**Linux Cheatsheet:**

**Set root password:**

su root > passwd > nano /etc/sudoers > add line “Defaults rootpw”

Defaults env\_reset

Defaults mail\_badpass

Defaults secure\_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

Defaults rootpw

**Show Users:** cat /etc/passwd | grep /bin/bash && cat /etc/passwd | grep /bin/sh

**Delete Users:** sudo userdel username / sudo deluser username

**Remove Home Directory:** sudo rm -rf /home/username

**Show Groups:**

cat /etc/group

cat /etc/group | grep sudo && cat /etc/group | grep admin

**Remove Users from Group:**

*2 Methods:*

1. sudo gpasswd -d username group
2. Remove manually > sudo nano /etc/group

**Install nmap:**

sudo apt-get install net-tools

sudo apt install nmap

sudo yum install nmap

sudo dnf install nmap

**Use nmap to enumerate services:**

nmap -sT -sV 127.0.0.1 > services.txt

nmap -p- 127.0.0.1 (run in background) > allports.txt

UDP scan: nmap -sU localhost

**Verify and Identify Service:**

sudo netstat -tulpn | grep LISTEN

**Kill Process:**

sudo killall process\_name

sudo kill processid

**Configure SSH:**

nano /etc/ssh/sshd\_config

Change permitrootlogin no

Consider changing to key based authentication

**Stop SSH:**

sudo service sshd stop

sudo service sshd status

OR

sudo systemctl stop sshd

sudo systemctl status sshd

**Start SSH:**

sudo service sshd start

sudo service sshd status

OR

sudo systemctl start sshd

sudo systemctl status sshd

**Install fail2ban:**

sudo apt install fail2ban

sudo yum install fail2ban

sudo dnf install fail2ban

sudo fail2ban-client status

**View Auth Logs:**

/var/log/auth.log

**Install UFW:**

sudo apt-get install ufw

sudo yum install epel-release

sudo yum install --enablerepo=”epel” ufw

sudo ufw enable

sudo ufw status

**Configure UFW:**

sudo ufw default deny incoming

sudo ufw default allow outgoing

(Case by case) Sudo ufw allow ssh,http,https,dns,22,80,443,53

To Do:

Mysql hardening

FTP hardening

SMB hardening

RDP hardening (Port 3389)

Telnet hardening (Take down)