# Linux Checklist (Console Edition)

1. **Update all packages**
    - **a. Debian/Ubuntu:**
        - *i. apt-get update*
        - *ii. apt-get upgrade*
    - **b. Fedora/RHEL/CentOS**
        - *i. yum update*
        - *ii. yum –qa*
    - **c. OpenSUSE**
        - *i. yast*
    - **d. ArchLinux**
        - *i. pacman –Syu*
    - **e. Mandriva**
        - *i. urpmi --auto-update*

    - f. Some updates will be ignored, force them to be updated
        - **i. Debian/Ubuntu:**
            - *1. apt-get install <package>*
        - **ii. Fedora/RHEL/CentOS**
            - *1. yum –i <package>*
        - **iii. OpenSUSE**
            - *1. yast*
        - **iv. ArchLinux**
            - *1. pacman –S <package>*
        - **v. Mandriva**
            - *1. urpmi <package>*

    - g. Do not run in background, you will get run over quickly
        - i. Do not use an ‘&’ at the end of the command

2. **Block Telnet in IPTables**

   a. _iptables –A INPUT –p tcp --dport telnet –j DROP_
   b. _iptables –A OUTPUT –p tcp --dport telnet –j DROP_

3. **Shutdown and disable services that are not needed**

   a. _service <service> stop/start/restart_
   b. _/etc/init.d/<service> stop/start/restart_

4. **Users:**
   a. _Delete unused and/or suspicious users_
      **_i. Complete Step List to Completely Erasing Users_**
         **_1. Lock User_**
            a. _passwd –l <user>_
         **_2. List and kill processes by user_**
            a. _pgrep –u <user>_
            b. _ps –fp $(pgrep –u <user>)_
            c. _killall –KILL –u <user>_
         **_3. Delete User_**
            a. _deluser –r <user>_
         **_4. Delete user's jobs_**
            a. _crontab –r –u <user>_
         **_5. Delete Print Jobs by User (if any)_**
            a. _lprm <user>_
         **_6. Find all files owned by user and delete_**
            a. _rm (find / -user <user>)_
   b. _Modify service accounts to use /dev/null instead of /bin/bash or /sbin/nologin_
      i. _vim /etc/passwd_
      ii. _find a service account:_
         1. _/etc/passwd format is:_
            a. _<user>:<password>:<UID>:<GID>:<Name>:<home dir>:<shell>_
         2. _Change <shell> to /dev/null_

5. **Baseline check:**

   a. _netstat - Connections currently established_
   b. _ps aux - Processes currently running_

6. **Delete ALL folders in /root**

   a. _rm –fr /root/*_

7. **Delete .ssh directories in all home directories**

    a. *rm –fr /home/<user>/.ssh*

8. **Regenerate SSL keys**

    a. *ssh-keygen –t rsa*
    b. *Copy id_rsa.pub to client user's .ssh folder*

9. **Install chkrootkit**

    a. *wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz*
    b. *tar –xzf chkrootkit.tar.gz*
    c. *mkdir /usr/local/chkrootkit/*
    d. *mv chkrootkit*/* /usr/local/chkrootkit*
    e. *cd /usr/local/chkrootkit*
    f. *make sense*
    g. */usr/local/chkrootkit/chkrootkit*

10. **Install AVG**

    a. *wget http://download.avgfree.com/filedir/inst/avg2013flx-r3110-a6015.i386.tar.gz*
    b. *tar xzvf avg2013flx-r3110-a6015.i386.tar.gz*
    c. *cd <directory>*
    d. *./install.sh*

11. **Modify Config files**

    **a.** Example of config files: (sshd, vsftpd, apache, etc…)

12. **Monitor Log Files, 'netstat', 'ps aux', and 'who' for any indication of entrance into the system.**