CSCI 400 Security Lab 6 Topic: Firewalls

4.1.1-

Firstly, I changed my hostname of my firewall machine to firewall1 by nanoing into etc/hostname

Next, I needed to configure the NFS server and made sure to include the hostname client in etc/exports file for the NFS Kernel Server. This was done via adding a line in etc/exports for the ip address of the client machine.
For installing iptables i did sudo apt-get install iptables.
Some configuration files I had to mess with were rules.v4 located in /etc/iptables directory

-A TCP -p tcp --dprt 22 - j ACCEPT

-A INPUT -m conntrack ESTABLISHED,RELATED -j ACCEPT
-A INPUT -i lo -j ACCEPT

-A INPUT -m conntrack --ctstate INVALID -j DROP

-A INPUT -p udp -m conntrack --ctstate NEW -j UDP
-A INPUT -p tcp --syn -m conntrack --ctstate NEW -j TCP
-A INPUT -p icmp -m conntrack --ctstate NEW -j ICMP

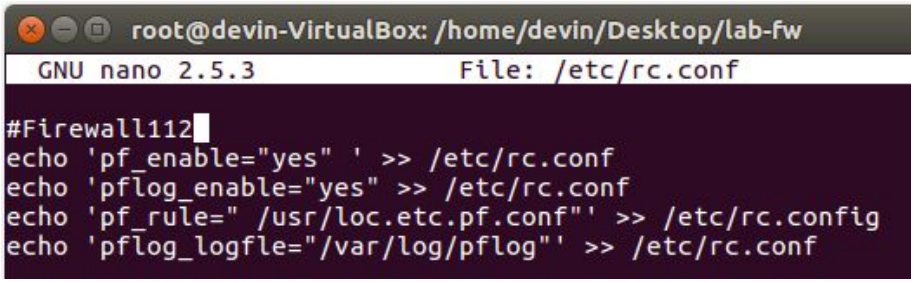
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
-AINPUT -p tcp -j REJECT --reject-with icmp-port-unreachable
-A INPUT -j REJECT --reject-with icmp-proto-unreachable

The firewall configuration was relatively easy, all I needed was the following commands:

sudo apt-get install ufw
Sudo ufw default deny incoming
Sudo ufw default allow outgoing
sudo ufw disable
sudo ufw allow icmp
sudo ufw allow ssh/tcp
sudo ufw allow 143/tcp
sudo ufw allow 80/tcp
sudo ufw allow 2049/tcp
sudo ufw status
sudo ufw enable

4.1.2 pf-

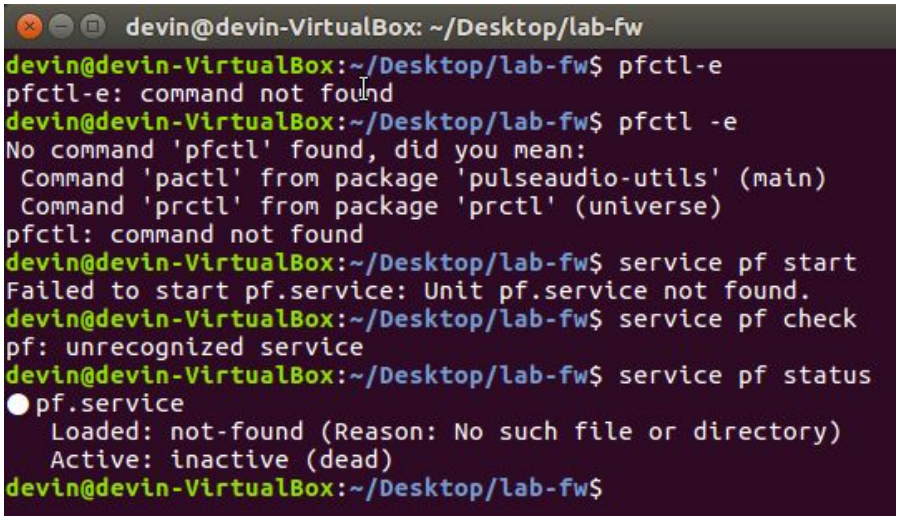
I began this task by using Ubuntu and entering the code sudo su. This code is to enable the firewall within and requires the use of a password before proceeding. We then have the GNU nano pop up in order for us to enter our new lines of code to change the file. The new code is shown below with regarding the Firewall 112 as the host In this.



Then we exit the GNU nano and save the file within. The new file is named nano /etc/rc.conf. The next step was now to check and ensure the pf file was working properly.

As shown below when testing the pf file to ensure it was saved I encountered issues. I attempted using codes to search for all pf files and nothing was working. I checked the service of it and nothing, status and the overall pf check and still ended up with nothing. Upon research I noticed that it was having an issue saving the file in Ubuntu and after attempts of restarting and trying over it was not allowing me to execute the pf files. If

this would of worked I would have been able to create a new firewall using pflog and changed the security of it to make it more secure.



4.3 Meeting of the teams

For 4.1.2 the struggle really was creating the new file within the GNU to then make it as the firewall. I was sure I was proceeding in the correct way but was falling short in trying to execute the Firewall112 file within Ubuntu. I was checking all possible outcomes inside the Ubuntu terminal to locate this new file that was saved but had no luck on locating it. It was mentioning that the active status was inactive and dead and there was an unrecognized service for pf. I then restarted the commands by doing a full reset on Ubuntu because sometimes it need to be rebooted to show any new files in my case of encounters, but still was receiving the same end result. For 4.2.1 we were unsuccessful in locating the instance in the experiments on DETER. We were then left to attempt this with our old lab 5 and it was then saying we had no access into the experiment. This in the end result did not allow us to begin the task of testing the Frobozz co firewall.