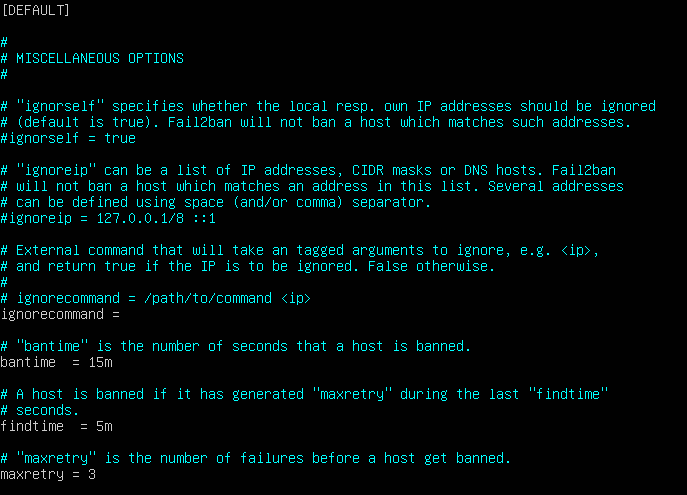
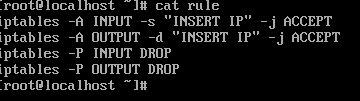
**Networking Setup**

**February 19, 2020** - Updates done on both CentOS and Unbuntu VM's. Installed and configured fail2ban settings such as bantime, findtime, maxretries. Ssh enabled on port 22.





**March 2, 2020** – Configured iptable rule to block all IP addresses except for mine.



**Important File Locations Unbuntu**

/etc/netplan/50-cloud-init.yaml <--- Network configuration file.

/usr/sbin/iptables <-- all iptables live in /usr/sbin/ with a link to /etc/alternatives.

/etc/fail2ban/jail.local 🡨 fail2ban configuration file

**Important File Locations CentOS**

/etc/netconfig <-- Network configuration file.

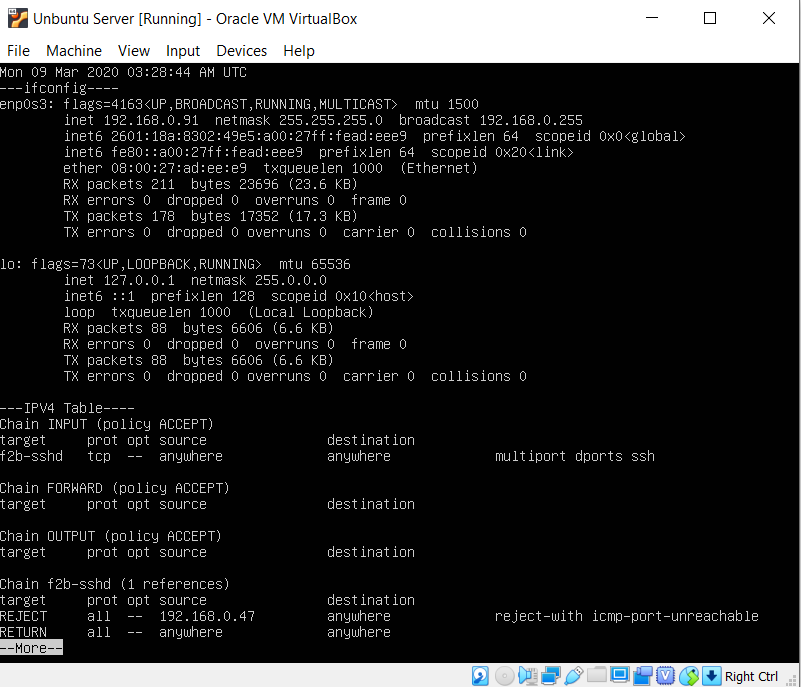
/usr/sbin/iptables 🡨 all iptables live in /usr/sbin

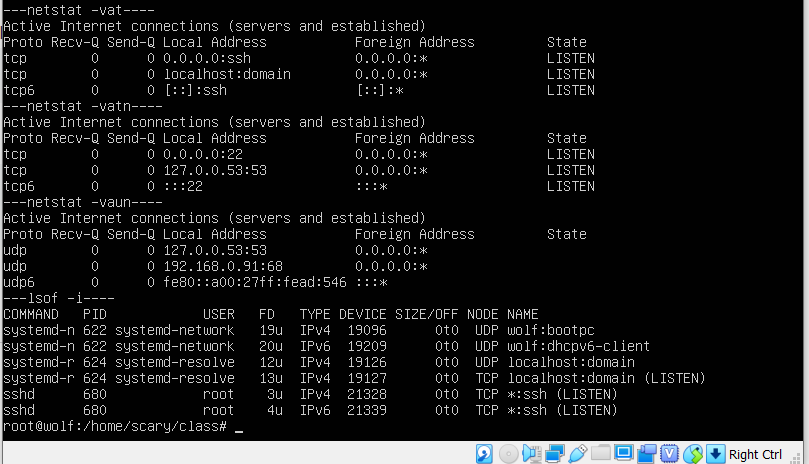
/etc/fail2ban/jail.local 🡨 fail2ban configuration file

**Network Info Script** – execute net\_info script and redirect it to a text file to capture current network information. Syntax is “./net\_info >> netinfo.txt”

Script is executed from my user home directory: /home/scary/ this is because I am the admin for these servers.

Sample output from Unbuntu server





Copy of script submitted with word doc, see net\_info.

Netinfo.txt is output run from CentOS VM.

The commands included in the netinfo script were selected because they display basic network information about my VM that I may want to monitor such as my IP address, open ports, and established connections. These would all allow me to spot potentially suspicious activity and harden my server.

**Github** - https://github.com/SCary120/Linux-Admin-Portfolio