RedHat/Fedora Checklist

* Change Password
  + passwd <username>

Lock account = passwd -l <username>

Unlock account = passwd -u <username>

* SSH Timeout (FOR IRIS ONLY)
  + open sshd\_config within the /etc/ssh directory
    - Change the following values:  
       ClientAliveInterval 1200 (in secs)

ClientAliveCountMax 0

* Show Unauthorized Users with Root Access
  + type the following command in terminal
    - awk -F: '($3 == "0") {print}' /etc/passwd

Valid Output: root:x:0:0:root:/root:/bin/bash

Any other lines that are produced, passwd -l <username> should be done immediately (locking accounts may not be enough)

look at all logins with bash and if we don’t need it look it= cat /etc/shadow | grep bash

* Restart/Manage Services
  + sudo systemctl start <servicename>.service
  + sudo systemctl stop <servicename>.service
  + sudo systemctl enable <servicename>.service
* Enabling Firewall
  + sudo systemctl start firewalld
  + sudo systemctl enable firewalld
* Disabling Critical Services (Use to eliminate unnecessary services)
  + sudo systemctl disable <service>
* Reviewing active services
  + systemctl list-units | grep service
* Reviewing Updates
  + General Updating sudo yum update (similar to apt-get update)
  + Reviewing Security Update
    - yum check-update --security (checks for additional security update
    - yum update --security (actually updates security updates)
  + installation of packages
    - yum install <package\_file.rpm>
* Password Security
  + Creation of secure password
    - pwmake 128 (makes a randomized password of 128 bits)
  + Configuration of passwords
    - within the /etc/pam.d/passwd/ directory
      * pam\_quality.config - configure the length of password,required etc
      * passwd -d assigns a null password to user (need to check against users to see if theres passwords are null, if so lock their accounts)
    - locking root user
      * within the /etc/pam.d/password-auth and /etc/pam.d/system-auth

add the following lines to both files to deny root user after 3 unsuccessful logins

* + - * auth required pam\_faillock.so preauth silent audit deny=3 even\_deny\_root unlock\_time=600 auth sufficient pam\_unix.so nullok try\_first\_pass auth [default=die] pam\_faillock.so authfail audit deny=3 even\_deny\_root unlock\_time=600 account required pam\_faillock.so
    - unlock user (make sure that users who have been previously locked do not use this to unlock themselves
      * sudo faillock <user>
  + Firewall Configuration (either use firewalld or iptables-services)
    - system-config-firewall(shows firewalld GUI)
    - sudo systemctl start iptables
    - sudo systemctl enable iptables
      * checking status of firewalld if chosen
        + sudo systemctl status firewalld
      * check if firewall-cmd (Adding firewall rules to firewalld)
        + firewall-cmd --state
      * drop all incoming and outgoing packets
        + firewall-cmd --panic-on
      * start passing incoming and outgoing packets
        + firewall-cmd --panic-off
      * adding whitelist exception for certain programs
        + sudo firewall-cmd --add-lockdown-whitelist-command=”/usr/bin/python” -Es
      * then
        + sudo firewall-cmd --reload
      * Getting context of programs
        + ps -e --context
      * Using firewall-cmd to whitelist uid or users
        + sudo firewall-cmd --add-lockdown-whitelist-user=<user> or “-uid=<uid>
    - Starting Auditing for filesystems for file modifications
      * sudo service auditd start
    - setting auditing for /etc/passwd
      * auditctl -w /etc/passwd -p wa -k passwd\_changes
  + Denying hosts
    - editing /etc/hosts.deny gives the ability to deny particular ip addresses