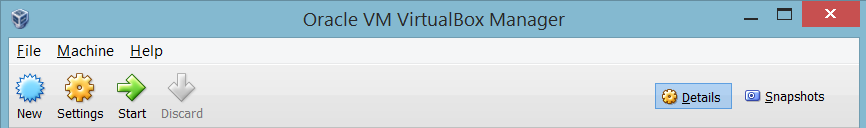
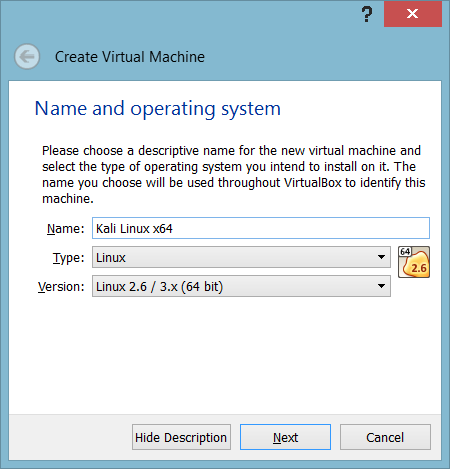
A how-to guide for constructing a basic, but effective Virtual Penetration Testing Lab within VirtualBox. Assuming Virtual is already downloaded in your system, if not, simply go to <https://www.virtualbox.org/wiki/Downloads> and find the download file that pertains to your operating system. We will begin with the creation of your first virtual machine, Kali Linux. You can find the download of Kali Linux at <http://www.kali.org/downloads/>. I will be providing steps to create and install Kali Linux (64 bit).

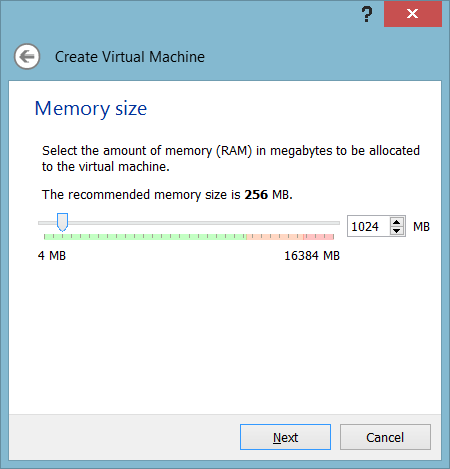
Creation of a new virtual machine starts by clicking the new icon on the top far left side.



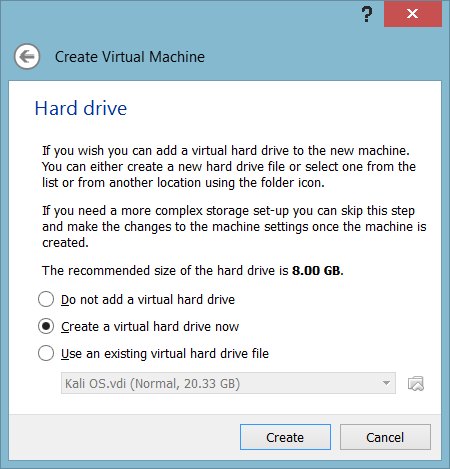
A screen will pop-up prompting you to give the virtual machine a name and give the operating system type and version. \*\*Important\*\* If you have downloaded or are trying to use a 64 bit version of an OS and within the Version drop-down you are only seeing (32 bit) versions, there is a setting in the BIOS that needs to be appended. I ran into this issue when setting up my virtual machines. Here is an effective and easy to understand article that instructs what on your BIOS needs to be enabled: <http://www.sysprobs.com/disable-enable-virtualization-technology-bios>.



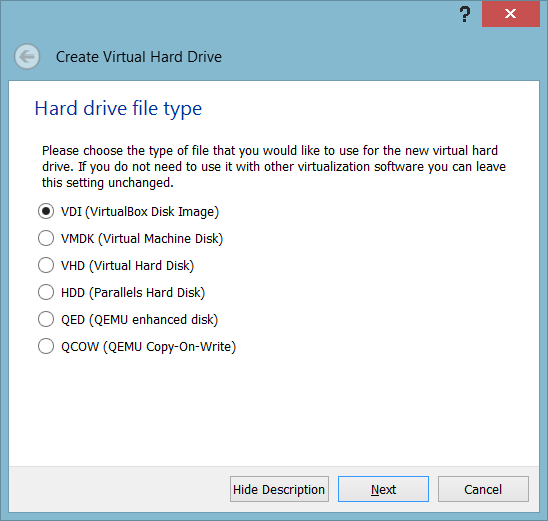
When you are asked to define the amount of RAM memory you would like the machine to use, take in account the total amount of ram you have in your host computer and how many virtual machines you might want to be running at once. Kali Linux as a VM(virtual machine) should handle running at 512 MB just fine. Although VirtualBox recommends only 256MB, it still sits better knowing that there are more than recommended features in these machines. I was generous with mine and gave it 1024 MB just to avoid any future issues that might come up with memory usage.



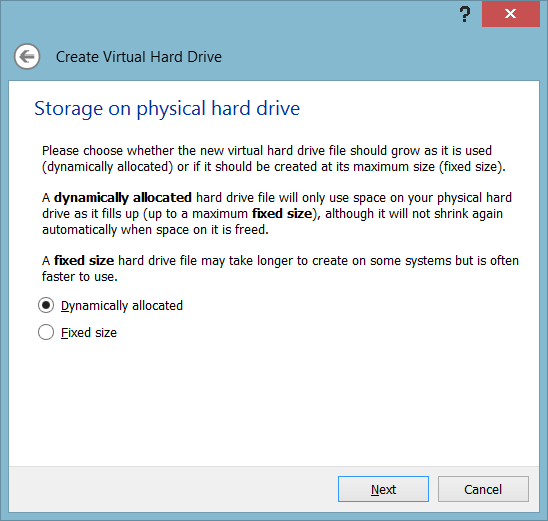
A virtual hard drive is needed for the partitioning and installation of the OS. Select Create a virtual hard drive now and hit Create.



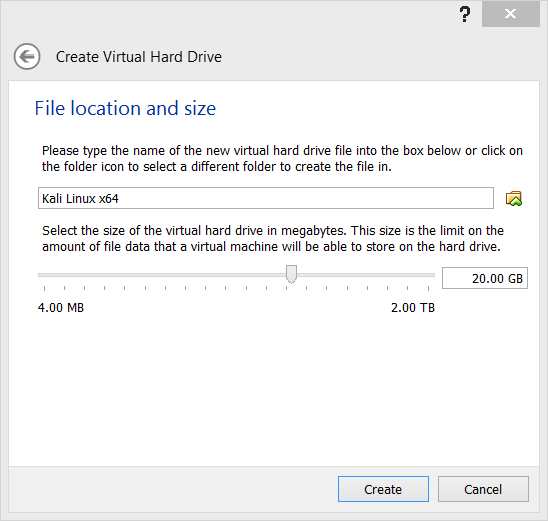
The default selection for the VDI(Virtual Disk Image) is the file type you will need for this creation, so keep it and hit Next.



Again, with this prompt, go ahead and leave it to default. The dynamically alocated file, as described on the prompt, will expand in space only when the VDI drive needs to. A space savor if you will, while the fixed option will take up the amount of space you delegate to it all at ounce.

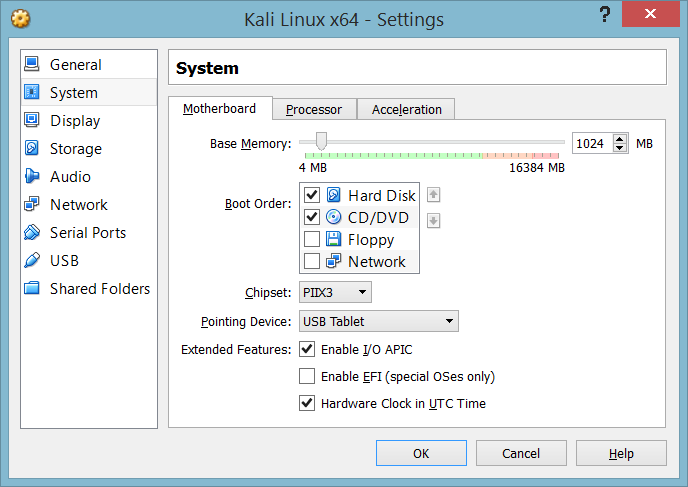


Here you can simply provide the amount of space you wish to give your VDI drive for your VM. \*\*Important\*\* Another run-in with error I had while creating the 64 bit version of Kali Linux, was trying to create a quick VM, I only gave it 10GB of space and during the installation process I received a very bright red error message “Installing Step Failed” at around the 80% mark. I scrapped the installation and the VM and rebuilt it exactly the same. Ran into the same error, so I just raised the drive size to 20GB and everything worked as it should.

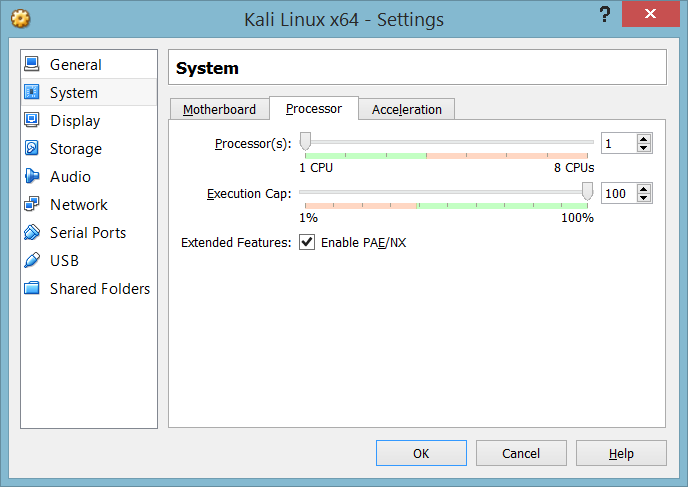


After you hit Create on the last prompt screen it will disappear and bring you back to the VirtualBox main interface screen. The VM you just created should be high-lighted, but if not just click on it and next to where you originally hit the New icon is the Settings icon. Click that and the prompt below with pop-up giving you options for every customization of the “physical” state of you VM.

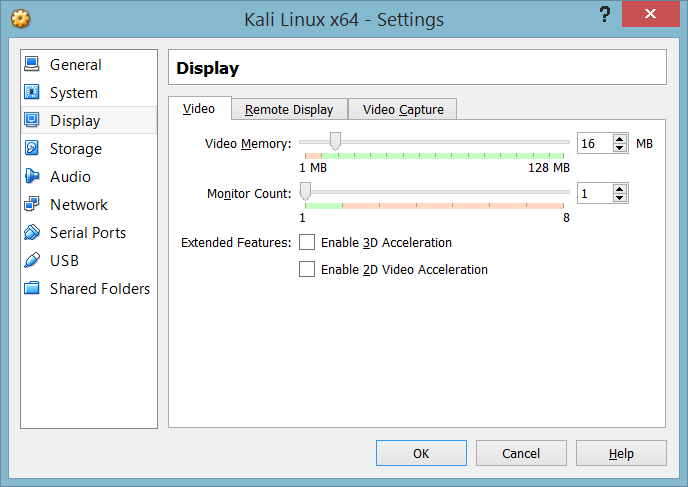
First go to the System tab and deselect the floppy drive. Click on the Hard Disk and use the up arrow on the right to guide it to the top of the boot list. Everything else is fine as it is. Go to the Processor tab next.



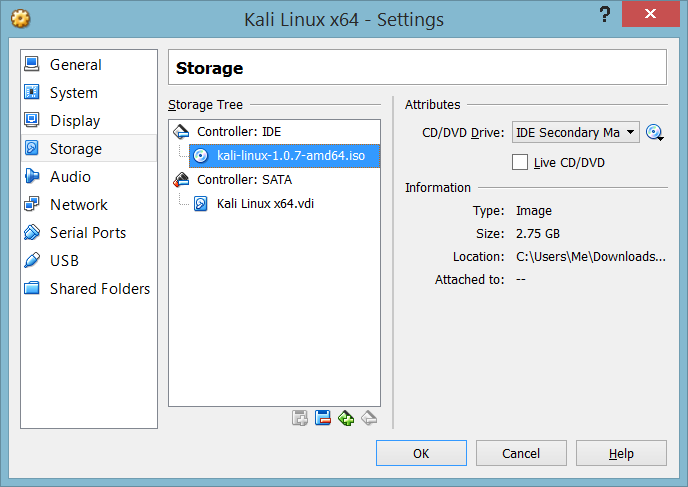
The Processor prompt just gives you options for your CPU. Although, when you first create the VM, the Extended Feature: Enable PAE/NX will not be checked. …



The Display tab has options for a lot of additional features to add to your VM, but in a simple test-lab nothing needs to be altered, in my opinion, unless you would like to boost your video memory slightly. No need to get crazy though. Move on to storage from here.

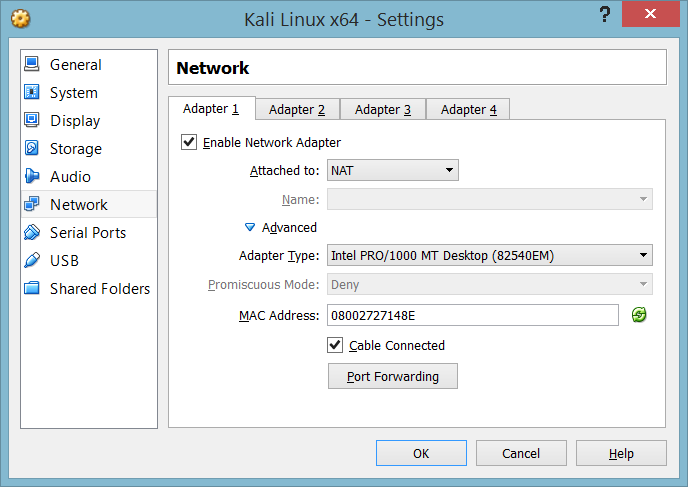


The storage tab will provide the means to process the .iso file for installation on the VM. Under the Attributes section on the right is CD/DVD Drive: Click the icon for the Disk. A drop-down with a list of .iso files will come up along with an option to look one up. Wherever you stored that .iso, find and select it and it will appear under the Controller: IDE within the Storage Tree. That is all here, move onto the Network tab.



The Network tab is very \*\*Important\*\*. This screen could be the difference from learning in a very safe and inexpensive environment to waking up the next morning with a loud knocking on your door from the local PD, which, in turn, would be very expensive. In other words, working in a test lab is like being in a quarantine zone. There’s not a way to get out and infect the outside world, unless you want it to. So, to help you run a safe test-lab you will have to do a couple things.

First, you will need to set up a NAT connection to the outside world/network. I know I just said to make a quarantine, but you must keep a NAT connection at first to run any necessary updates to the new OS you will be installing. After you are done with any updates or use of the connection to the outside world, go back to this screen and uncheck the Enable Network Adapter for this NAT connection, but for now, enable a NAT connection and move on to Adapter 2.

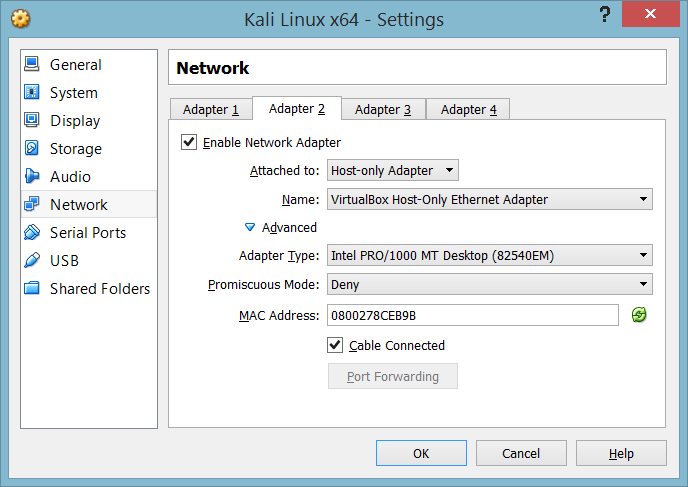


In Adapter 2, you will need to set up your Host-only Adapter. This is where your quarantine is initiated. Select the Host-only Adapter and it will automatically set everything you will need. VirtualBox will act as a DHCP Server for the virtual network and give each VM its own network settings like a real server would in a real network. After you are done selecting the Host-only Adapter, you will have to disable it for the time being. The only Adapter you need enabled at the moment is the NAT on Adapter 1. Now you can hit Ok and start your VM for the first time. To do this just click on the VM you want to start and it will high-light. Click start with the green arrow icon on the top on the VirtualBox screen next to the settings icon from before.

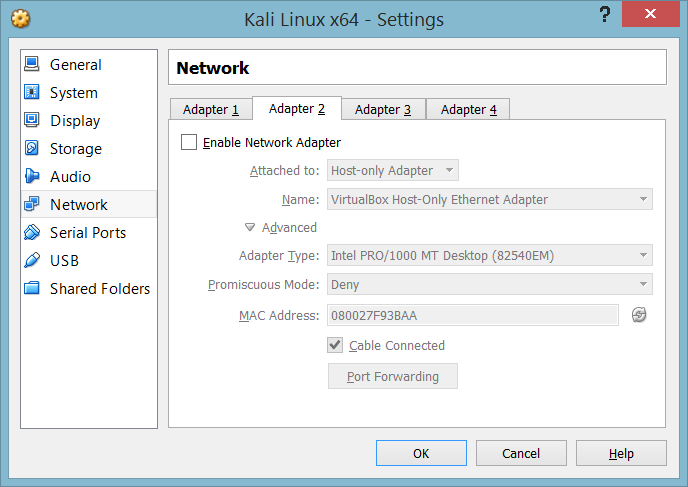
If you would like to manually alter this function, go to File>Preferences>Network

From there you can choose a static IP or disable the DHCP Server. If not, just leave it and you will have your virtual network.

\*\*Important\*\* If you are creating clones of your VM’s, which is not a bad idea at all, you will have to click on the green rotating arrow icon on the right of the MAC Address option. This will give each clone and your original their own MAC Addresses, otherwise you will be running multiple VM units on the same network ID. (To clone a VM, right-click on the VM you want to clone and select Clone. Second option down the list.)

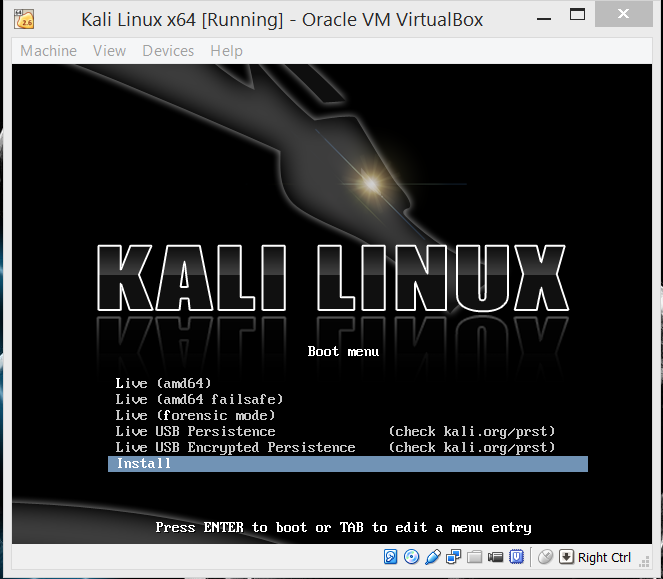


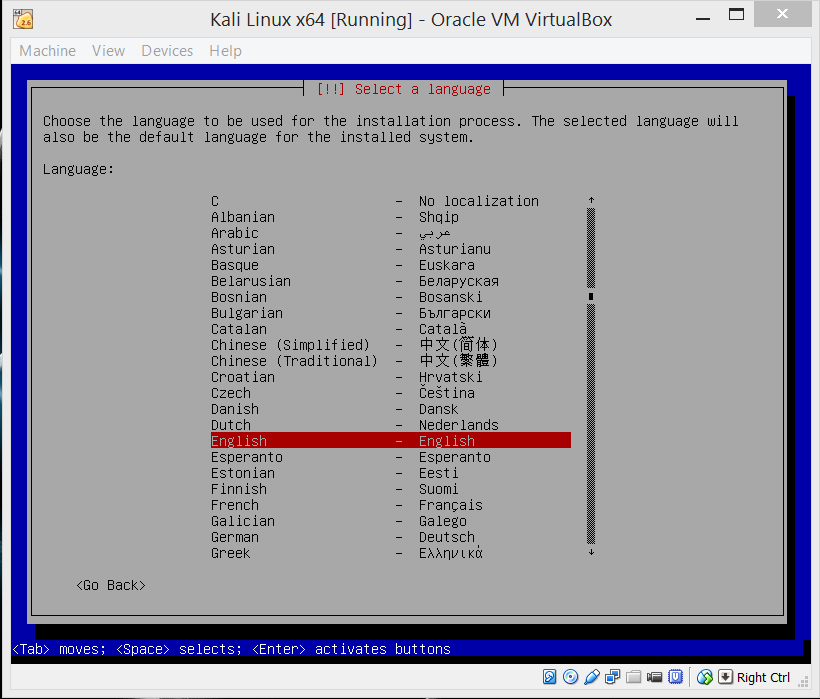
This is what Adapter two should look like after you disable it. The options will be completely greyed-out.

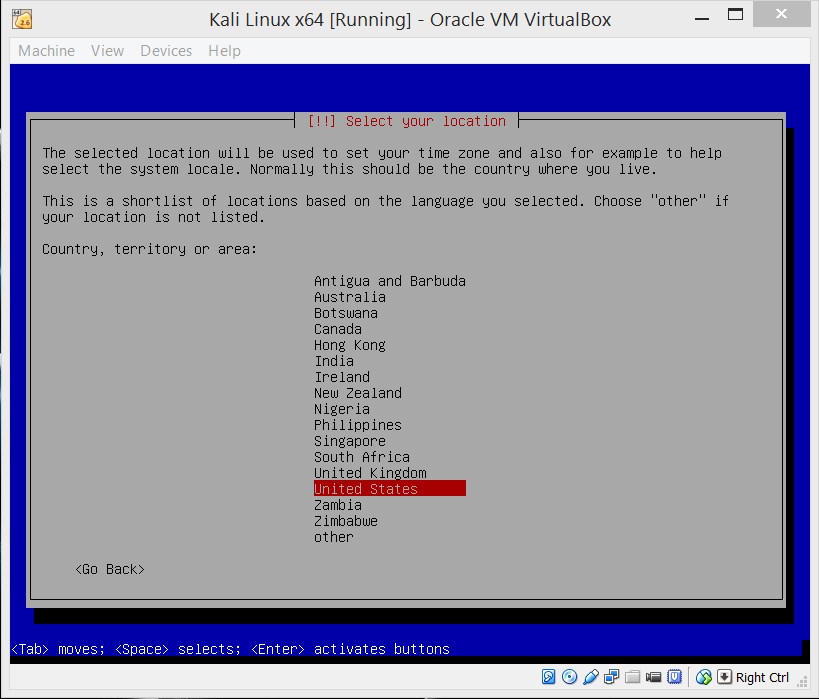


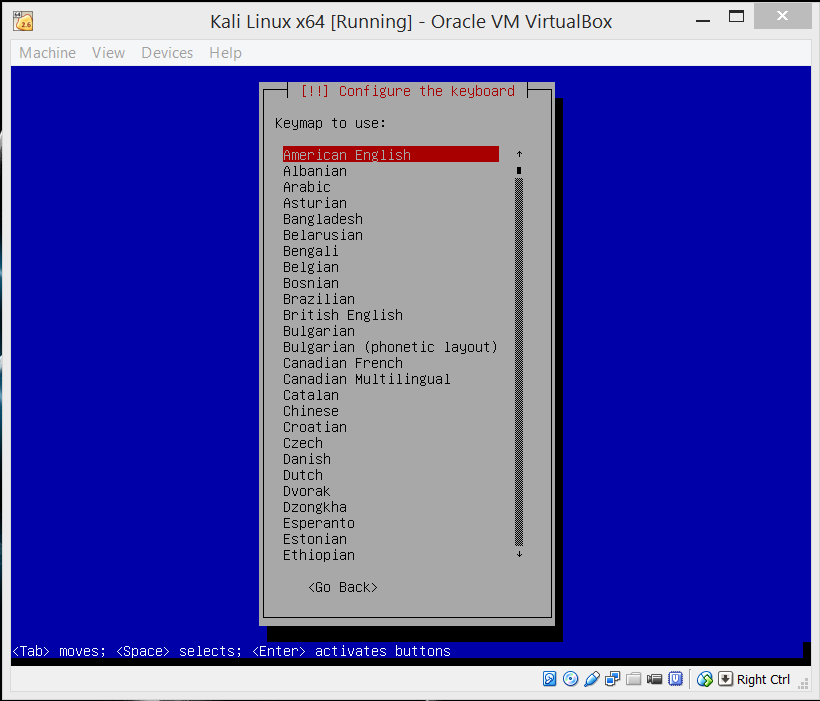
The installation process of Kali Linux x64.

Once the VM starts up it will boot the .iso to begin the installation process. For the normal installation process, just arrow down to install and hit enter. The next few slides cover the basic installation inquiries, so select which options pertain to you.

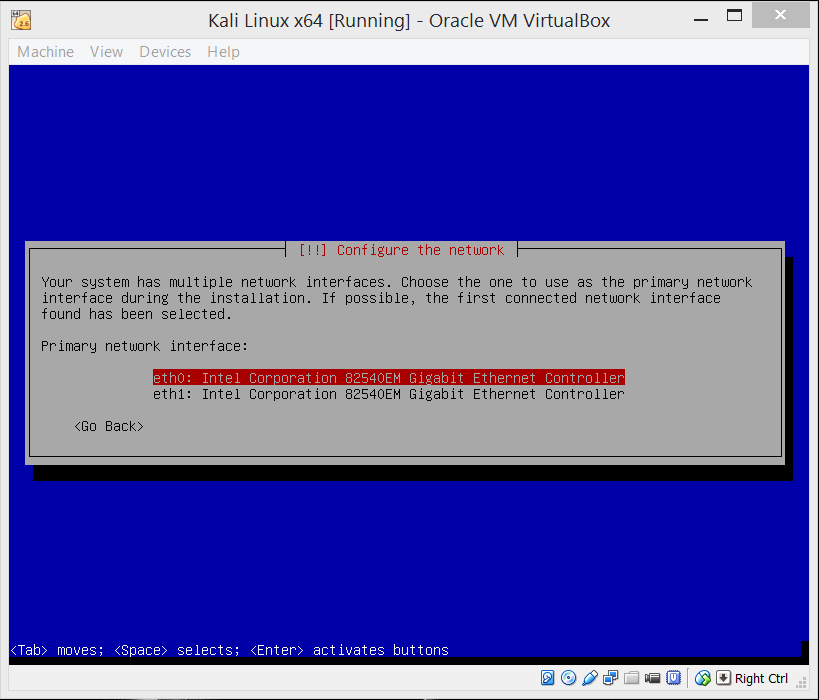




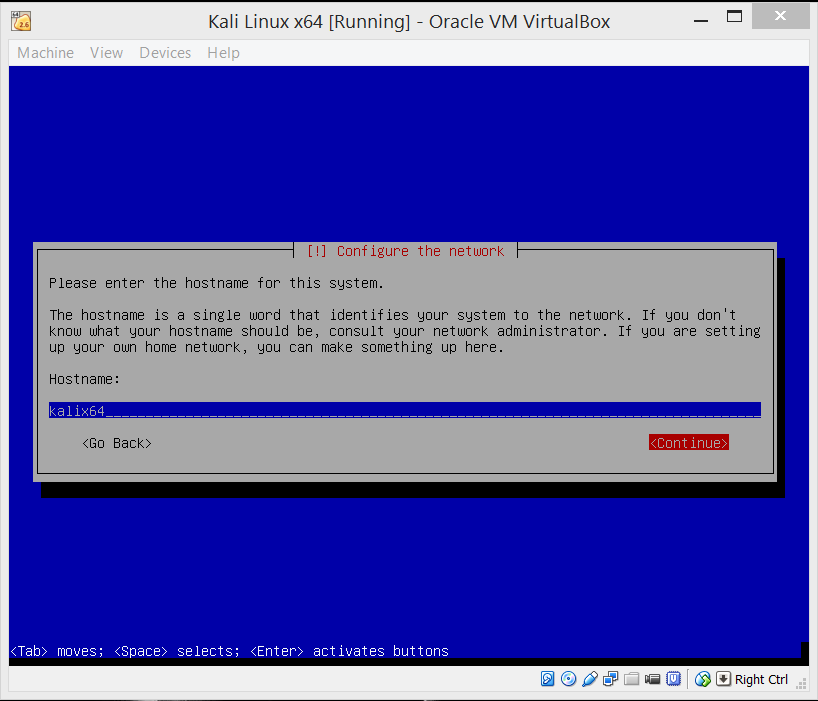




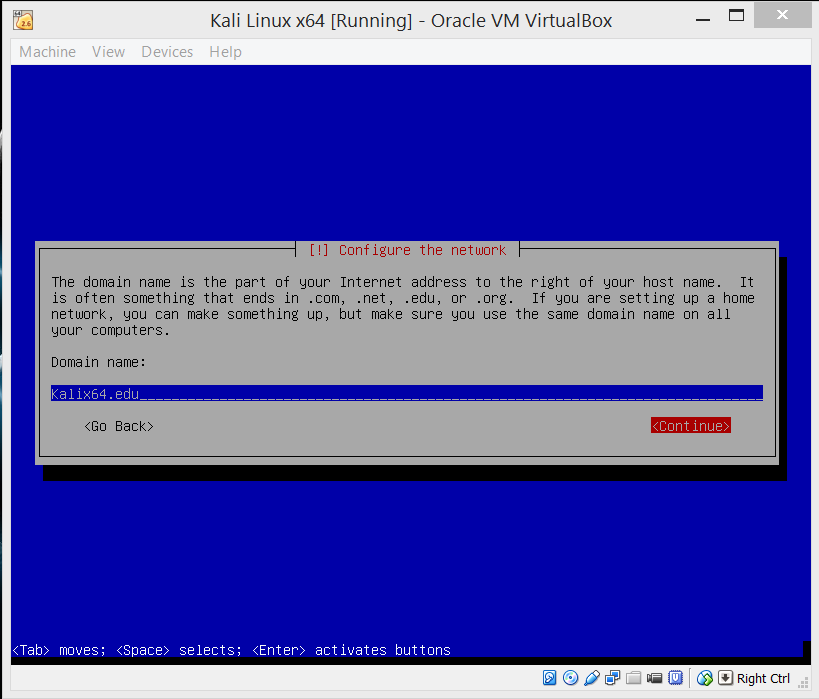
If you followed the way I had previously set up both the NAT and Host-only Adapters, the eth0 is the NAT adapter and the eth1 is the Host-only adapter. When going through the installation process, if you plan on updating Kali Linux or any other OS you install, make sure you choose your NAT adapter.



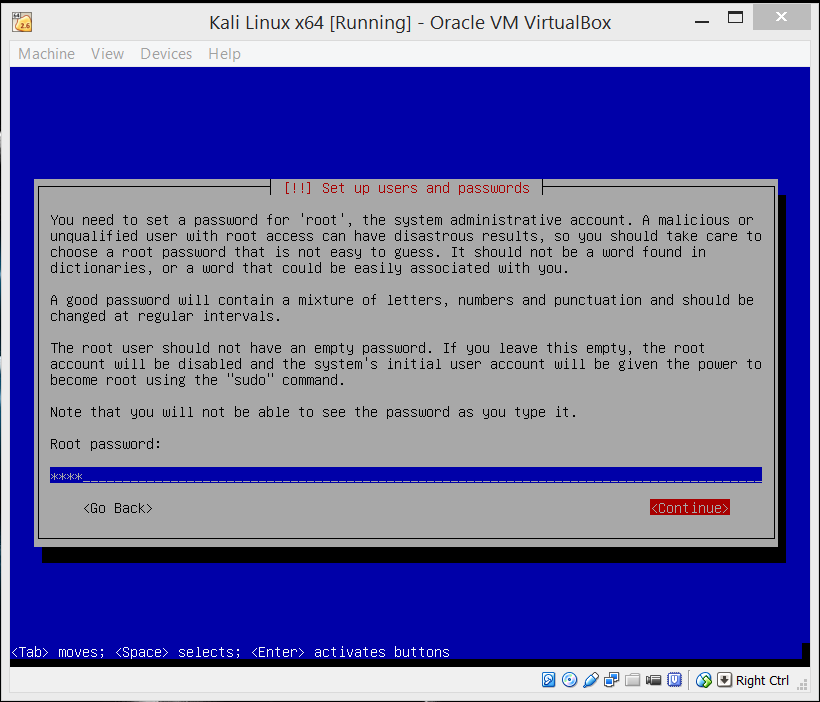
The installation will go through a couple quick loading sequences, so let it run. After a minute or so, you will be asked to provide a hostname. This host name will be what your OS is referred to. While in the command shell it will use this hostname. I chose Kalix64, so when in the command shell I am prompted with, (root@Kalix64 :~#).



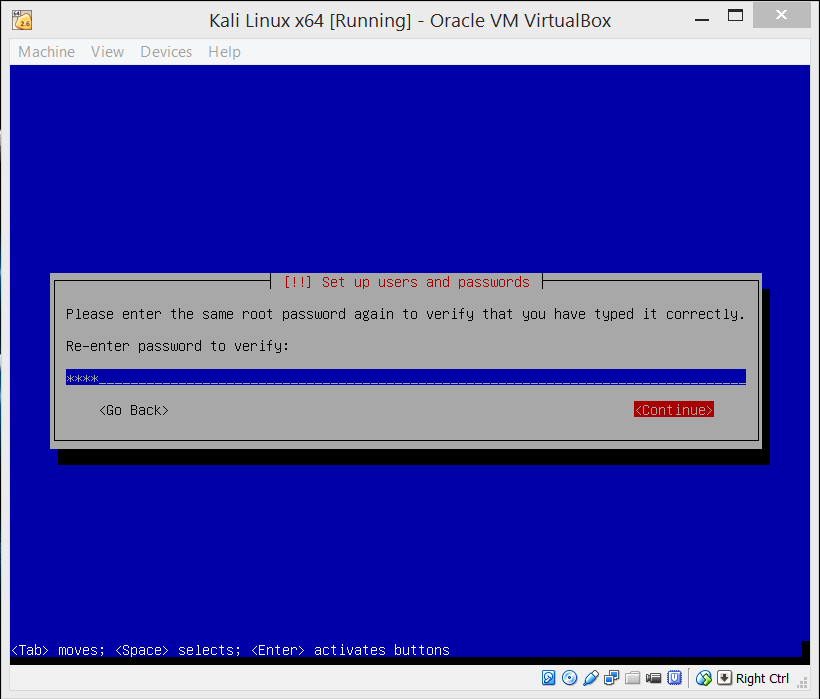
The domain name is not needed, if you do not want to make one, you can leave it blank and continue on. Otherwise, use whatever domain name you desire and continue on.

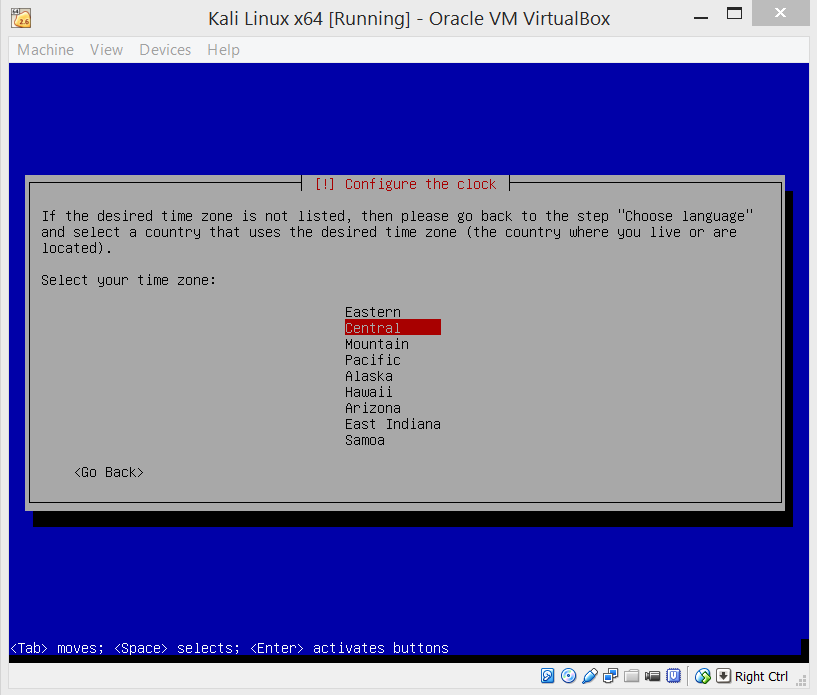


The automatic username for Kali Linux is, root. Here you just need to assign a password of your choosing for root.



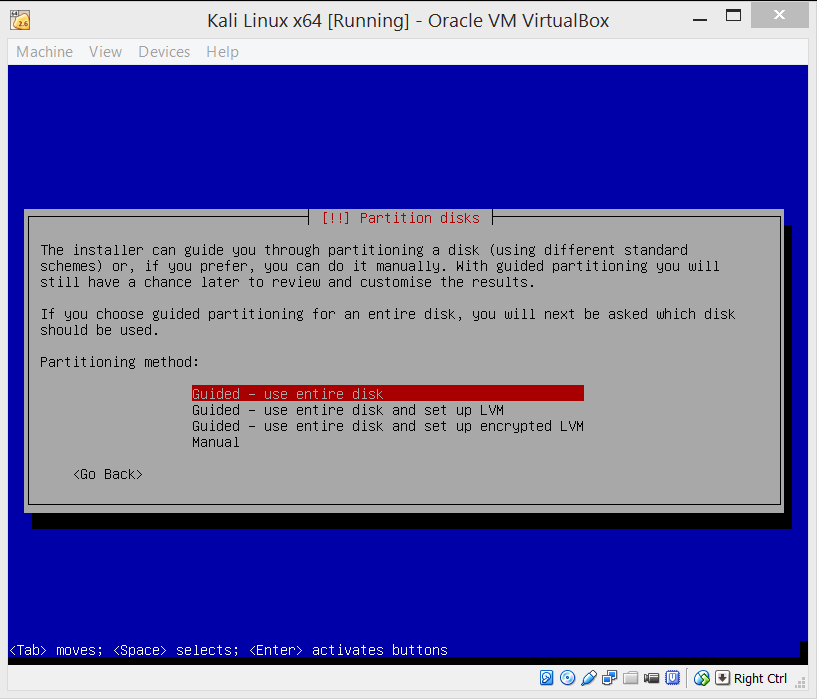
Re-enter your desired password.



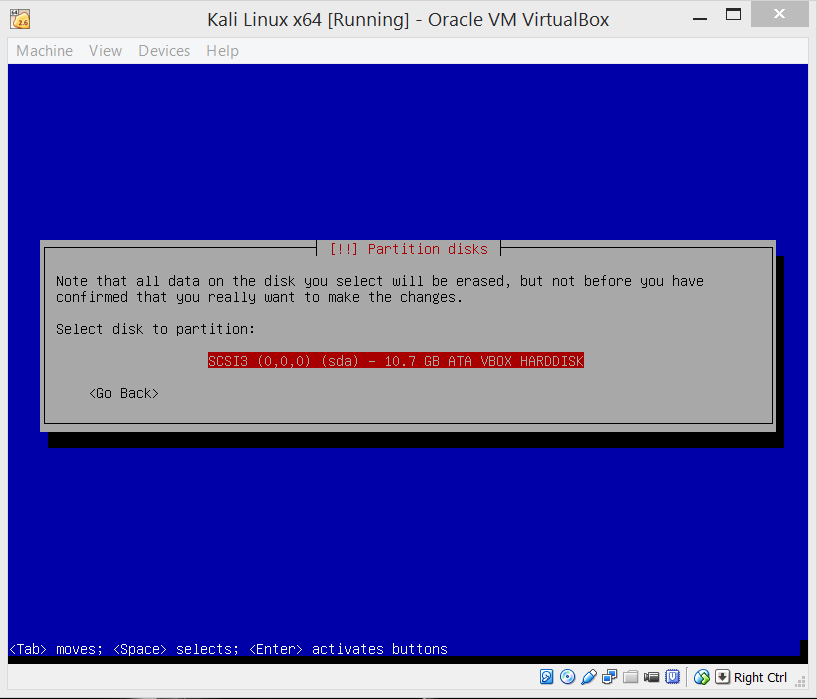


More loading sequences to run through.

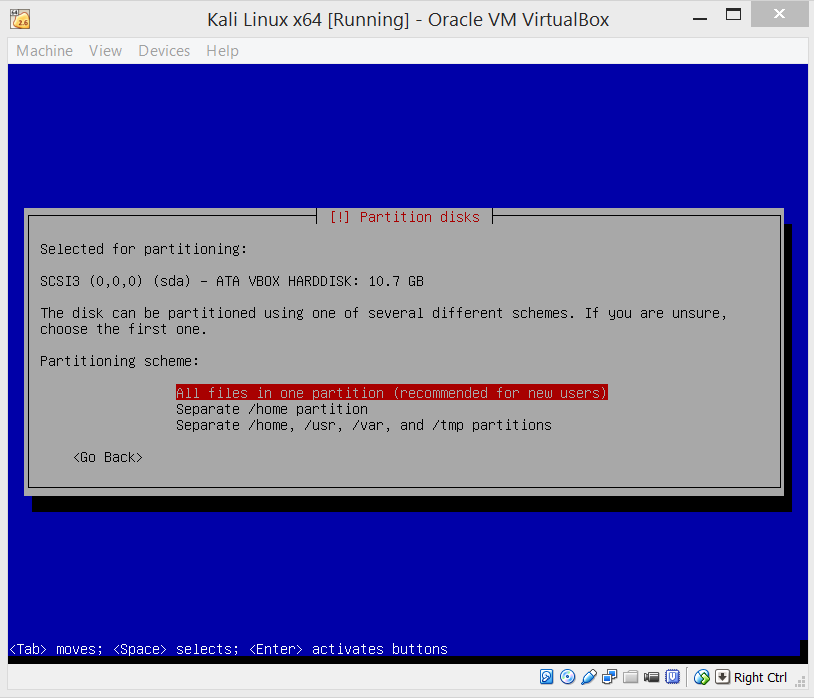
For the simple setup of Kali, keep the default selection of the (Guided-use entire disk) option.



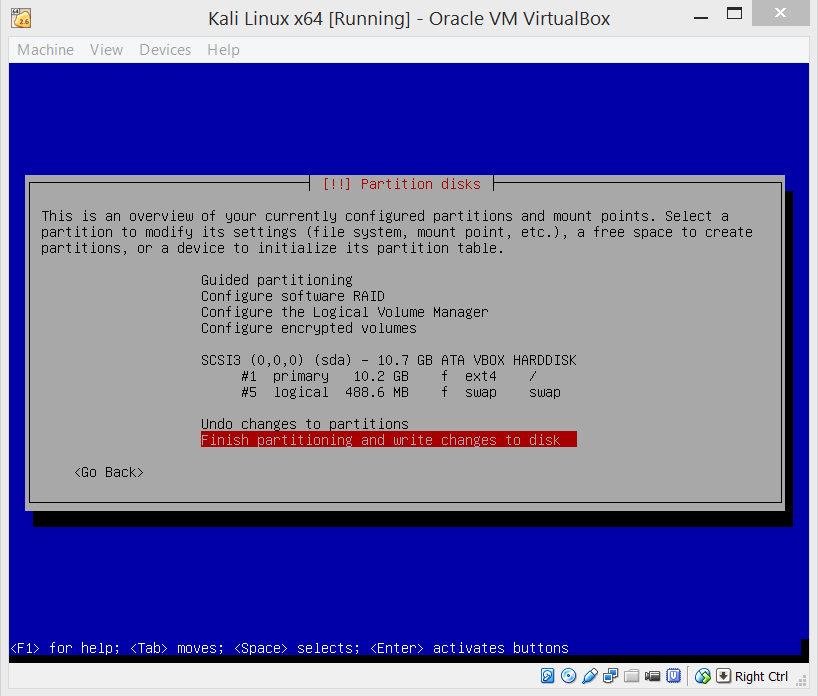
In most cases you will only have one option here to choose from, unless you have created your VM differently from the steps we went through above.



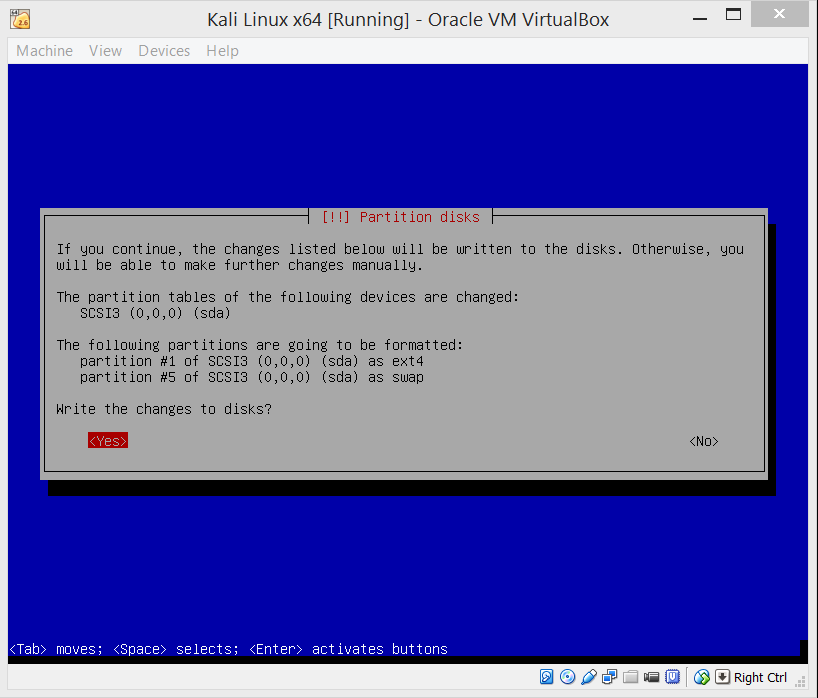
Once again, no need to get crazy for setting up a simple testing-lab, keep the default option and hit enter.

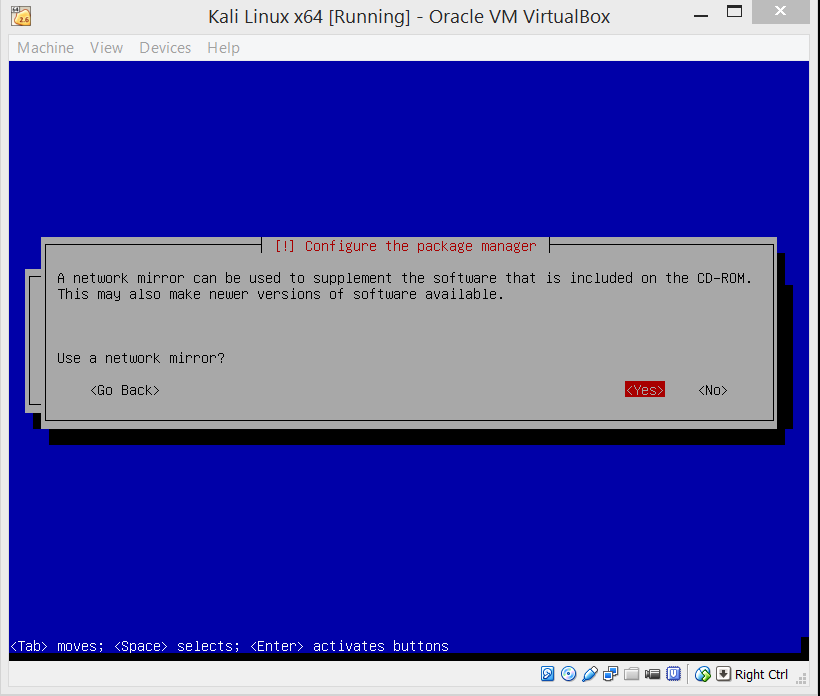


We are almost finished here, keeping everything simple, just keep the defaults and hit enter again.

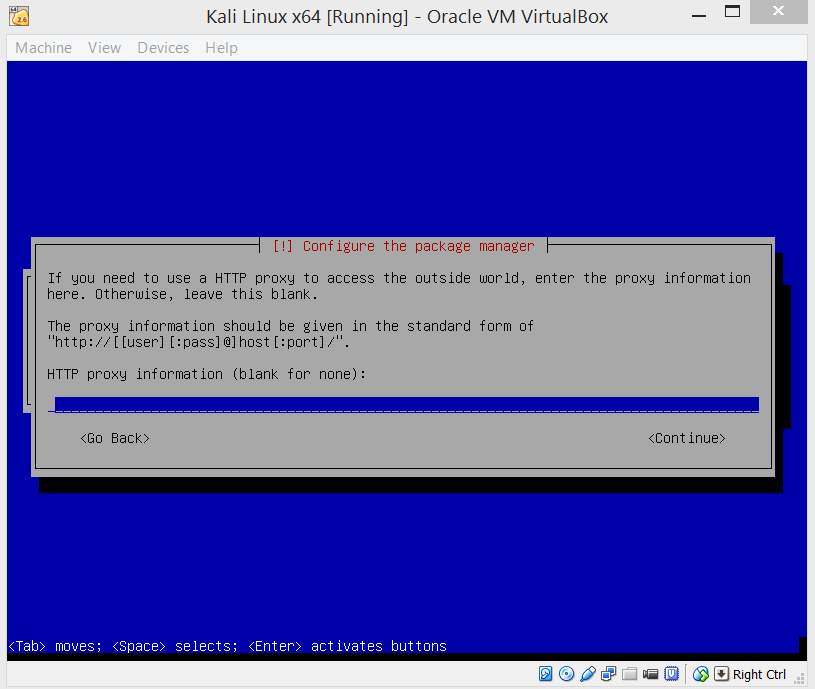


This will be the final partition prompt, but this you will have to change from No to Yes if you would like to continue with the installation process.



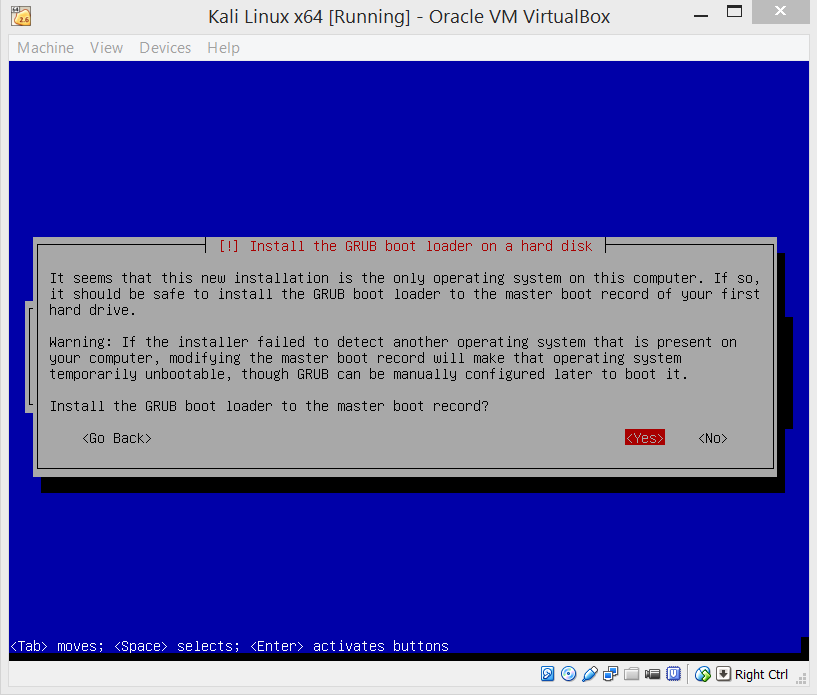
Let the installation continue its loading sequences. This session will be longer than the others, but will break and ask you if you would like to create a network mirror. Select yes and continue on.

These is no need to put anything in for this prompt. Just continue on with it blank.

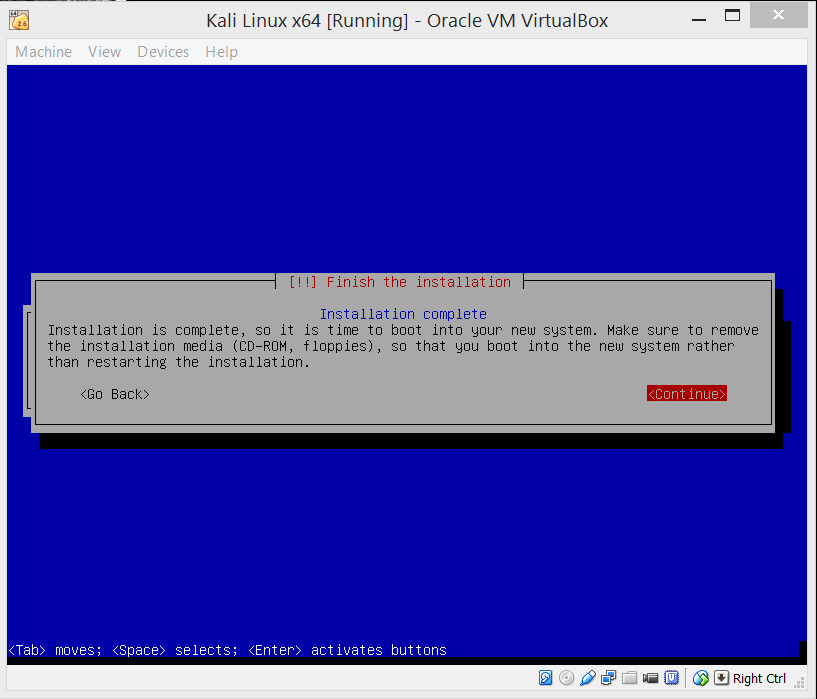


The loading sequence will continue again.

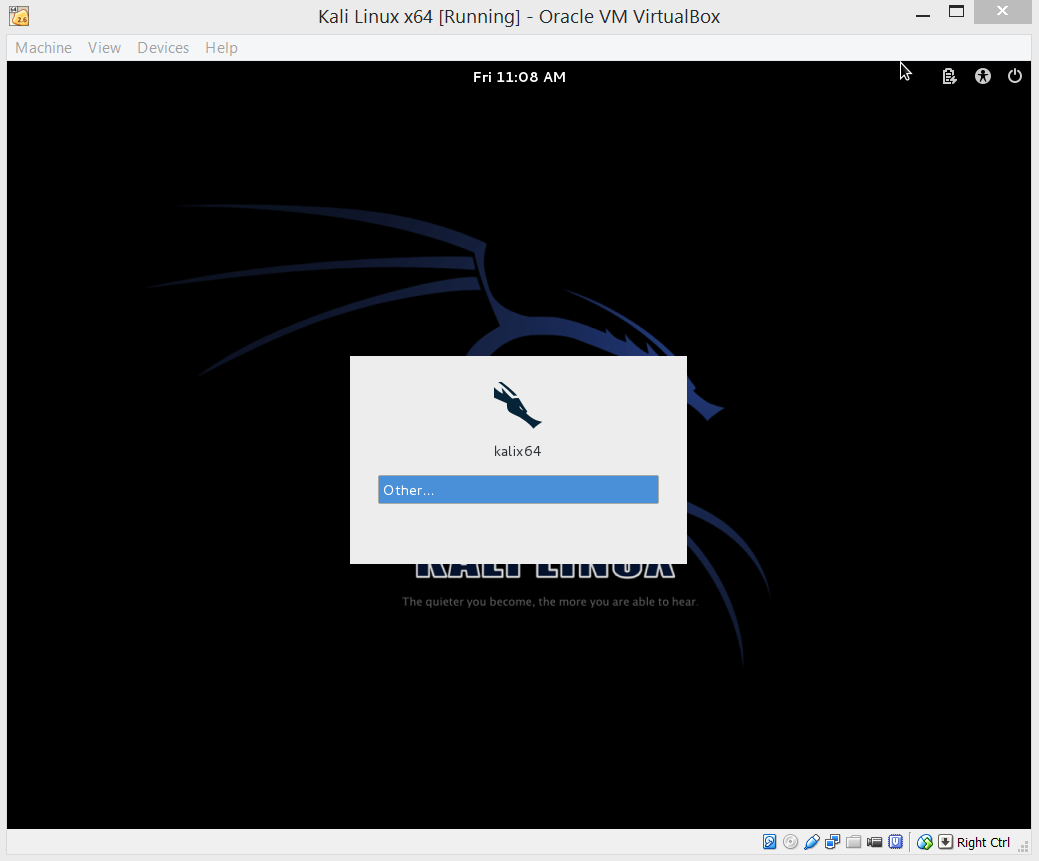
Select Yes and install the GRUB boot loader for the installation for this VM.



The installation will load through until the process informs you that it is finished. Once you are informed, select continue and do just that.



After selecting continue, you will go through the last phase of the OS installation process.

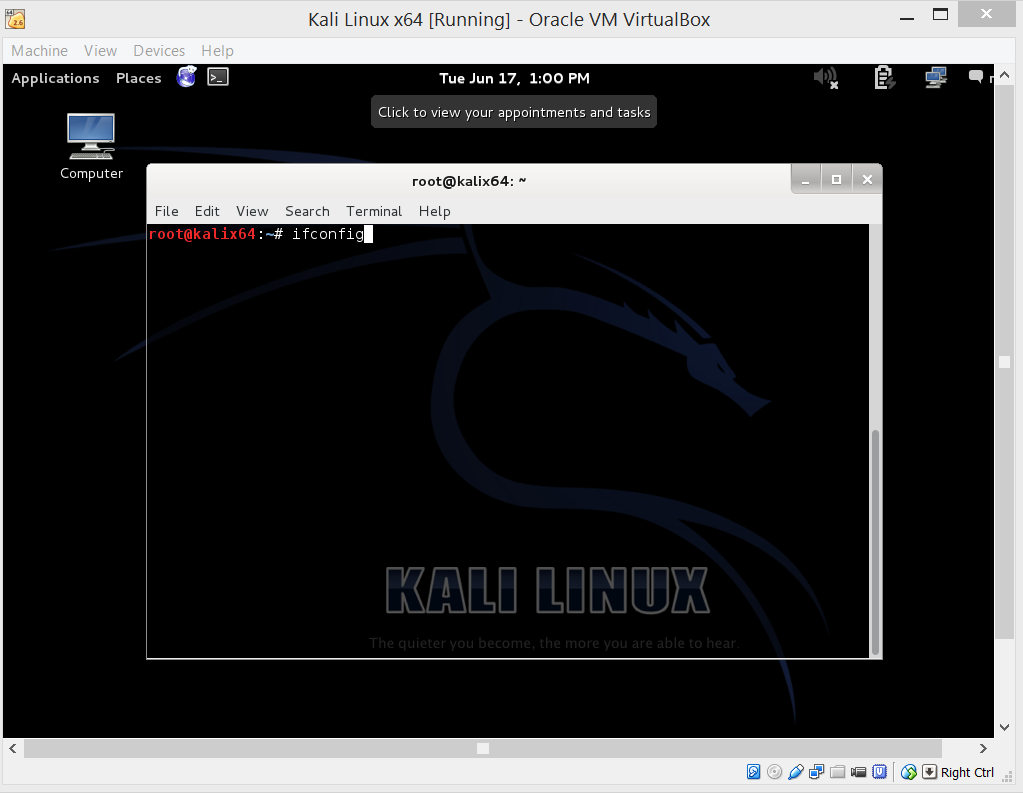
From now on, the VM for Kali Linux will start up with the screen below for the user log in. Hit enter when you come to this screen and you will be asked to enter the user name. Remember that the user name is “root” and then you will be asked to enter in your password, do so and you will be logged in. 

After logging in to Kali Linux, you should think about updating the OS to ensure you have the most current versions of the hacking equipment built-in to Kali Linux. So, first thing you should do, is make sure you do have a connection to the outside world. You can do this a couple different ways:

Both ways are simple, but everyone has their preference.

Notice at the top-left of the desktop there are the words “Application” “Places” and on the right of that is the Iceweasel icon, which is the browser (Iceweasel…Firefox…get it. Ok, good.) and to the right of that is the Terminal (command line/shell).

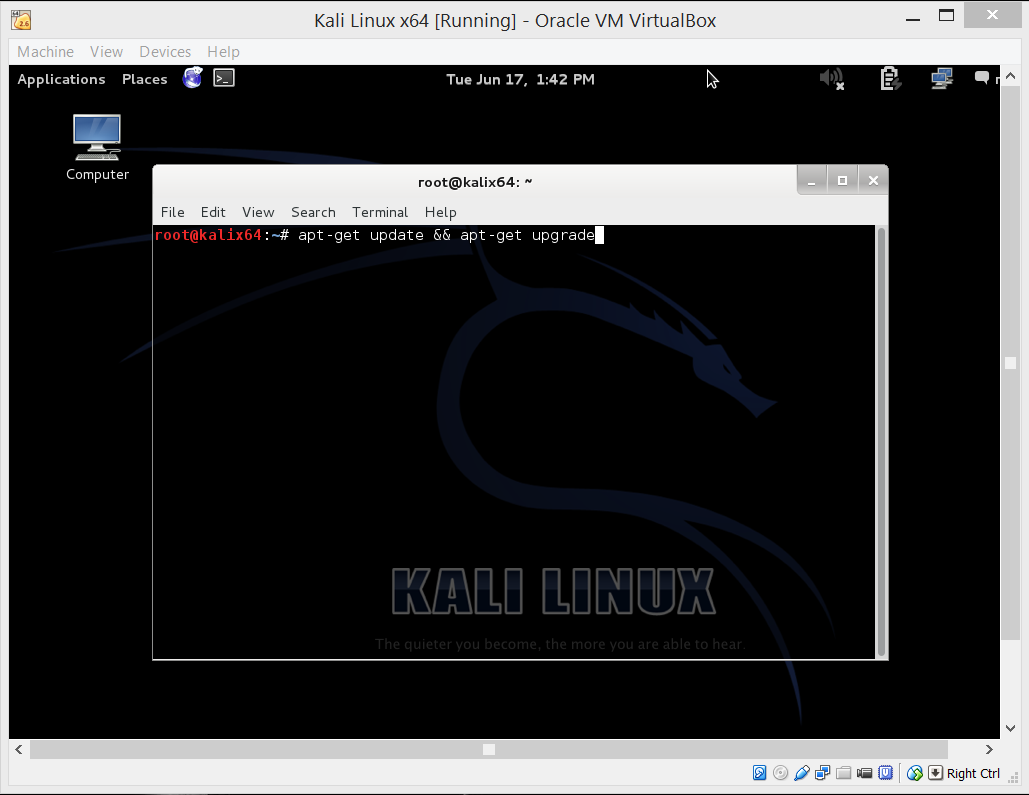
Below is the image of the Terminal opened up and the script “ifconfig” written into it. This ifconfig is like ipconfig in the Windows Command Prompt. Once you type ifconfig in, you will receive your network information for each adapter currently enabled within your VM. As we had enabled the Adapter 1 previously, you should see two outputs: eth0 will be your Adapter 1 (NAT as we set up earlier) and “lo” (Local Loopback).



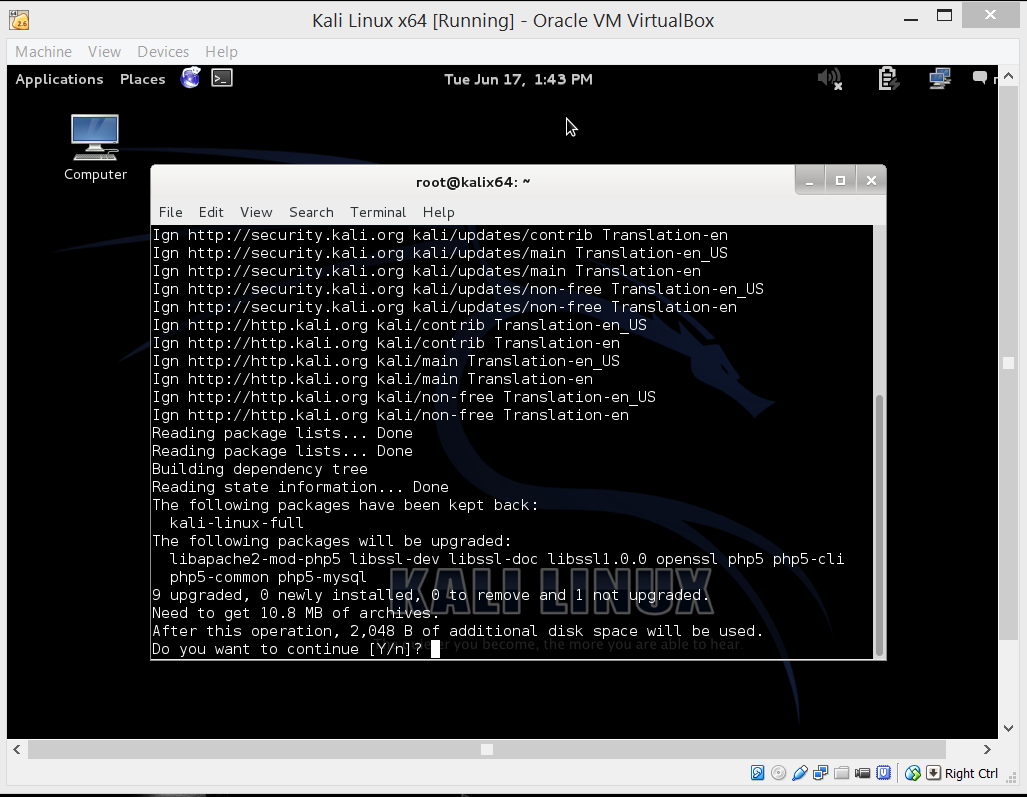
The second way to figure out if you have a network connection to the outside world, one that is easier to understand for most, is to click on the Iceweasel icon and you will now have a browser in front of you. As you can see below, the homepage for Kali Linux comes up automatically. We are not out of the water yet, this does not mean you are connected. So, to check your connection, just use the side search-bar with “Google” in it and attempt to look up anything or any website your heart desires. If you are able to go to Google’s search page or where ever your destination was, you are connected.



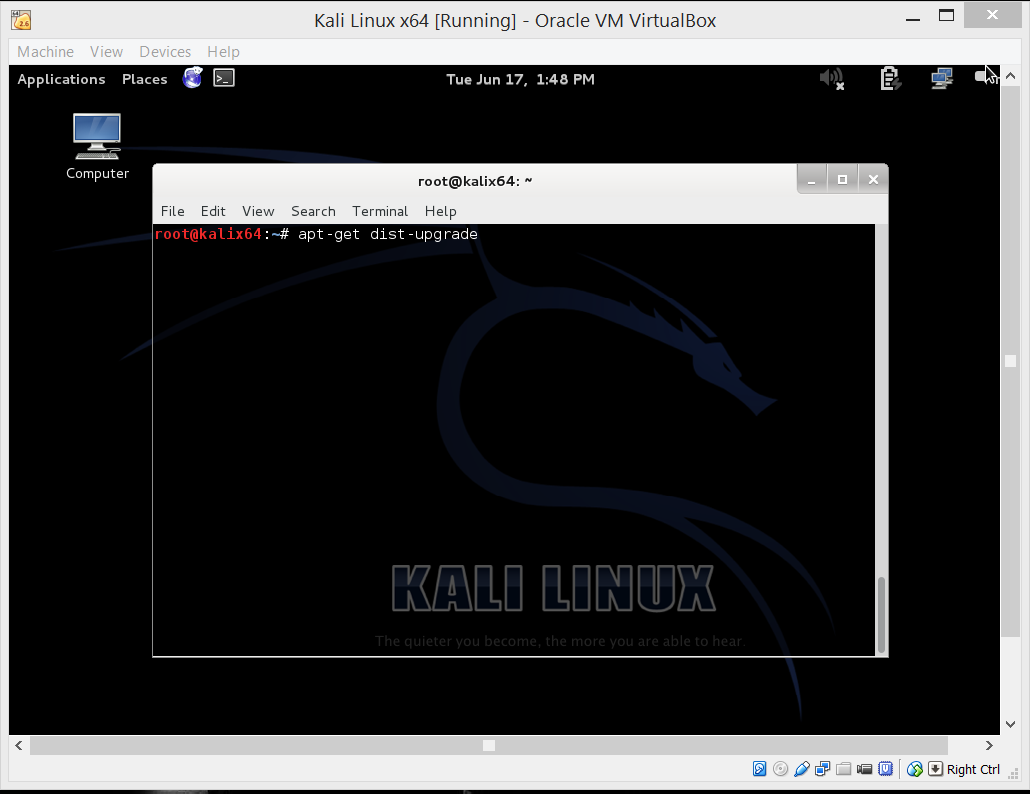
Now that we know there is in fact a connection, updating the OS is the next step. If you used the Kali Terminal to check for the connection, good. You will need to be in the Terminal to give the proper commands to get this task complete. You should be looking at a prompt like was shown before with the “ifconfig” image. This time you are going to want to type a few different commands, I will give you the list of commands now and you can decide if you want to use them all at once like I will show you or one at a time, which is fine as well. The first set of commands are “apt-get update” (to update Kali), “apt-get upgrade” (to upgrade versions on Kali if needed), and “apt-get dist-upgrade” (a more higher-end upgrade that can upgrade the version of Kali if need be). The commands should be used in the sequence I have given. You want to update before you upgrade. (To use all commands at once, add “&&” between lines as shown below.)



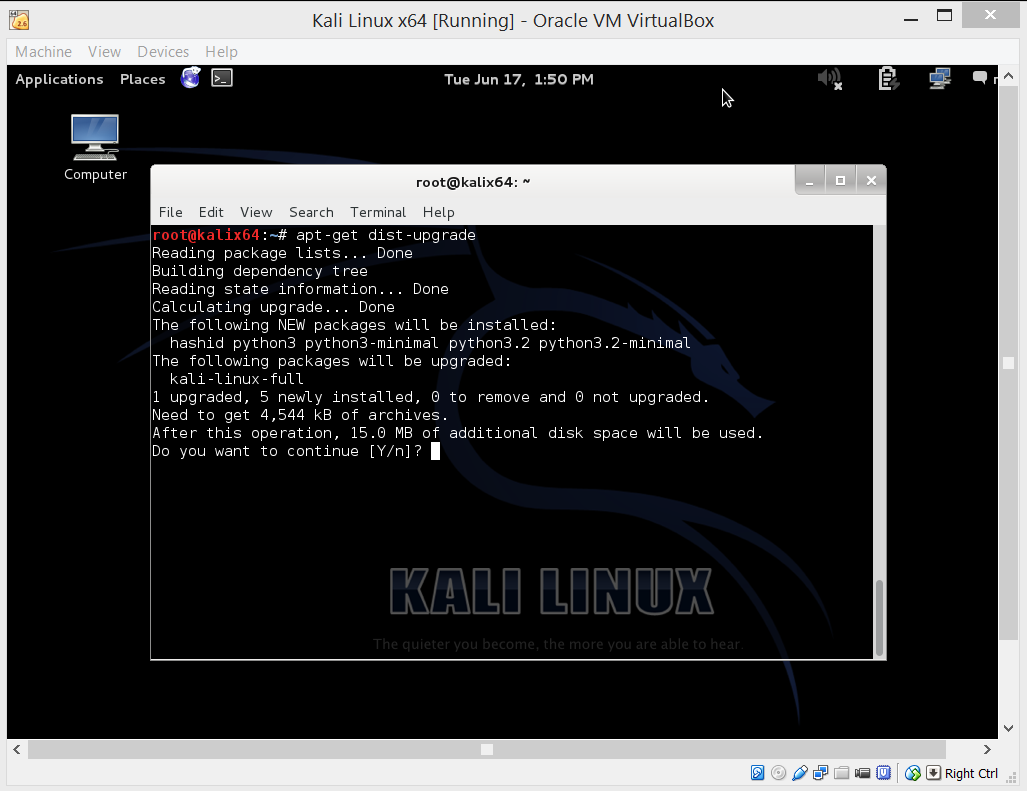
After hitting enter, the process will start and then prompt you with a question. Hit “y” and enter to continue on.



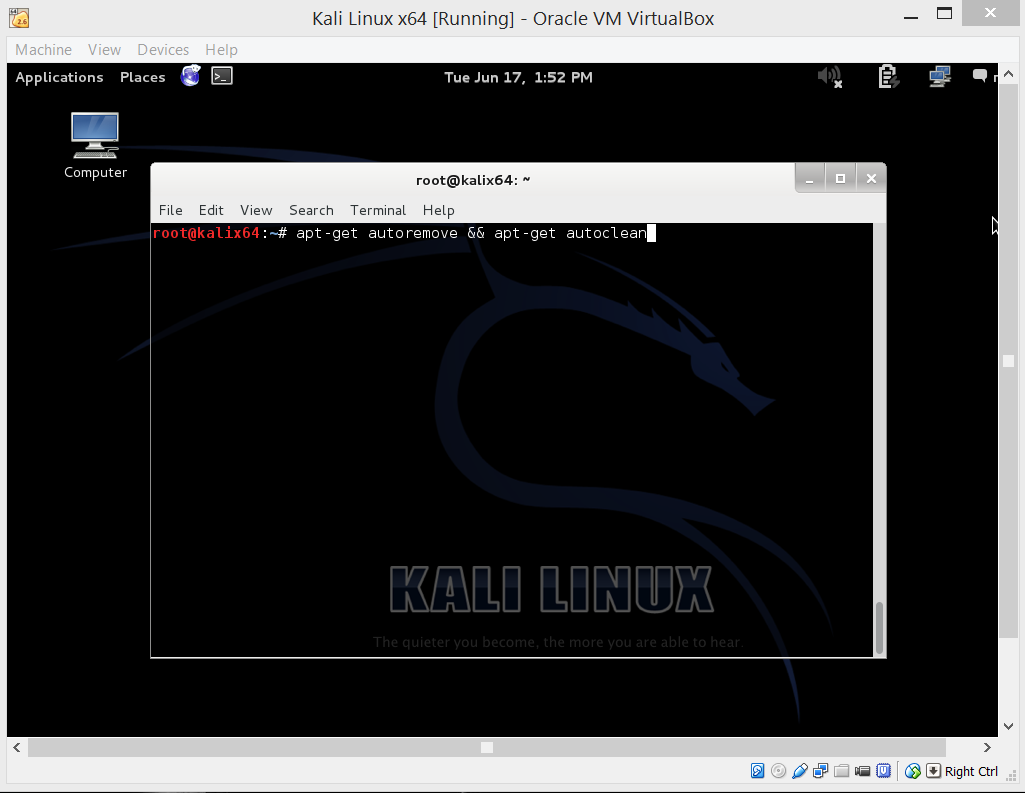
After that process is complete, you can now input the command “apt-get dist-upgrade”.



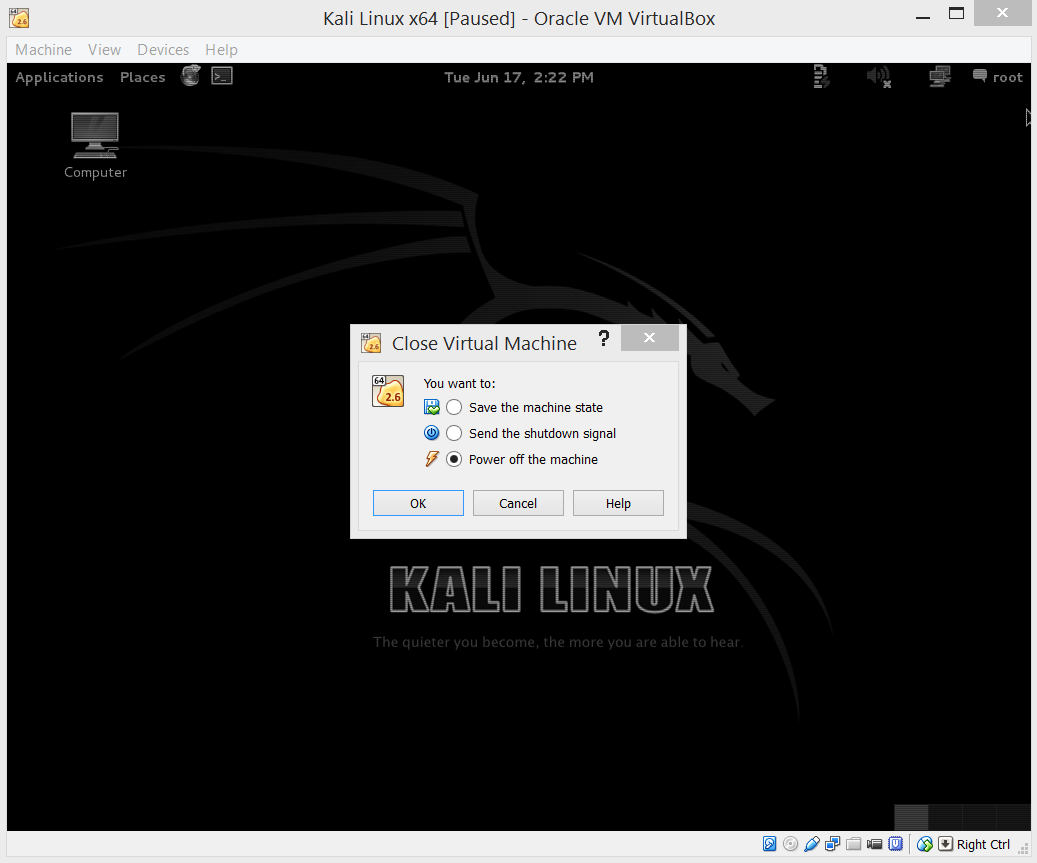
You will again be prompted with a question. Put in a “y” and hit enter to continue.



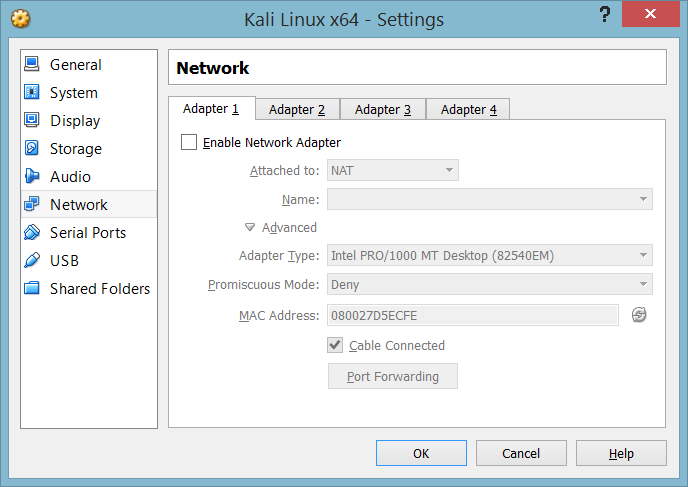
After updating and upgrading, you should run two more commands. “apt-get autoremove” (which will remove any old or garbage pieces of data that are no longer needed) and “apt-get autoclean” (which will clean up disk space within your VM).



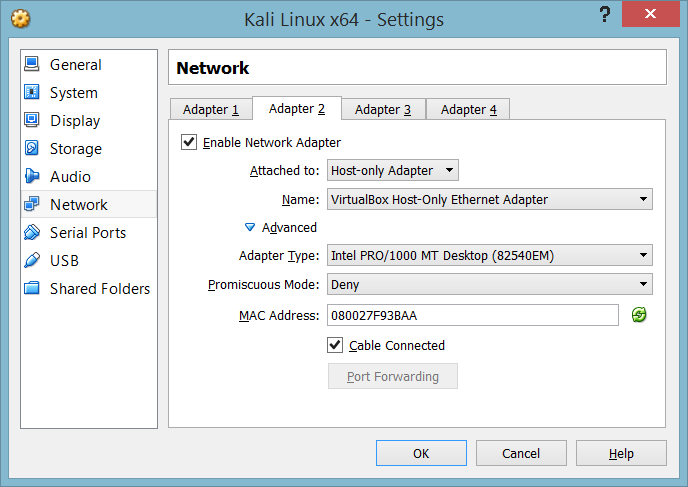
You now have a complete update and upgrade of Kali Linux.

The last step to complete Kali Linux and make it test ready, is to disable the NAT adapter. To do this you must shut down the VM, by clicking the red “X” on the window of the Kali Linux VM. You will then get the option screen with a few options on what to do. Select the Power off the machine option and Kali will shutdown. 

Back at the VirtualBox screen. Click on the Kali Linux VM you have created and move your curser back up to the top and click on the Settings icon. The settings screen will pop up, go to the Network tab and the first Adapter available is Adapter 1, which is what we had previously enabled as our NAT Adapter. Uncheck the checkmark where it states Enable Network Adapter. Everything below should be greyed-out and you are no longer connected to the outside world with this Kali Linux VM.



Proceed to the Adapter 2 tab with the Host-only Adapter and check the box to enable it.



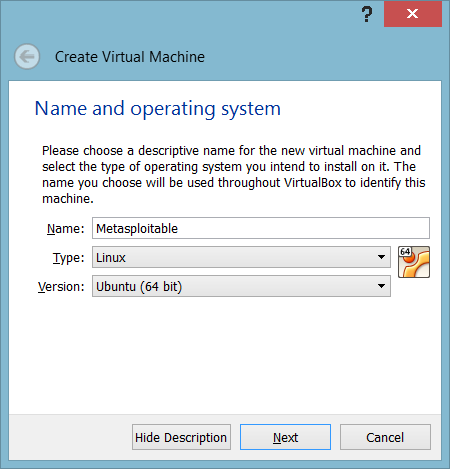
Just to be safe though, check through the rest of the Adapter tabs and make sure that Adapter 2 (Host-only Adapter) is the only Adapter that is enabled. If that is all done, you are good to go and move on.

Creating and installing Metasploitable as your vulnerable victim VM.

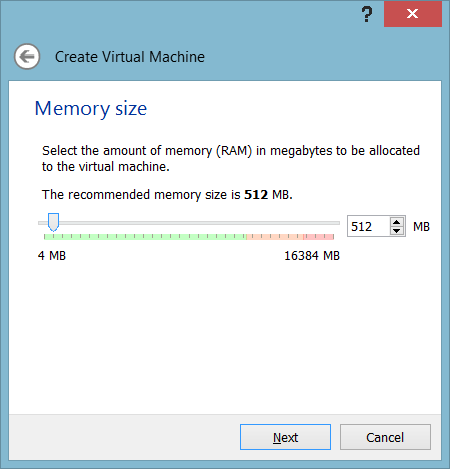
Information on Metasploitable is located at <http://www.offensive-security.com/metasploit-unleashed/Requirements>

First you will need to download the .iso for Metasploitable available at <http://sourceforge.net/projects/metasploitable/> You will have to extract the .iso out of the Zip folder.

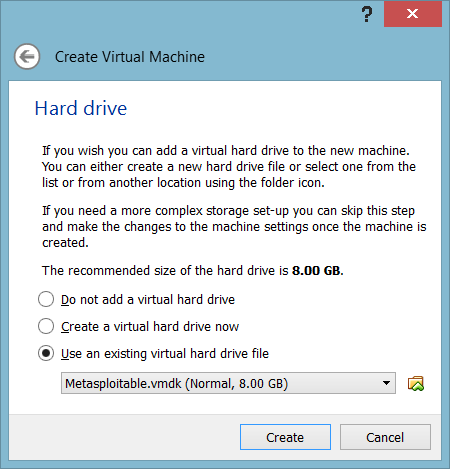
The process of creating a Metasploitable VM is much simpler than creating a VM for Kali Linux. Just as you started the creation process for Kali Linux, go up and click the new icon at the top of VirtualBox. You will see the screen below which now you name Metasploitable whatever you would like and go down to Type, select Linux. Version and select Ubuntu(32 or 64 bit version does not matter much for this, in my opinion).



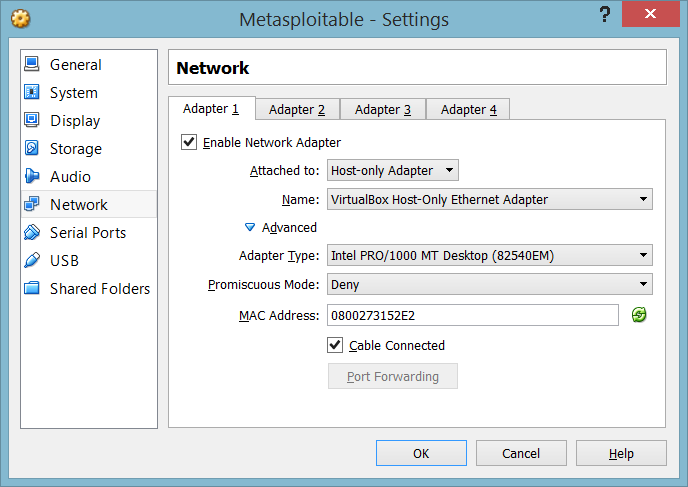
You will then be prompted with the below screen to decide how much ram to give Metasploitable. I again was generous and gave my VM 512MB of RAM, but you should be just fine with 256MB, because the OS does not take much of anything to run.



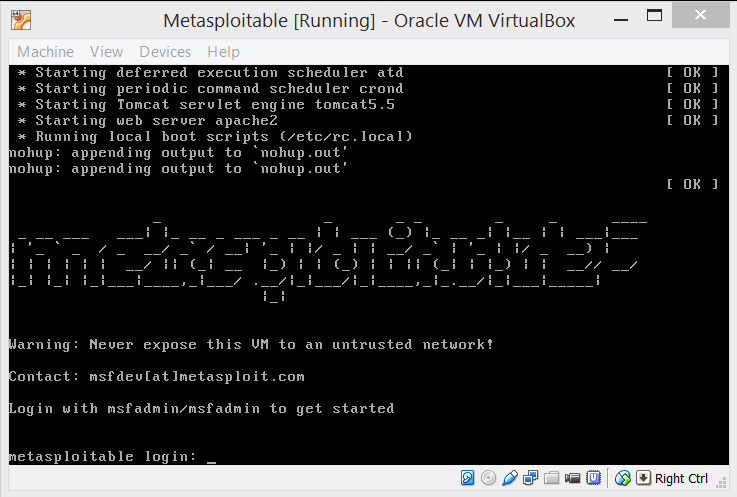
The Hard drive step is where the process differs. Instead of creating a virtual hard drive, we need to select Use an existing hard drive file and next to the drop-down is the folder icon with a green echelon in front of it. Click that icon and search for the Metasploitable.vmdk file as it shows below. The VM is ready to create.



The only setting to alter is the Network adapter settings. There is no need to create two Adapters like with Kali Linux. Making one Host-only Adapter will make this VM available to your Kali Linux VM for penetration and attack.



After you set the networking, you can hit Ok and the prompt will close. Start up your new Metasploitable VM and remember that Metasploitable username and password are both (msfadmin).



Now you can practice and enjoy the Penetration/Hacking test-lab you have created.