To view users

cat /etc/passwd

Change Passwords (good idea to write what you change the password to down)

sudo passwd username

Configure Firewall

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

To check open ports

netstat -lntp

Example for allowing specific incoming ports. Ex. allowing 3389

sudo iptables -A INPUT -p tcp --dport 3389 -j ACCEPT

To save iptables

sudo service iptables save or **service iptables-persistent save**

If restart is needed.

sudo service iptables restart or **sudo systemctl restart iptables**

If flushing initial rules is needed.

sudo iptables -F

sudo iptables -X

sudo iptables -Z

To list the rules

sudo iptables -L -n

1. Secure root
   set `PermitRootLogin no` in `/etc/ssh/sshd_config`
2. Secure Users
   i. Disable the guest user.
      Go to `/etc/lightdm/lightdm.conf` and add the line
      `allow-guest=false`
      Then restart your session with `sudo restart lightdm`. This will log you out, so make sure you are not executing anything important.
   ii. Open up `/etc/passwd` and check which users
      a. Are uid 0
      b. Can login
      c. Are they allowed?
   iii. Delete unauthorized users:
      `sudo userdel -r $user`
      `sudo groupdel $user`
   iv. Check `/etc/sudoers.d` and make sure only members of group sudo can sudo.
   v. Check `/etc/group` and remove non-admins from sudo and admin groups.
   vi. Check user directories.
      a. cd `/home`
      b. `sudo ls -Ra *`
      c. Look in any directories which show up for media files/tools and/or "hacking tools."
   vii. Enforce Password Requirements.

Add or change password expiration requirements to `/etc/login.defs`.

```
PASS_MIN_DAYS 7
PASS_MAX_DAYS 90
PASS_WARN_AGE 14
```

3. Secure sensitive files from being viewed and edited by standard users:

   chmod 600 /etc/shadow

   chmod 600 /etc/passwd

      a. Add a minimum password length, password history, and add complexity requirements.

        a. Open `/etc/pam.d/common-password` with sudo.
        b. Add `minlen=8` to the end of the line that has `pam_unix.so` in it.
        c. Add `remember=5` to the end of the line that has `pam_unix.so` in it.
        d. Locate the line that has pam.cracklib.so in it. If you cannot find that line, install cracklib with `sudo apt-get install libpam-cracklib`.
        e. Add `ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-` to the end of that line.
    b. Implement an account lockout policy.
        a. Open `/etc/pam.d/common-auth`.
        b. Add `deny=5 unlock_time=1800` to the end of the line with `pam_tally2.so` in it.
    c. Change all passwords to satisfy these requirements. `chpasswd` is very useful for this purpose.

4. Check crontabs for anything suspicious.

   crontab -e

5. Enable automatic updates
   In the GUI set Update Manager->Settings->Updates->Check for updates:->Daily.
6. Secure ports
    i. `sudo ss -ln`
    ii. If a port has `127.0.0.1:$port` in its line, that means it's connected to loopback and isn't exposed. Otherwise, there should only be ports which are specified in the readme open (but there probably will be tons more).
    iii. For each open port which should be closed:
        a. `sudo lsof -i :$port`
        b. Copy the program which is listening on the port. `whereis $program`
        c. Copy where the program is (if there is more than one location, just copy the first one). `dpkg -S $location`
        d. This shows which package provides the file (If there is no package, that means you can probably delete it with `rm $location; killall -9 $program`). `sudo apt-get purge $package`
        e. Check to make sure you aren't accidentally removing critical packages before hitting "y".
        f. `sudo ss -l` to make sure the port actually closed.
7. Secure network

i. Enable the firewall (can skip if iptables working fine)
`sudo ufw enable`
ii. Enable syn cookie protection
`sysctl -n net.ipv4.tcp_syncookies`
iii. Disable IPv6 (Potentially harmful)
`echo "net.ipv6.conf.all.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf`
iv. Disable IP Forwarding
`echo 0 | sudo tee /proc/sys/net/ipv4/ip_forward`
v. Prevent IP Spoofing
`echo "nospoof on" | sudo tee -a /etc/host.conf`

8. Install Updates
Start this before half-way.
   i. Do general updates.
      a. `sudo apt-get update`.
      b. `sudo apt-get upgrade`.
   ii. Update services.
      a. Google to find what the latest stable version is.
      b. Google "ubuntu install service version".
      c. Follow the instructions.
9. Configure services
   i. Check service configuration files for required services. Usually a wrong setting in a config file for sql, apache, etc. will be a point.

   ii. Ensure all services are legitimate.
   `service --status-all`

   `How to shutdown a service`

   sudo systemctl stop ssh

10. Check the installed packages for "hacking tools," such as password crackers.