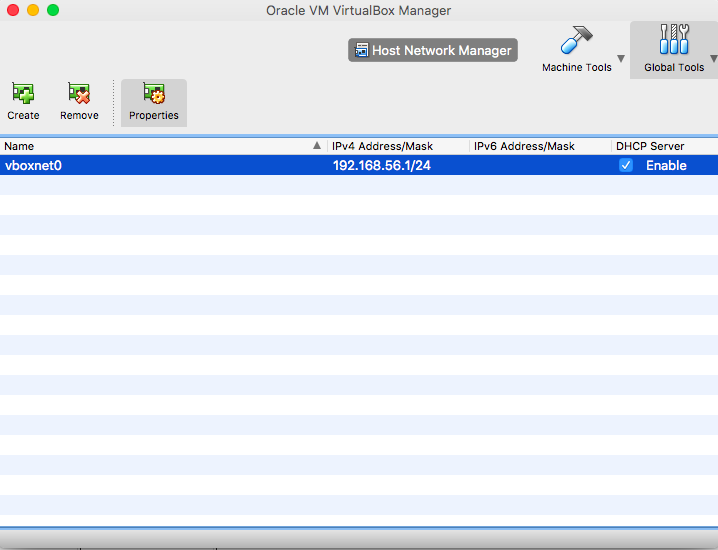
* Now, we will activate the Host Network Manager. On the home screen, select **“Global Tools”** on the top right corner.

****

* Select the icon next to the “Host Network Manager” option to get started!

****

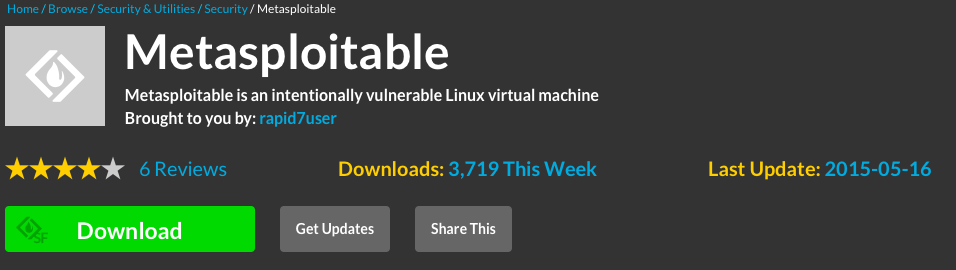
* Select “create”, which will automatically add the “vboxnet0” network and have it ready to be used by our virtual machines. Once again, **make sure to enable the DHCP Server.**

****

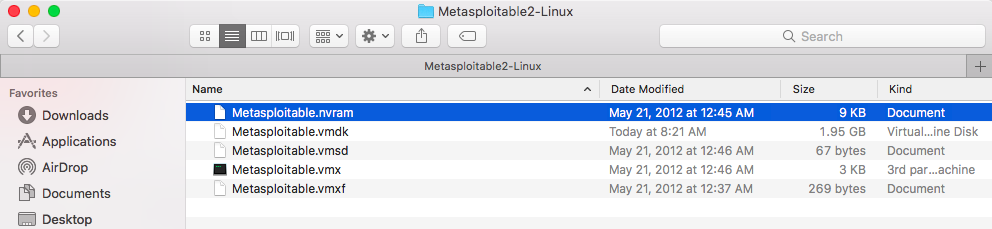
* Now that we have our VirtualBox and network setup, we can proceed with the next steps.

#### **Step 2- Downloading Metasploit 2**

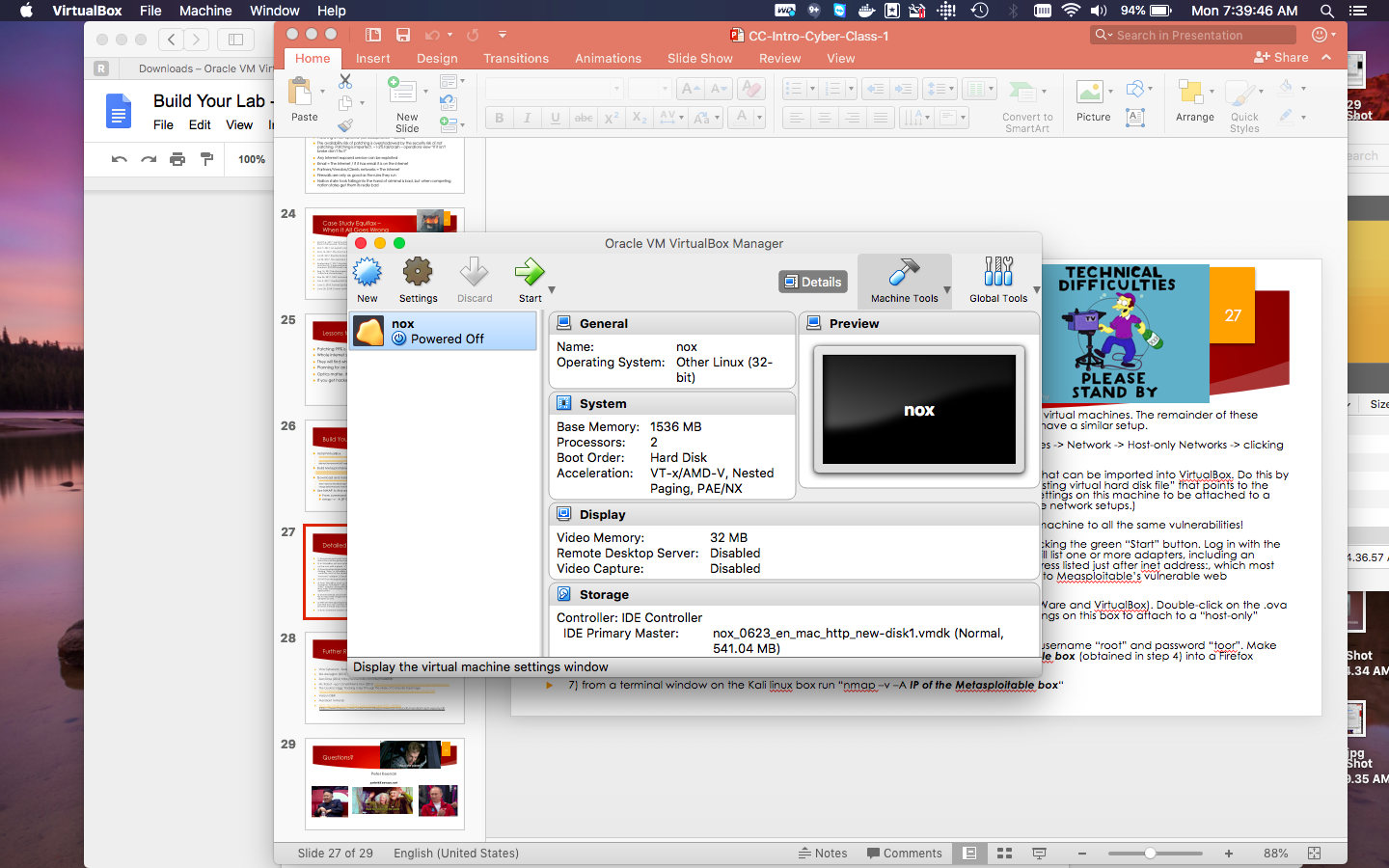
* Here is documentation on Metasploit:
  + [**https://metasploit.help.rapid7.com/docs/metasploitable-2**](https://metasploit.help.rapid7.com/docs/metasploitable-2)
* You can download Metasploit 2 from either website. This tutorial will be using sourceforge.
  + [**https://information.rapid7.com/metasploitable-download.html**](https://information.rapid7.com/metasploitable-download.html)
* [**https://sourceforge.net/projects/metasploitable/**](https://sourceforge.net/projects/metasploitable/)

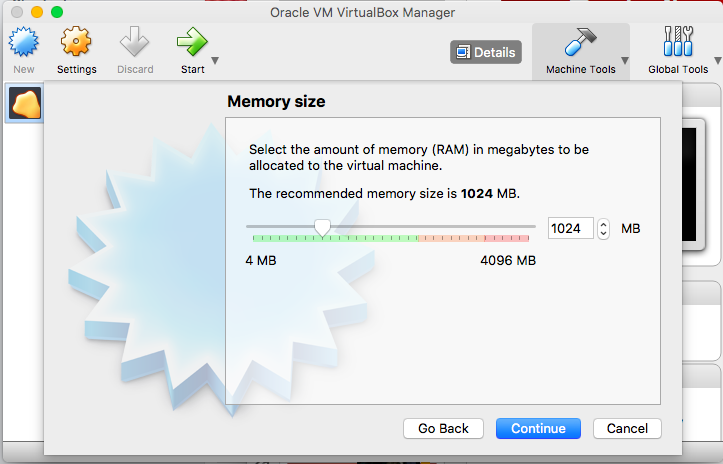


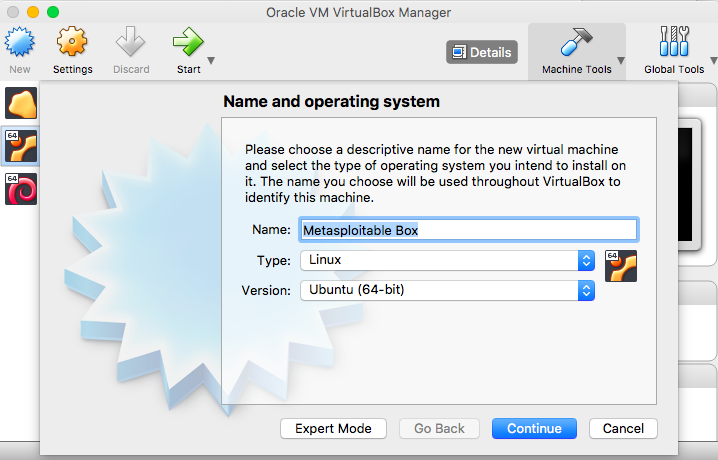
* Unzipped, this folder will contain a virtual disk **(.vmdk)** file that can be imported into VirtualBox.



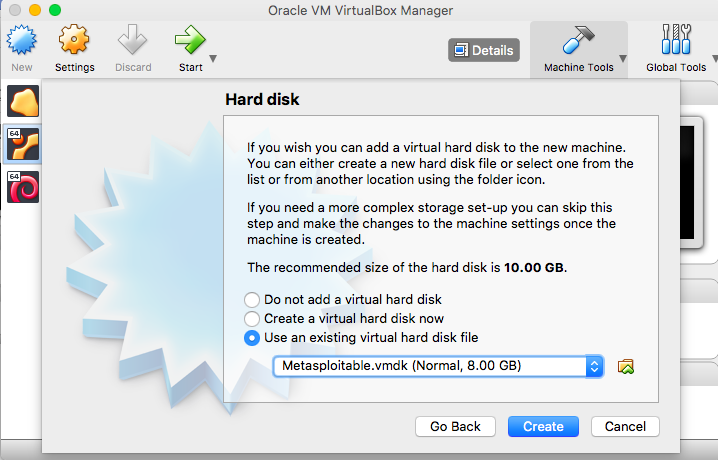
* Going back to the **VirtualBox** home screen, click **“New”** on the top menu bar to create a  **Linux Ubuntu (64-bit)** virtual machine. We will name this “Metasploitable Box”. Additionally, keep the recommended settings for memory (1024 MB).

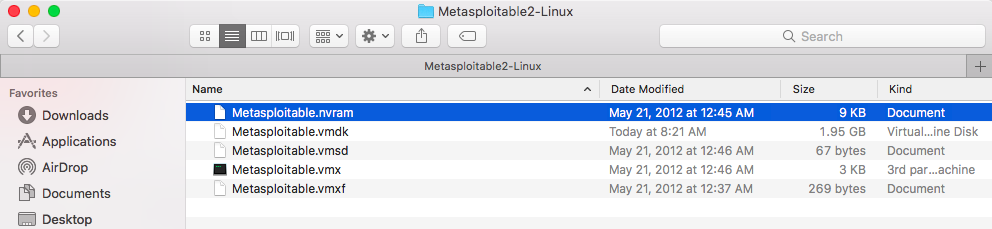
****



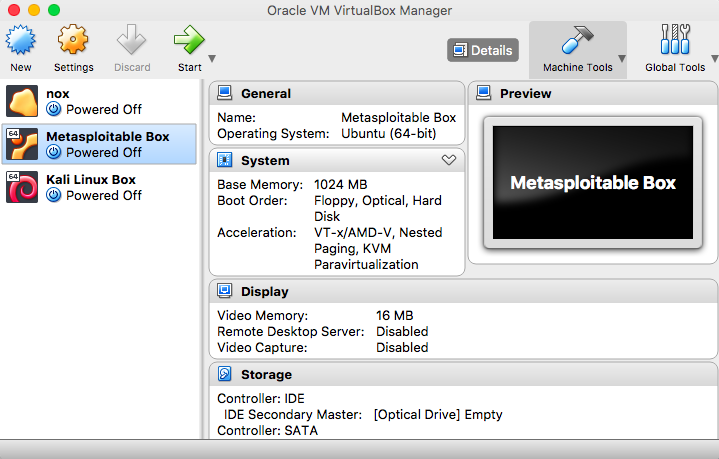


* Choose “Use an existing virtual hard disk file” and point it to the **.vmdk file** located in your unzipped Metasploitable folder that was previously downloaded.

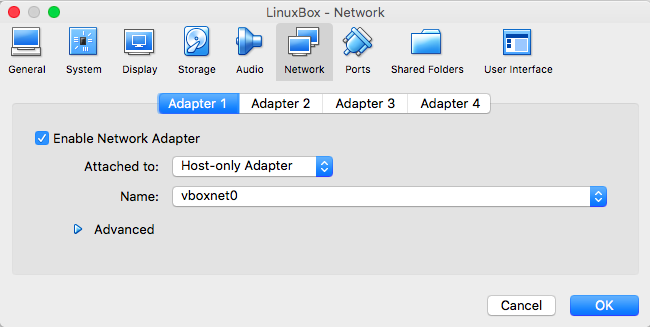




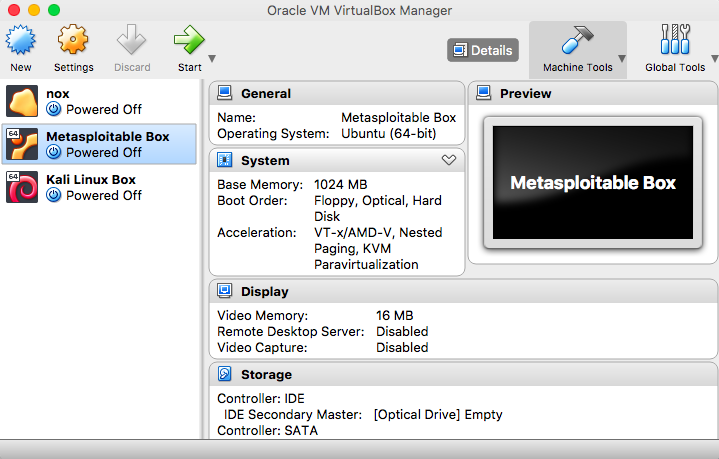
* Congratulations, you now have a new linux virtual machine! We will now change our network settings for this VM.



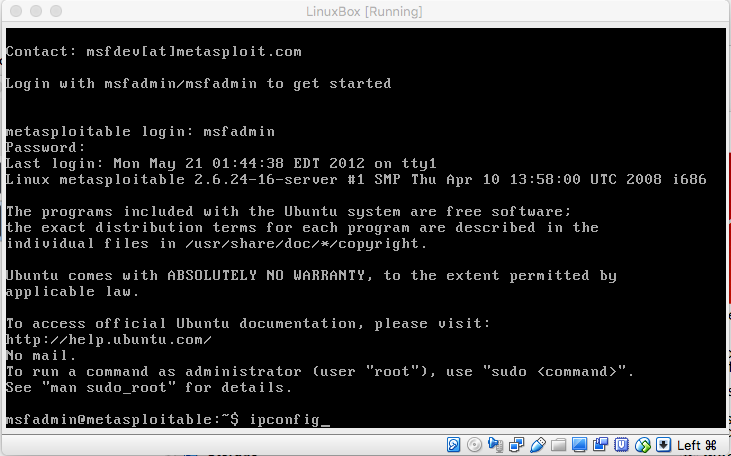
* Click **Settings** -> **Network** on the top menu bar. Select “Host-Only Adapter” and choose “vboxnet0”. **\*\*DO NOT run Metasploitable in “bridged” mode, or you will have opened your own local machine to all the same vulnerabilities\*\***



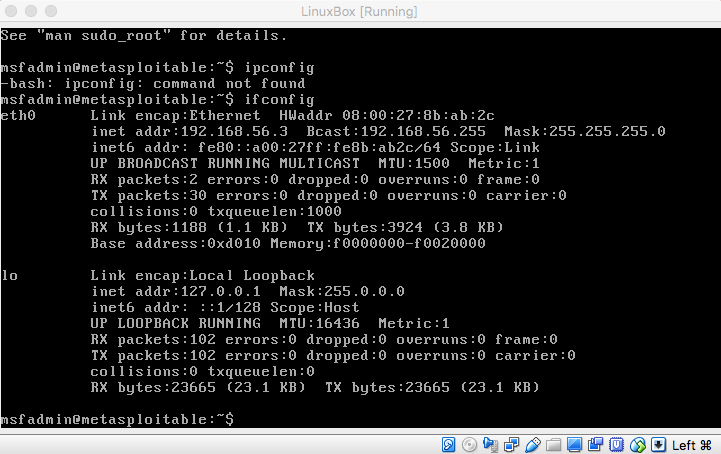
* You are all set to run your virtual machine! Once you are on the home screen, select from the sidebar **“Metasploitable”** and click “**Start**”.

****

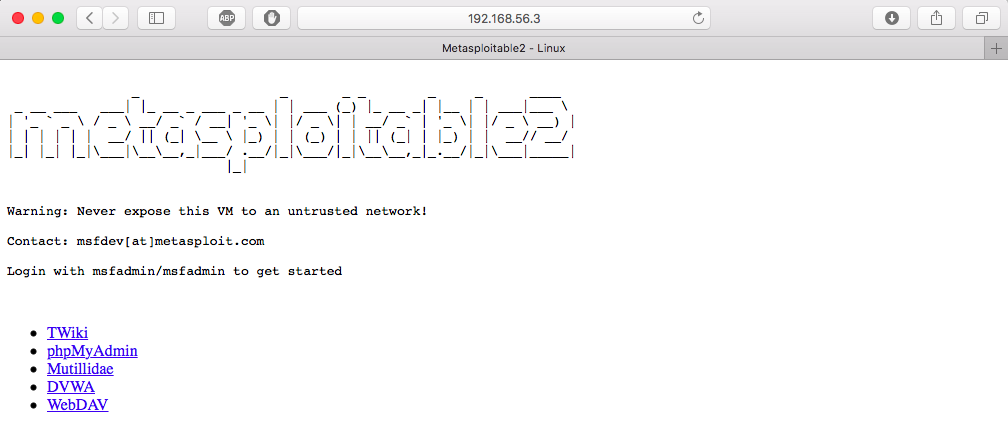
* Log in with the username: “**msfadmin**” and password: “**msfadmin**”.



* Run the command **ifconfig**. This will list one or more adapters, including an “**eth0**” adapter, along with their networking details.
* Under the **eth0** entry, note the IP address listed just after ***inet address***, which most likely looks something like **192.168.56.10x.** This is the IP address we will use later to connect to Measploitable’s vulnerable web application.



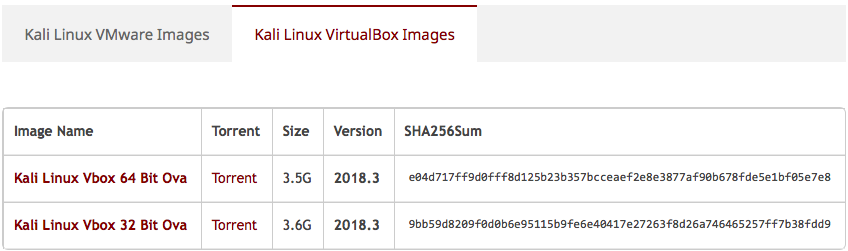
* To test your configuration, go to your browser and enter the IP in the navigation bar. This should take you to a page with a list of apps.



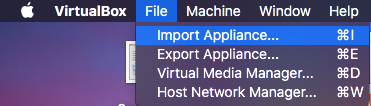
* Great job! Finally, we will install Kali Linux.

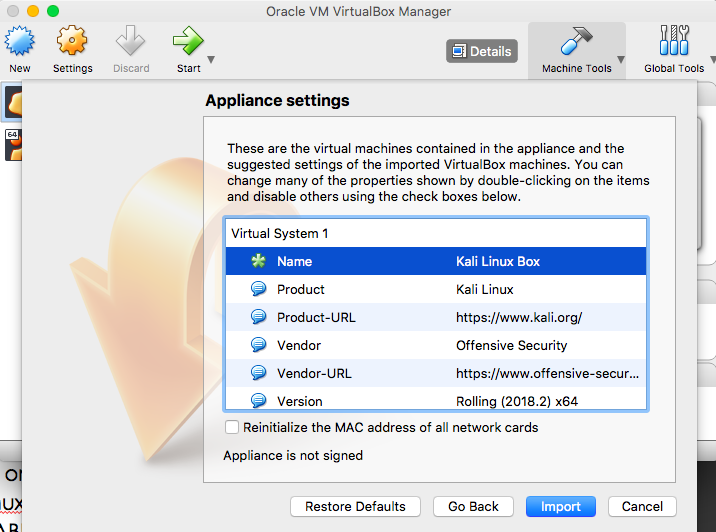
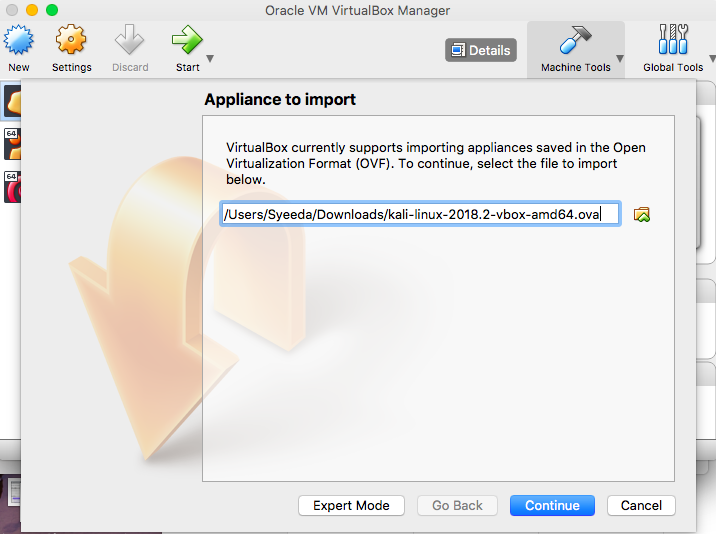
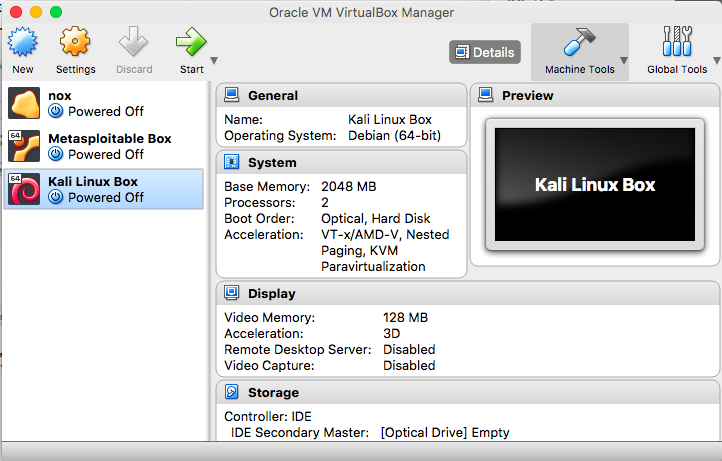
#### **Step 3 - Downloading Kali Linux for VirtualBox**

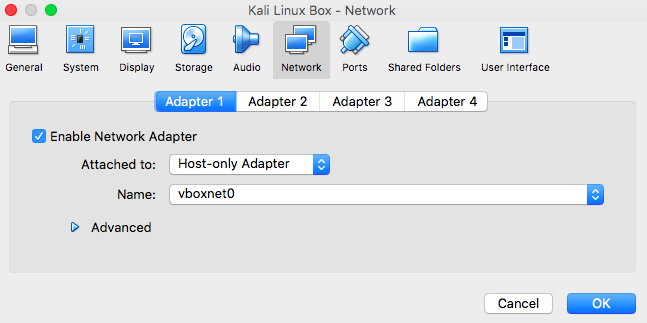
* Go to <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>
* Click on “Kali Linux VirtualBox Images” and download the Kali Linux VBox 64 Bit [OVA] file.



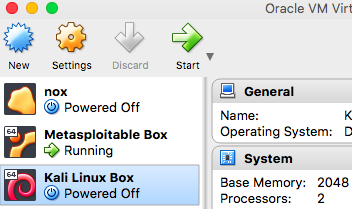
* Once you have finished downloading, go back to VirtualBox -> File -> Import Appliance. This will create a Kali Linux Virtual Machine by importing the .ova file.

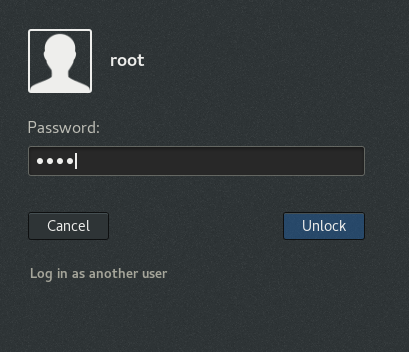


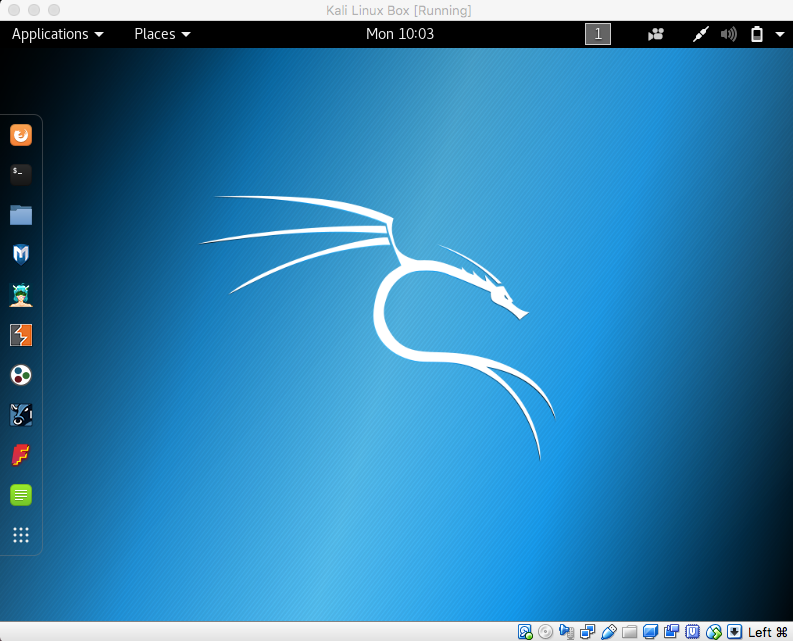
* Select the directory that contains your .ova file and click “Continue”. We will name it the “Kali Linux Box”. 
* Congratulations, you now have a Kali Linux virtual machine! As with the Metasploitable Box, we will configure the network to be “Host-Only”.
* Click **Settings** -> **Network** on the top menu bar. Select “Host-Only Adapter” and choose “vboxnet0”.



* You are all set to run your “Kali Linux Box”! **\*\*Make sure that the Metasploitable Box is running as well in the background and that you are logged in.\*\***
* Once you are on the home screen, select **“Kali Linux Box”** from the sidebar and click “**Start**”.



* Log in with the username “**root**” and password “**toor**”. 
* In the home page, click “Terminal” on the sidebar



* Run “nmap –v –A [***IP of the Metasploitable box]*** ” to find exposed services on the Metasploitable Host. Click [here](https://drive.google.com/file/d/1t9F8QRLAbZOdL6mQ5bbxxntXcV2JuDlf/view?usp=sharing) to see the results!

