**Locate rouge accounts**

cat /etc/passwd – lists some users

vi /etc/passwd — go all the way down to see more users

**NTP Connection**

sudo cat /etc/systemd/timesyncd.conf

sudo systemctl restart systemd-timesyncd.service

timedatectl status

**Clamav**

<https://linuxhint.com/install_clamav_ubuntu/>

**Locating Files**

cd /etc/pam.d

ls -lart -lart means last touched files

vi into any files that may be needed

Browse for bad files

cd /etc

ls -lart

**Locating Services**

List services

service --status-all lists all services

**Remove directories**

rm -rf directory name

**Locating Crons**

sudo vi /etc/crontab

**IPtables list commands**

https://www.cyberciti.biz/faq/how-to-list-all-iptables-rules-in-linux/

sudo iptables -S to list entered commands

sudo iptables -S INPUT

iptables -S OUTPUT

# iptables -L INPUT

# iptables -L FORWARD

# iptables -L OUTPUT

# iptables -L

Put into effect:

sudo netfilter-persistent save

sudo netfilter-persistent reload

-----------------------

**IPtables configuration commands**

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

Drop IPS

sudo iptables -A INPUT -s 192.168.1.3 -j DROP

$IPT6 -P INPUT DROP

$IPT6 -P OUTPUT DROP

$IPT6 -P FORWARD DROP

<https://www.hostinger.com/tutorials/iptables-tutorial>

<https://www.cyberciti.biz/faq/how-to-list-all-iptables-rules-in-linux/>

**NMAP**

sudo apt install nmap

nmap IP ADDRESS

nmap 10.254.0.0/24 > nmapscan.txt

netstat -tulpn | less

**Install rkhunter**

<https://www.vultr.com/docs/how-to-install-rkhunter-on-ubuntu/>

Static IP (fix):

sudo nano /etc/netplan/01-netcfg.yaml

network:

version: 2

renderer: networkd

ethernets:

ens18:

addresses: []

dhcp4: true

sudo netplan apply

sudo systemctl restart systemd-networkd

sudo apt install iputils-ping --- installs ping to check connectivity