**Networking Setup**

**PREPERATION:**

* Ensure updates have been done on both CentOS and Ubuntu servers.
* Have configured and installed settings for fail2ban
* SSH enabled on port 22

**FILE LOCATIONS FOR UBUNTU:**

/etc/netplan/50-cloud-init.yaml

/usr/sbin/iptables

**FILE LOCATIONS FOR CENT OS:**

/etc/netconfig

/usr/sbin/iptables

/etc/fail2ban/jail.local

**RUN CONFIG SCRIPT:**

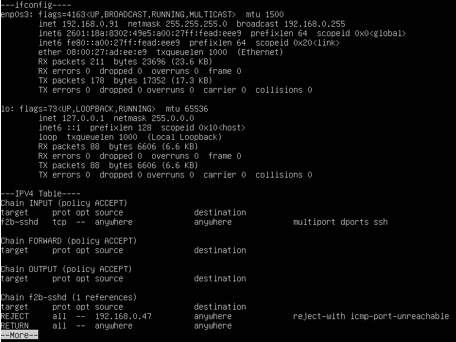
* Ensure you run the script from the home directory:

/home/yourusername/

* When running the script ensure you redirect the output to a text file using:

*./script\_name >> text\_file.txt*

SAMPLE:



NOTE:

Script is submitted in a text doc with this word doc. I chose to include the network information in my script to be able to monitor the same things you would if you ran ipconfig /all on a windows machine. This is important to monitor connections, my IP, and possible unwanted activity within my server.

**GITHUB -** <https://github.com/trevortrites/Linux_Admin_Portfolio>