Github : <https://github.com/trevortrites/Linux_Admin_Portfolio>

**MIDTERM PORTFOLIO OVERVIEW**

**1 Biggest Challenge so far?**

My biggest challenge has been the individual scripting for each lab. Each one is different in each way and working on them takes some time. In addition to getting my VMs configured.

**2 Moment you were most proud of so far.**

So far, my proudest moment is getting servers up and running and configured, with things working correctly.

**3 One thing you will do to improve for the second half of the class**

One thing I will improve on is my regex and scripting efficiency, with more organization.

**4 One thing from term you could see yourself using in a job in the future**

I can see myself working on networking and firewall scripts and rules in the future. This is a very important skill to receive and be able to master.

**5 One thing you want to add or change to make this portfolio better for the final**

I want to organize my GitHub more with folders with more organization structure that is easier to view when viewing my work.

**Setup of a CENT OS and Ubuntu server**

**Preparation:**

To create a working Ubuntu and CentOS server you must start with an updated version of VMware. In my process I used version 15.5 PRO. After ensuring you have an updated VMware application, download ISOs from these links…

CentOS: <http://mirrors.mit.edu/centos/8.2.2004/isos/x86_64/>

Ubuntu: <https://ubuntu.com/download/server>

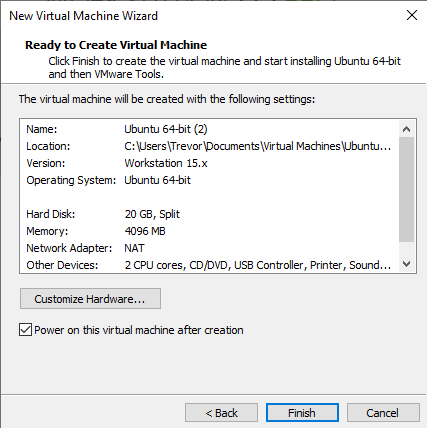
Put them in a folder together that it is easily accessible…



**Ubuntu:**

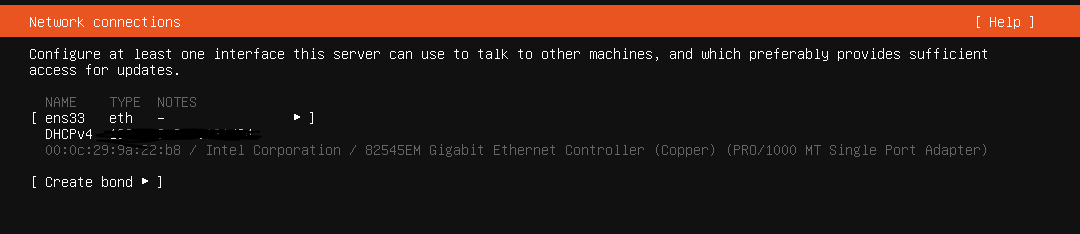
We will start with the ubuntu install, creating a new virtual machine from the home menu on VMware. Select **installer disc image file (iso):** then select browse and find your Ubuntu ISO.

Take default settings and enter in you name, username, and password. Click next till you get to this screen:

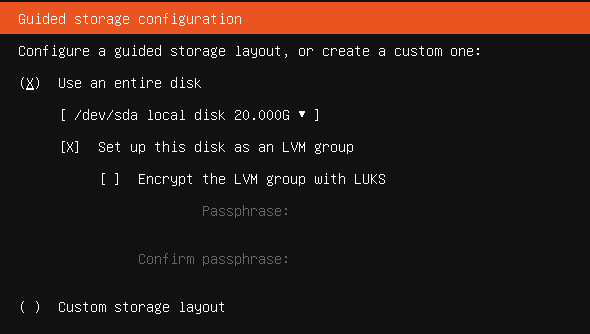


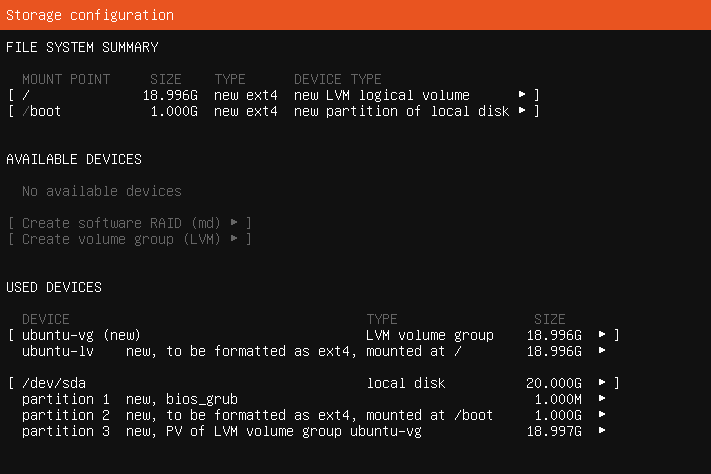
Click Finish and your VM of Ubuntu will boot up. Ubuntu will check its integrity and make sure it is up to date. You can press enter if it is not installing anything.

Once everything has been checked and updated it will bring you to the first setting screen which will be to select your language. Press enter until you get to the network connections tab. Ensure your IP and connection to your network is there. It should look like this with IP next to DHCPv4.



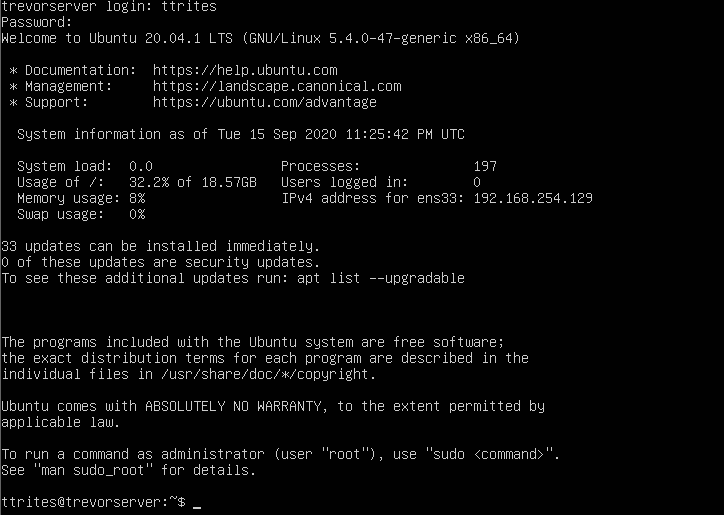
Press enter to configure proxy and archive mirror and ensure you are partitioning the correct amount of your local disc. In addition to your file summary.



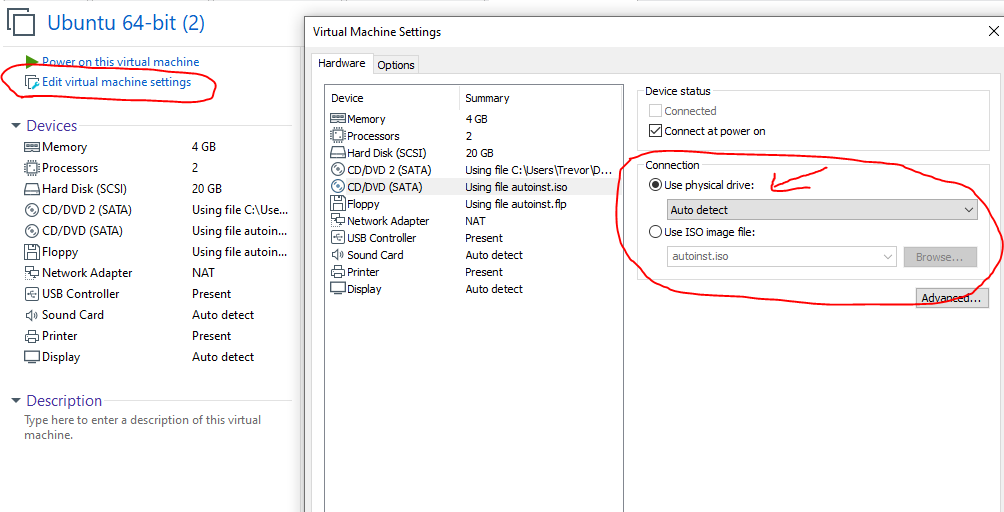


Continue through the menu by pressing enter on **Done**

Once everything has been installed and the disk has been partitioned, login as the user that you created in the setup menu of ubuntu. After getting logged in you will be prompted with your command line in your server. Which will look like this:



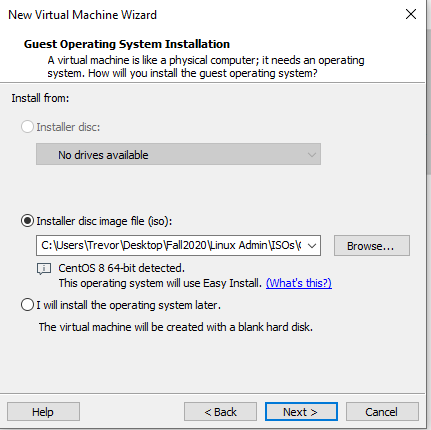
After a successful login, shut down the server and edit the VM settings to change the CD to **Use physical drive** instead of the ISO as usual.



**CentOS:**

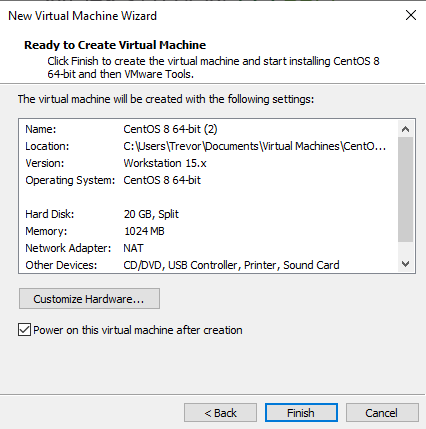
Set up CentOS the same way as Ubuntu.

Create another VM from the home tab and ensure you select the CentOS ISO:

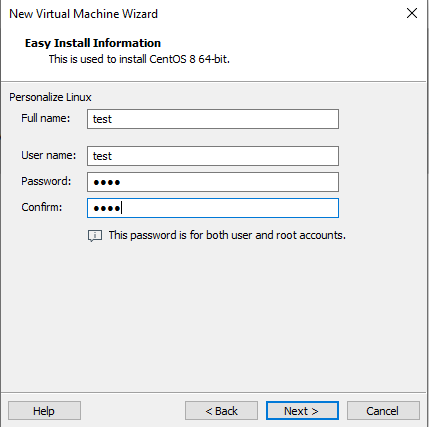


Use the same username, and password for CentOS as you did for Ubuntu. Remember this login.

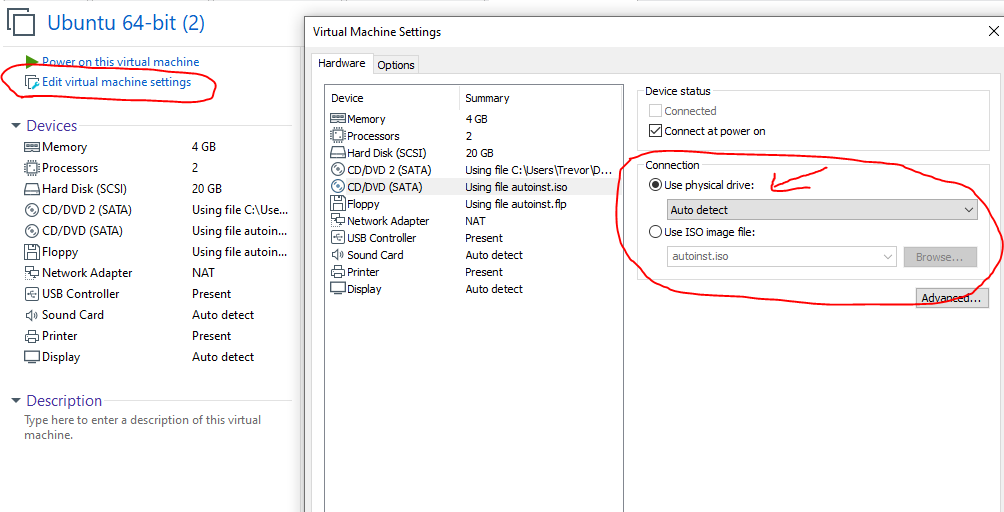
Click finish and CentOS will boot up. The install will take a little while and will reboot after it installs.



Once the installs are finished you will be prompted with a login screen. You will use what you typed in for your username and password on this screen when you did the set up:

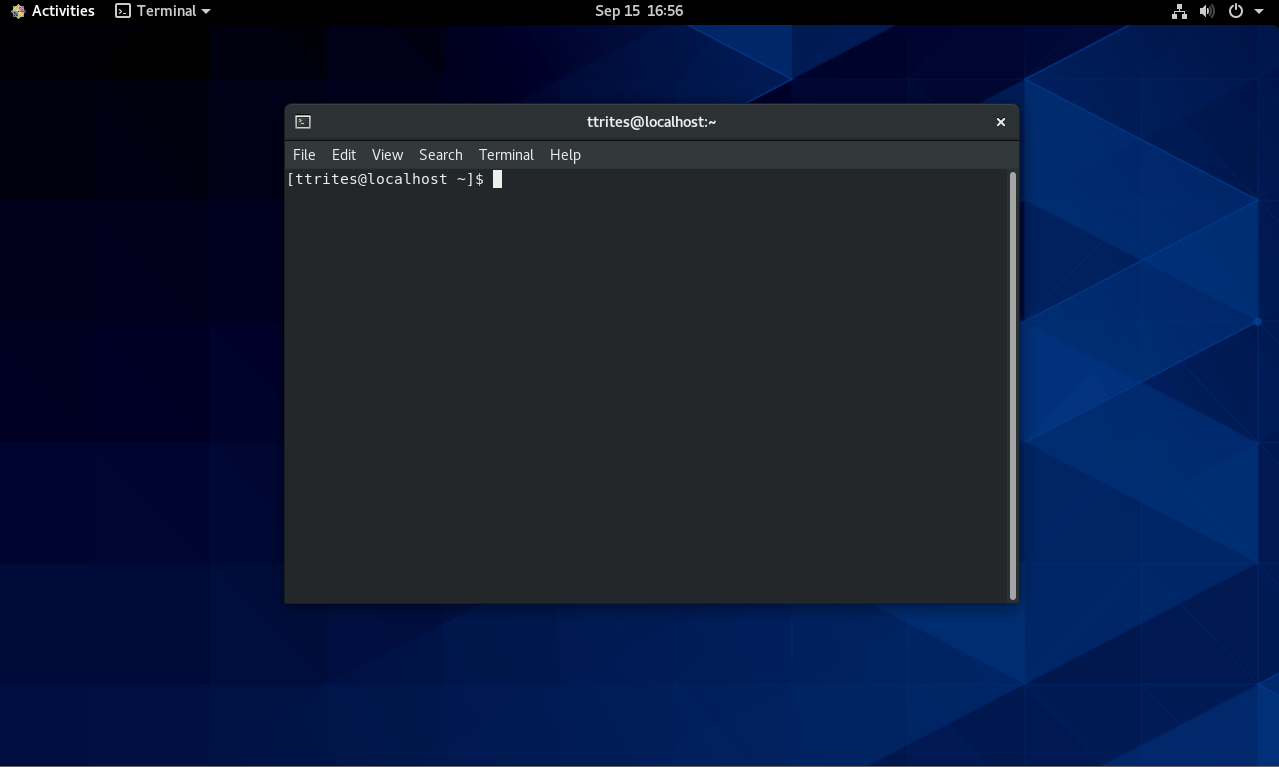


Use command line for any other installs or updates you may have to do. In addition to changing to the physical drive after getting the OS up and running. Also insure both operating systems have internet and fully are fully updated to ensure correct connectivity.



**Resolution:**

Successful setup of CentOS should look as so:



Successful setup of Ubuntu should look as so:

**INSTALL AND CONFIGURE FAIL2BAN, EMACS, VIM FOR CENTOS**

First, we must install fail2ban, to do this we will use this command followed by the next command:

**$ yum install epel-release**

**$ yum install fail2ban fail2ban-systemd**

Now that we have run both of those commands we have to enable and start fail2ban. They come disabled at install. To do this we will start with the enable command then the start command:

**$ system enable fail2ban**

**$ system start fail2ban**

We have now installed, enabled, and started the service. We must configure fail2ban. To do this enter this command:

**$ cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local**

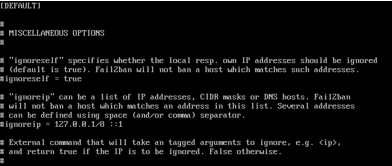
Open the jail.local file in any of the text editors EMACS, VI, or NANO. The file path will be the same as the previous comman file path. Locate the [DEFAULT] section of jail.conf and set these values:

**bantime = 20m**

**findtime = 5m**

**maxrety = 4**

[DEFAULT] Section should look like the image below:



These values are self-explanatory.

* bantime is how long and IP address is banned. The default is 10 mins.
* maxretry is the number of failures until the address is banned
* findtime is mixed with maxretry and bantime, if the host exceeds the maxretry setting determined by the findtime it is banned for the bantime that is entered.

After editing the values above go to [SSHD] section and add the values below:

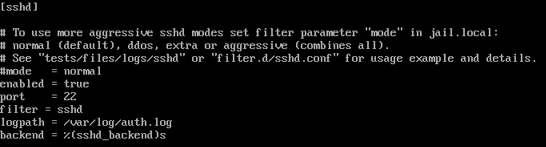
**enabled = true**

**port = 22**

**filter = sshd**

**logpath = /var/log/auth.log**

SSHD should look like the image below:



**INSTALLS:**

**TMUX –**

TMUX should already be installed but it is not run this command:

**$ yum install tmux**

**EMACS and VIM –**

Run this command:

**$ yum install emacs**

After being prompted answer with “Y” to confirm installation

**VIM –**

VIM should already be installed but if it is not run this command:

**$ yum install vim**

**Some useful commands**

**GREP:**

**Print all lines where the person's first name starts with J.**

grep '^J' datebook.txt

**Print all lines that don't contain 834.**

grep -v -e '834' datebook.txt

**Print lines containing Lincoln or lincoln (remember that grep is insensitive to case).**

grep grep -E '(L|l)incoln' datebook.txt

**SED :**

**Change the name Jon to Jonathan .**

sed -e 's/Jon/Jonathan/g' datebook.txt

**Delete lines containing Lane .**

sed -e '/Lane/d' datebook.txt

**Delete all blank lines.**

sed '/^$/d' datebook.txt

**AWK:**

**Print all the phone numbers.**

awk -F: '{print $2}' lab3.data