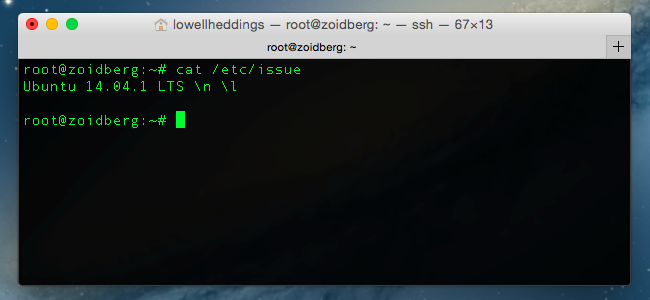
Step One



After this proceed to the appropriate checklist

Centos 7 Hardening

1. Restrict root

**#echo “tty1” > /etc/securetty**

**#chmod 700 /root**

1. Set password policy
   1. Make them expire every 180 days

**#perl -npe ‘s/PASS\_MAX\_DAYS\s+99999/PASS\_MAX\_DAYS 180/’ -i /etc/logins.defs**

1. Can only be changed once a day

**#perl -npe ‘s/PASS\_MIN\_DAYS\s+0/PASS\_MIN\_DAYS 1/g’ -i /etc/logins.defs**

1. Update system to sha512 instead of md5

**#authconfig --passalgo=sha512 --update**

1. Restrict umask file sharing

**#perl -npe ‘s/umask\s+0\d2/umask 077/g’ -i /etc/bashrc**

**#perl -npe ‘s/umask\s+0\d2/umask 077/g’ -i /etc/csh.cshrc**

1. Reap idle users

**#echo “readonly TMOUT=900” >> /etc/profile.d/os-security.sh**

**#echo “readonly HISTFILE” >> /etc/profile.d/os-security.sh**

**#chmod +x /etc/profile.d/os-security.sh**

1. Restrict cron and AT to prevent cronjobs and timed scripts
   1. Cron:

**#touch /etc/cron.allow**

**#chmod 600 /etc/cron.allow**

**#awk -F: '{print $1}' /etc/passwd | grep -v root > /etc/cron.deny**

1. AT

**#touch /etc/at.allow**

**#chmod 600 /etc/at.allow**

**#awk -F: '{print $1}' /etc/passwd | grep -v root > /etc/at.deny**

Red Hat Enterprise Linux Checklist to Secure on Setup

1. Disable interactive setup
   1. Enter “PROMPT=no” in */etc/sysconfig/init* file
2. Ensure users create good passwords with one of two methods:
   1. Create passwords for users
   2. Verify that user created passwords are of acceptable quality
      1. Edit */etc/pam.d/passwd* file with appropriate settings

**password required pam\_cracklib.so retry=3 minlen=8 minclass=4 maxsequence=3 maxrepeat=3**

1. Edit the */etc/pam.d/login* file to lock inactive accounts after a certain number of days

**chage -M <number of days> <username>**

1. Edit */etc/security/access.conf* to customize access control based on login names following the access.conf(5) man page. Do the following to restrict logins from certain accounts:
2. In both /etc/pam.d/login and /etc/pam.d/gdm-\* files:

**account required pam\_access.so**

1. In the /etc/security/access.conf file:

**- : <user you want to restrict> : ALL**

1. Disable root access
   1. Set the root account's shell to */sbin/nologin* in the */etc/passwd* file
   2. Prevent root user from logging in with command **echo > /etc/securetty** in shell prompt
   3. Disable root SSH logins with “**PermitRootLogin no**” in */etc/ssh/ssh\_dconfig* file

\*For more detailed information look at Red Hat Enterprise Linux 6 Security Guide Chapter 2 pages 29-49

Ubuntu Checklist

1. Enable automatic security updates

**#apt install unattended-upgrades**

1. Install normal updates:

**#apt update && apt upgrade**

1. Configure PAM by installing pwquality and setting good configurations
2. Install pwquality: **#apt install libpam-pwquality**
3. Edit */etc/pam.d/common-password* with settings like the following (reference **man pam\_pwquality** for more info):

**password requisite pam\_pwquality.so minlen=10 retry=3**

1. Configure firewall and iptables to limit traffic:

\*\*\*Accept all incoming traffic on local interface\*\*\*

**#iptables -A INPUT -I lo -j ACCEPT**

\*\*\*Allow traffic to SSH (to port 2222), SMTP (25), and our web server (80, 443)\*\*\*

**#iptables -A INPUT -p tcp -m tcp –dport 2222 -m state –state NEW,ESTABLISHED -j ACCEPT**

**#iptables -A INPUT -p tcp -m tcp –dport 25 -m state –state NEW,ESTABLISHED -j ACCEPT**

**#iptables -A INPUT -p tcp -m tcp –dport 80 -m state –state NEW,ESTABLISHED -j ACCEPT**

**#iptables -A INPUT -p tcp -m tcp –dport 443 -m state –state NEW,ESTABLISHED -j ACCEPT**

\*\*\*Drop all traffic in input chain\*\*\*

**#iptables -A INPUT -j DROP**

1. Make sure AppArmor is installed and is in *enforce* mode:

**#sudo apt install apparmor-profiles** (install)

**#sudo aa\_status** (checks status)

**#sudo aa-enforce /path/to/bin** (puts into *enforce* mode)

Fedora Hardening

* Either disallow root access. Three ways:
  + Change the root shell: edit the */etc/passwd* file to make the shell */sbin/nologin* instead of */bin/bash*
  + Empty */etc/securetty* file:

**#echo > /etc/securetty**

* + Edit the */etc/ssh/ sshd\_config* file and set the **PermitRootLogin** parameter to **no**.
    - Restart ssh with: **#kill -HUP `cat /var/run/sshd.pid`**
* Or limit root access via su and sudo:
  + Simplest way to control **su** access is adding specific users to the *wheel* group:

**#usermod -G wheel <username>**

* Control **sudo** use by editing */etc/sudoers* file with the **visudo** command:

**#visudo <username> ALL=(ALL) ALL**

\*\*\*See Red Hat checklist for additional security measures because the two are pretty similar