

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>)`
 - ii. 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.