Creating a virtual network in VMWARE using pfsense

For the purpose of this write up, we are creating a virtual network to connect 3 virtual machines (VMs) for an Ethical Hacking practice lab environment.
Note: VMWare workstation Pro 17.5 is installed
Downloadable Items needed, for easy access, place all downloaded vm's in the same folder:

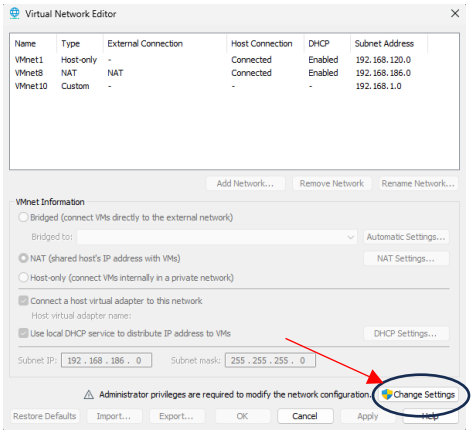
Pfsense https://www.pfsense.org/download/
Windows 10 https://azureforeducation.microsoft.com/devtools or chose your iso image
Kali Linux https://www.kali.org/get-kali/#kali-virtual-machines
Metasploitable 2 https://docs.rapid7.com/metasploit/metasploitable-2
7-ZIP https://www.7-zip.org/

Note: 7-zip is needed to extract the Kali Linux and Metaspolitable2 VM files.

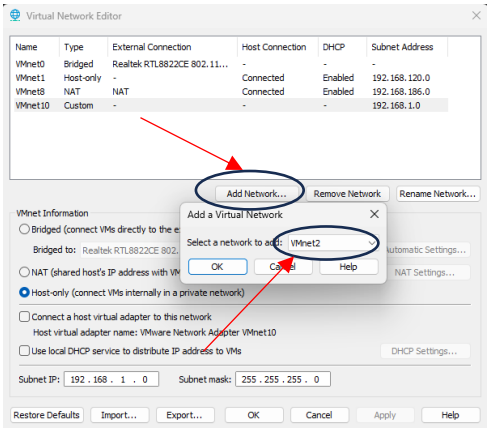
Step 1: Create a network for pfsense

In the VMWare menu select edit > Virtual Network Editor

Select change settings and yes.

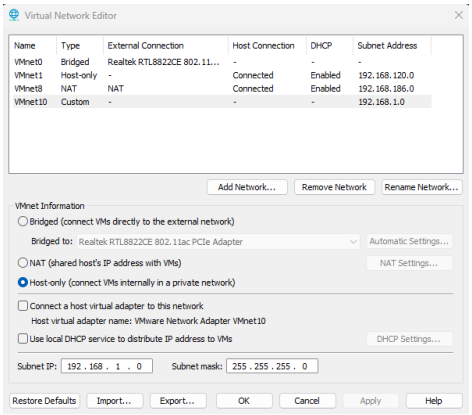


Navigate to Add Network and chose a VMnet in the dropdown.



For the purpose of this write-up, chose VMnet10 and add create the following settings:

Select Host only and set the Subnet IP to 192.168.1.0



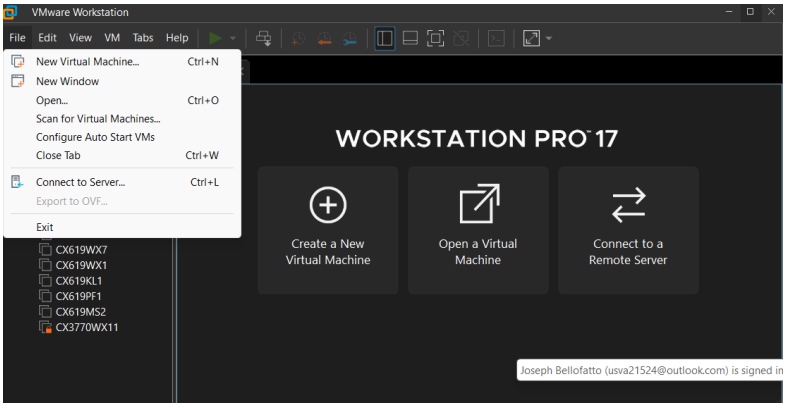
Subnet mask will 255.255.255.0 This will provide 254 available IP addresses.

Select Apply > OK and you have set the network portion of your network.

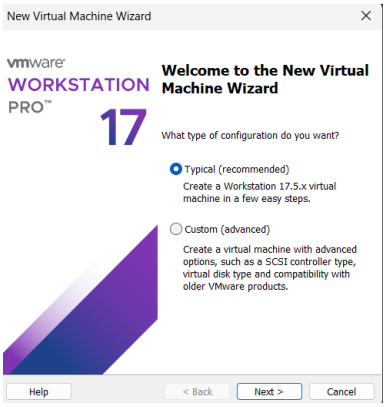
Note: There are two ways to add a virtual machine to VMWare. Creating a virtual machine with an iso image and open a virtual machine with a vmx file.

Step 2: Adding your virtual machines.

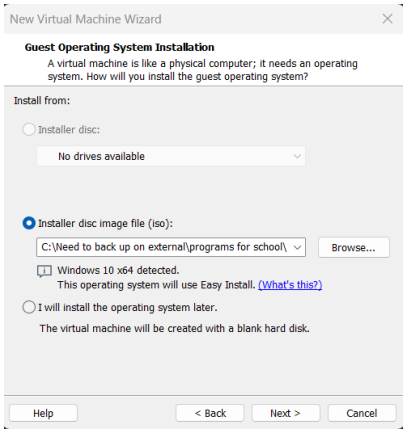
On the home page of workstation pro 17 or in the menu chose File > “new/create a new virtual machine”.



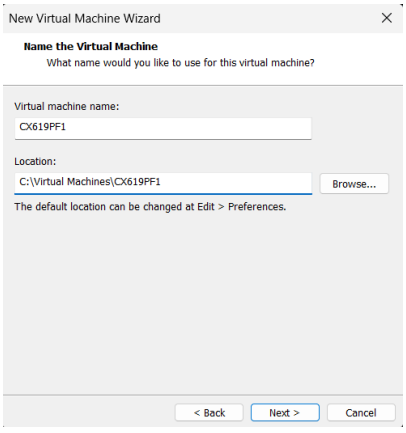
In the New Virtual Machine Wizard, chose typical



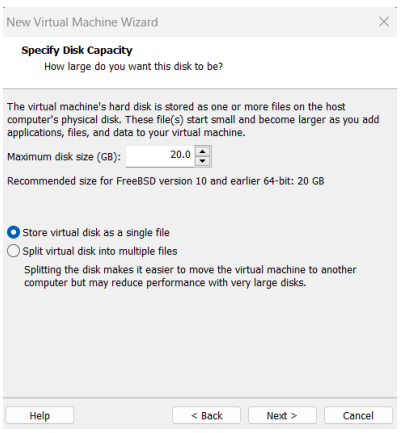
In the wizard, chose location of install



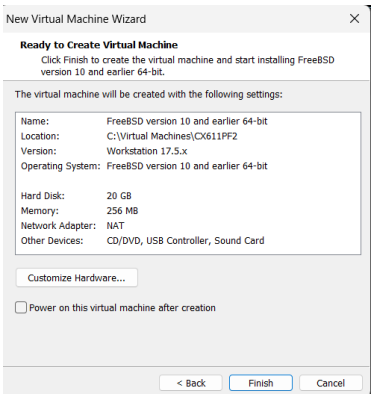
Chose a name and location for the vm



Default disk size
Single file

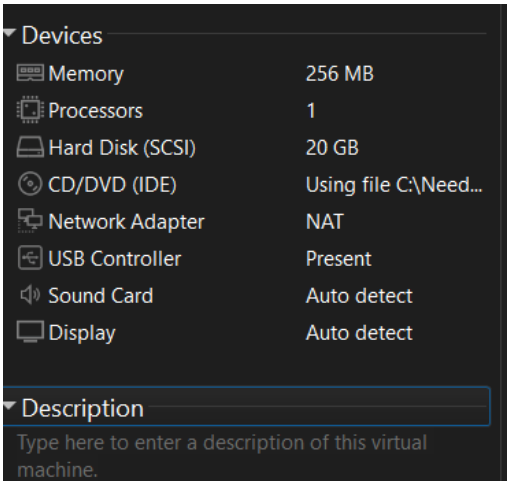


Default hardware settings as they are listed in the VM wizard

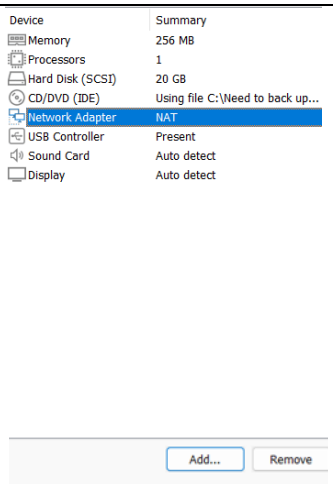


Step 3: pfsense we will need to be adjusted to add a network device. some settings.

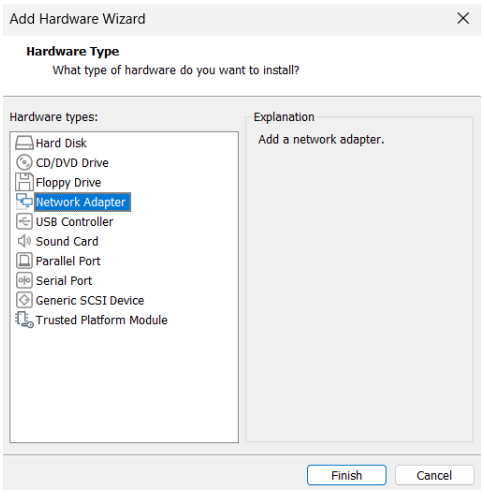
Navigate to the network adapter:



On the VM Settings window that opens up the Network Adapter and select add at the bottom:

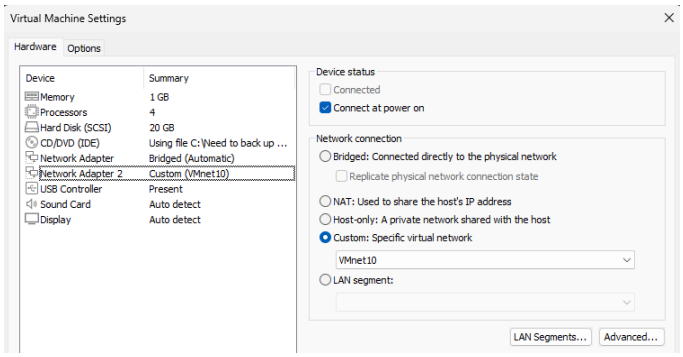


In the hardware types window select Network Adapter and select Finish.



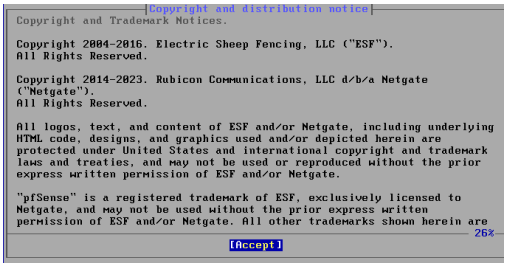
The adapter settings are the most important part of this setup. Ensure you make the next two changes.

In the hardware window, two Network Adapter should be visible. On the first Adapter select bridged. The second Adapter select Custom and, in the drop-down box, select the network created in step 1. For the purpose of this write up, we will use VMNET10. select ok to finish.

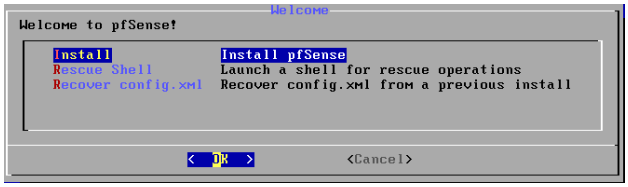


Step 4: Power on the pfsense VM and begin the installation.

Select “Accept” on initial screen

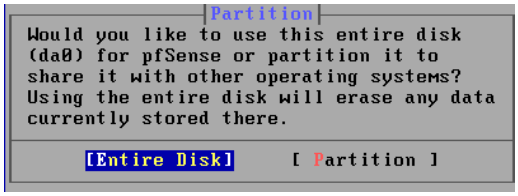


Install: Install pfsense > ok

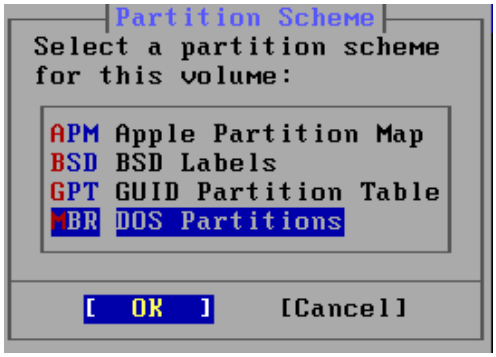


Auto (UFS) – Anything else is beyond the scope of this writeup.

Use the entire disk – Partition is beyond the scope of this install.

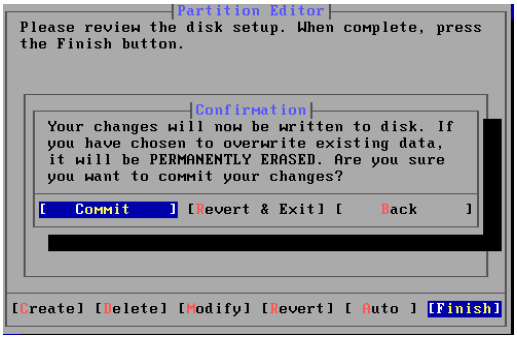


MBR DOS Partition

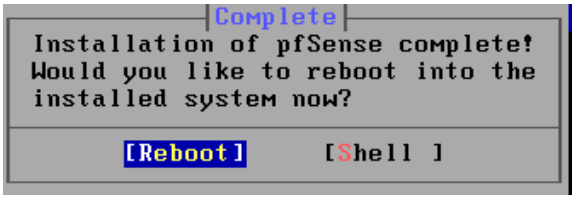


20 GB MBR and Finish

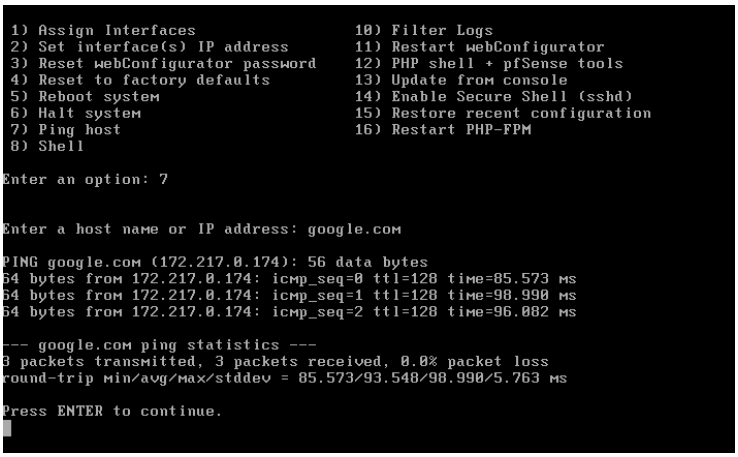
Select Commit



Select Reboot



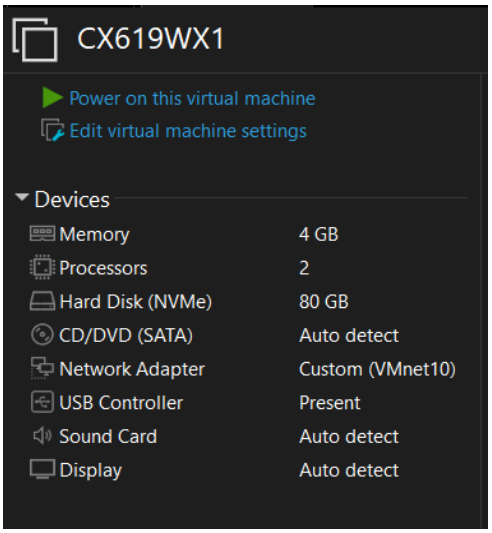
Once reboot is complete, select 7 for ping. Use an IP or a site to verify internet connectivity. If no connectivity appears, verify step 1 is setup correctly and you are on VMNET10.



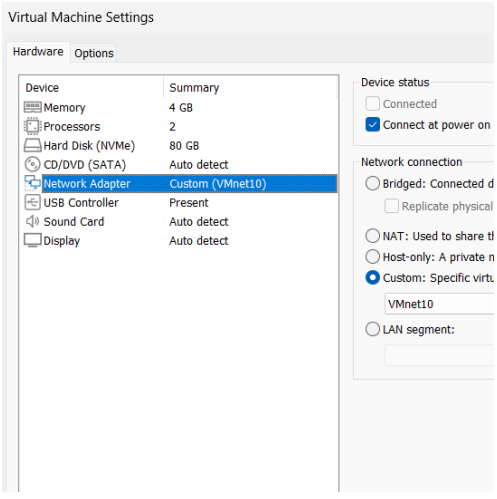
Step 5: Install Windows 10 from your point of origin. For the sake of this write up, we are using an iso downloaded from the Microsoft Azure for Education website. There will be a product key available upon download.

Create a virtual machine: repeat step 2 above with the Windows 10 iso. Chose a name and location for your machine. For this writeup we will use CX619WX1, location for machine files will be user choice.

On the start-up page, select your Network Adapter.



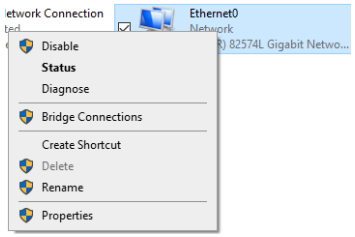
On the VM settings page, select VMNET10 (or the VMNET you created)



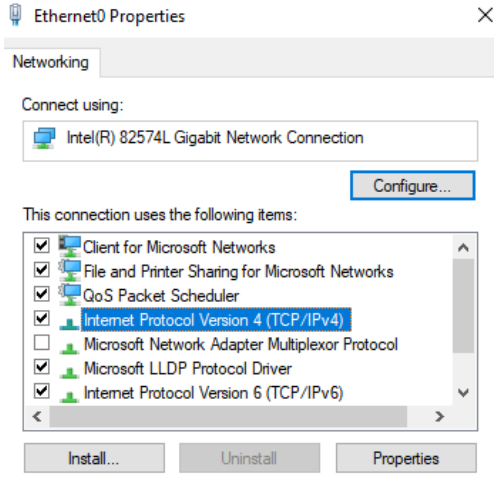
Note: Once Windows installs and boots, change the DNS settings to match the pfsense software.

Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings

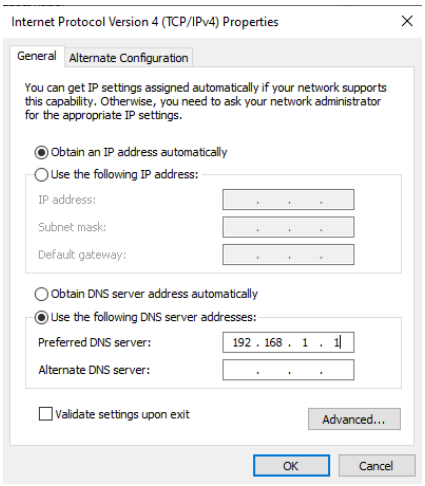
Right click on the Ethernet Adapter and select Properties:



Chose the IPV4 connection and select properties



In the DNS enter: 192.168.1.1
Restart after finished.



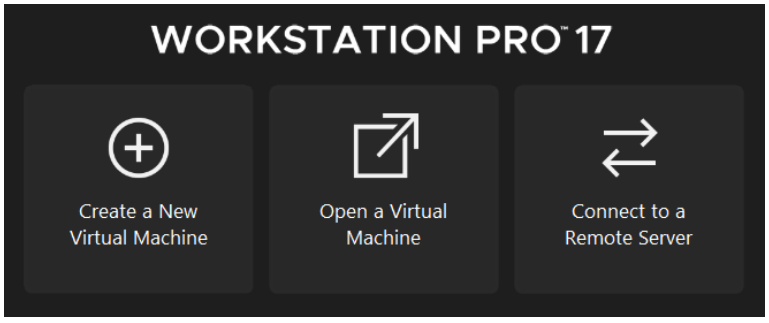
Windows should now have connectivity. If it does not, ensure it is connected to the VMNET that was created. That is what connects the Windows VM to the phsense VM for internet.

Step 6: Install Kali Linux

Download Kali VM form Kali.org, link above.
Download 7-zip from 7-zip.org, link above and uncompress Kali.

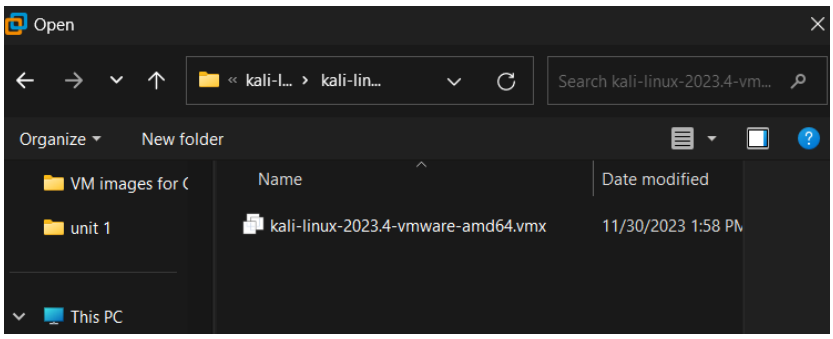
Kali Linux is compressed using 7-zip

For your Kali installation, chose “Open a Virtual Machine” in the home panel.

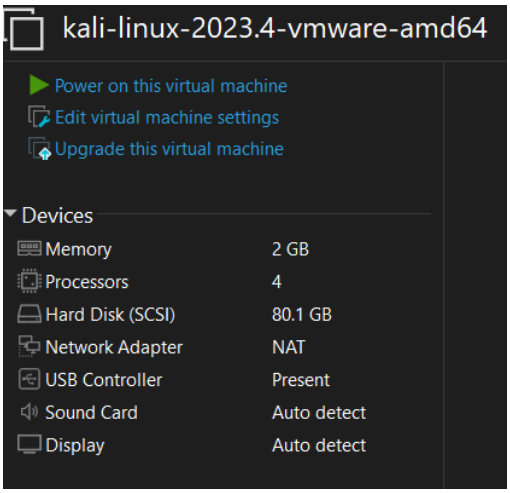


Navigate to the location of the now, uncompressed, folder on your hard drive.

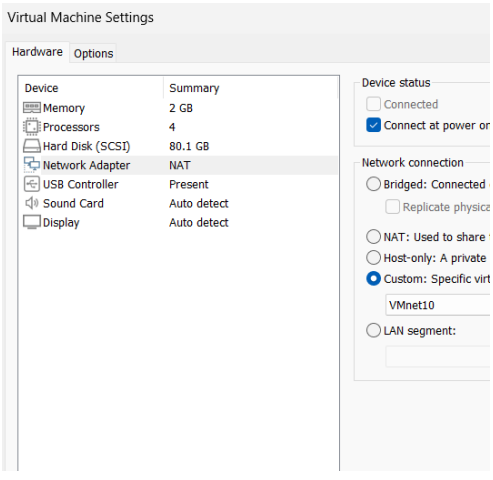
Select the .vmx file located in the folder.



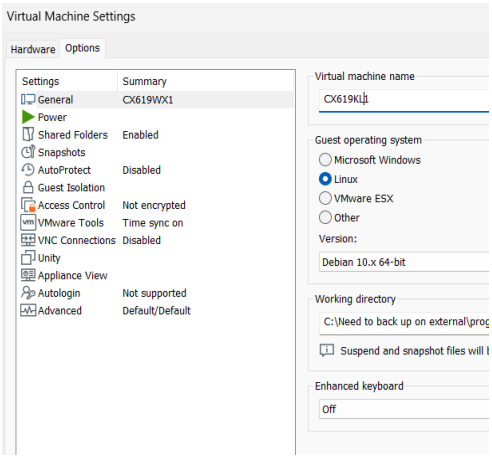
Before opening the Kali VM, navigate to “Edit Virtual Machine Settings”



On the VM settings page, select VMNET10 (or the VMNET created)



Go to the Options tab and chose a name and location for the Kali VM



Power on the Kali VM. Once it is powered up, the default username and password will be kali. Open a command prompt to confirm connectivity.

ifconfig

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.129  netmask 255.255.255.0  broadcast 192.168.1.255
```

ping site of choise, ctr c to quit

```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (172.217.2.46) 56(84) bytes of data.
64 bytes from ord37s52-in-f14.1e100.net (172.217.2.46): icmp_seq=1 ttl=54 time=25.2 ms
64 bytes from atl14s78-in-f14.1e100.net (172.217.2.46): icmp_seq=2 ttl=54 time=20.2 ms
64 bytes from ord37s52-in-f14.1e100.net (172.217.2.46): icmp_seq=3 ttl=54 time=23.1 ms
64 bytes from ord37s52-in-f14.1e100.net (172.217.2.46): icmp_seq=4 ttl=54 time=29.5 ms
^C
```

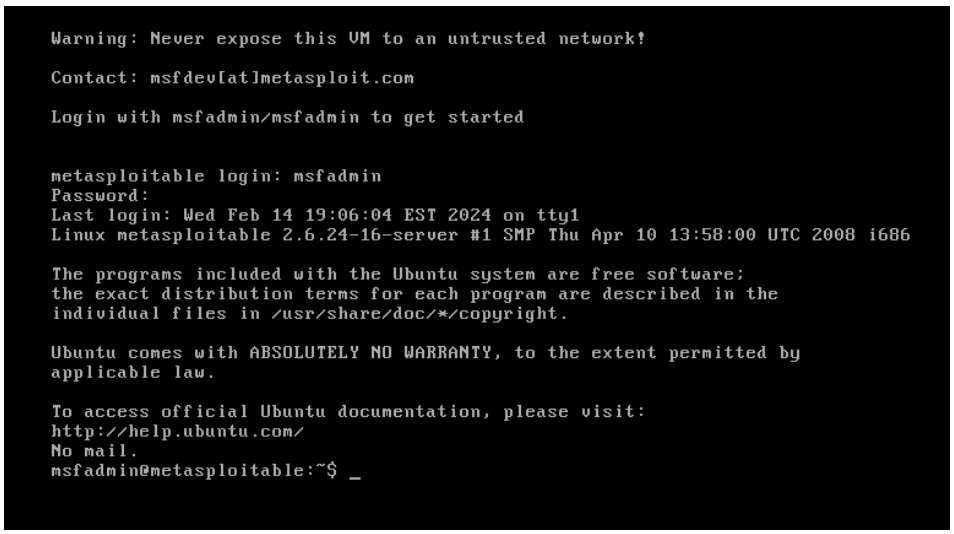
Kali should have connectivity at this point. If it does not, ensure you are connected to the VMNET that was created. That is what connects the Kali VM to the phsense VM for internet.

Step 7: Install Metasploitable2

The process to install Metasploitable2 is the same as Kali Linux.

The default username and password are msfadmin

Metasploitable2 is Linux based and uses basic Linux commands to find IP and test connectivity.



Note: Metasploitable2 is an intentionally exploitable Virtual Machine, run it only when needed!

Note: When checking connectivity, if issues arise, trouble shoot as you would for the other VMs.