eForensics Magazine

Workshop

BUILD YOUR OWN PENTEST LAB

BY PAUL JANES

250+ Pages

VOL.05, NO.10
ISSUE 09/2016, (59) NOVEMBER
ISSN 2300 6986

eForensics Magazine

TEAM

Editor-in-Chief
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Editors:

Marta Sienicka
sienicka.marta@haking.com

Marta Strzelec
marta.strzelec@eforensicsmag.com

Marta Ziemianowicz
marta.ziemianowicz@eforensicamag.com

Senior Consultant/Publisher:
Paweł Marciniak

CEO:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP
Marta Strzelec
marta.strzelec@eforensicsmag.com

Cover Design
Hiep Nguyen Duc

Publisher
Haking Media Sp. z o.o.
02-676 Warszawa
ul. Postępu 17D
Phone: 1 917 338 3631

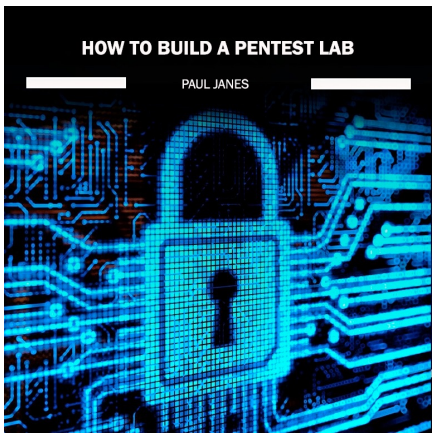
www.eforensicsmag.com

ABOUT THIS EBOOK

This eBook is based on workshop materials from our **"How to build your own pen-test lab"** online course. It does not include everything the course did - obviously, we had to leave out all videos and graded assignments. While the text is all here, the videos do teach extra information, show other types of scans and go deeper into some programs and vulnerabilities. We believe that this eBook is great for setting up the basics, but if you would like to learn more, please consider joining the course.

Your instructor:

Paul Janes, CISSP, GIAC – GISP, is an Information Security Analyst at Corning Incorporated with over 19 years of experience in IT Security, (DLP) Data Loss Prevention, Project Management and Server Management. He has been involved in creating his own ethical hacking lab and enhancing his skills as an ethical hacker.



Course format:

- The course is self-paced – you can visit the training whenever you want and your content will be there.
- 18 CPE points
- Once you're in, you keep access forever, even when you finish the course.
- There are no deadlines, except for the ones you set for yourself.
- We designed the course so that a diligent student will need about 18 hours of work to complete the training.
- You time will be filled with reading, videos, and exercises.

SEE COURSE ON WEBSITE

Table of contents

PAGE 7: Pre-Course Materials

- Why Do I Need a Pen Test Lab
- Definitions
- Creating Directory Structure For the Course\
- Download Virtual Images
- Acquire Nessus Licenses

PAGE 13: Module 1 The Build:

- Definitions
- Some Basic Linux Commands You Need to Know
- Installation of VMPlayer and Virtual Box. You Decide, We Will Cover Both.
- Setup of Our Penetration Testing System – Kali Linux Distribution
- Setup a Linux Client as a Virtual Machine
- Setup Our First Vulnerable Machine Metasploitable2
- Setup Our Second Vulnerable Machine Bee-box (BWAMP)

PAGE 64: Module 2 Port Scanning:

- Nmap and Zenmap Installation
- Nmap Basic Scanning
- ZenMap Basic Scanning
- db_map Scanning

PAGE 147: Module 3 Vulnerability Scans:

- Installation Nessus Vulnerability Scanner Windows
- Installation Nessus Vulnerability Scanner Kali Linux
- Installation Nessus Vulnerability Scanner Ubuntu
- Basic Nessus Scanning Metasploitable2
- Basic Nessus Scanning Bee-box

PAGE 249: Module 4 Advanced Scanning and Reporting:

- Nessus Advanced Scans
- Nmap Advanced Scans
- Metasploit Reporting

PRE-COURSE

Before we start the course you have to ask yourself:

Why Do I Need A Pen Test Lab?

Why do you need a PenTest lab?

1. Hacking and or scanning machines without consent is against the law in most countries.

2. To become an effective penetration tester or ethical hacker you need to practice to enhance your skills

3. Freedom to install, run, and configure any tool you like

Now that we know the why let's define the requirements. I assumed you are using a single computer for this activity.

Hardware Requirements

- Hard Disk – 200GB of disk space or more depending on the number of guest operating systems you plan on installing. A good use of an external hard drive.

- CPU – I recommend the latest technology but any of the I3/I5/I7 families are ok. The more processing power you have the better

- Memory – 2 GB minimum, I recommend 8GB or 16GB. Memory is critical. The more memory you have the more virtual systems you will be able to have running at one time

Virtualization Software

You will also have to decide what virtualization software you plan to use (Virtual Box or VMPlayer). Select one and follow what we are doing in class with the other so you learn how to use both.

Definitions

Kali Linux – Is the most advanced Penetration Testing environment available and is based on the Linux operating system. It has a large number of pen testing tools included. It includes tools for information gathering, vulnerability analysis, wireless attacks, web applications, exploitation tools, forensics tools, stress testing tools, sniffing and spoofing, password attacks, maintaining access, reverse engineering, reporting tools, and hardware hacking. For more information visit the website at https://www.kali.org/

UBUNTU – Is an open source desktop operating system which is based on the Debian Linux. It includes all the basic tools you need and could be used instead of Windows…

Metasploitable2 – Per Rapid7's website, "The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download and ships with even more vulnerabilities than the original image. This virtual machine is compatible with VMware, VirtualBox, and other common virtualization platforms. By default, Metasploitable's network interfaces are bound to the NAT and Host-only network adapters, and the image should never be exposed to a hostile network."

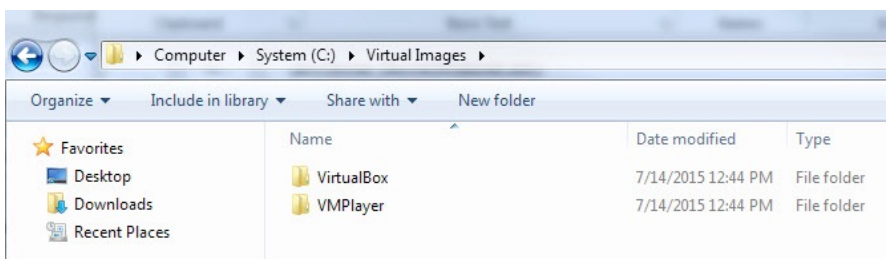
Bee-Box – Is an open source virtual machine with numerous web application vulnerabilities.

Directory Structure

Open up a command prompt (get used to the command line we will be using it throughout the course. We will also make use of my documents or file explorer as well.

1. `cd\` (to get to the root of the drive where you will store your virtual images and run your virtual machines)
2. `mkdir Vms` (This is where you will store your virtual Machines)
3. `mkdir "Virtual Images"` (Be sure to use the quotes or you will have a directory called virtual)
4. `cd Virtual Images` (Change directory to Virtual Images)
5. `mkdir VirtualBox` (Where you will store all your VirtualBox images)
6. `mkdir VMPlayer` (Where you will store all your VMPlayer images)

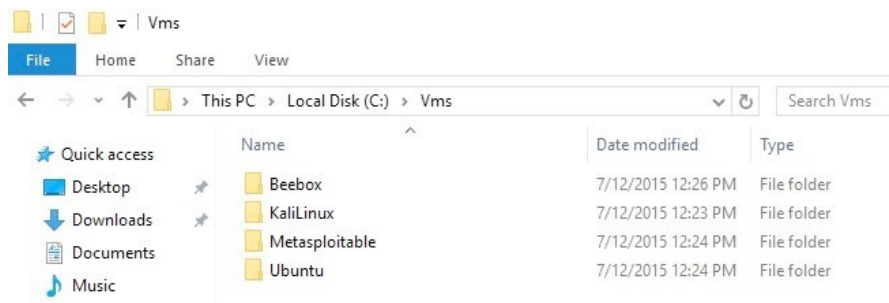
When you look at the structure from my computer it will look like this:



Now you will create the directory structure for your actual VMs.

- `CD Vms`
- `Mkdir KaliLinux`
- `Mkdir Ubuntu`
- `Mkdir Metasploitable`
- `Mkdir BeeBox`

When you look at the structure from my computer or file explorer it will look like this:



At this point you need to download your images. This is going to take a while as some of these images are 2.5gbs in size.

Open your browser and connect to http://www.osboxes.org/. OS Boxes is a great place to get both VMware and VirtualBox images.

Select VM Images. Now you have to make a decision as to whether you are going to use VirtualBox or VMPlayer. We will start with VirtualBox. You can skip to VMPlayer if that is your selection.

VirtualBox

- Select VirtualBox Images
- Select Kali Linux
- Download VirtualBox (VDI) image
- Select the OS version you have: either 32bit or 64bit

Select download (It's 2.5GBs so it will take a while). Time to go get a snack and read the latest eForensics magazine.

Once the download is complete hit the back button on your browser and select Ubuntu. Select the VirtualBox (VDI) Image, again select 32bit or 62bit image and download (835MB) …have your eForensics magazine handy…

Move the images from your downloads directory to your \Virtual Images\VirtualBox folder.

Download:
http://sourceforge.net/projects/metasploitable/ from SourceForge and move it to your \Virtual Images\VirtualBox folder.

Connect to:
http://sourceforge.net/projects/bwapp/files/bee-box from SourceForge.

Select bee-box_v1.6.7z to download and then move the file to your \Virtual Images\VirtualBox folder.

VMPlayer

- Select VMware Images
- Select Ubuntu
- Download VMware (VMDK) image
- Select the OS version you have either 32bit or 64bit

Select download (It's 853MB so it will take a while). Time to go get a snack and read the latest eForensics magazine.

I have had some issues with the Kali VM so we will go directly to offensive security's website: https://www.offensive-security.com/kali-linux-vmware-arm-image-download/

Select either 32 bit or 64 bit and download to your \Virtual Images\VMPlayer folder.

The download is 2.5 gbs so have your eForensic magazine handy…

Move the images from your downloads directory to your \Virtual Images\VMPlayer folder.

Download:
http://sourceforge.net/projects/metasploitable/ from SourceForge and move it to your \Virtual Images\VMPlayer folder.

Connect to:
http://sourceforge.net/projects/bwapp/files/bee-box from SourceForge.

Select bee-box_v1.6.7z to download and then move the file to your \Virtual Images\VMPlayer folder.

Nessus Licensing and Activation Codes

Before you can install Nessus you will need valid activation codes.

Connect to:
https://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code

Select Nessus Home Free Register Now. Enter your name, email address, country, and select **I agree to the terms of service**. Open up the activation email to see the activation code.

Create a text file on your desktop called Nessus.txt. Copy the activation code into the file and save it. We need two activation codes so go through the process again to obtain the second code. The codes can only be used once.

File Extraction

If you don't have WinZip you can use its open source counterpart 7-zip. 7-zip will extract and compress 7z and zip files amongst many others.

Connect to http://www.7-zip.org/download.html

Select the download that matches your system either 32 bit or 64 bit. Run the installer once the download is complete, accept all the defaults.

Once the installation is complete run the application.

VirtualBox File Extraction (Skip to VMPlayer if that is your choice)

BeeBox:

1. Select the Virtual Images\VirtualBox folder and you will see 3 7z files and a zip file
2. Select bee-box_v1.6.7z
3. Hit the extract button and specify Vms\Beebox as your location
4. Hit OK and OK again and watch as the files are extracted

KaliLinux:

1. Select VirtualBox\Kali_Linux_1.1.0-32 or 64bit.7z file
2. Hit the extract button and specify Vms\KaliLinux as your location
3. Hit OK and OK again and watch as the files are extracted

Metasploitable:

1. Select the VirtualBox\metasploitable-linux-2.0.0.zip file
2. Hit the extract button and specify Vms\Metasploitable as your location
3. Hit OK and OK again and watch as the files are extracted

Ubuntu:

1. Select the VirtualBox\Ubuntu_15.04-64 or32bit.7z file
2. Hit the extract button and specify Vms\Ubuntu as your location
3. Hit OK and OK again and watch as the files are extracted

That completes the extraction of all your VirtualBox images.

VMPlayer File Extraction

BeeBox:

1. Select the Virtual Images\VMPlayer folder and you will see 3 7z files and a zip file
2. Select bee-box_v1.6.7z
3. Hit the extract button and specify Vms\Beebox as your location
4. Hit OK and OK again and watch as the files are extracted

KaliLinux:

1. Select the VMPlayer\Kali_Linux_1.1.0-32 or 64bit.7z file
2. Hit the extract button and specify Vms\KaliLinux as your location
3. Hit OK and OK again and watch as the files are extracted

Metasploitable:

1. Select VMPlayer \metasploitable-linux-2.0.0.zip file

2. Hit the extract button and specify Vms\Metasploitable as your location

3. Hit OK and OK again and watch as the files are extracted

Ubuntu:

1. Select the VMPlayer \Ubuntu_15.04-64 or 32bit.7z file

2. Hit the extract button and specify Vms\Ubuntu as your location

3. Hit OK and OK again and watch as the files are extracted

This completes the extraction of all your VMPlayer images.

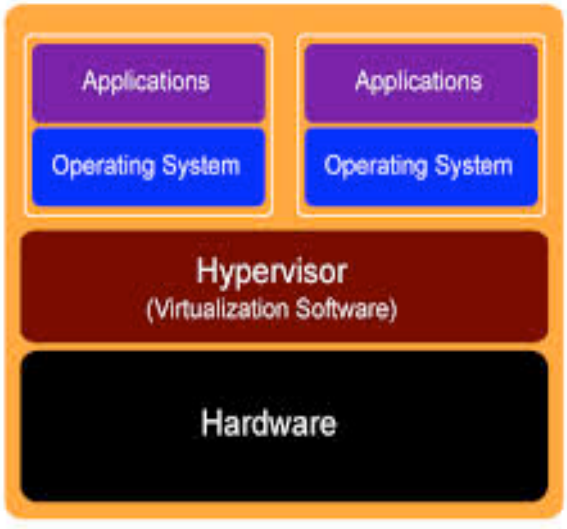
This completes the Pre-Course Material. Can't wait to see you in Module 1 where the real fun begins…

MODULE 1
THE BUILD

Welcome to Module 1 of How to Build A Pen Test Lab. We will be covering the following material:

- Virtualization Software Discussion and Definitions
- Some Entry Level Linux Commands
- Hands on Software installation and configuration
- Kali Linux Update Process

Virtualization Software



Server with Virtualization Software and Virtual Machines

In the past, physical machines were your only option to install operating systems and applications. This presented an issue for those of us in the technology business as we needed stacks of hardware in order to accomplish the tasks we are about to undertake. Fortunately,with the advent of virtualization software we are now able to have multiple machines running on a single computer which are sharing the same resources.

Today we have multiple options such as VMware, VirtualBox, Xen, and Microsoft's Hyper-V to choose from. Some of the software costs money, but we also have free options to choose from. For this course we are going to utilize VirtualBox and VMPlayer. VirtualBox is an open source option which has been developed by Oracle. VMPlayer is a free limited version of it's VMware Workstation software.

VMPlayer

Free virtualization software that lets you run multiple virtual machines. The free version is meant for personal use. If you plan on using the software for a business, then you need to pay for the VMware Workstation software; this version also offers additional benefits such as the ability to take snapshots for backup purposes.

VirtualBox

Free virtualization cross-platform software that is used to run multiple machines. It has its own native extension .vbox but also makes use of the vmdk extensions so you can run VMware builds on VirtualBox. It has the additional ability of taking snapshots for backup purposes.

Linux Commands

Since we will be working with Kali Linux, you will be required to have a basic understanding of Linux commands.

man – In Linux this is the " HELP "command. It provides you with information on each and every Linux command. This is important as there are some basic differences based on the version of Linux you are using. Some examples are Debian, Fedora, Red Hat, and openSUSE. The version of Linux that we will be using is Debian.

Example: `man ls`

ls – This is similar to the windows Dir command as it lists the files in the current directory. You can also list another directory.

Example `ls` *or* `ls Downloads`

cd – Is the same as the windows command to change the current working directory.

Example: `cd Downloads`

pwd – prints out the current working directory

cp – copy a file

mkdir – is the same command in windows which creates a new directory. We used this command in the pre-course.

Example: `mkdir Hacking`

cat – prints out the contents of a file to the screen.

Example: `cat eForensics.txt`

chmode – changes the permissions on a file.

Example: `chmode +x eForensics.txt`

whoami – displays the current username.

passwd – changes the password of a user.

Example: `passwd Fred`

ping – sends an echo request to another node on the network to validate whether it is on the network or not.

Example: `ping 192.168.1.128`

ifconfig – Provides IP address details based on each network interface. It is the equivalent to the Windows ipconfig command. We will use this to obtain the necessary IP addresses for scanning.

sudo – Allows a user to run commands as another user. Often used to run root commands to install software.

Example: `sudo apt-get update`

apt-get update - downloads the latest package files

apt-get upgrade – installs the package updates

apt-get dist-upgrade – updates the software and tools

clear or ctrl-l – clears the screen

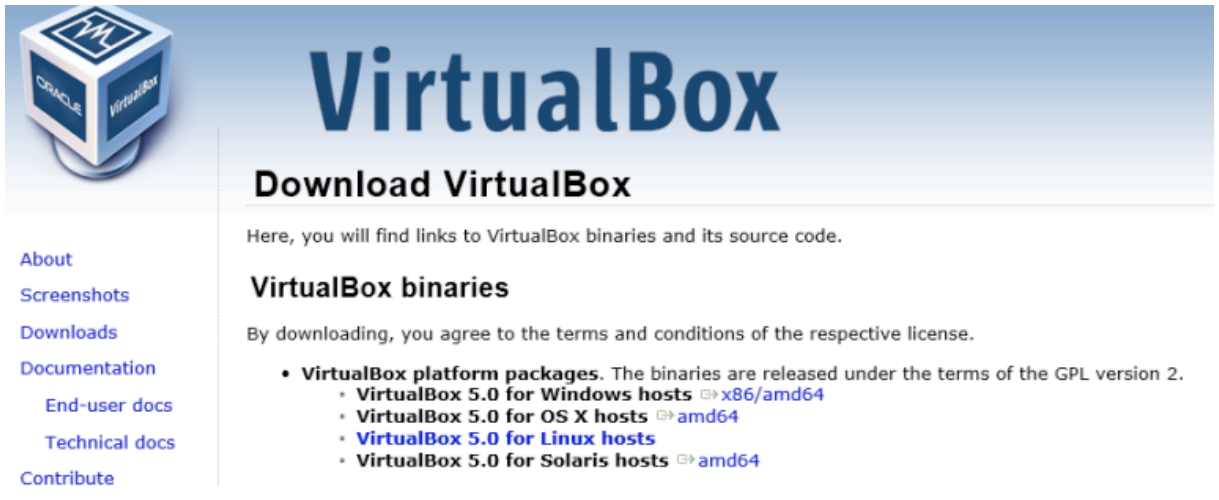
exit or ctrl+shift+q – exits the terminal session

Virtualbox

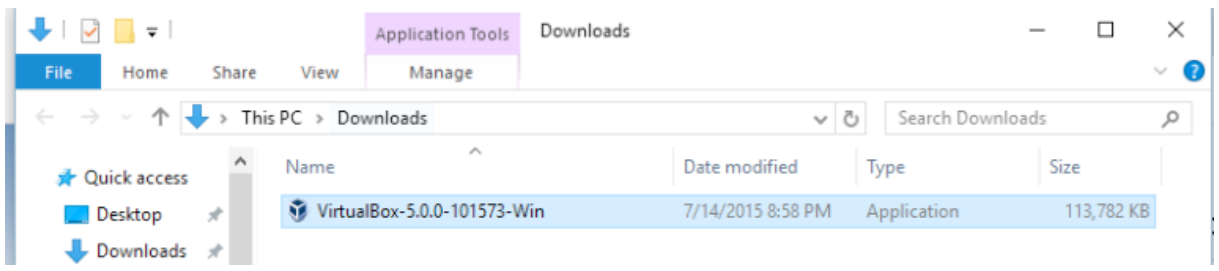
Download and Install Virtual Box

Connect to https://virtualbox.org/wiki/Downloads

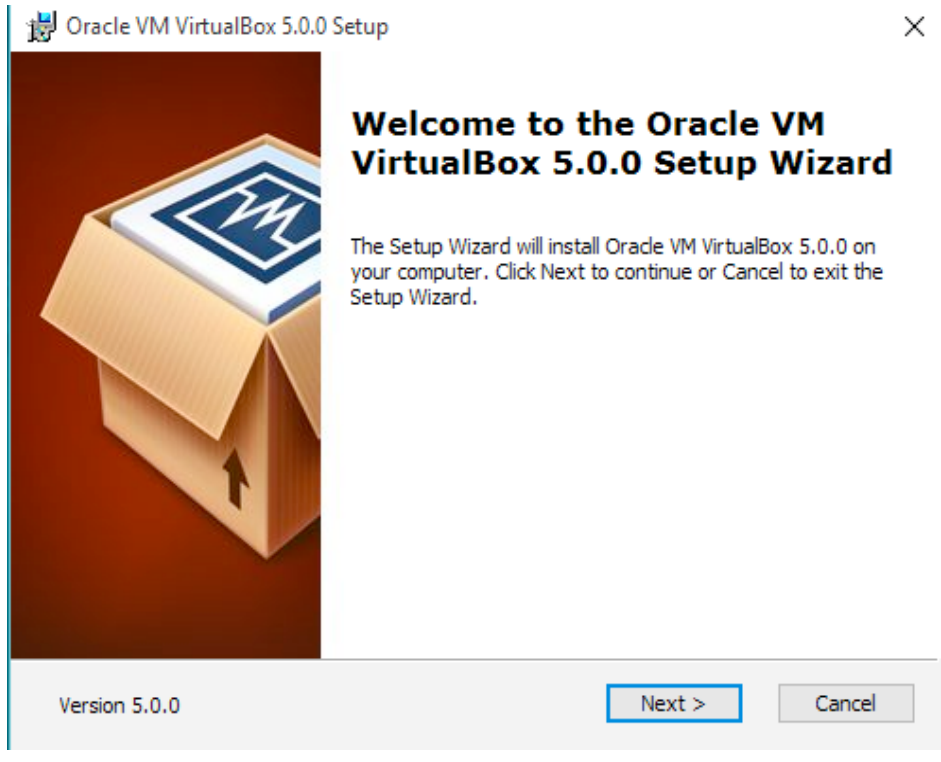
Select VirtualBox 5.0 for **Windows hosts x86/amd64**



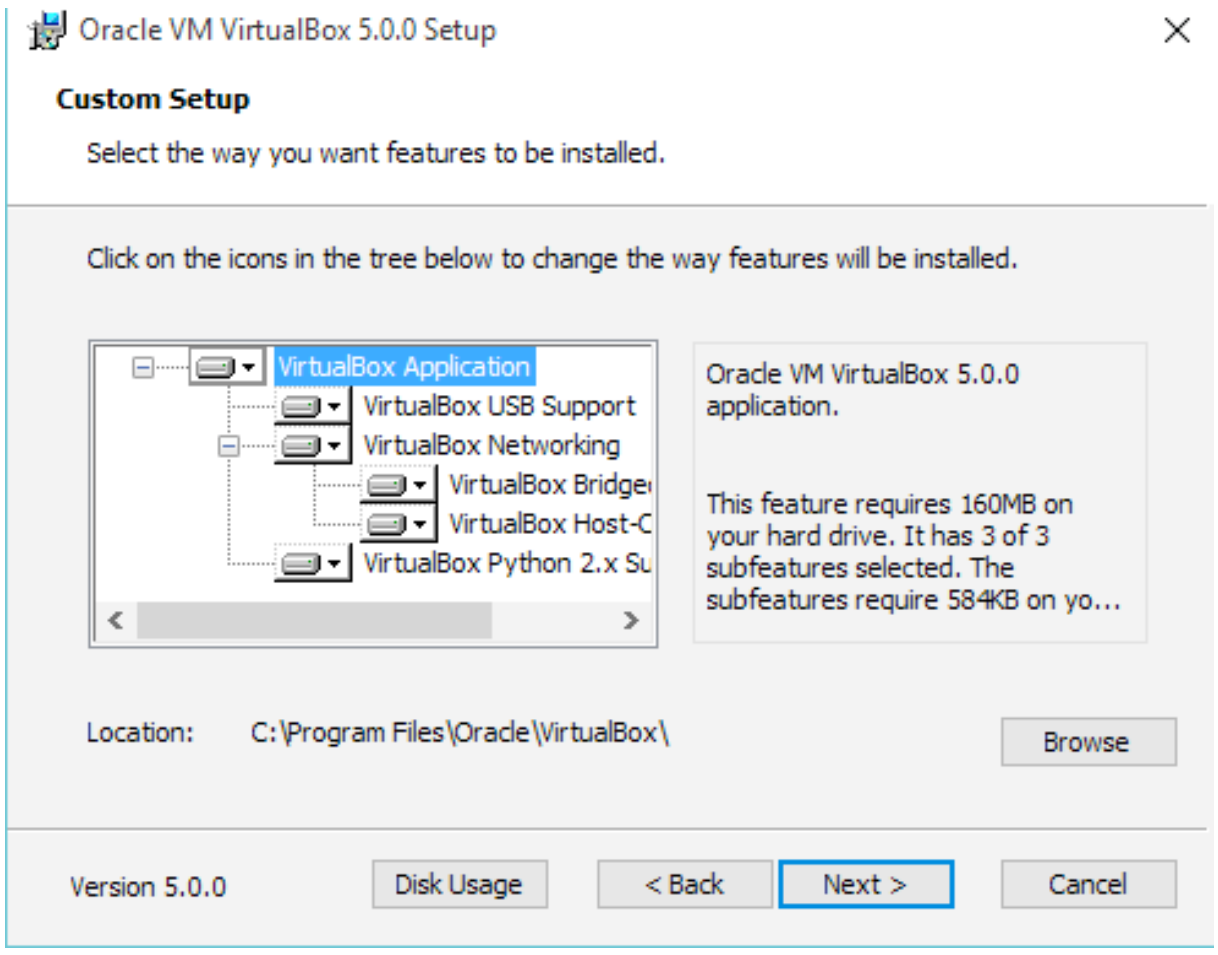
Open your downloads directory and run **VirtualBox-5.0.0.0-101573-Win.exe**



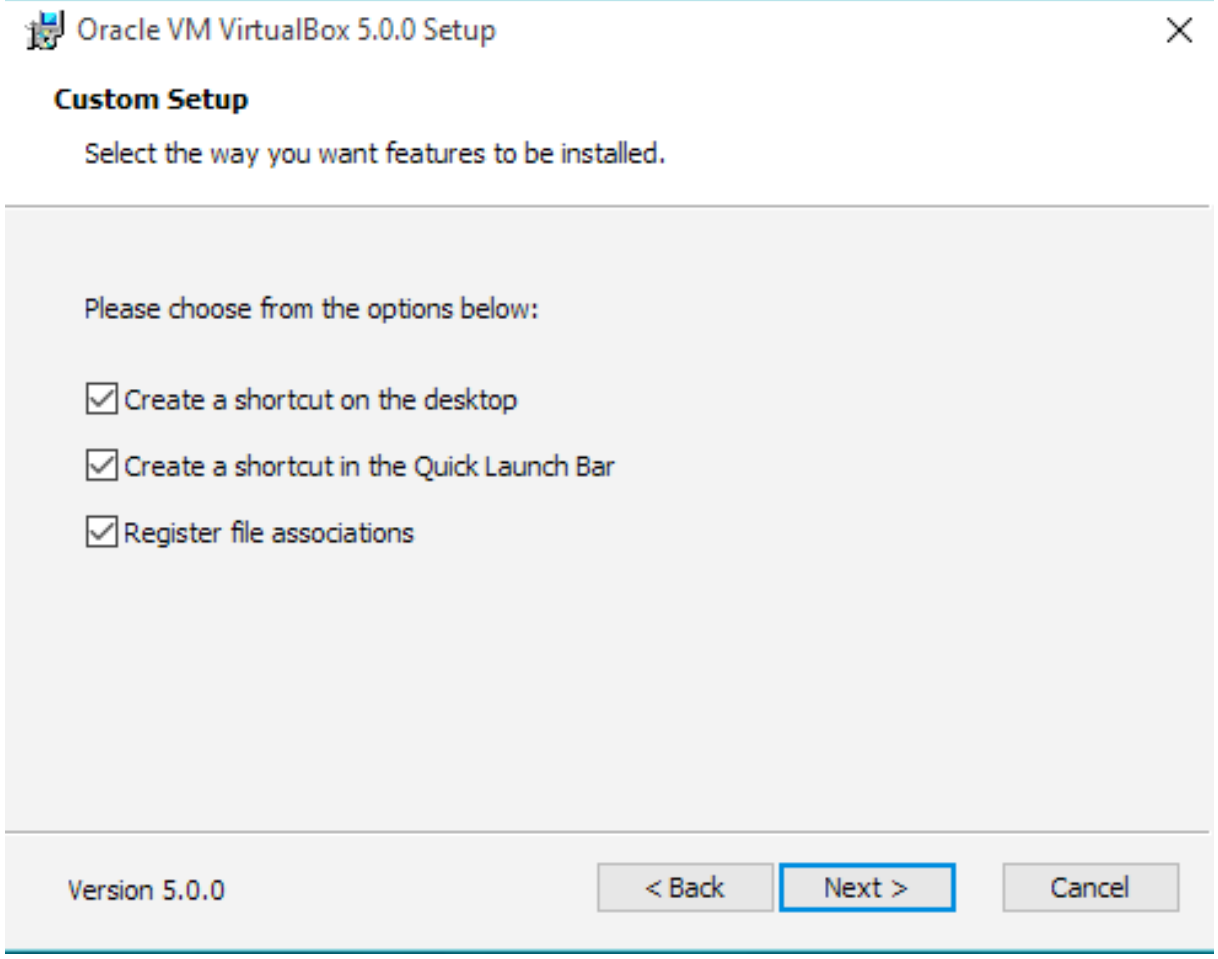
The installer will show the following:



Click **Next.**

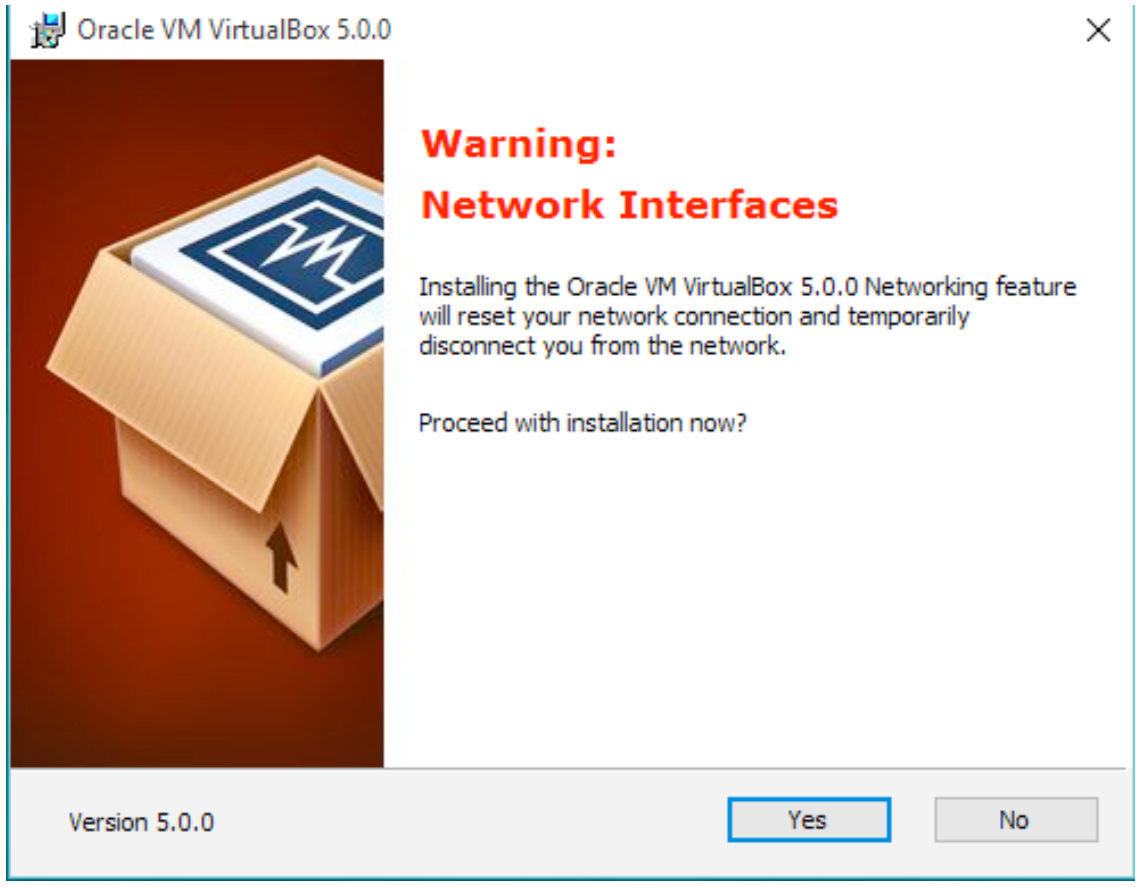


Accept the default location and **Select Next.**

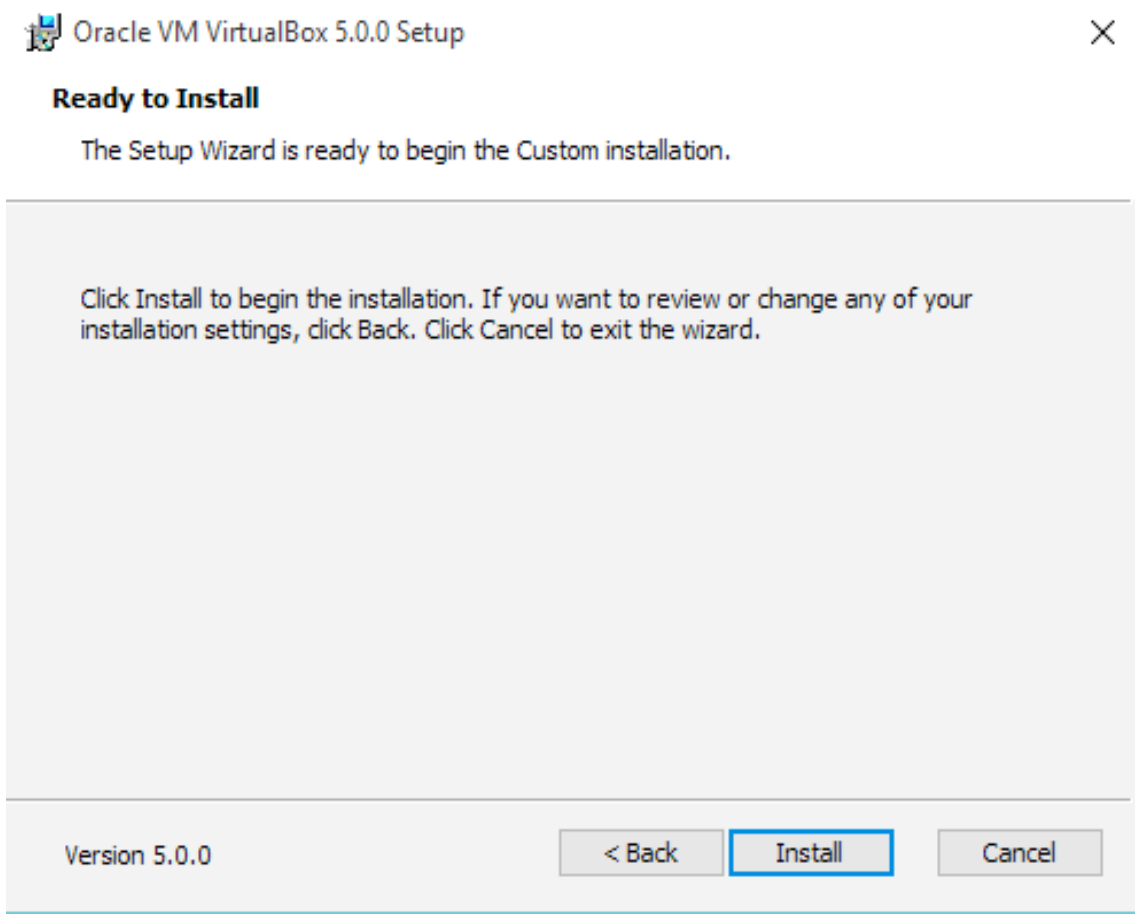


At the **Custom Setup:** accept the defaults and **Select Next.**

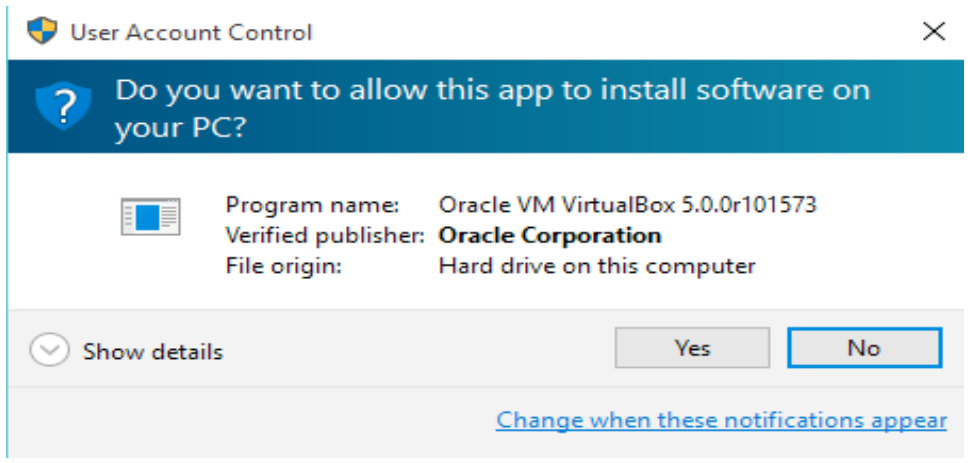
You will now get a Warning Network Interfaces message. Select **Yes.** You will temporarily lose network connectivity during the configuration.



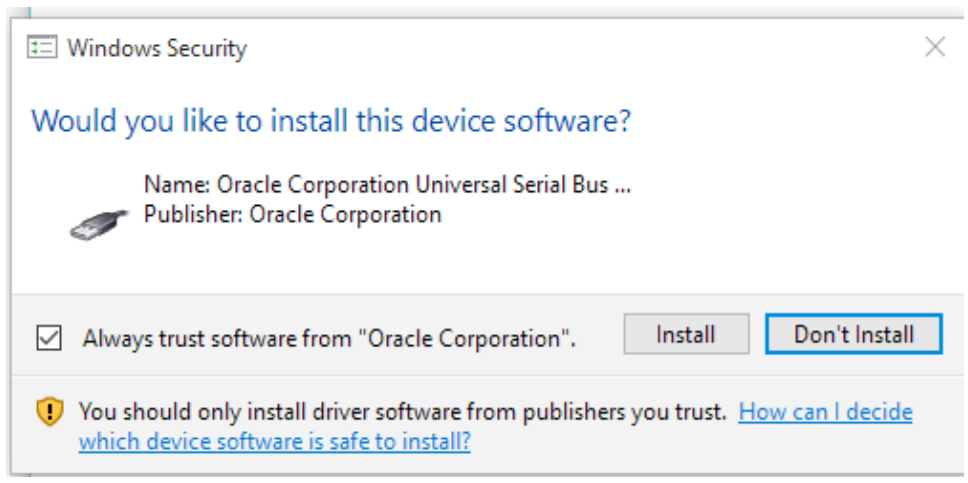
At this point you are Ready to Install. Select I**nstall**



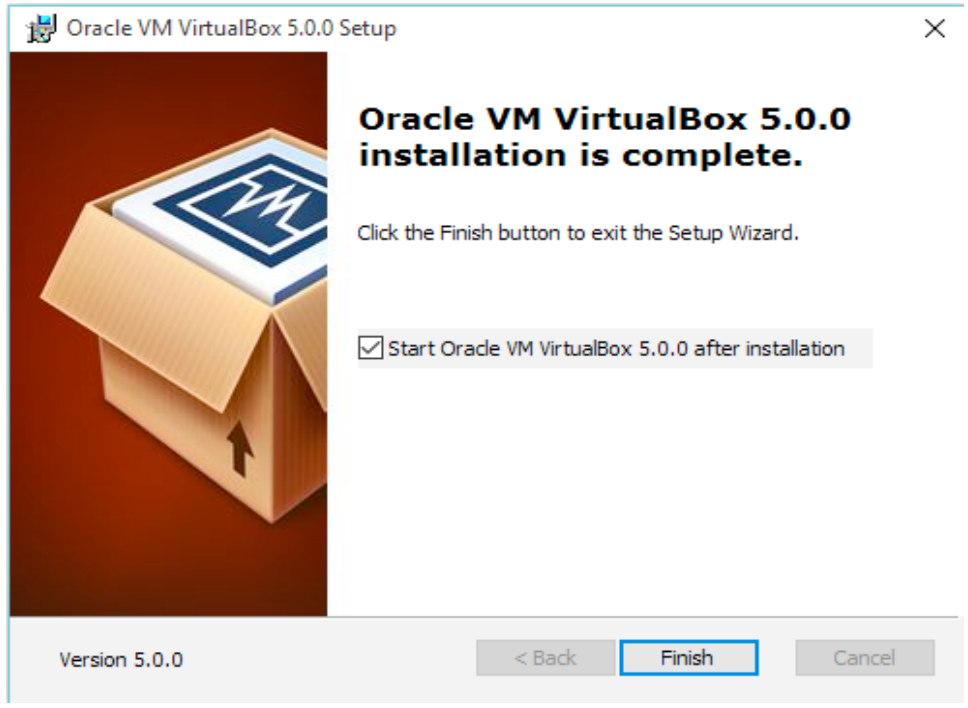
You may get a popup from User Account Control confirming your wishes to install the software. Select **Yes**.



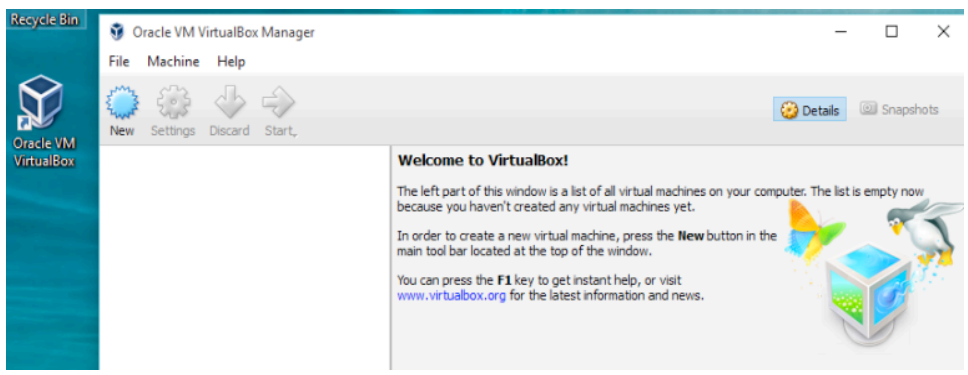
Now you will be asked if you want to install this driver. Select **Yes:**



Select **Finish** and Virtual box will start automatically.

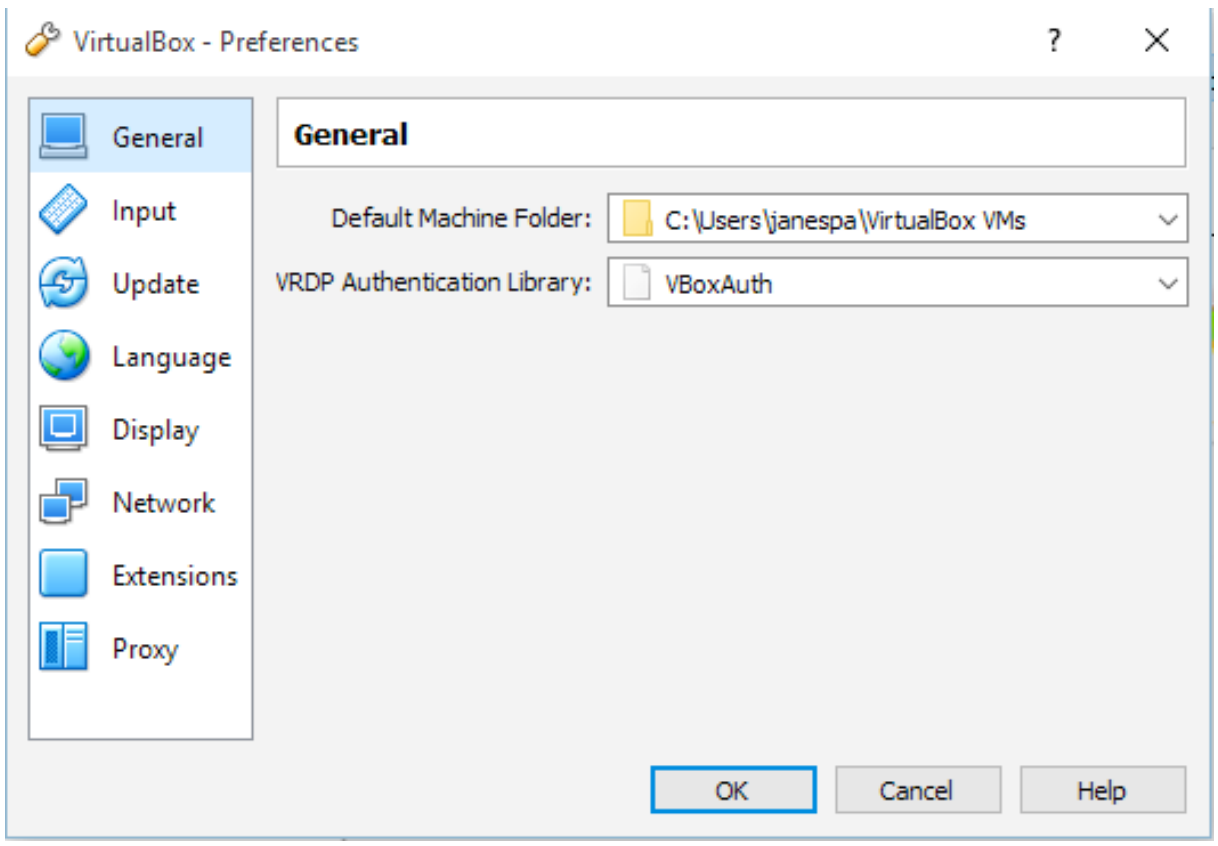


You will be greeted with this Welcome to VirtualBox! Screen.



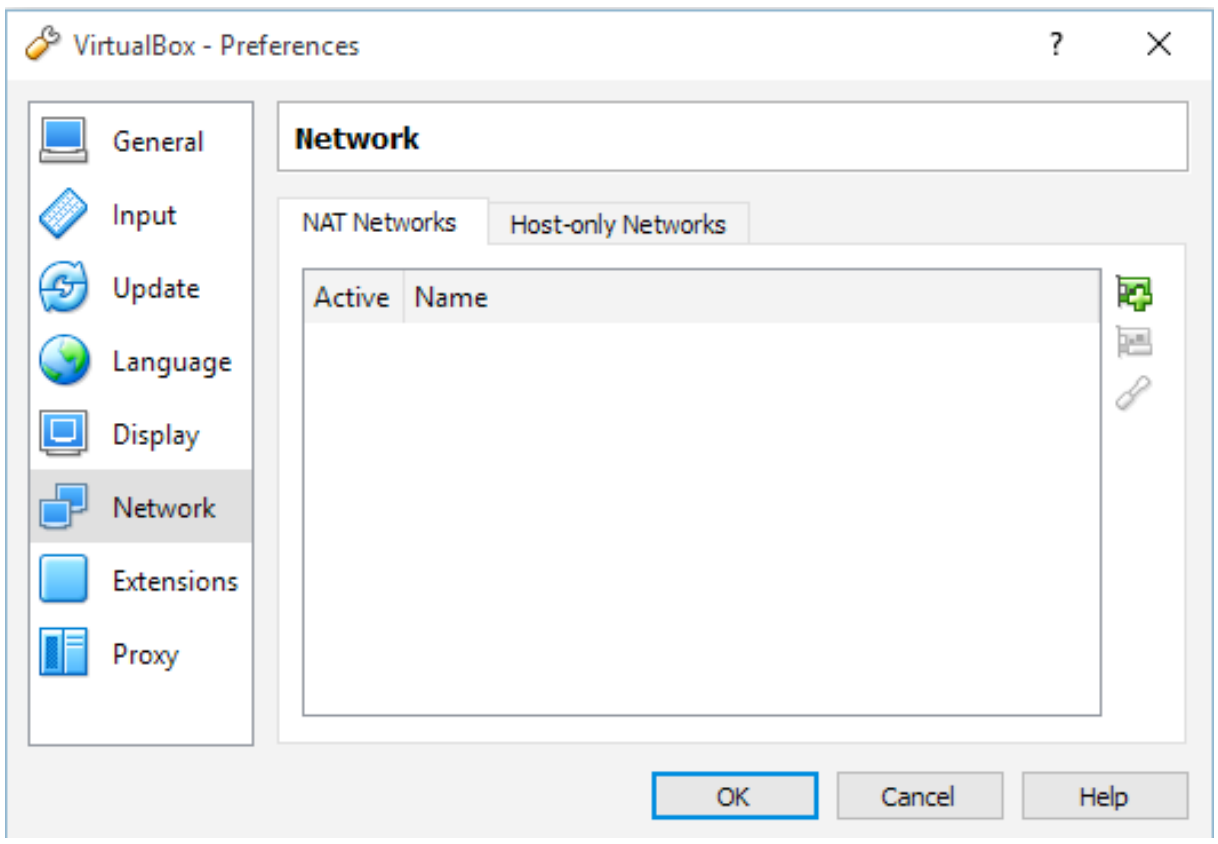
Now let's review some of the settings. Click on **File/Preferences** or hit **Ctrl+G.**

Note the Default Machine Folder location. This is where all your virtual machines will be stored:

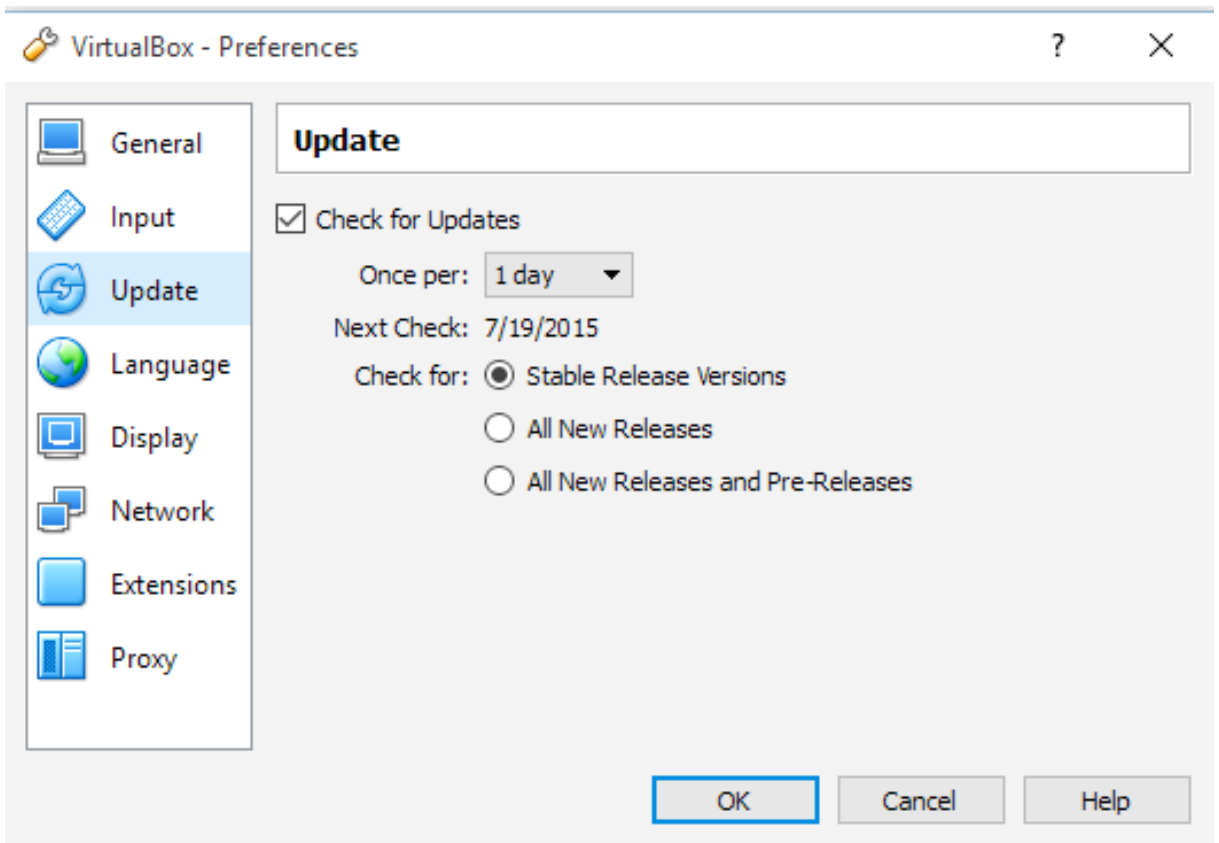


Select **Update.**

You will notice that by default VirtualBox will Check for Updates on a daily basis and will only update on Stable Release Versions.



Select **Network** and you will notice it only shows NAT and Host-only Networks. Select OK. We will now review what Virtual Networks are.



NAT – Network Address Translation

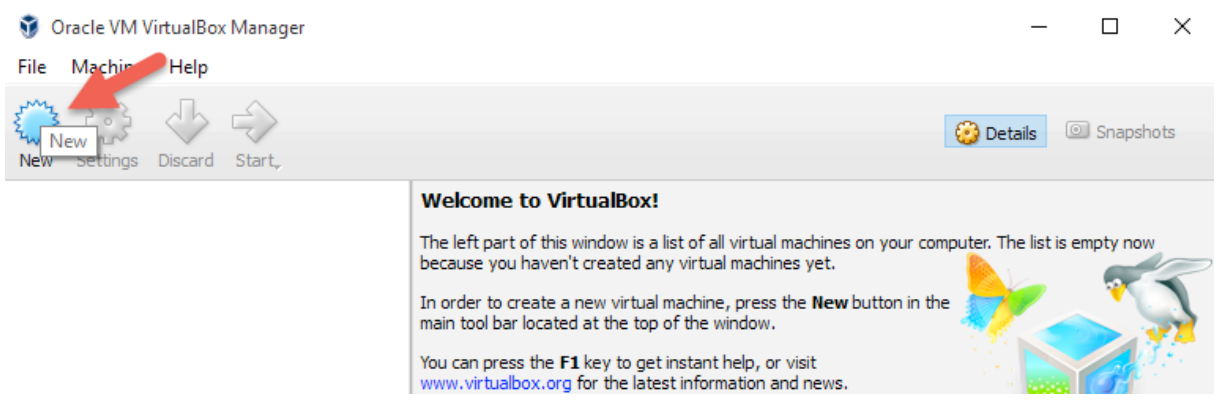
Just like your home network with a wireless router, the VM will be assigned in a separate subnet. For example, 192.168.6.1 is your host computer, and the VM is 192.168.6.3. Your VM can access outside networks like your host, but there is no outside access to your VM ; it's protected.

Host-only Network: The VM will be assigned one IP, but it's only accessible by the box VM is running on. No other computers can access it.

Bridged: Your VM will be in the same network as your host. If your host IP is 172.16.120.45, then your VM will be similar to 172.16.120.50. It can be accessed by all computers in your host network.

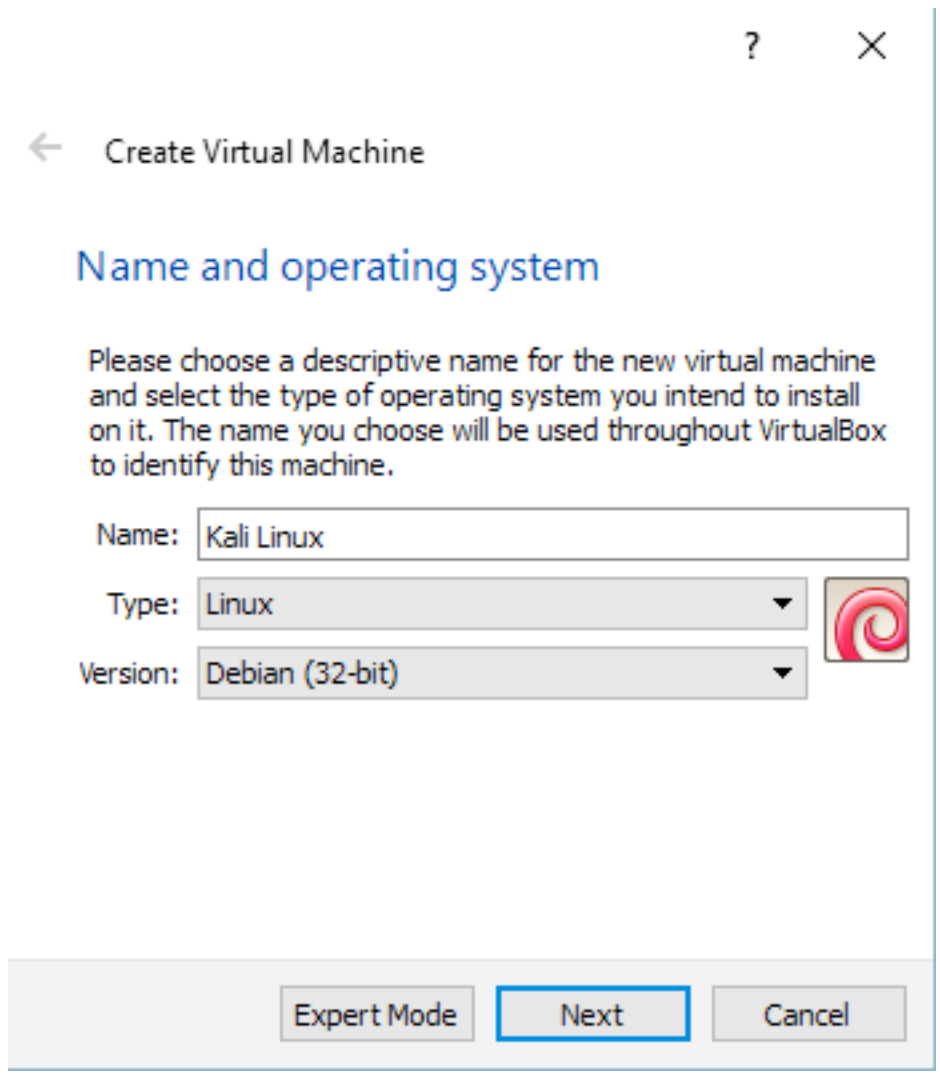
Kali Linux Virtual Machine

In VirtualBox select **New:**



When Prompted for Name and operating system Enter:

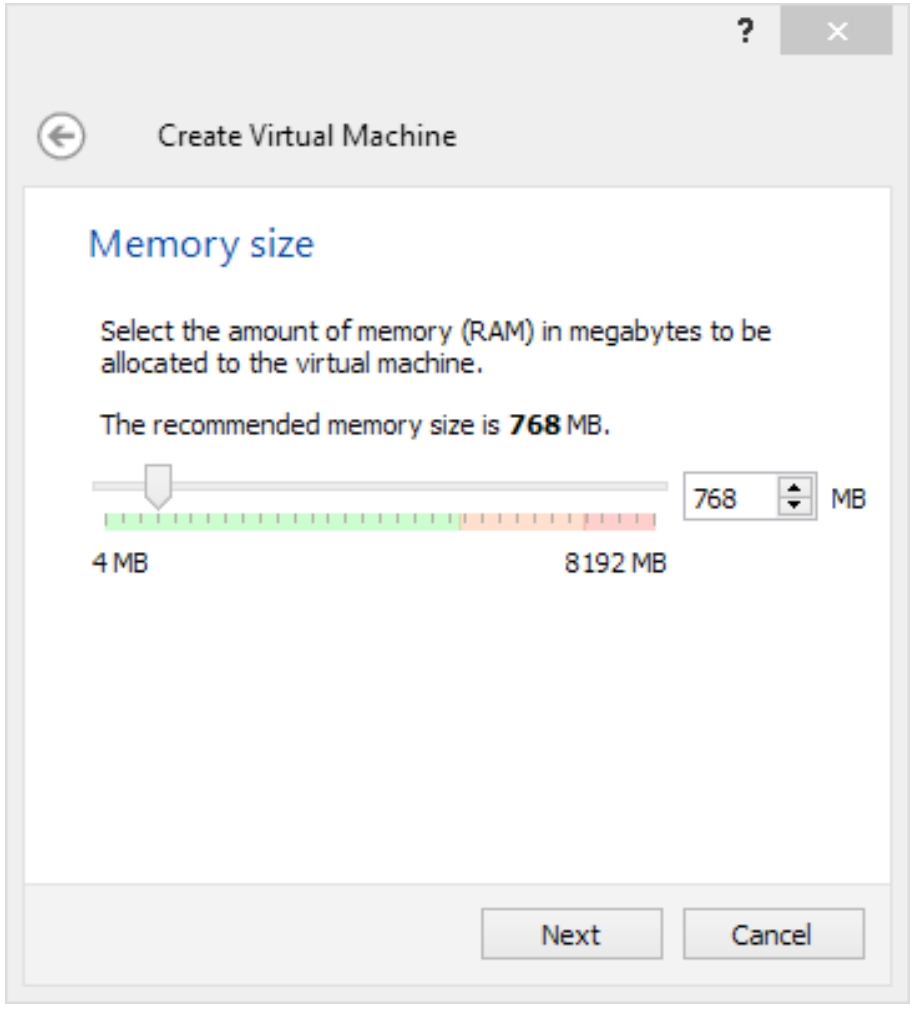
- Name – **Kali Linux**
- Type – **Linux**
- Version – **Debian** –(64 bit or 32 bit based on your system)
- Click **Next**



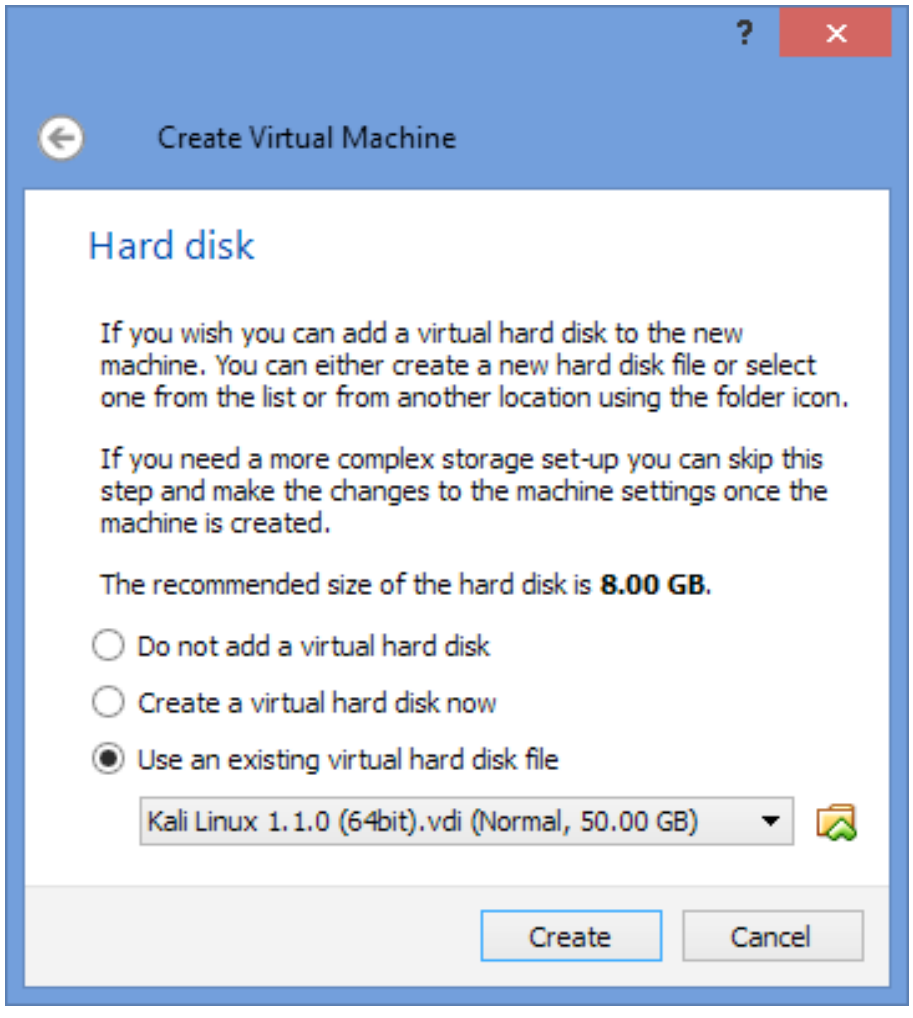
Memory size defaults to 768 MB. Depending on how much RAM you have, my recommendation would be to increase based on the following:

- If you have 4GB RAM I would leave the setting as the default 768
- Set the memory size to 2GB if you have 8GB RAM
- Set the memory size to 4GB if you have 16GB RAM

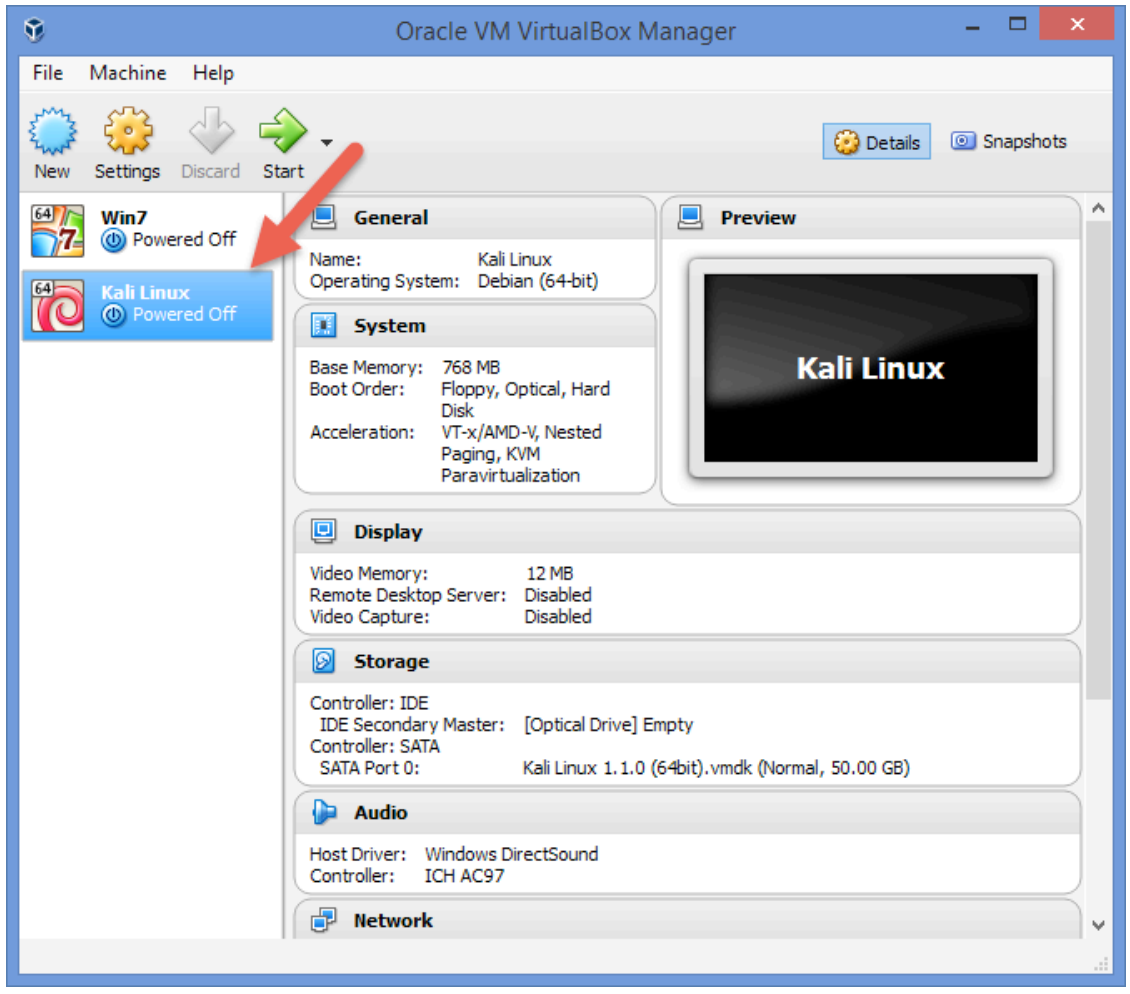
Modify the memory as suggested and select **Next.**



Create Virtual Machine will pop up. Select Use an existing virtual hard disk file. This I is the file you extracted in the pre-course. Select the folder icon and choose your VMS\KaliLinux\Kali-Linux_1.1.0-32 or 64 bit\ 32bit or 64bit\Kali Linux 1.1.0 (32bit or 64bit).vdi. Select **Open Create.**

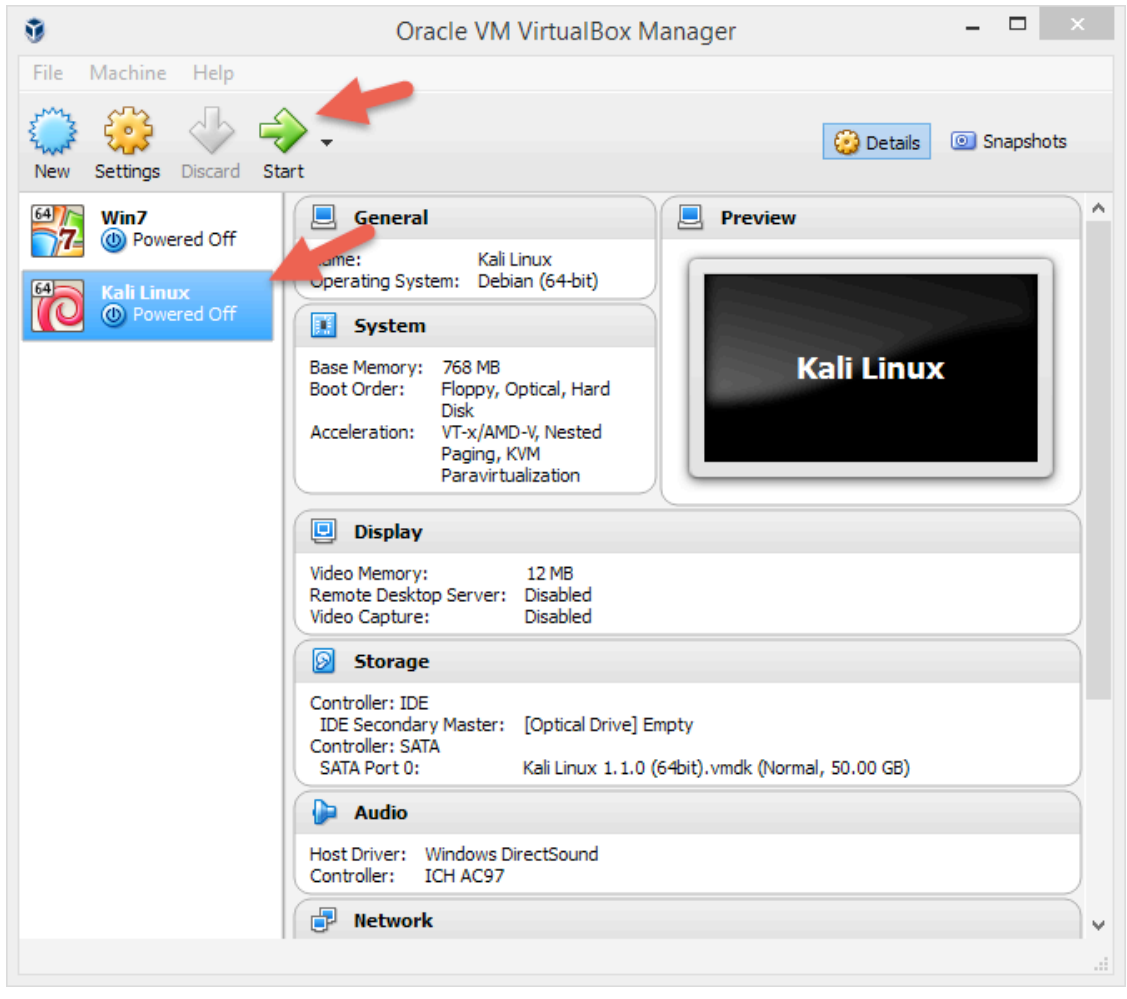


Now you will see the virtual box instance on the left side of the screen as below:

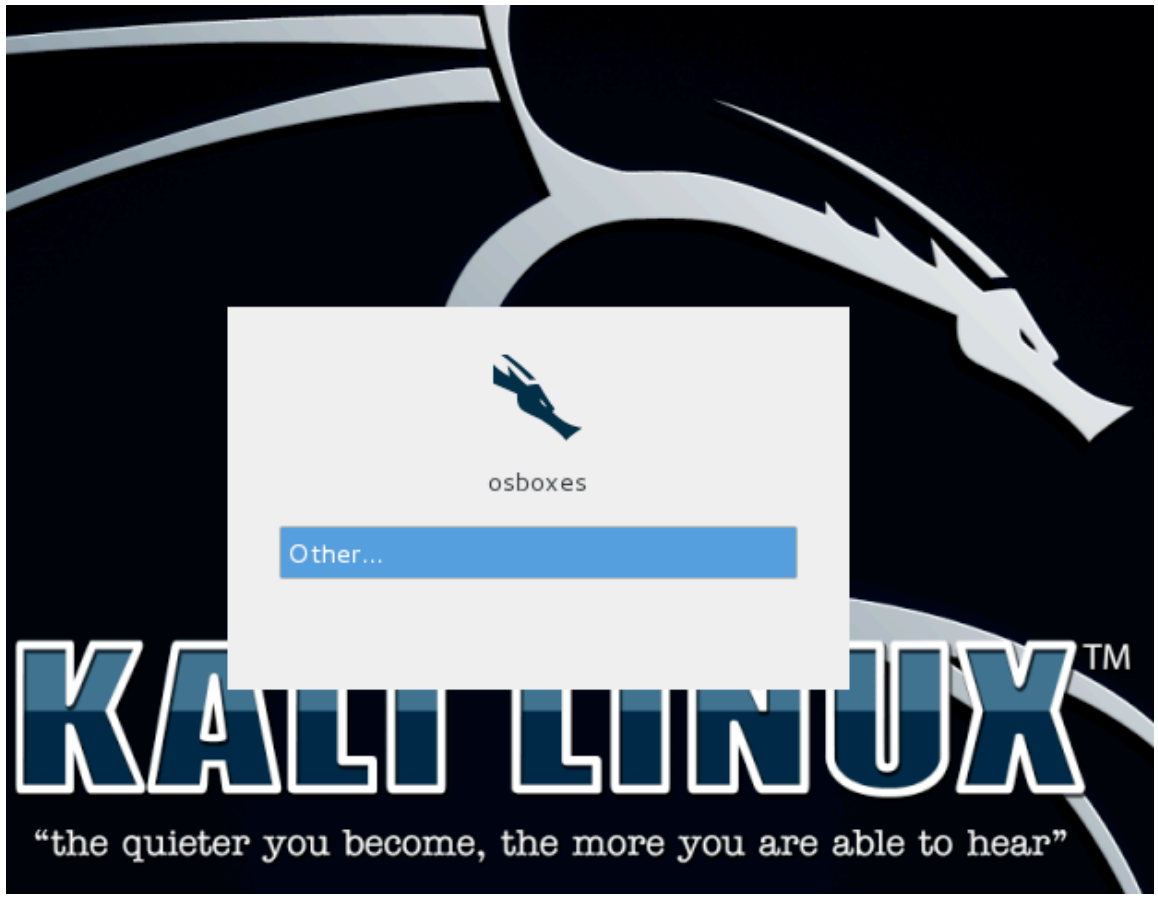


Click on the **Kali Linux Virtual Machine** as it is highlighted in blue. See arrow.

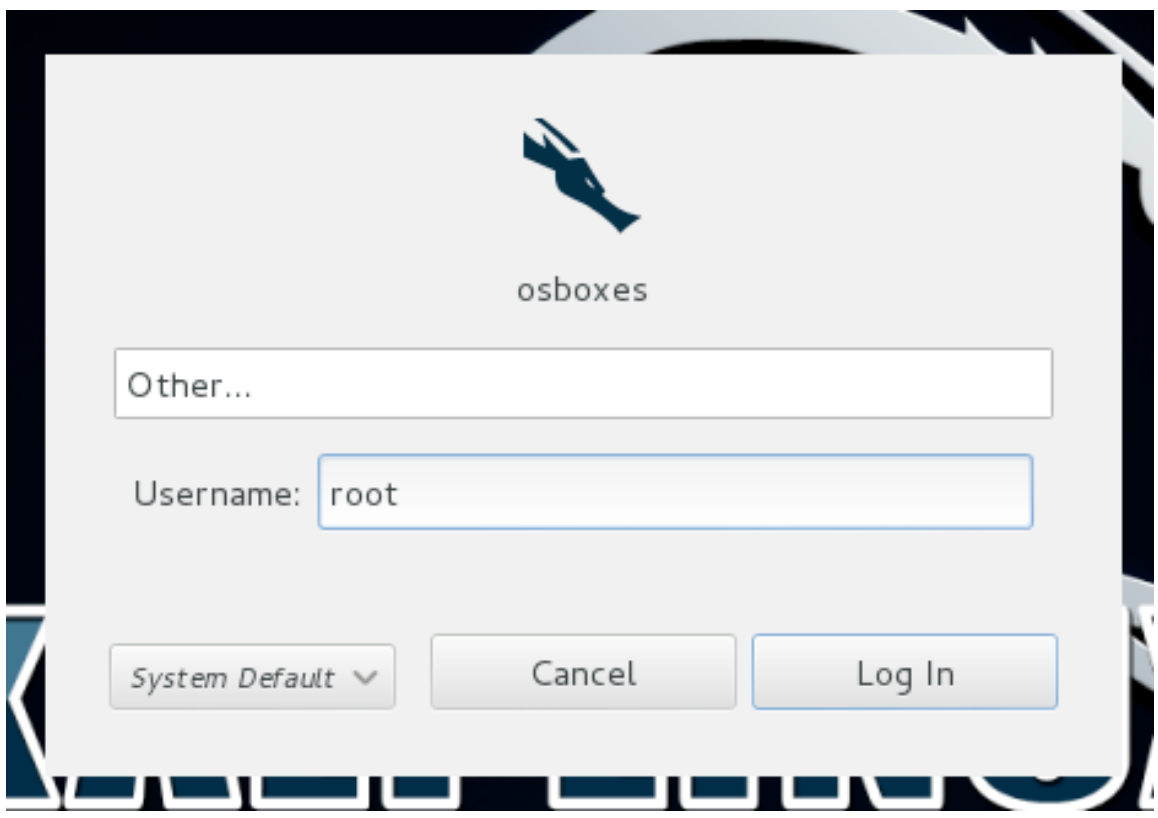
On the menu click the **green start button**. See arrow:



At this point Kali Linux will boot up. You will see lines scrolling on the screen. Wait until you see a white box in the center of the screen which says osboxes with the word "Other" highlighted in blue. Click on Other…

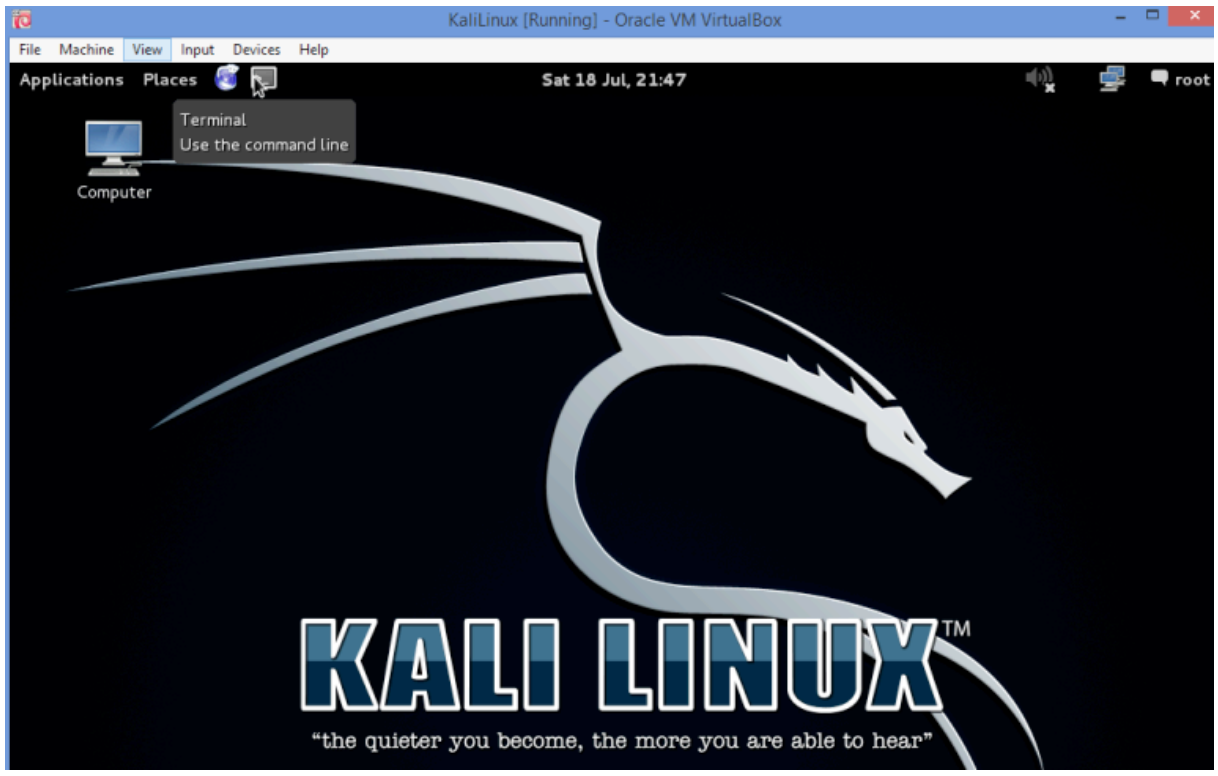


Once you select" Other" this will pop up. For Username: type root and select **Log In:**



Enter the password osboxes.org and click **Log In.**

The Kali Linux desktop will appear.



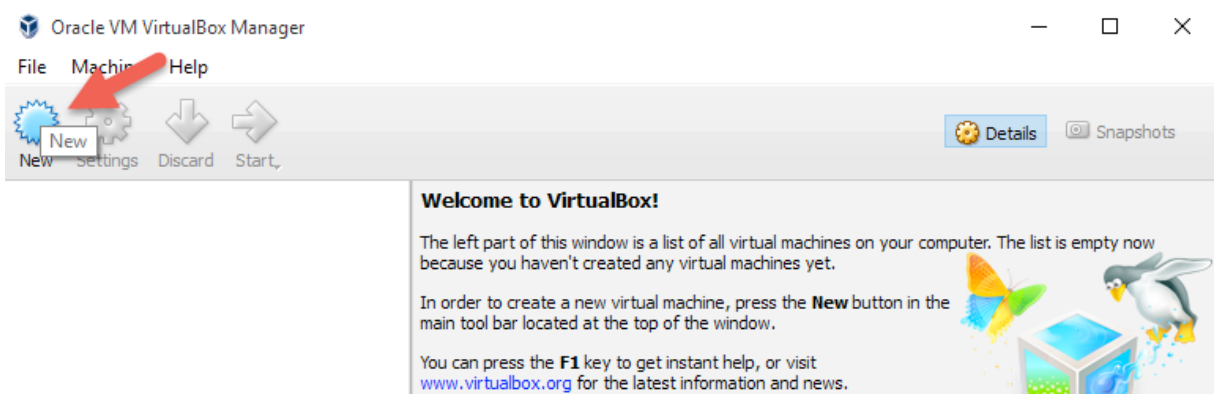
Now that we know it is working, let's shut it down and start our next virtual machine.

At the top right of the screen you will see the word root which is the currently logged in user. Click on it and select **Shut Down.**

Hit Shut Down again or it will automatically do so in 60 seconds.

Ubuntu Virtual Machine

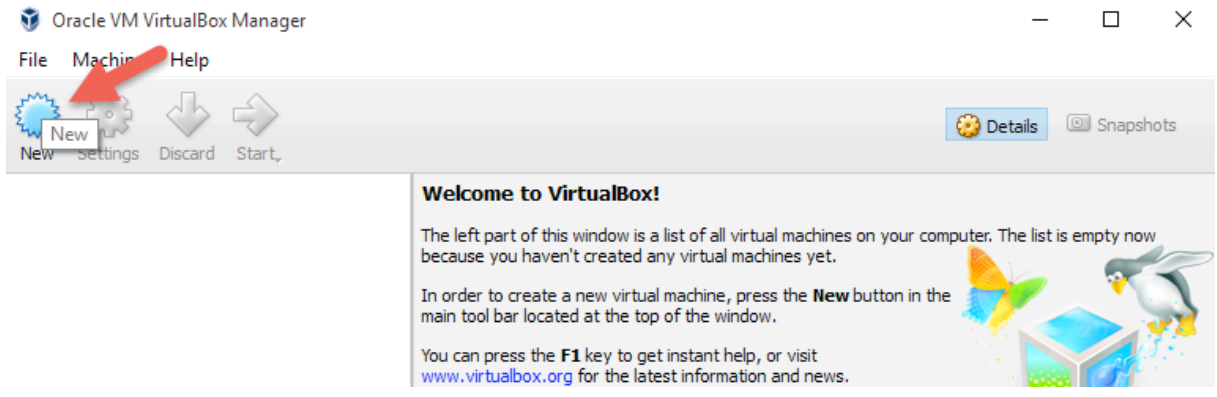
In VirtualBox select **New**



When Prompted for Name and operating system Enter:

- Name – **Ubuntu**

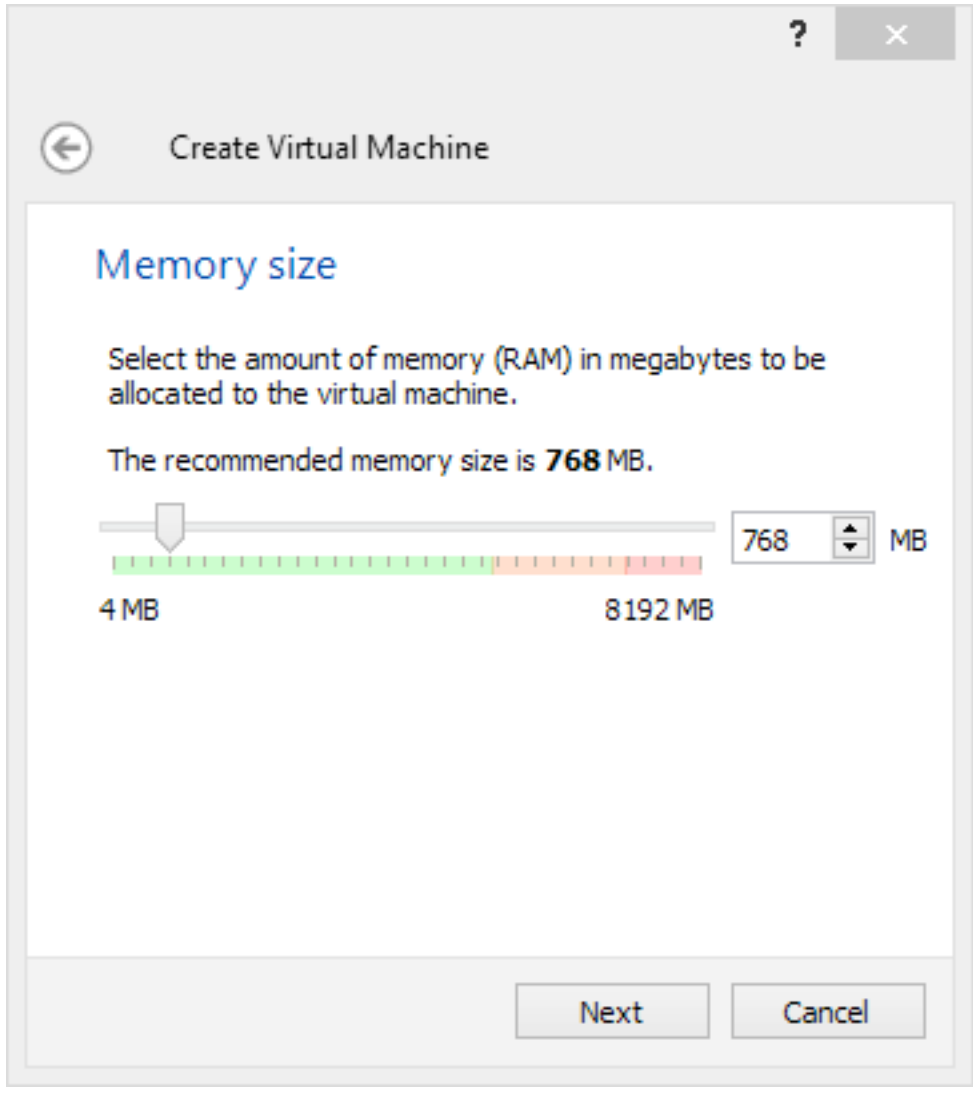
- Type – **Linux**
- Version – **Debian** –(64 bit or 32 bit based on your system) and click **Next.**



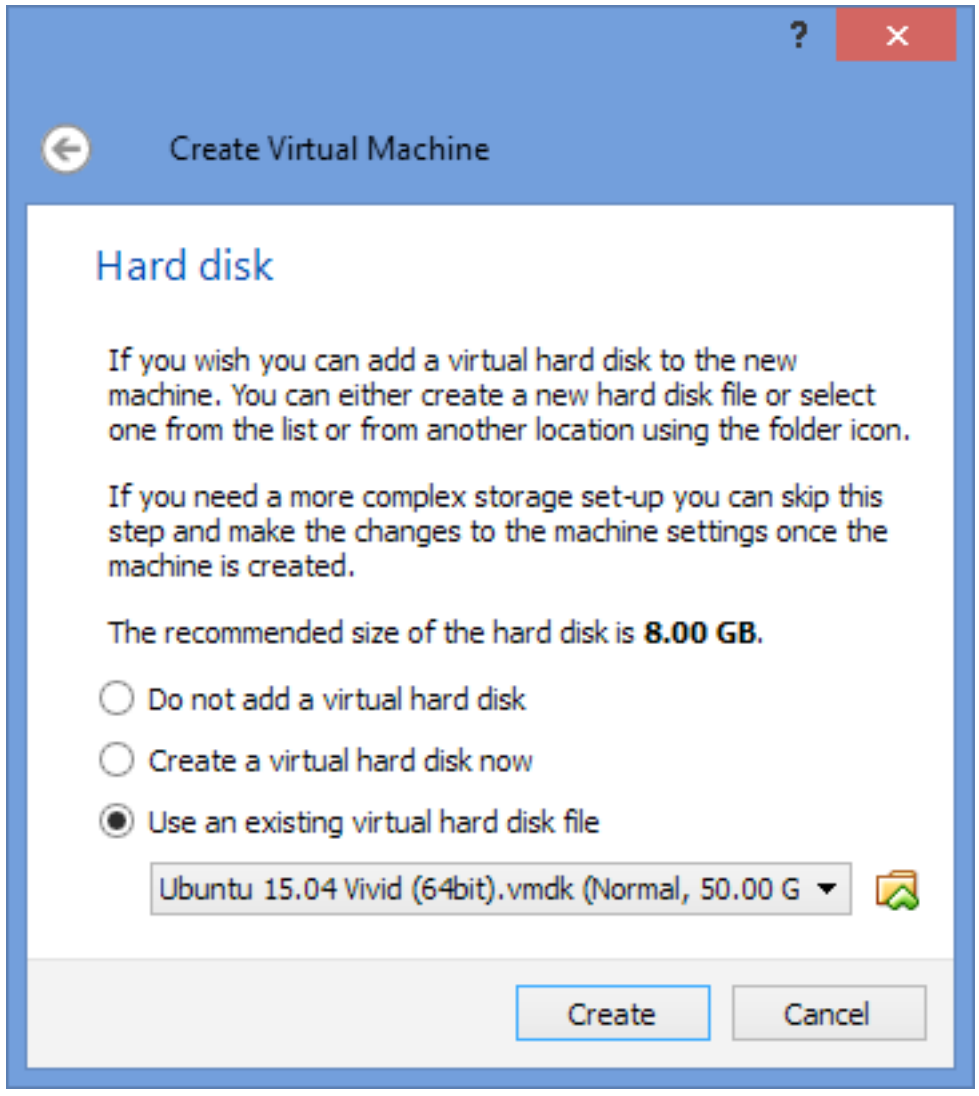
Memory size defaults to 768. Depending on how much RAM you have I would increase it based on the following:

- If you have 4GB RAM I would leave the setting as the default 768
- Change to 1GB if you have 8GB RAM
- Change to 2GB if you have 16GB RAM

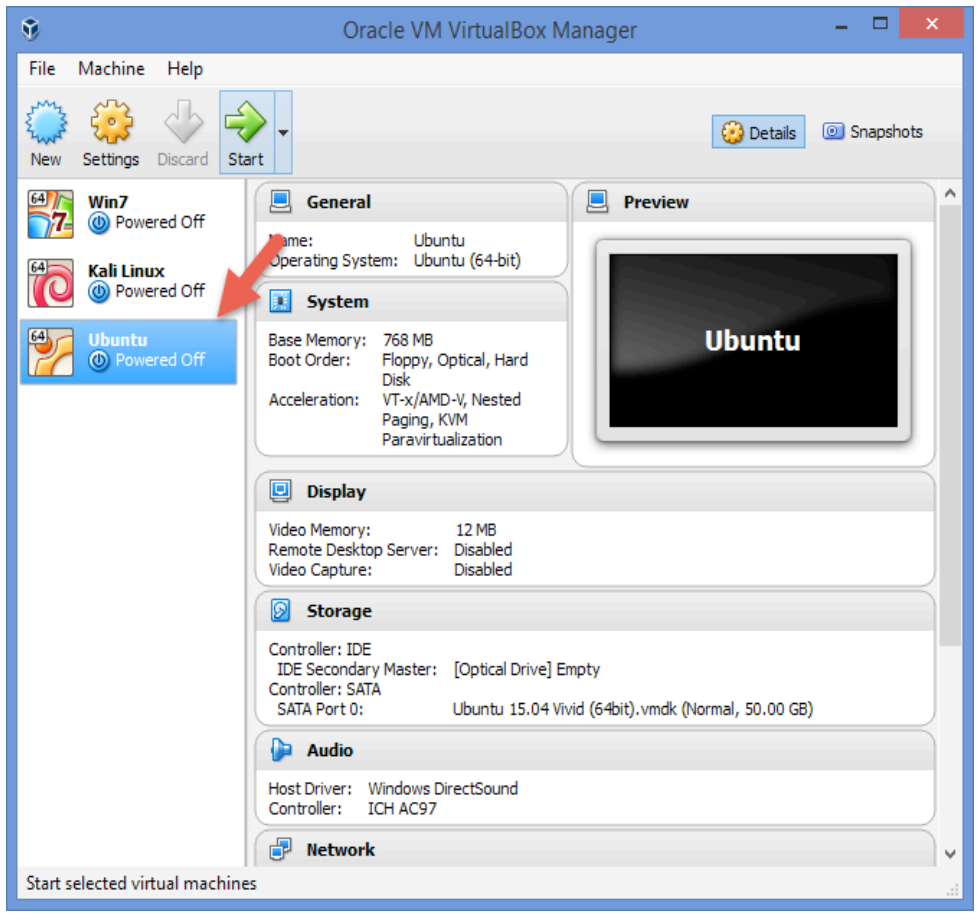
Modify the memory as suggested and select **Next:**



Create Virtual Machine selecting Use an existing virtual hard disk file. This is the file you extracted in the pre-course. Select the folder icon and choose your VMS\Ubuntu\32 or 64 bit\ Ubuntu 15.04 Vivid (32bit or 64bit).vmdk. Select **Open Create:**

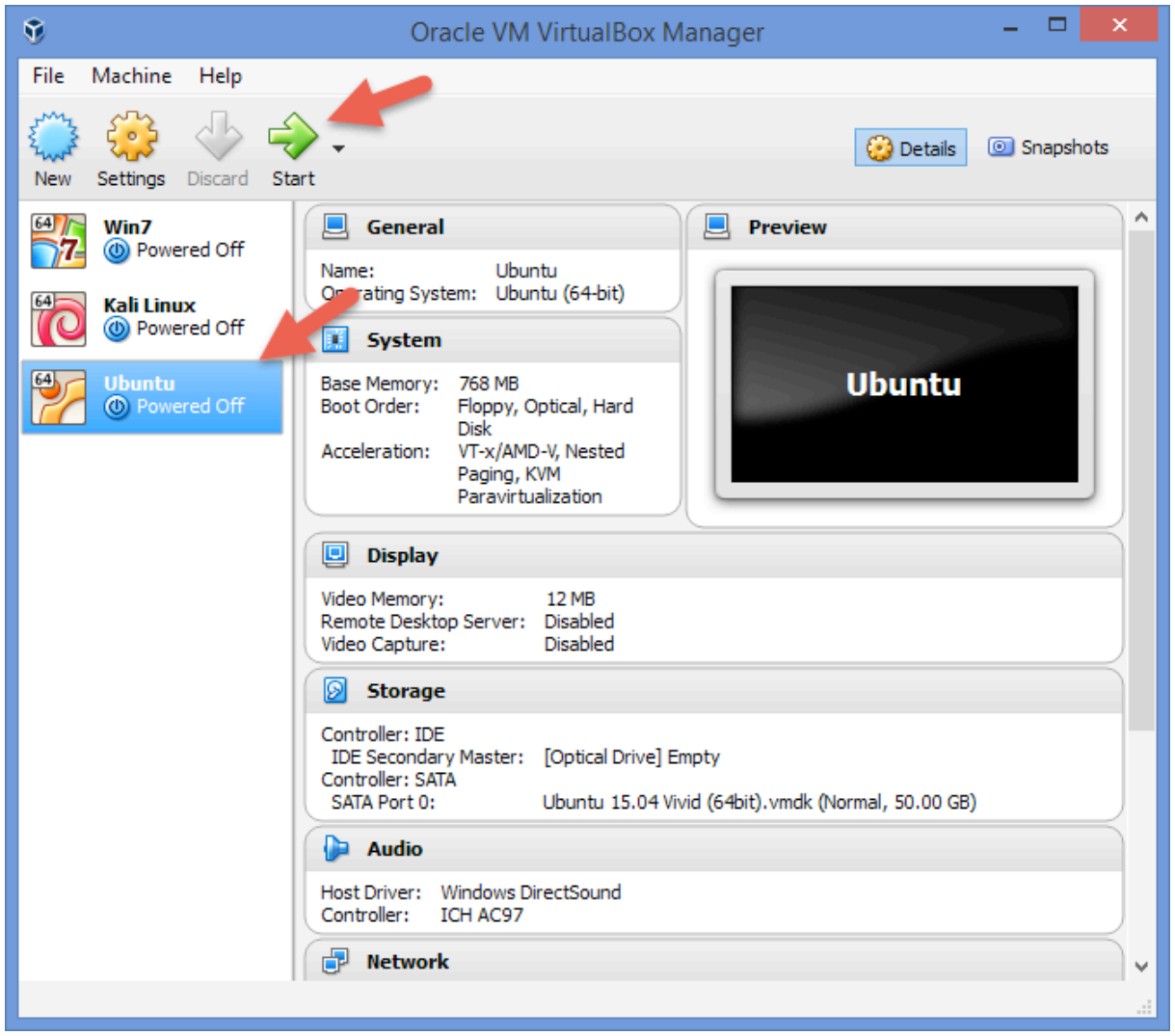


Now you will see the VirtualBox on the left side of the screen as pictured below:

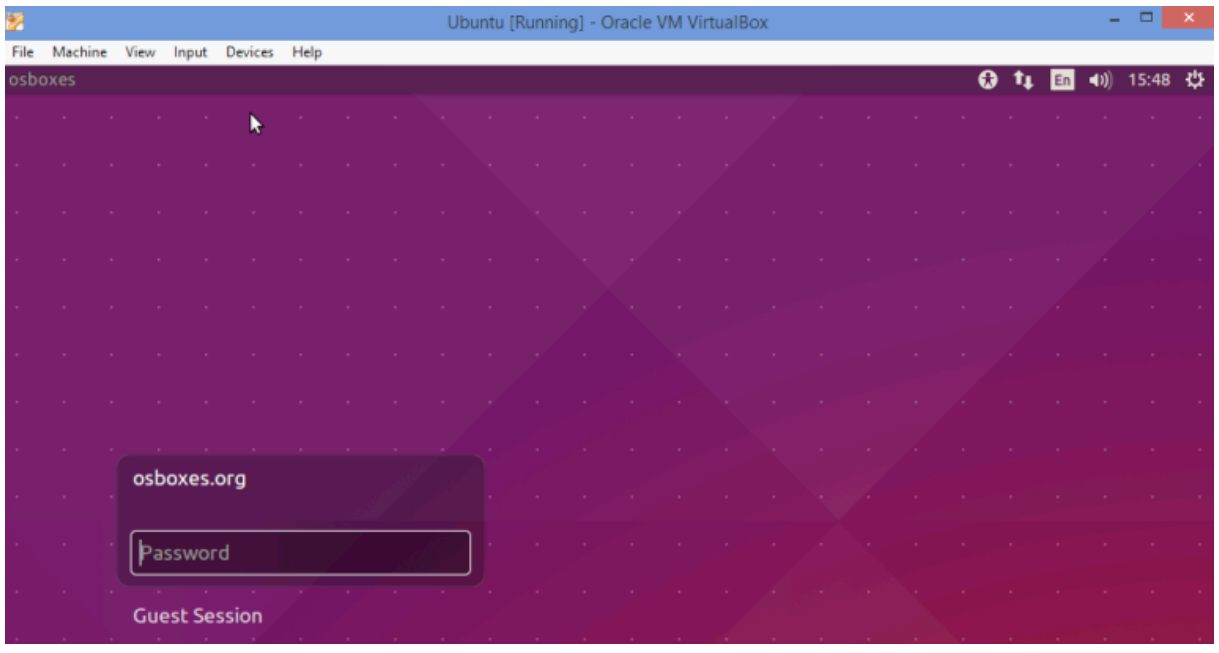


Click on **Ubuntu**. It is highlighted in blue as seen above.

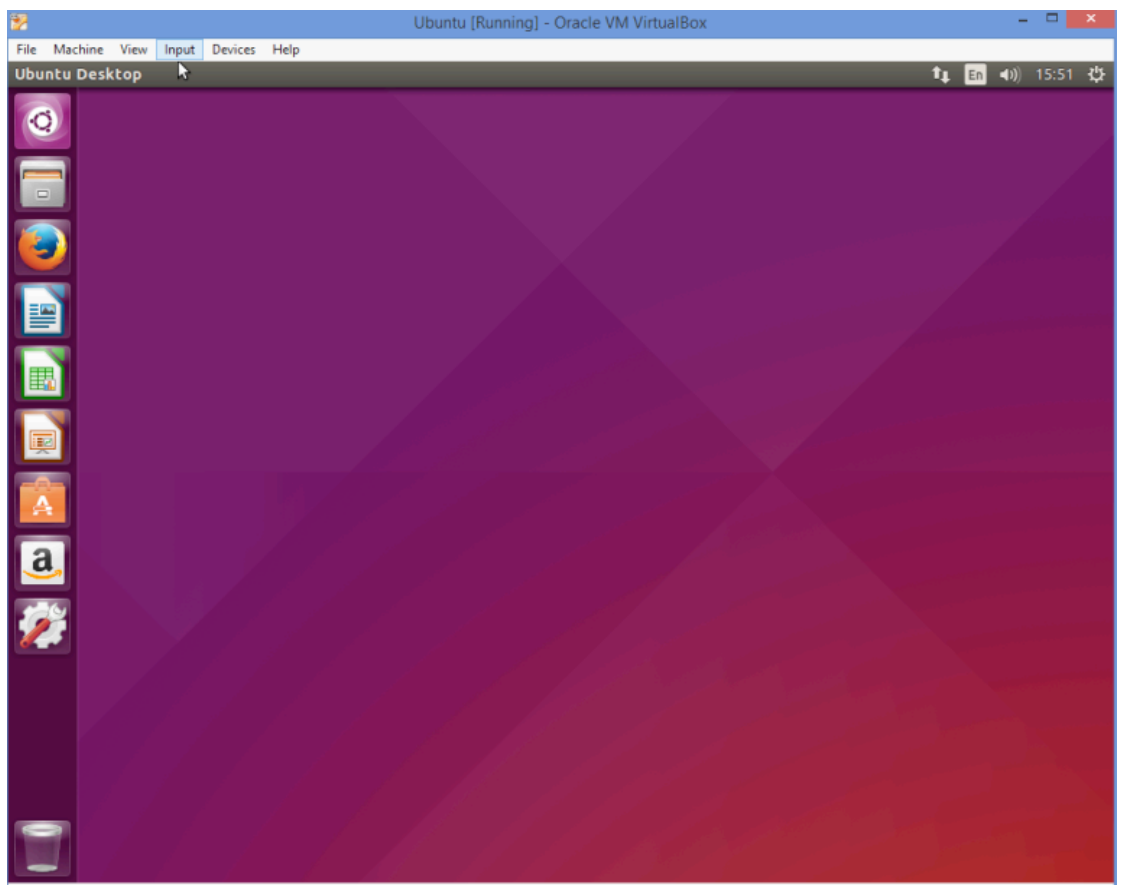
On the menu click the green **Start** button:



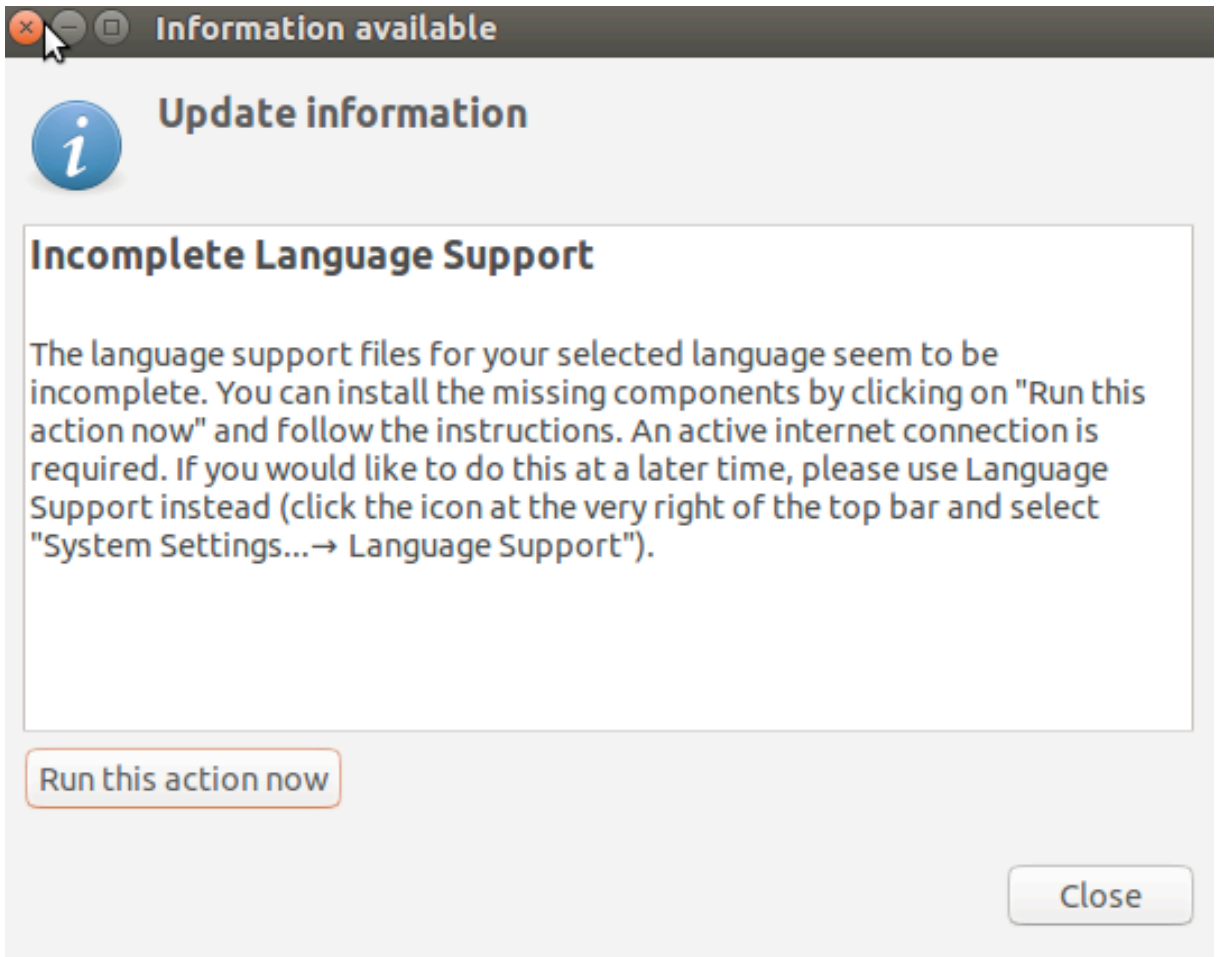
Ubuntu will boot up and you will see lines scrolling on the screen. Do not pay attention to the screen; it will boot up to the Ubuntu Login Screen. Wait until you see the **osboxes.org** login. Enter the password: **osboxes.org** and hit **Enter.**



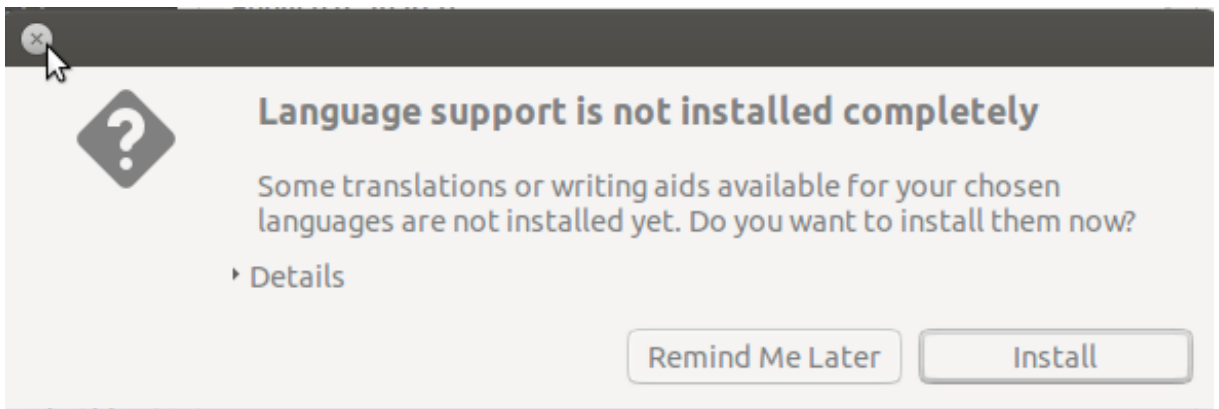
You will now see the Ubuntu Desktop. Congratulations! You have a successful Ubuntu build for use in your lab:



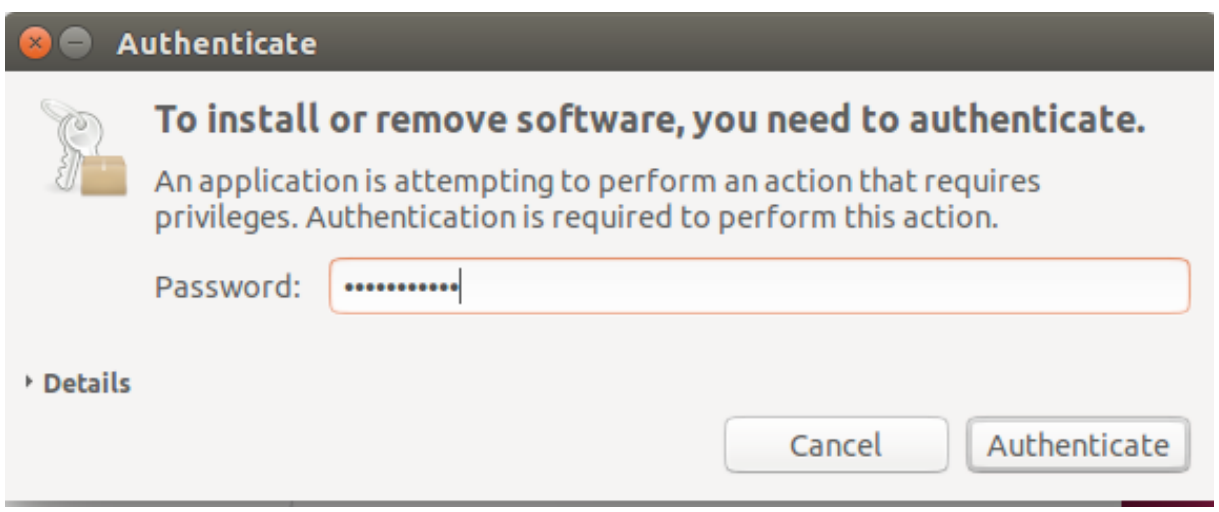
You may get an update information box pertaining to Incomplete Language Support. Click **Run this action now:**



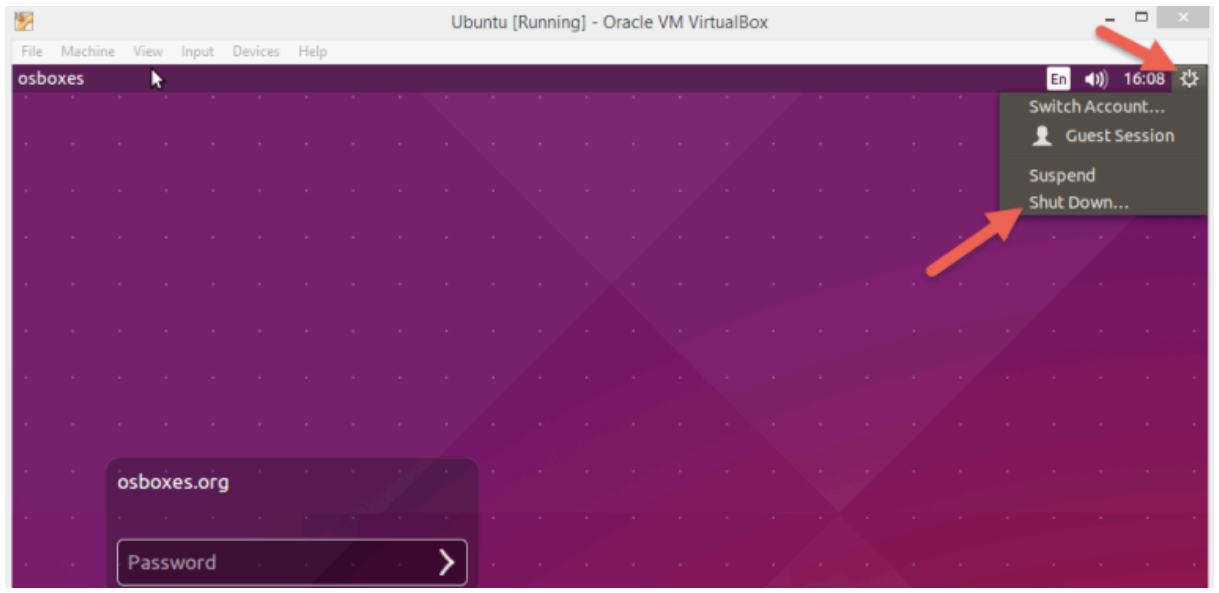
You will see **Language support is not installed completely**. Select **Install.**



You will be asked to **Authenticate.** Enter the password **osboxes.org** and select **Authenticate.**

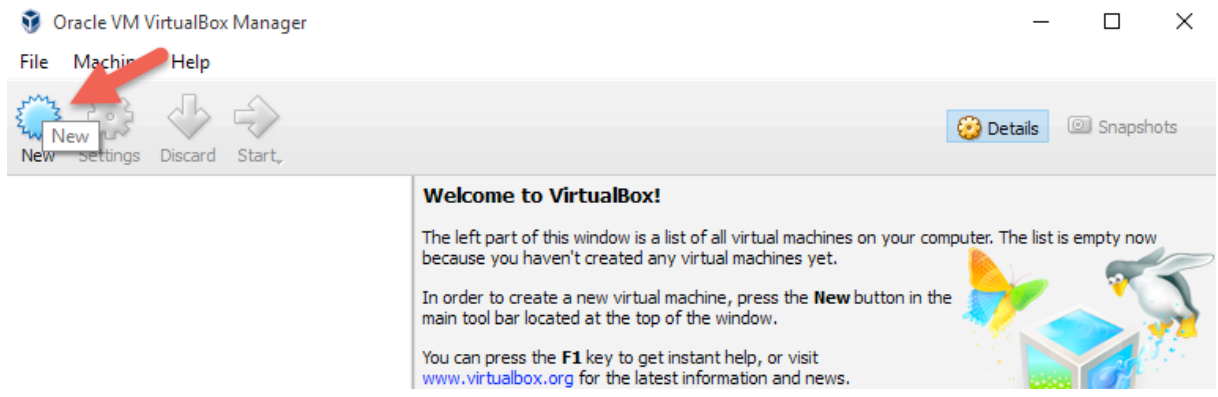


Once complete we need to shut down Ubuntu by clicking the button on the top right of the screen and selecting **Shut down** and **Shut down** again.



Metasploitable Virtual Machine

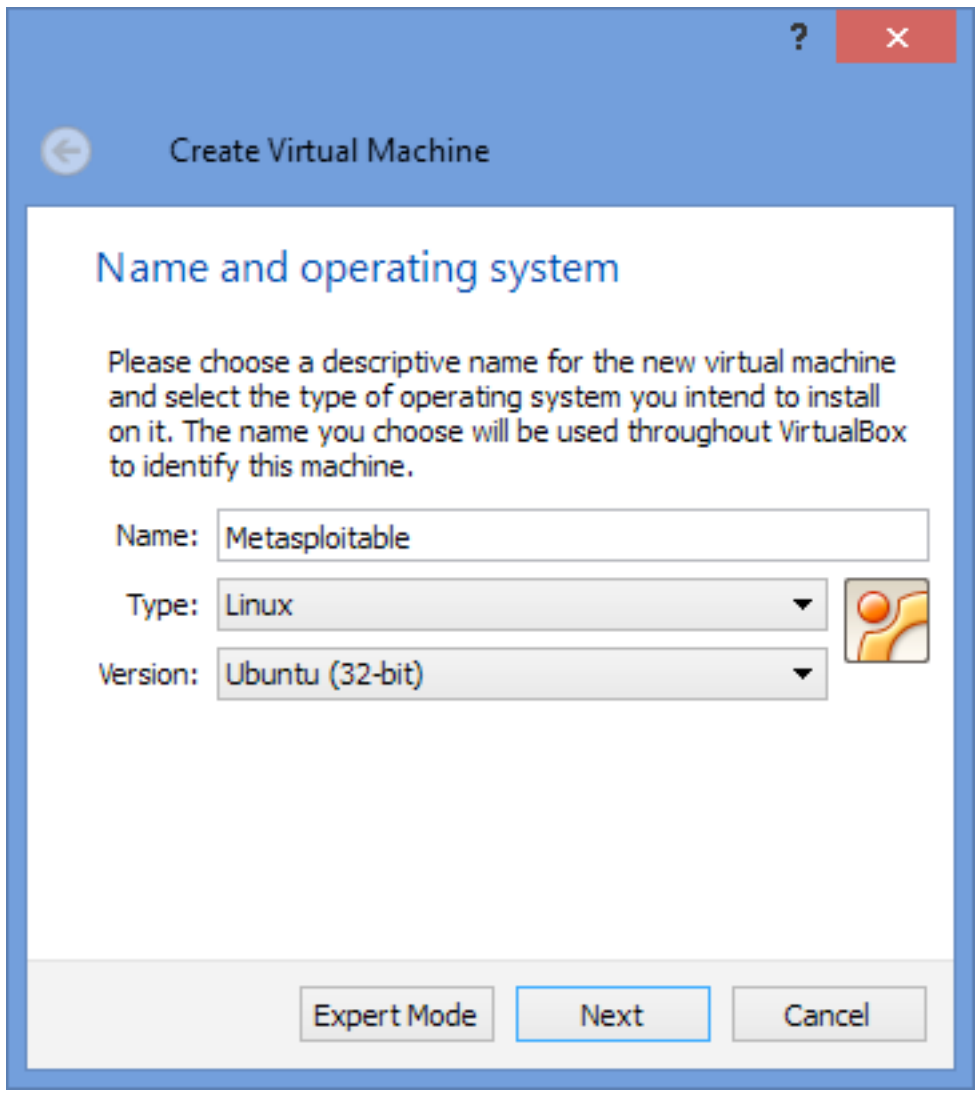
In VirtualBox select **New:**



When Prompted for Name and operating system **Enter:**

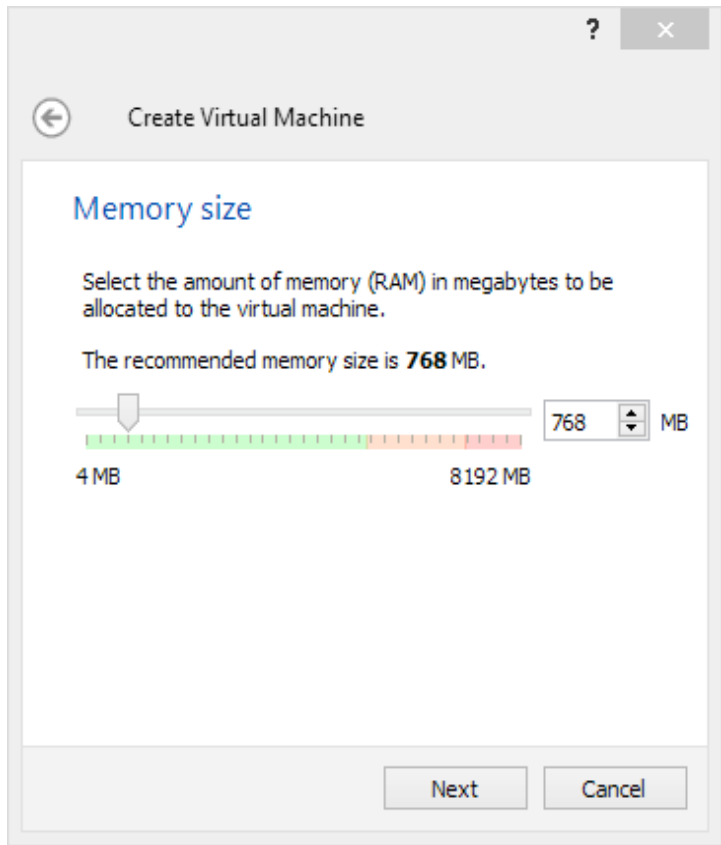
- Name – Metasploitable
- Type – Linux
- Version – Ubuntu (32 bit or 64 bit).

Click **Next:**

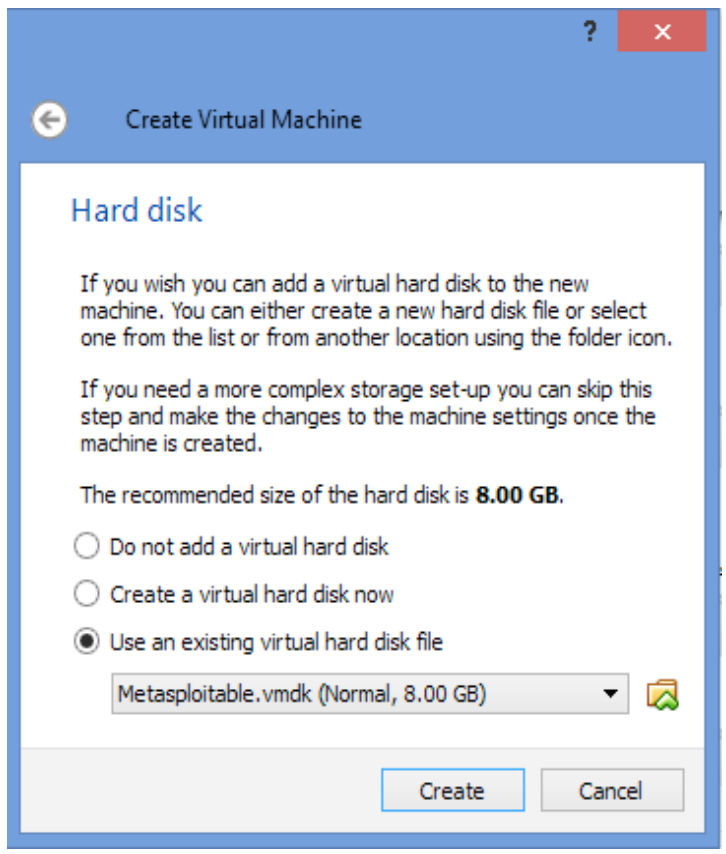


Memory Size defaults to 768. Accept the default and click **Next:**

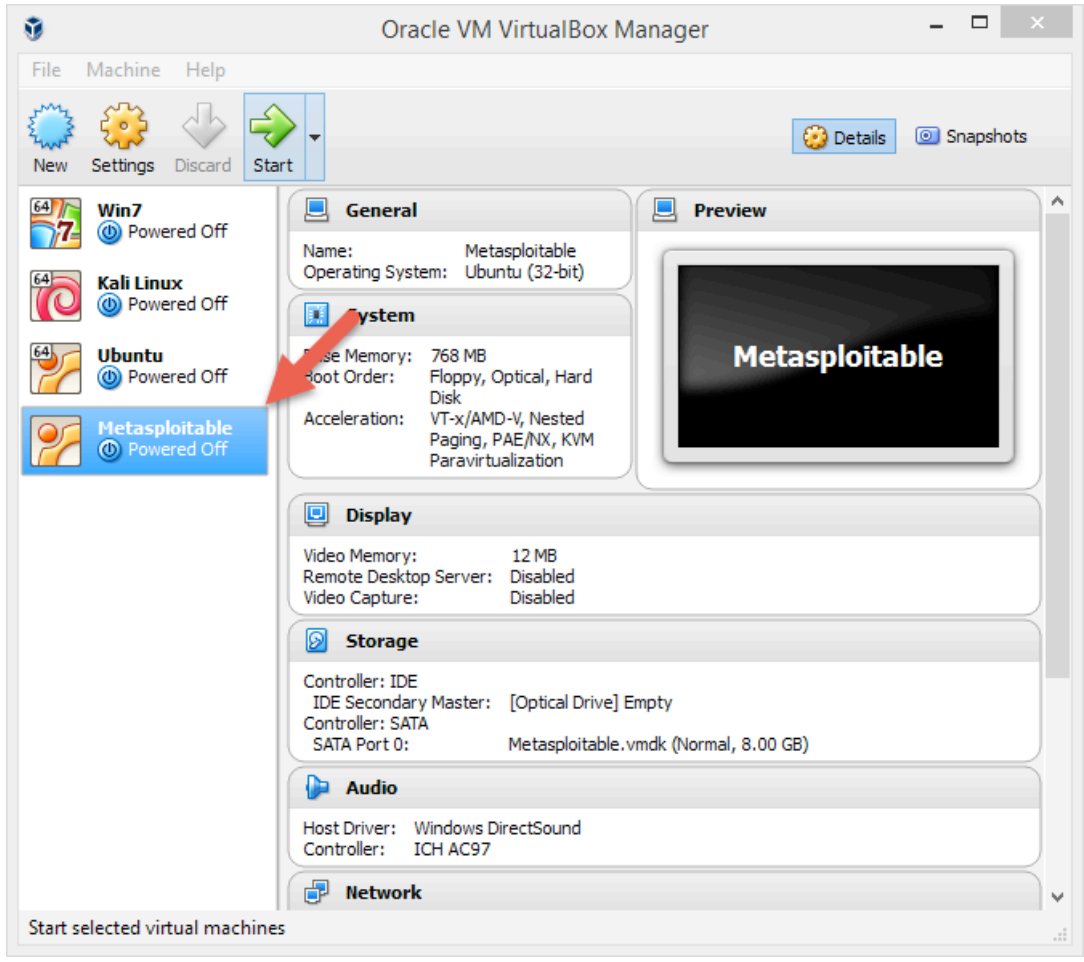
Create Virtual Machine by selecting **Use** an existing virtual hard disk file. This is the file you extracted in the pre-course.



Select the folder icon and choose your **VMS\ Metasploitable2-Linux\Metasploitable.vmdk** file and select **Open Create:**

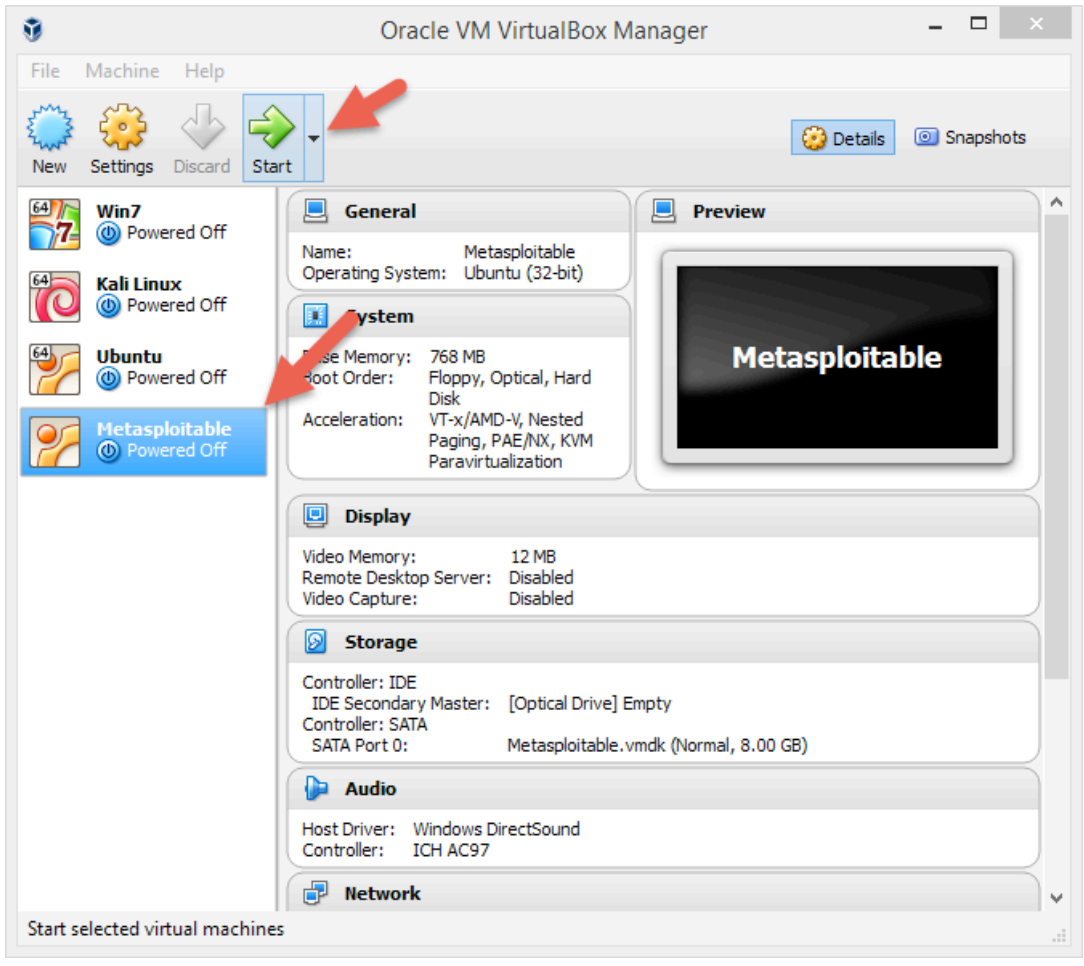


Now you will see the VirtualBox on the left side of the screen as depicted below:

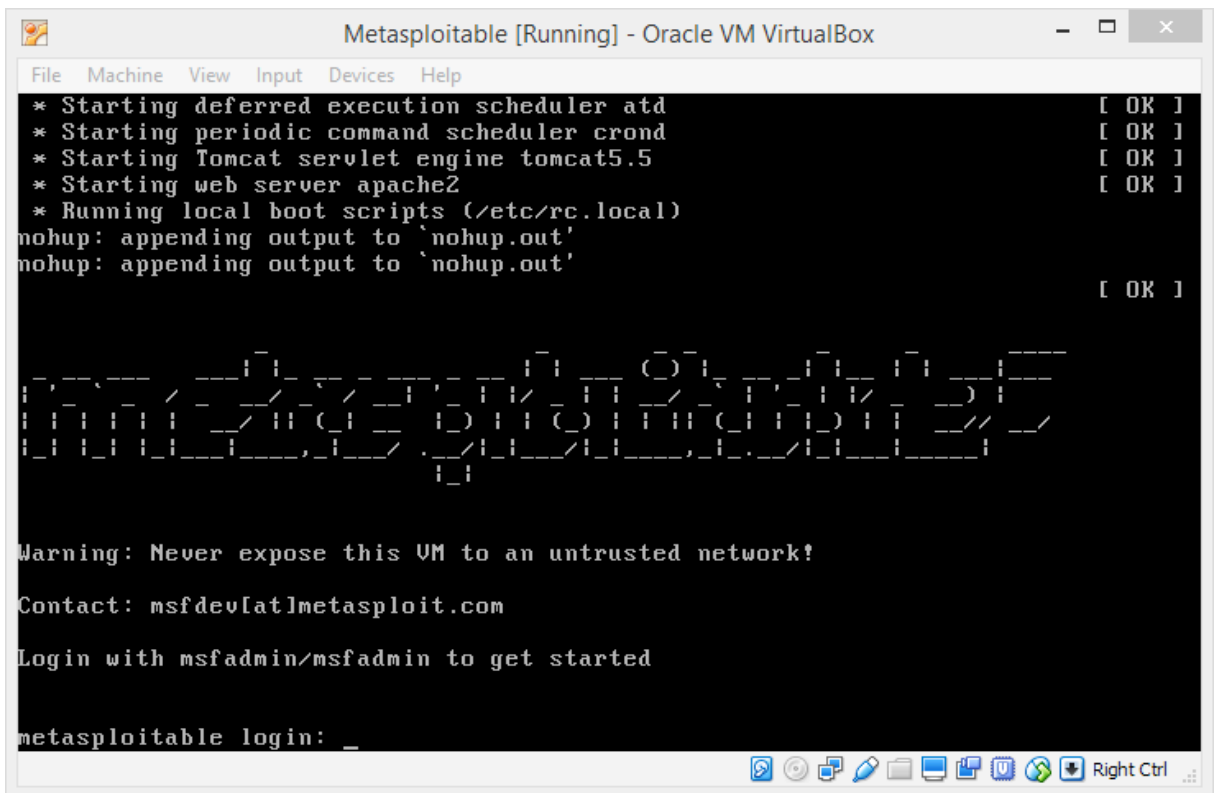


Click on the **Metasploitable Virtual Machine**. It is highlighted in blue as seen above.

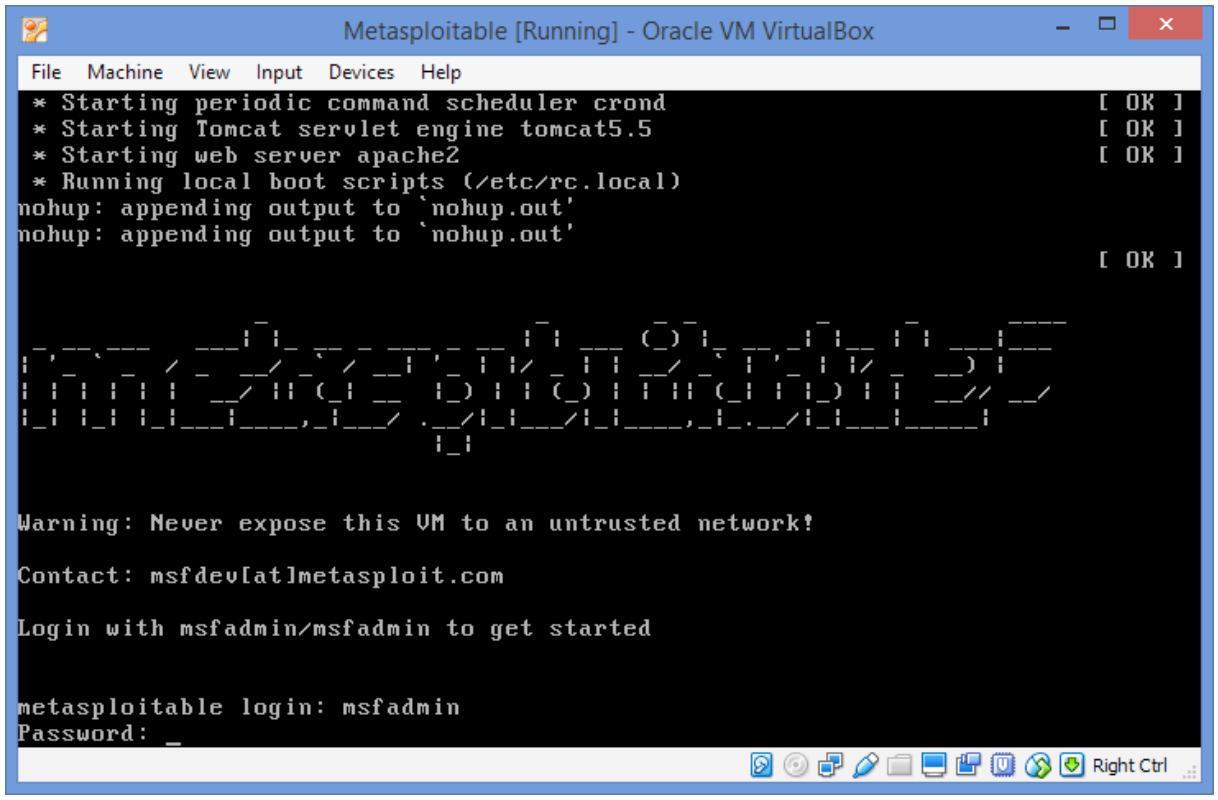
On the menu, click the **green START button:**



Metasploitable will boot up to the login screen. As you can see below, the login screen includes the userid and password **ofmsfadmin:**

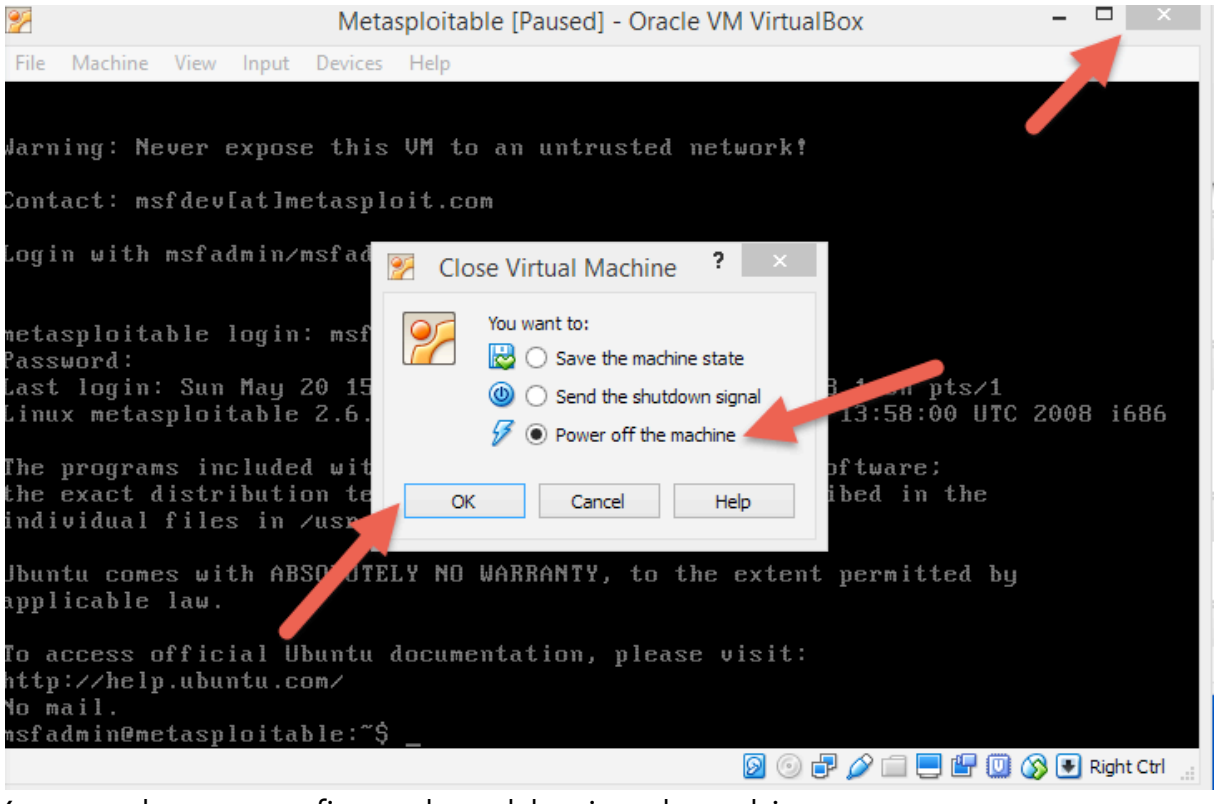


Enter the userid of **msfadmin** and the password of **msfadmin** and hit **Enter**:



Now that you have successfully logged in you do not need any further action on this VM as it is simply there as a vulnerable machine.

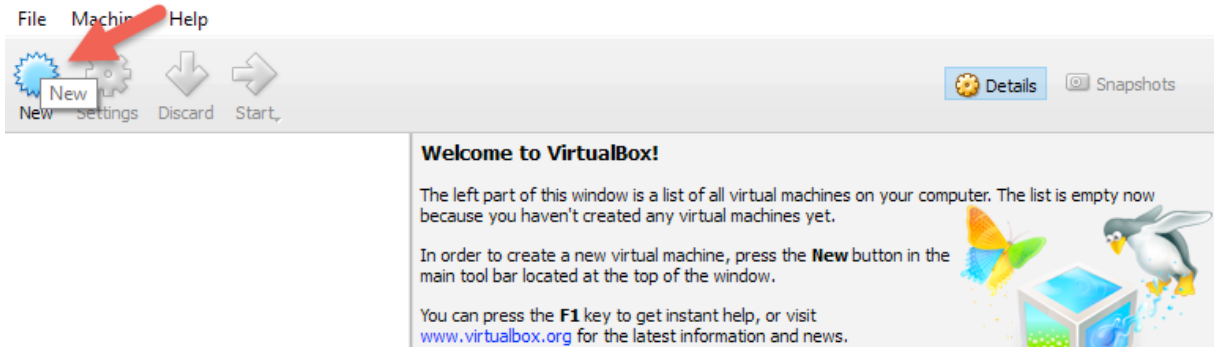
Select the **X** in the right hand corner of the **VirtualBox** virtual machine and select **Power off the machine.** Now select **OK.**



Congratulations! You now have your first vulnerable virtual machine.

Bee-Box Virtual Machine

In VirtualBox select **New:**



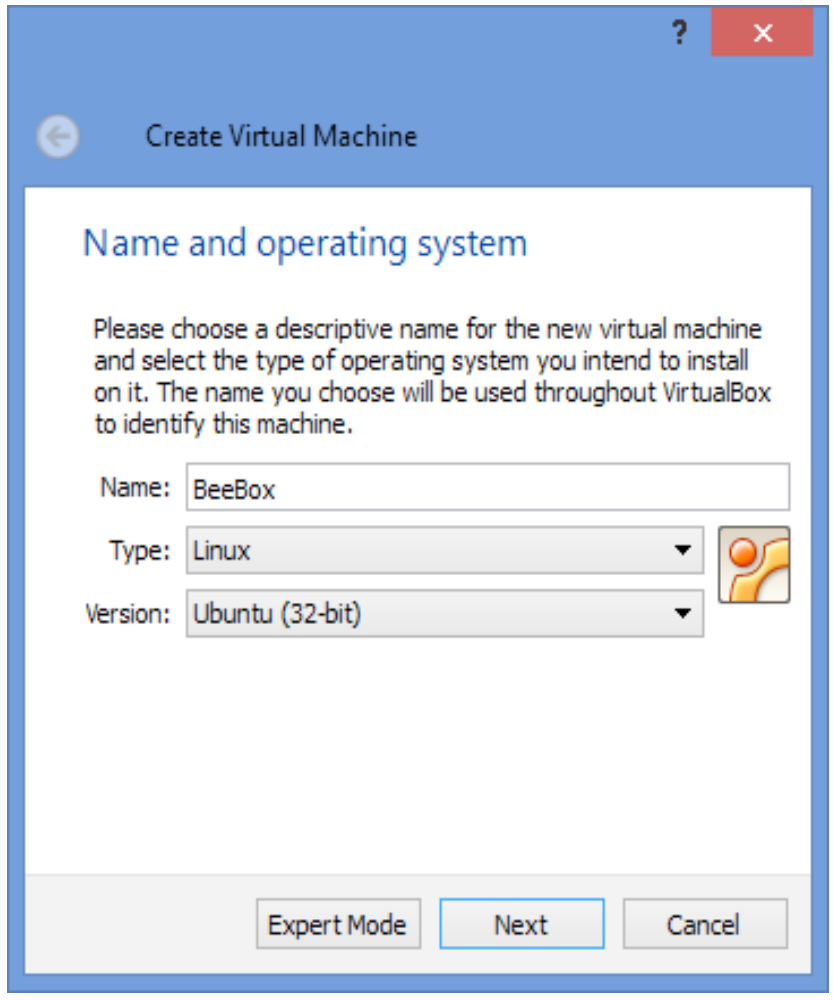
When Prompted for Name and operating System Enter:

- Name – **BeeBox**
- Type – **Linux**
- Version – **Ubuntu (32-bit or 64-bit).**

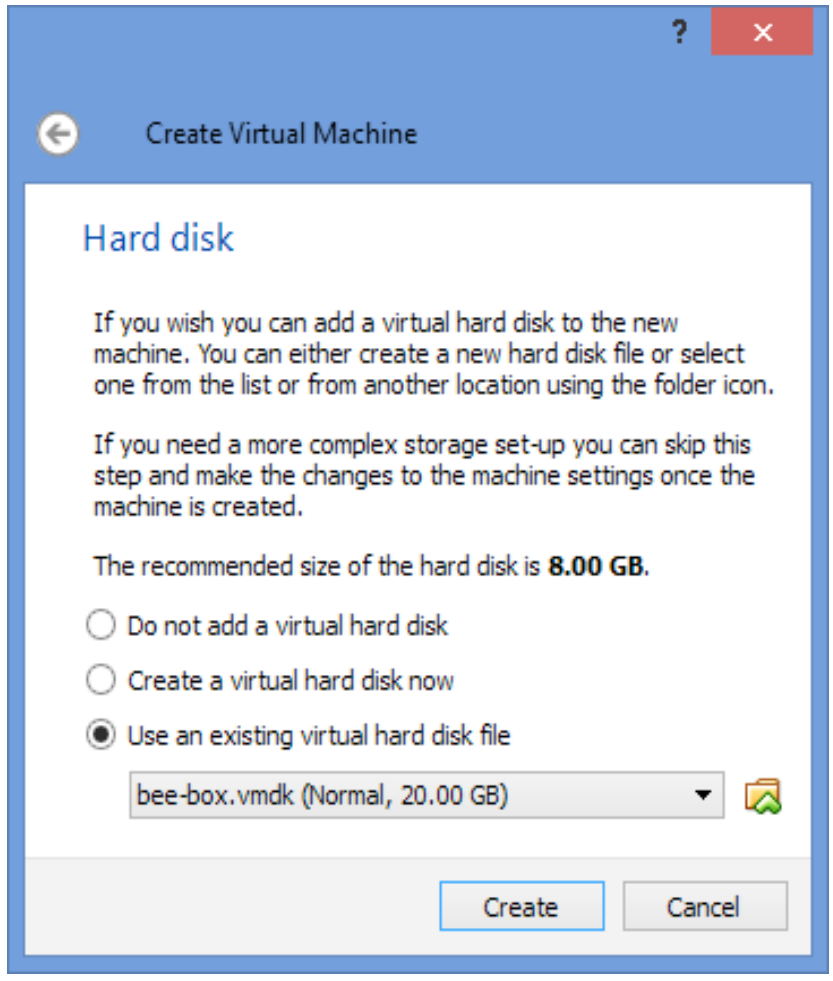
Click **Next**.

Memory Size defaults to **768.**

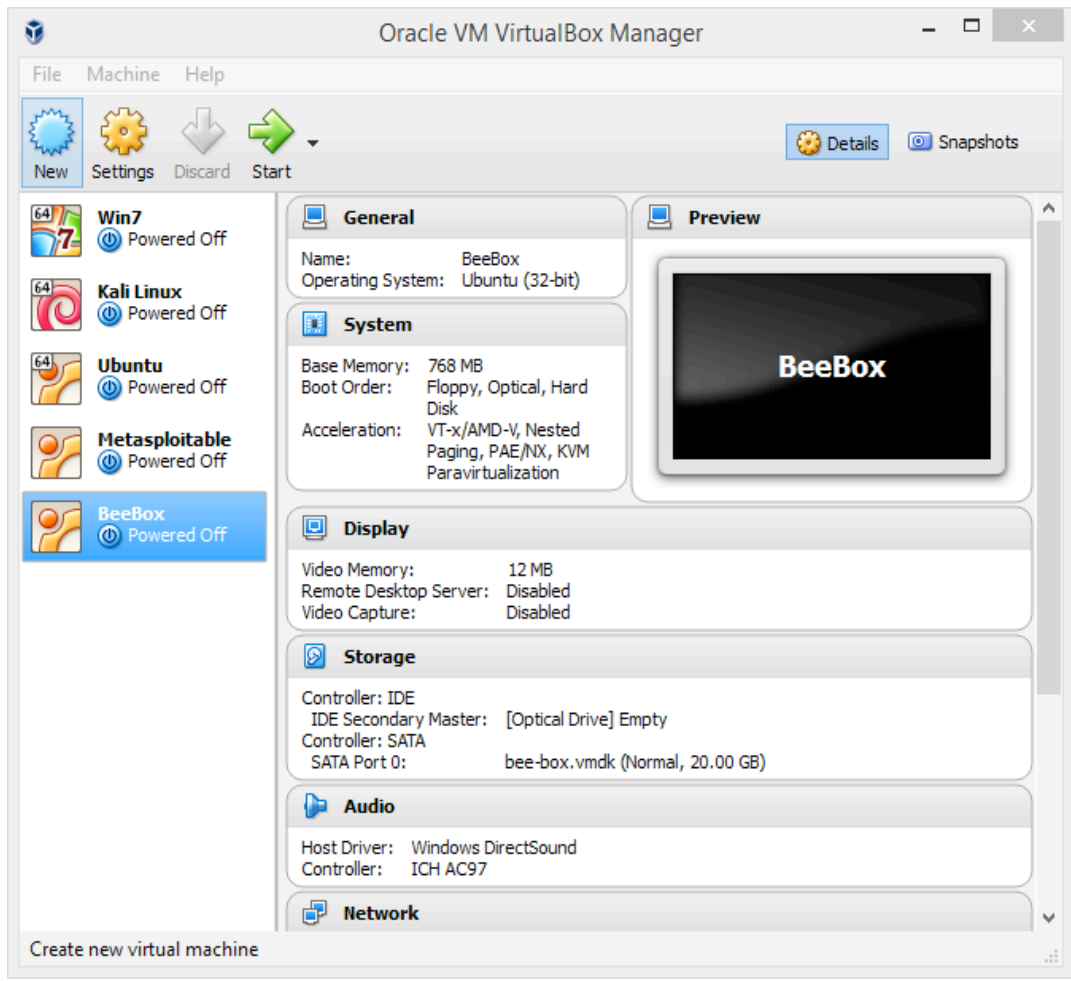
Accept the defaults and select **Next.**



Create Virtual Machine selecting Use an existing virtual hard disk file. This is the file you extracted in the pre-course. Select the folder icon and choose your VMS\ beebox\bee-box\bee-box.vmdk and select Create

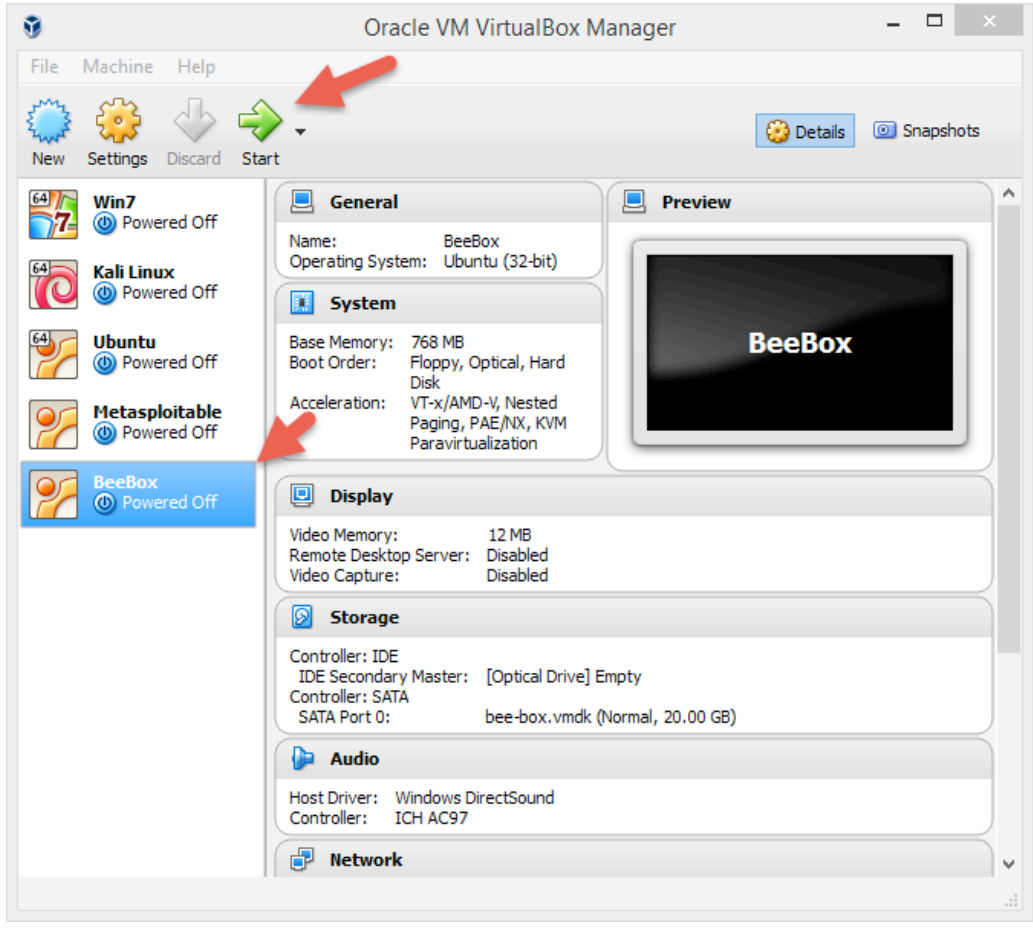


You will see the VirtualBox on the left side of the screen as pictured below:

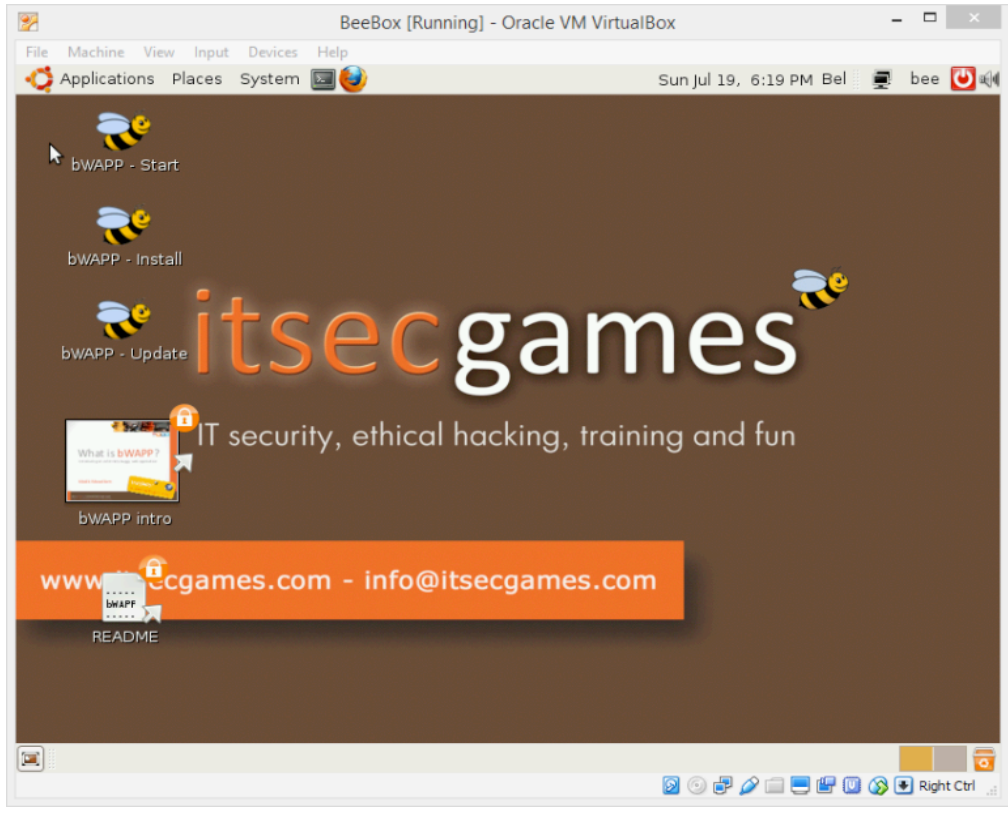


Click on the **Beebox Virtual Machine**. It is highlighted in blue as seen above.

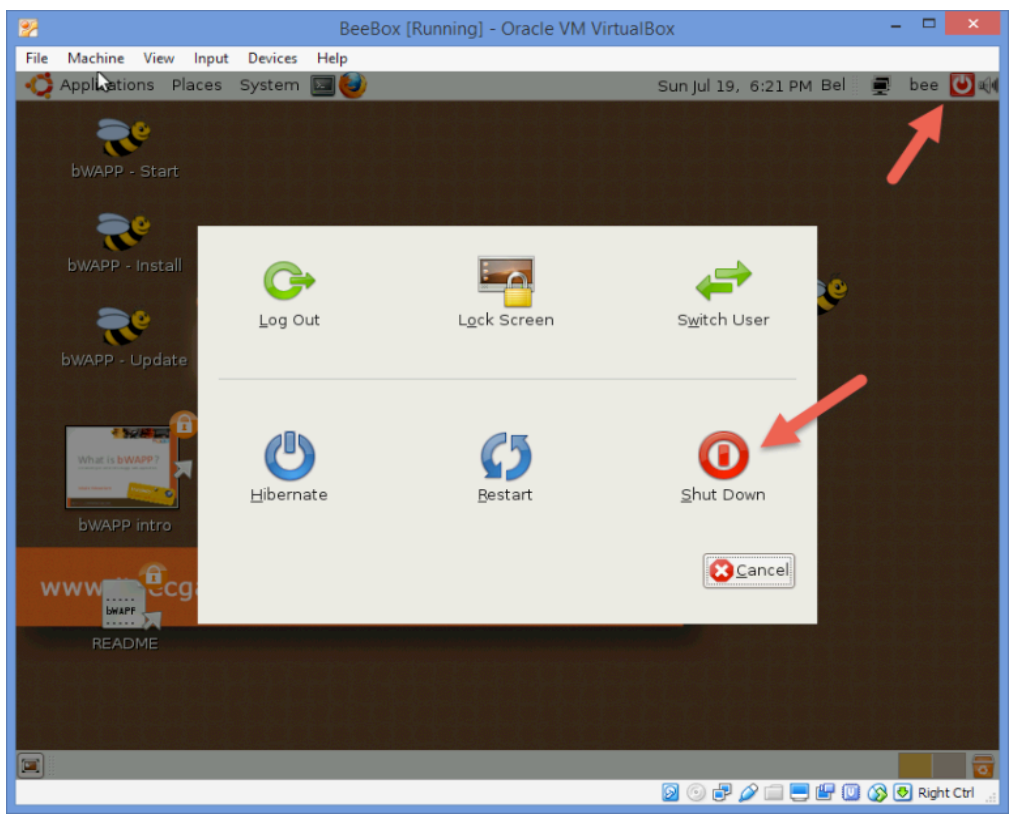
On the menu click the green **Start** button.



Beebox will boot up and you will see lines scrolling on the screen. You will notice the background is it-secgames with some bees on the screen. The system will automatically log in so there is nothing left to do. See the screen below:



Now that we have a successful install we need to shut it down. Click on the red power button on the top right of the screen. Then hit the red **Shut Down** icon.



Congratulations! You now have another vulnerable system.

Now that you have created these systems, let's get more familiar with Kali Linux and put our Linux commands to use.