

PROJECT TASK 4

SECURE NETWORKING: SETTING UP PFSENSE FIREWALL VM TO CONTROL TRAFFIC AND ENFORCE POLICIES

Alabi Kehinde Oluwasemilore

Information Systems Engineering and Management, Harrisburg University

CISSC 661: Principles of Cybersecurity & Cyberwarfare

Dr. Bruce Young

15/06/2023

Snort IPS Setup

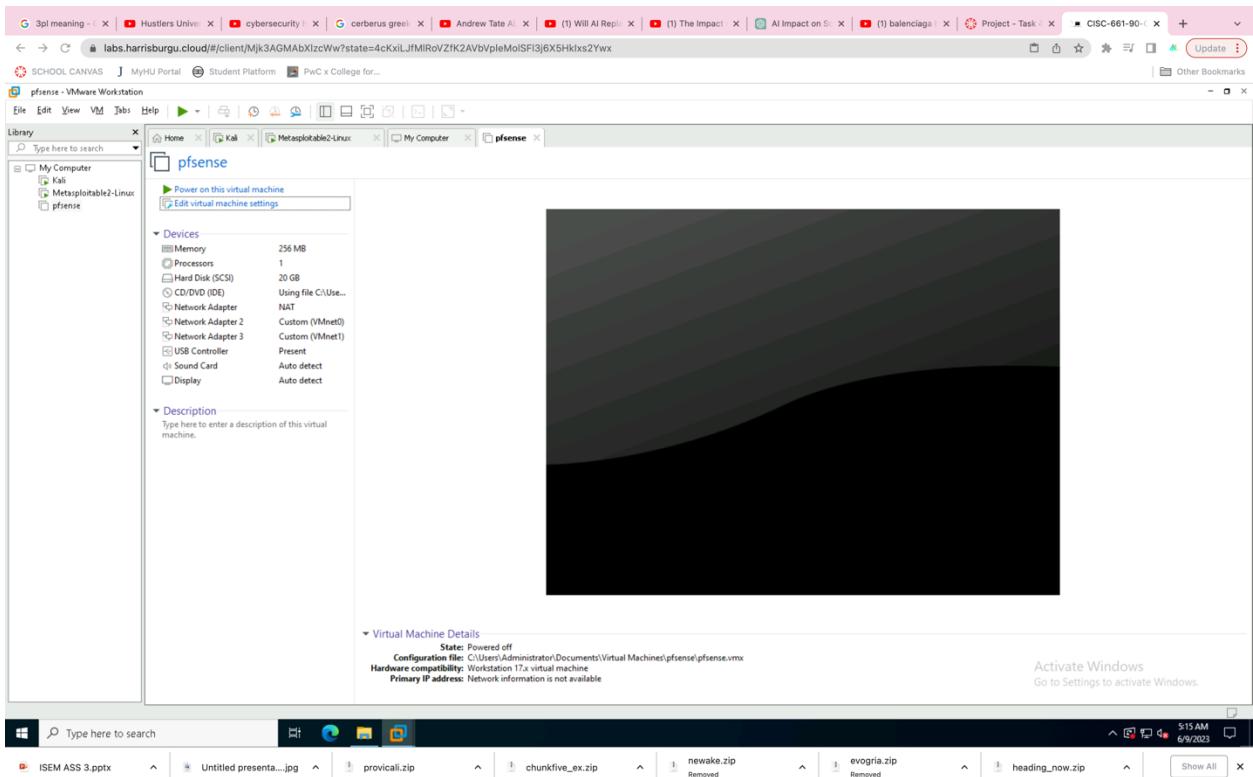
Performed a successful exploit for this project. For this project we needed Kali Linux, Metasploitable.

System Configuration:

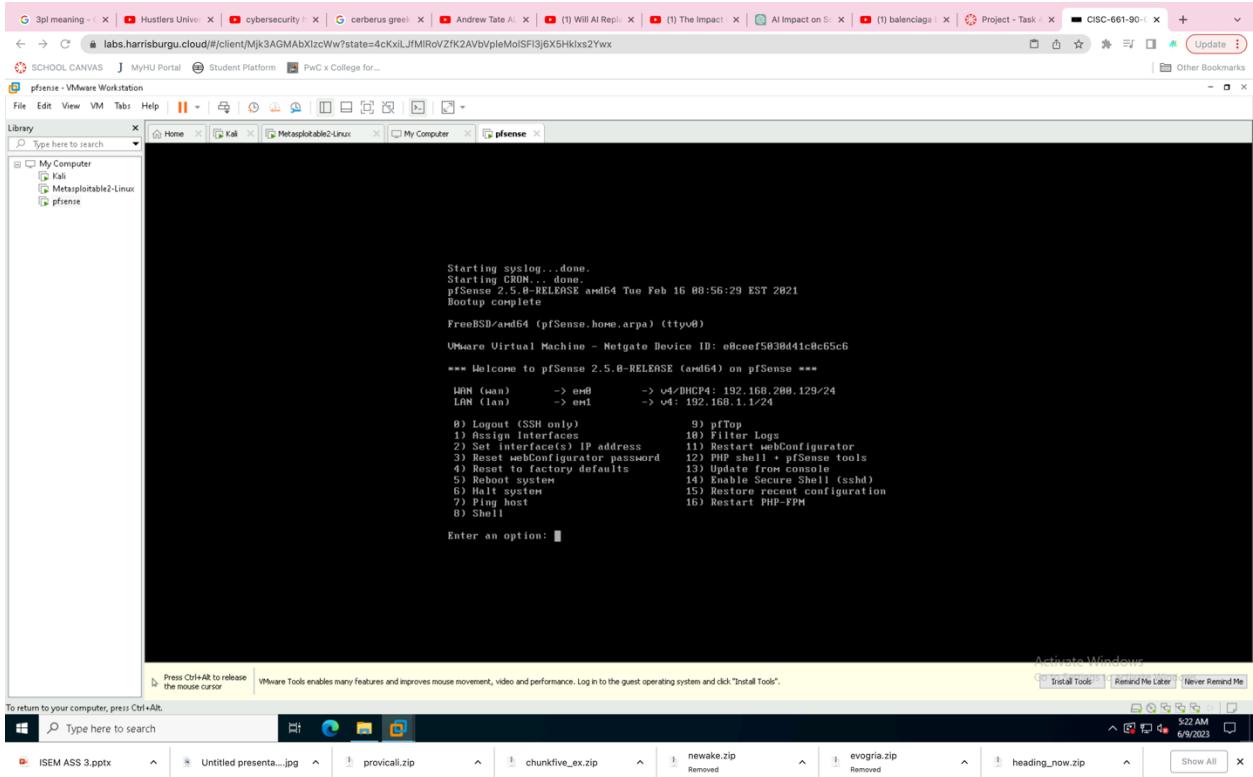
- Macbook Pro 2016
- Mac OS Ventura
- 32 GB RAM
- 2.3 GHz 8-Core Intel Core i9

Step 1: Create New VM, Set Interface IP address

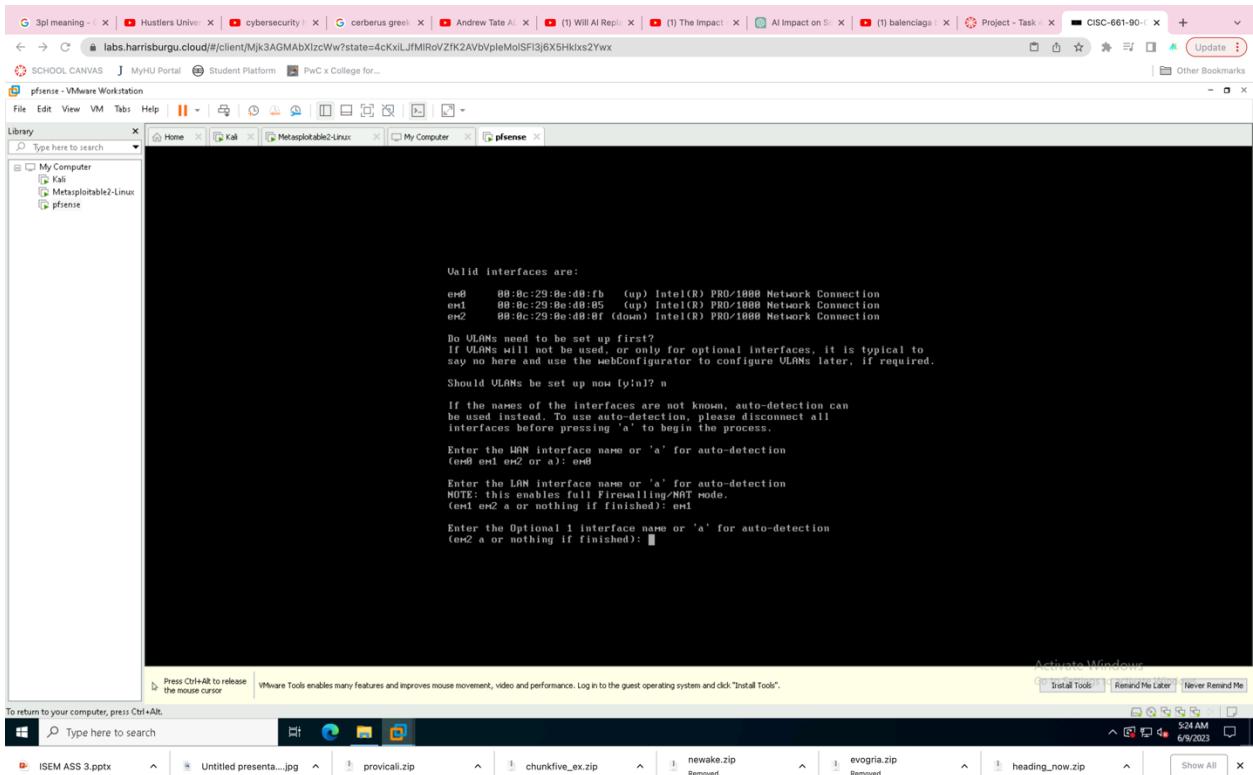
- Configure NAT 2 & NAT 2



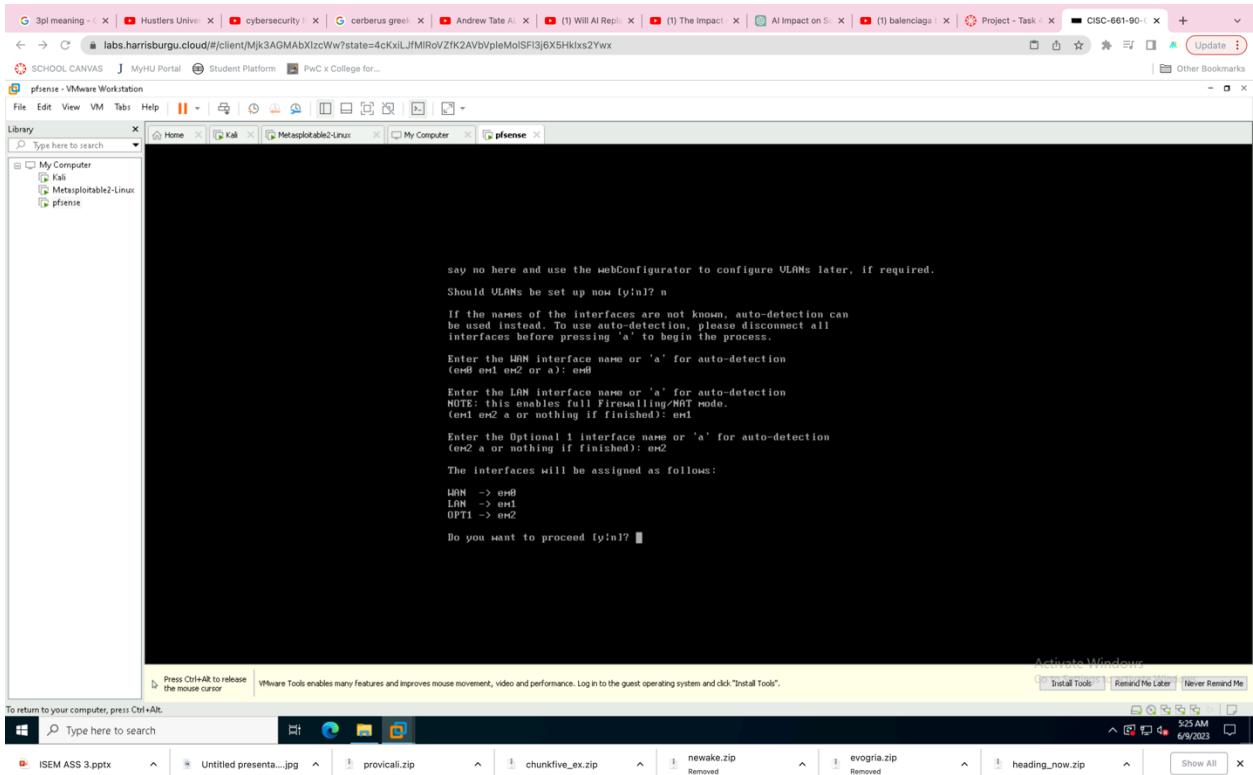
- Power VMware workstation
- Reboot into configuration mode



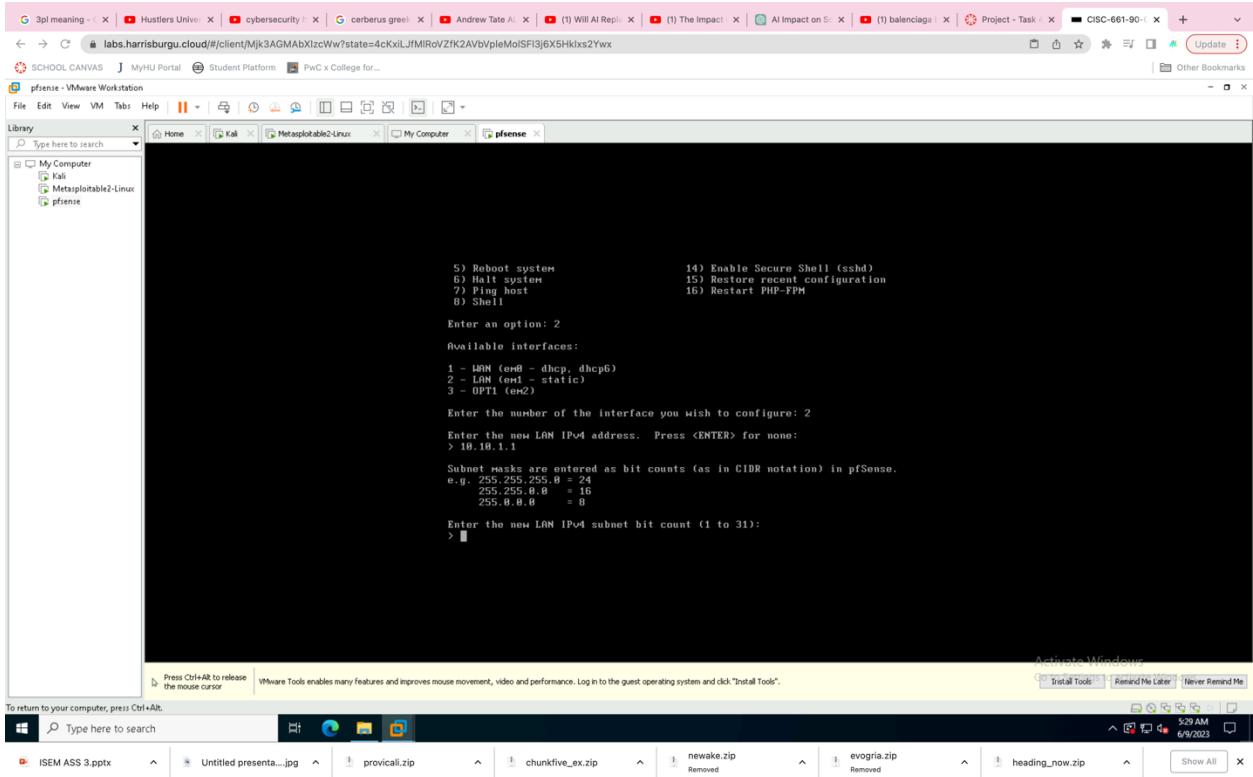
- Assign LAN to em1



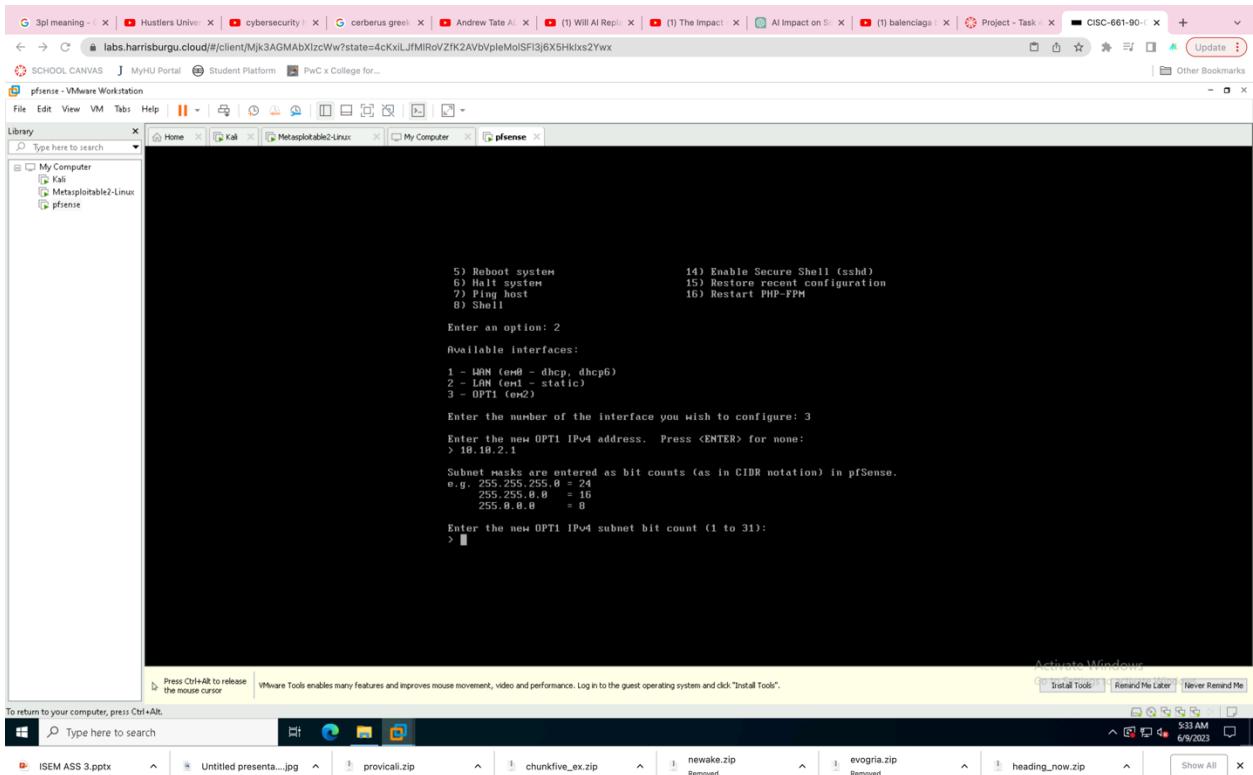
- Assign opt 1 to em2



- Set IPv4 address to 10.10.1.1

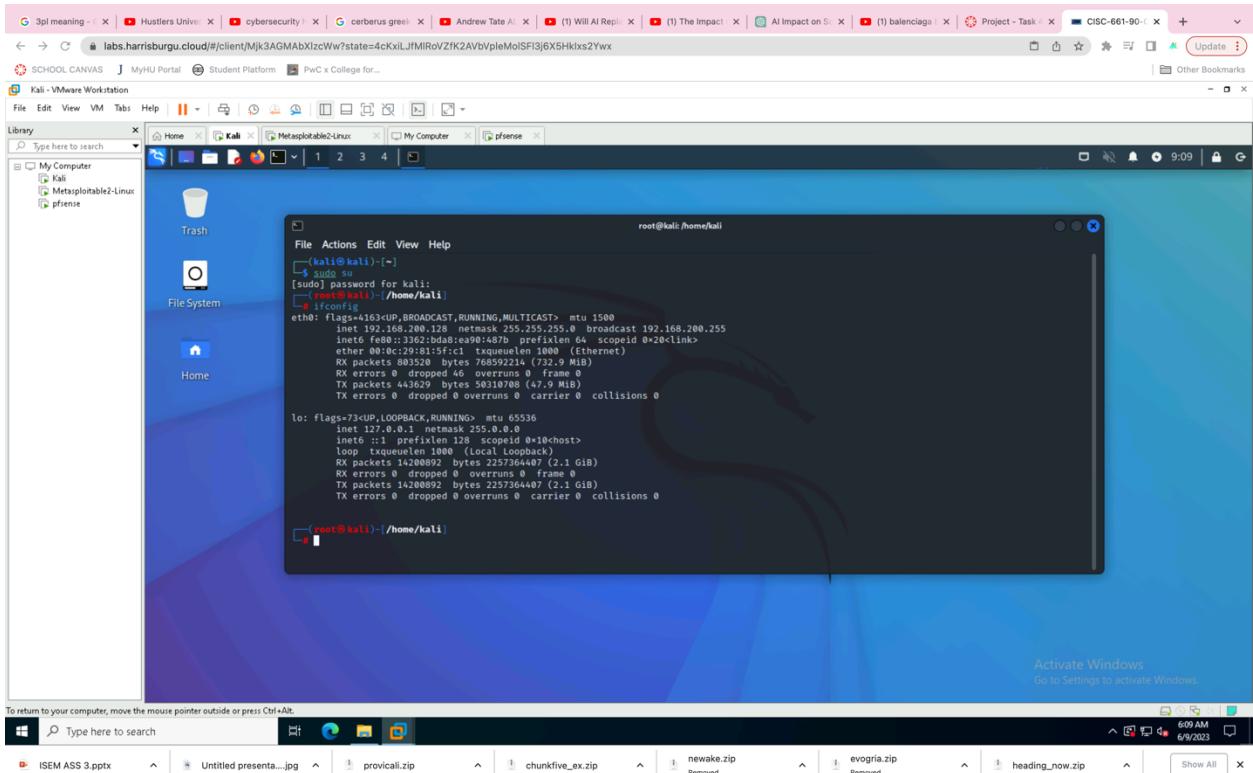


- Set OPT 1 interface to 10.10.2.1

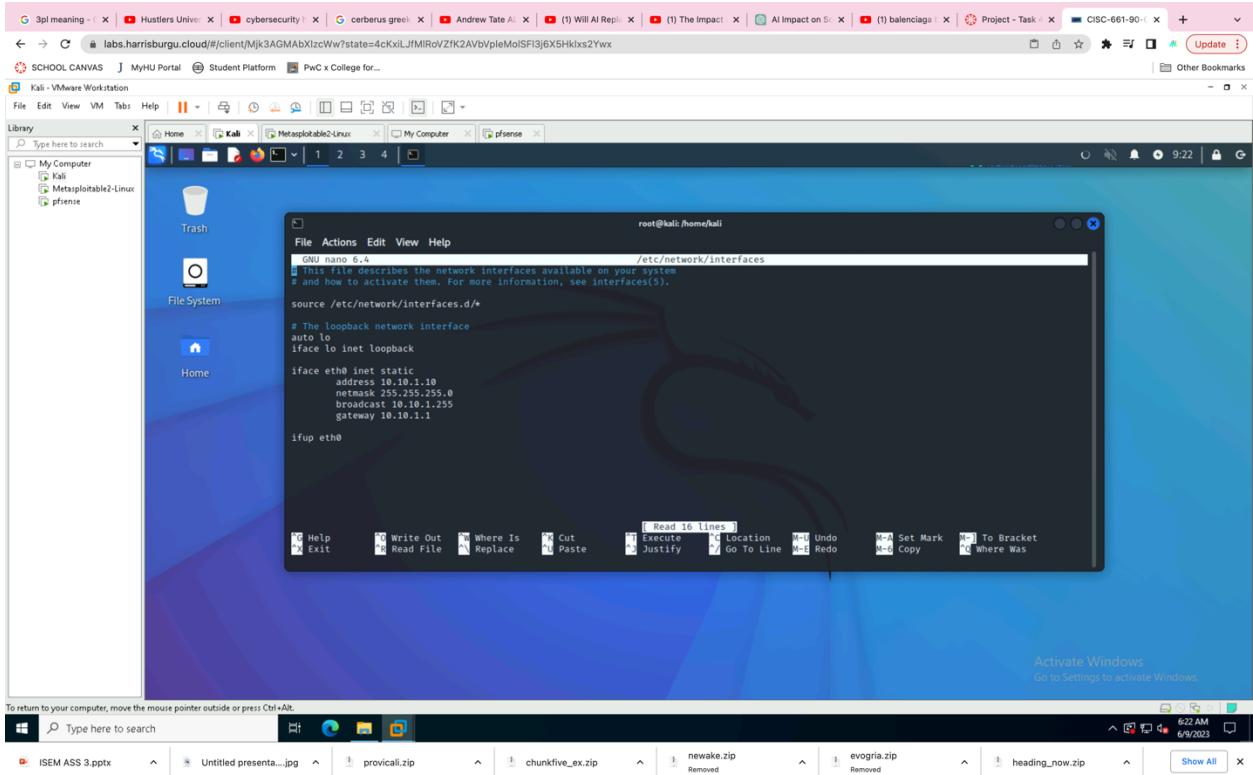


Step 2: Fix Kali interface

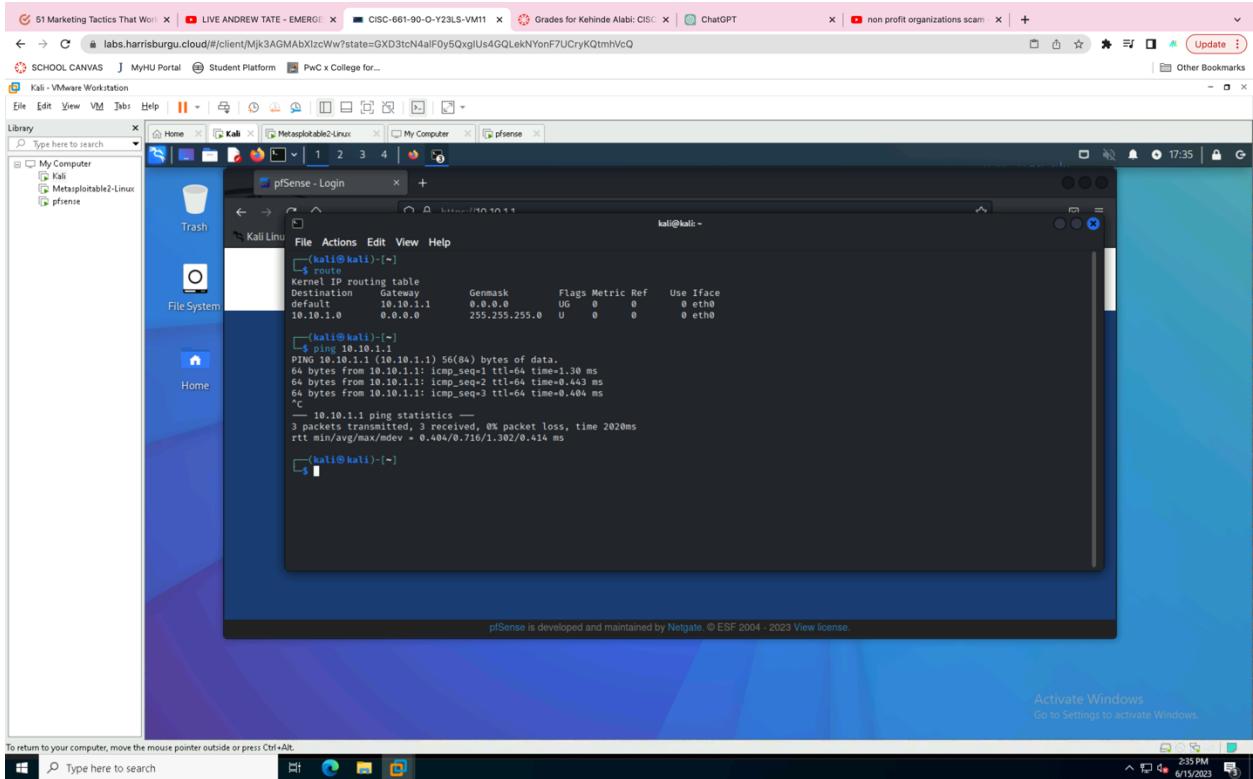
- Remove NAT 2
- Set NAT 1 to VMnet 0 to custom
- Run ifconfig on Kali system



- Create static IP address for eth0



- Use route command to view default route
- Ping 10.10.1.1



Step 3: Metasploitable and pFsense configuration

- Perform ifconfig to show eth0 [IP Config 10.10.1.12]

```

nsfadmin@metasploitable:~$ nsfadmin
-hetb nsfadmin: command not found
nsfadmin@metasploitable:~$ sudo su
[sudo] password for nsfadmin:
root@metasploitable:/home/nsfadmin# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:80:8c:ba
          inet6 addr: fe80::20c:29ff:fe80:8cba/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2767343 errors:57 dropped:57 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22922473 (213.5 MB)  TX bytes:1181341 (1.1 MB)
          Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:107895 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107895 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:52079857 (50.4 MB)  TX bytes:52079857 (50.4 MB)
root@metasploitable:/home/nsfadmin#

```

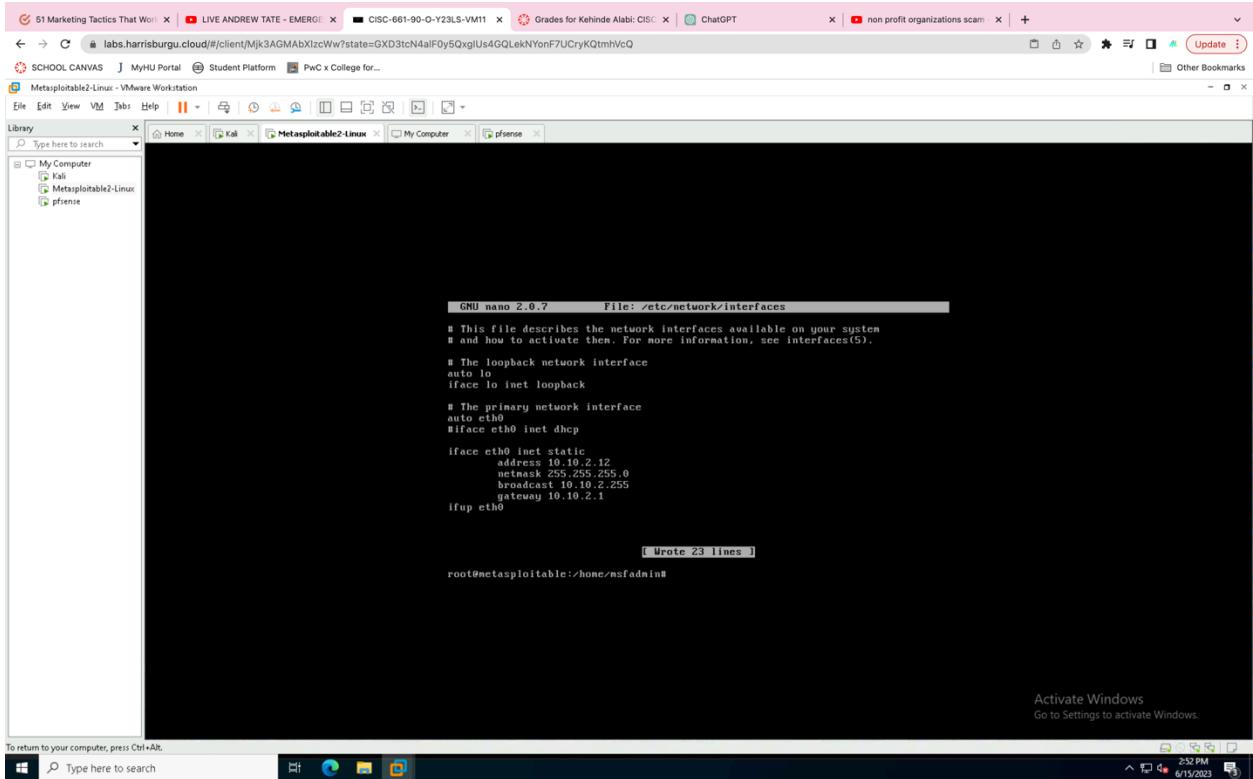
To return to your computer, press Ctrl+Alt.

Activate Windows
Go to Settings to activate Windows.

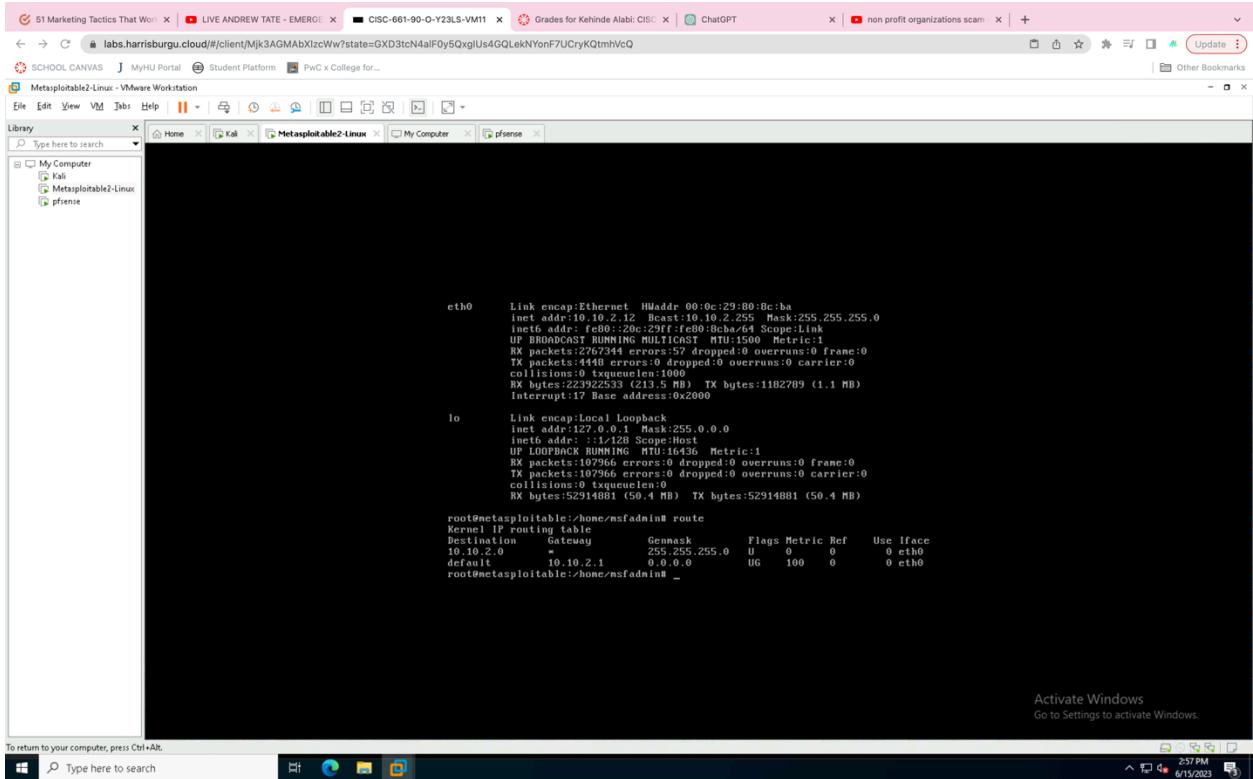
- Change network addresses in file directory using the command line

/etc/network/interfaces

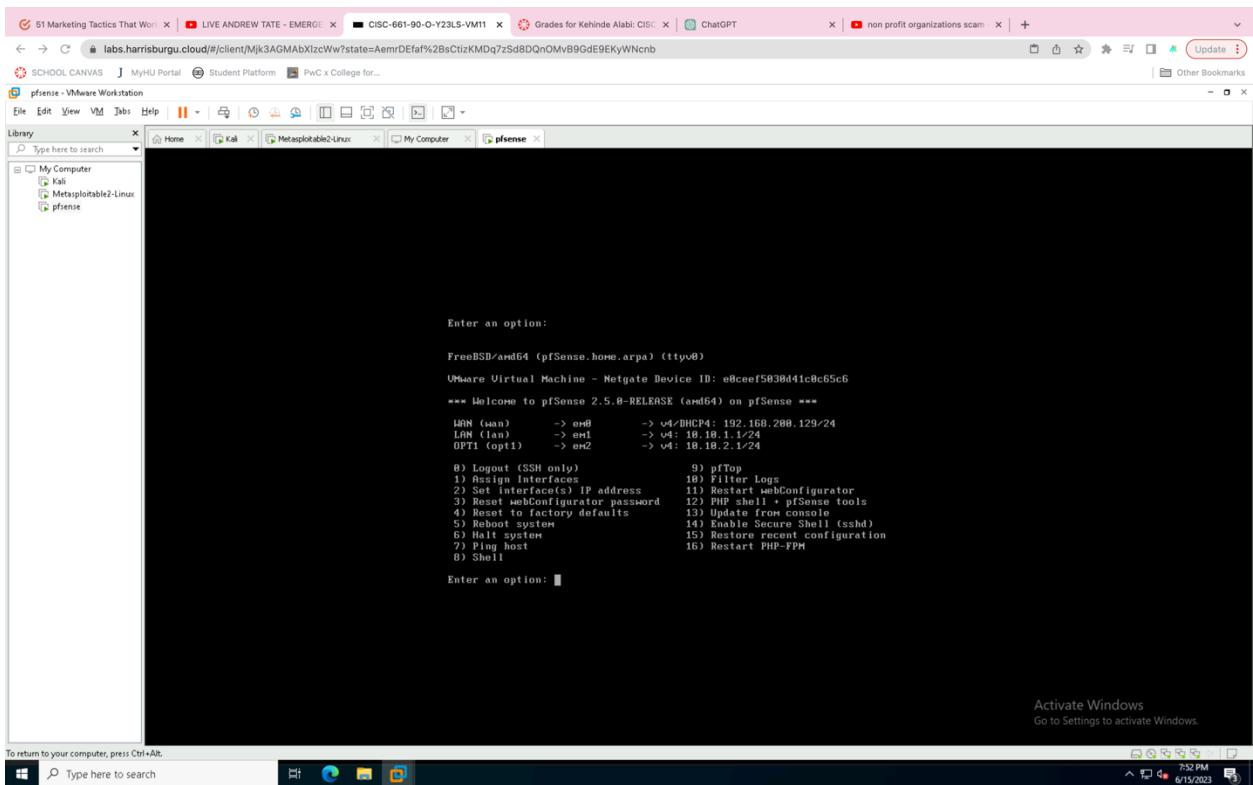
- Change IP address from 10.10.1.12 to 10.10.2.12
- Broadcast address from 10.10.1.255 to 10.10.2.225
- Add gateway [10.10.2.1]



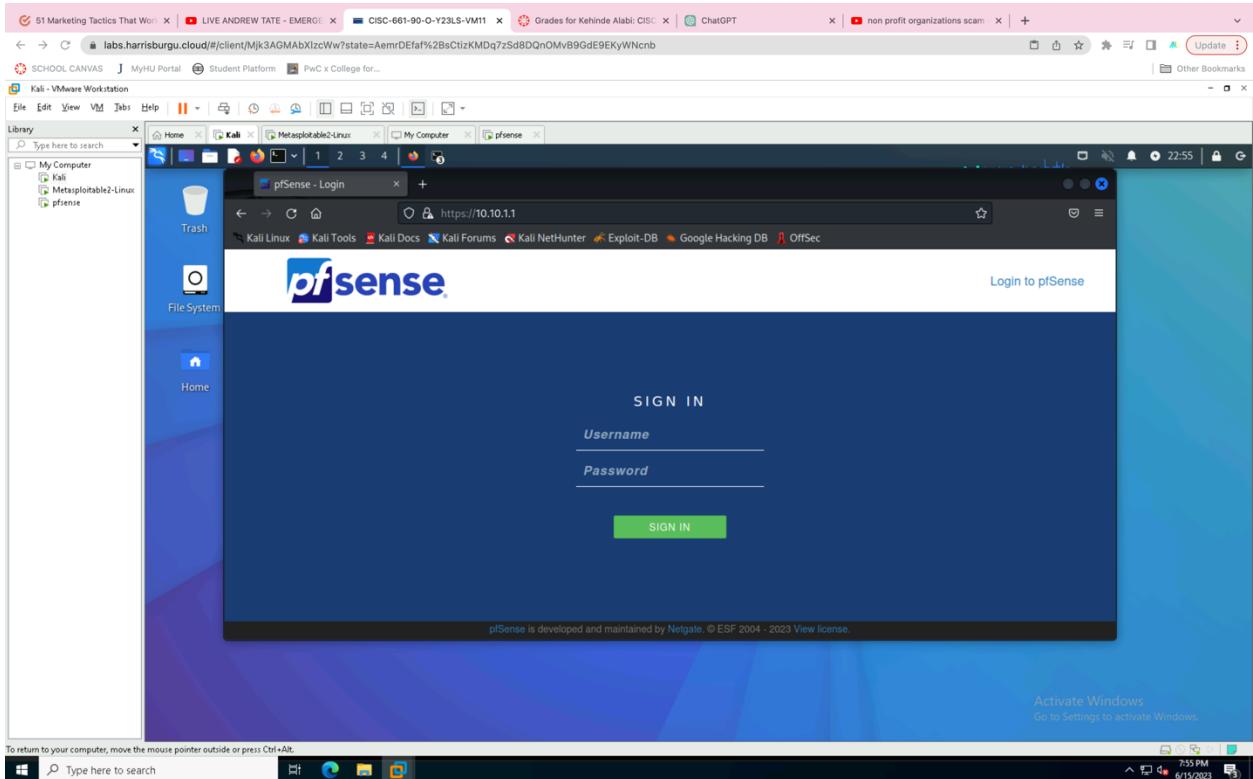
- Perform ifdown command to bring interface down
- Perform ifup command
- Perform ifconfig to view newly configured network details
- Perform route command



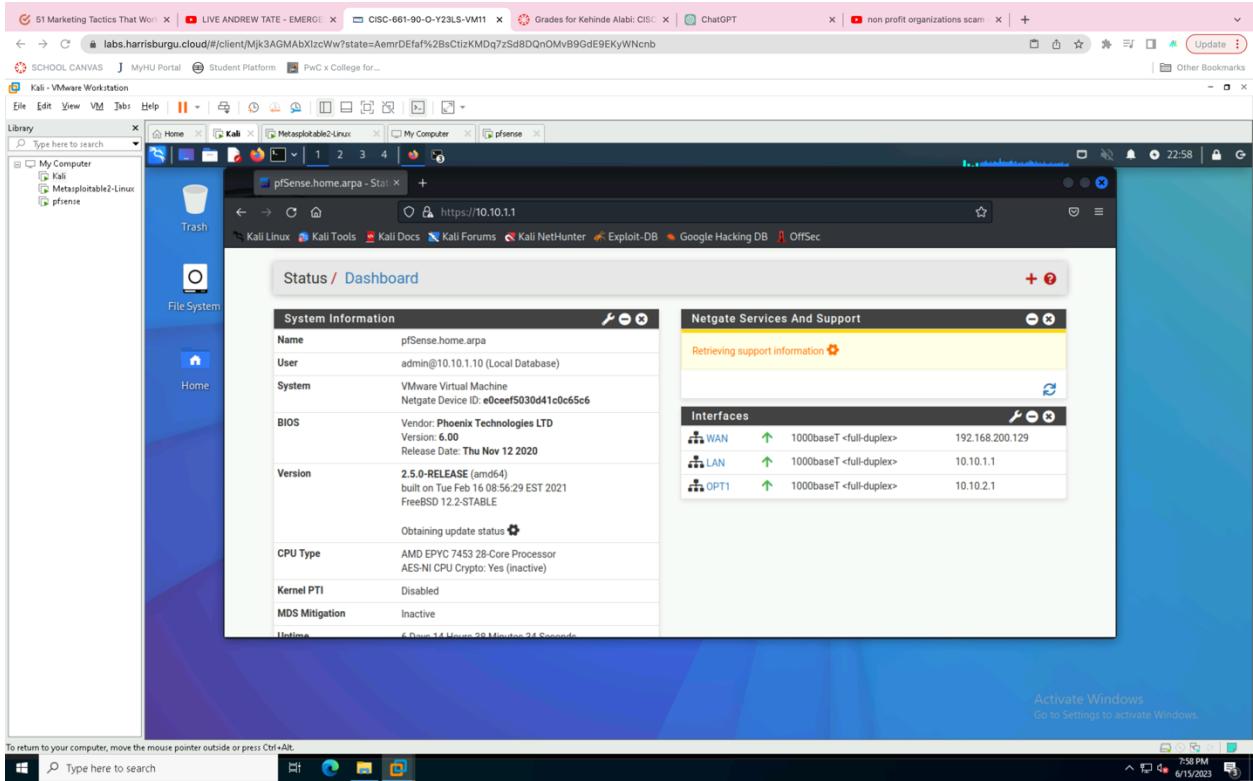
- Network used by firewall resides at LAN



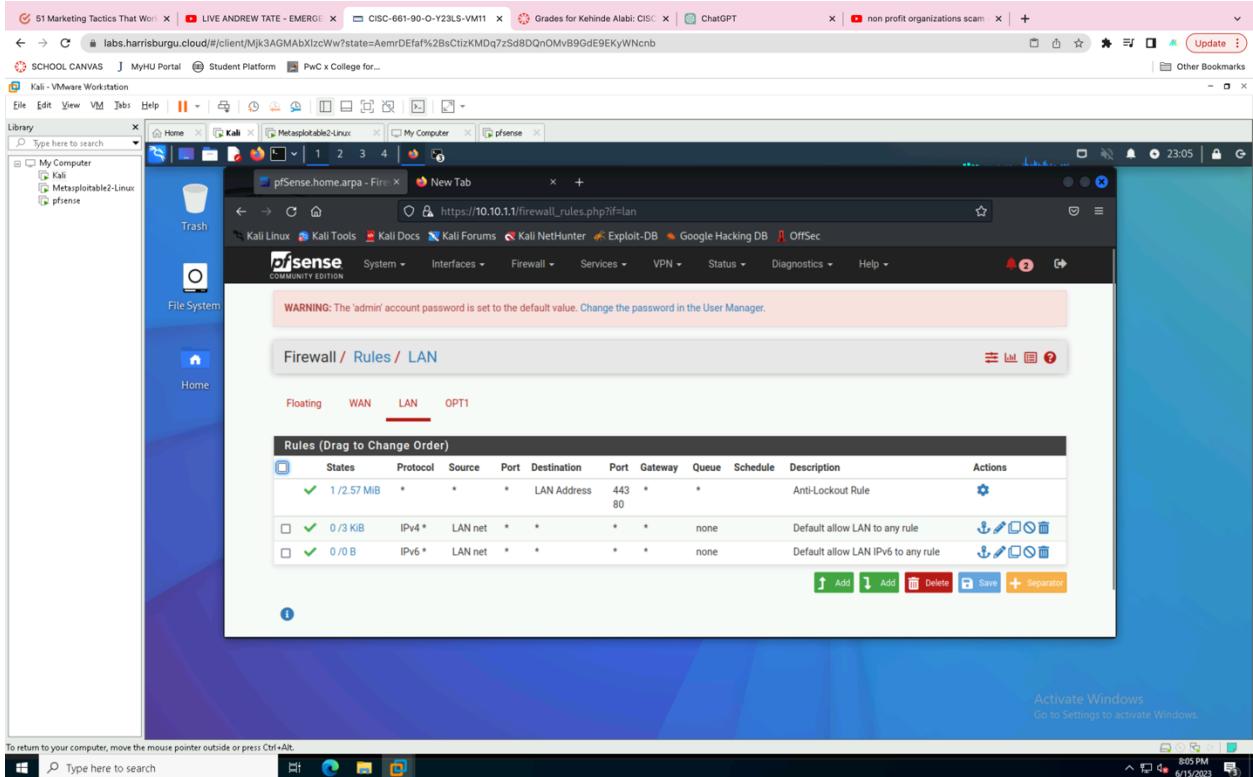
- Open browser
- Load up pFsense



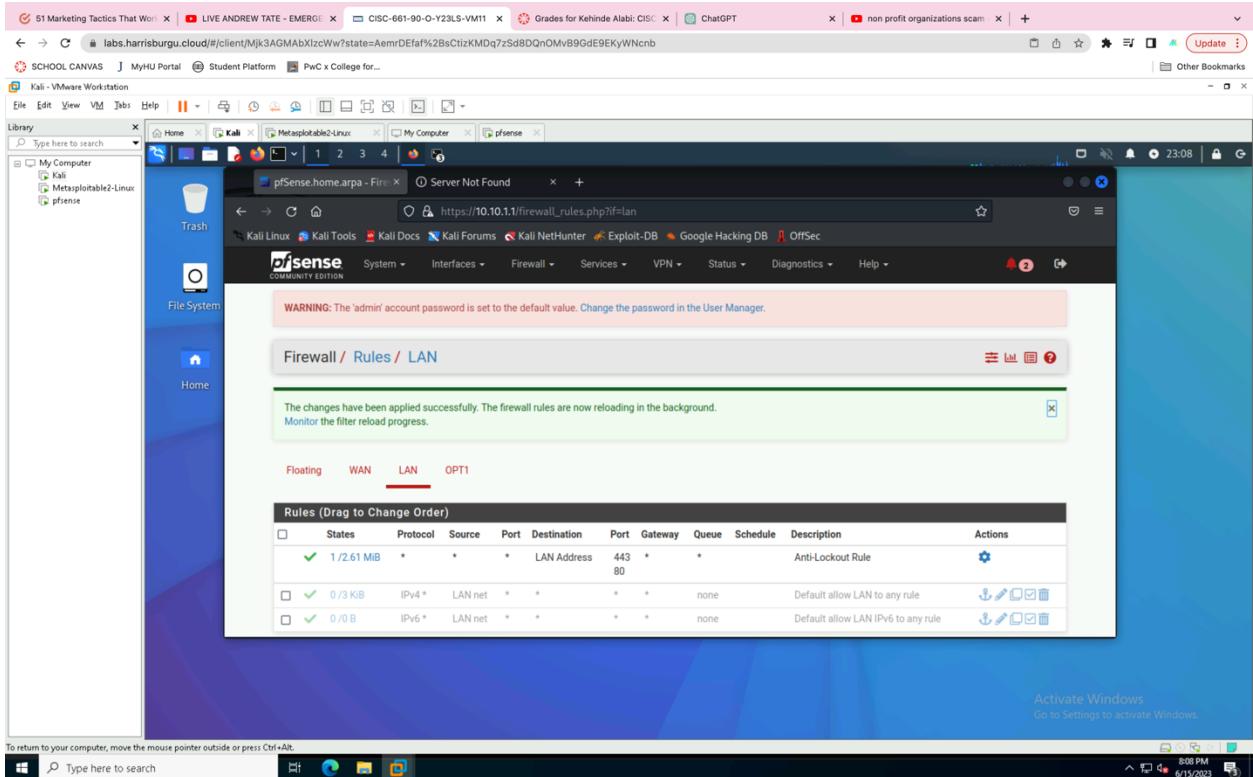
- Configure firewall



- Go to firewall rules



- Disable IPv4 and IPv6



Step 4: Create Firewall Policy

- Add and create policy for DNS, HTTP, HTTPS

- DNS

-TCP/UDP

-LAN net

-DNS (53)

- HTTP

-TCP

-LAN net

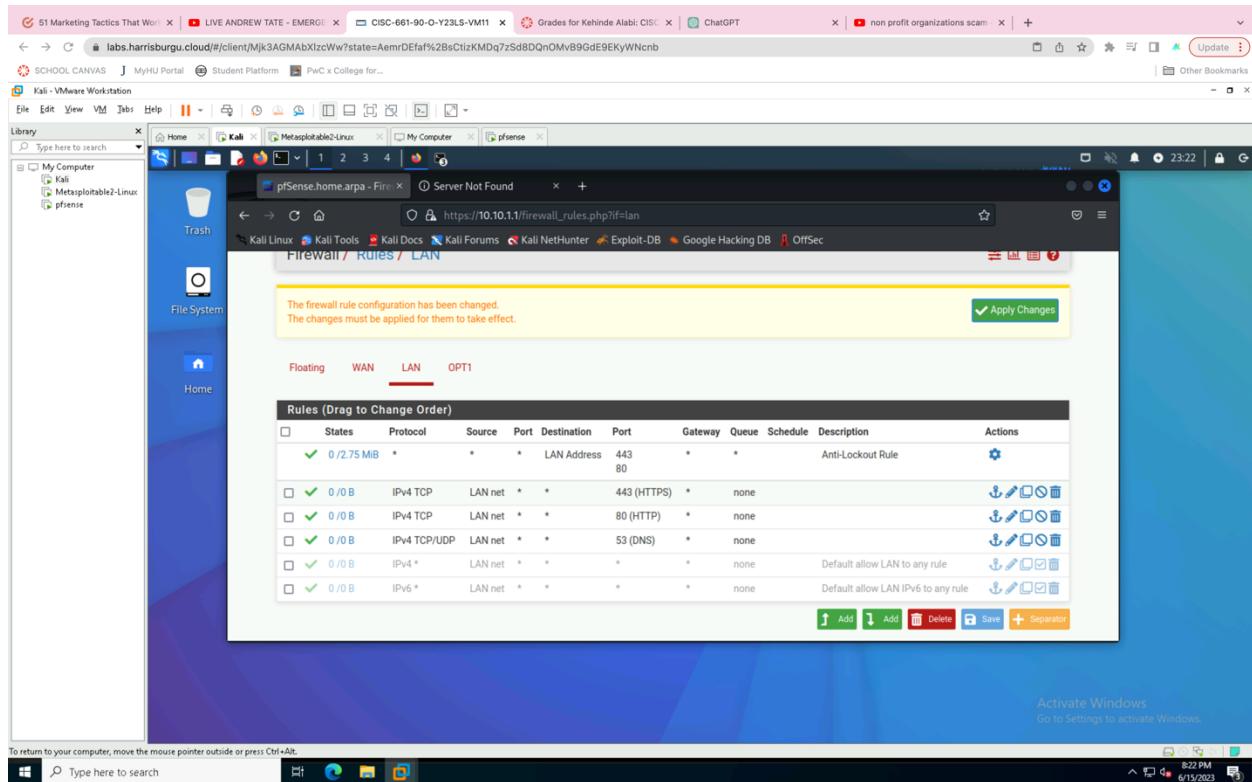
-HTTP (80)

- HTTPS

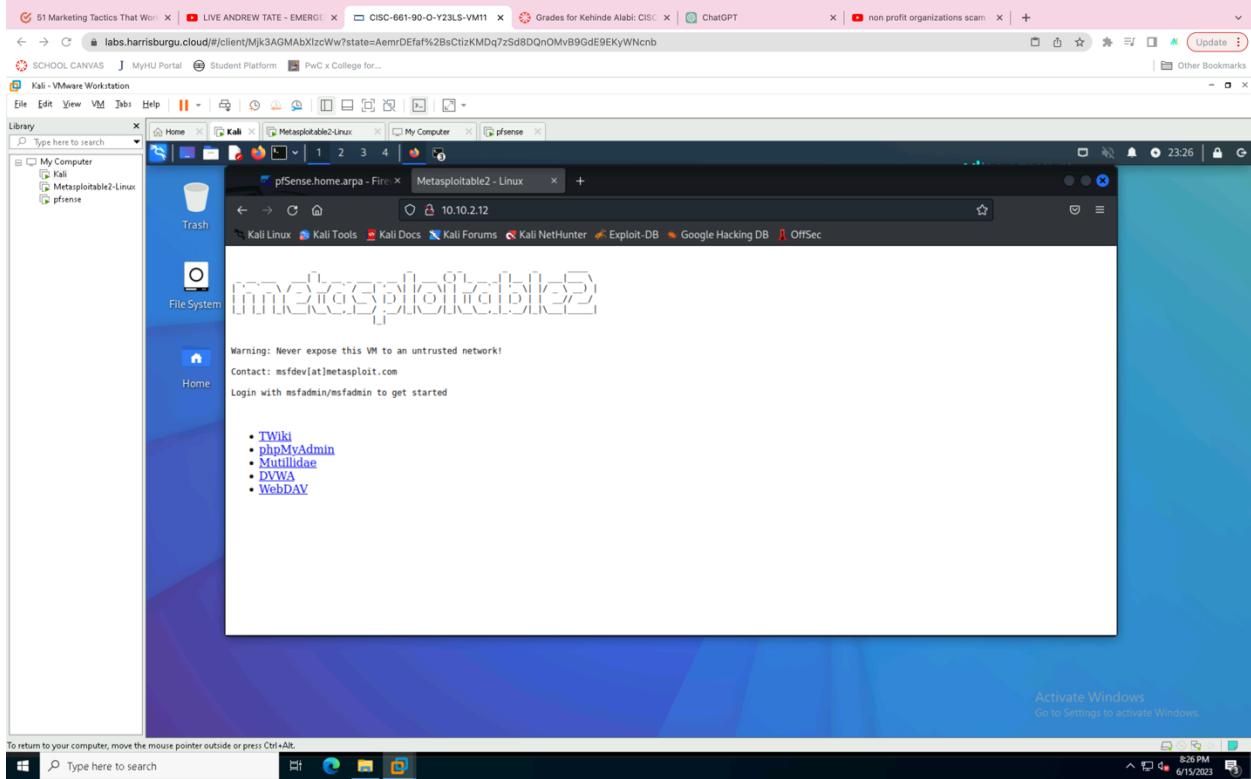
-TCP

-LAN net

-HTTPS (443)



- Firewall policy allows destination to any LAN network including Metasploitable.



NOTE: At the point of completing assignment , LAN connection to Harrisburg University was not functional hence I could not include google test after firewall configuration.