Hardening Linux

I used Debian 8 but this document should apply to Fedora and Ubuntu, most distros have these features below, and you can replace “apt-get” commands with “yum” for other Distros. Any commands in quotes please exclude the quotes. I used “root” for all the commands. This not a tutorial for beginners but intermediate to advanced Administrators.

After Installation

Download GRUB2 for Debian or Ubuntu 14.04, this is the latest in security safety. Debian actually separates individual partitions like “/dev/var/home/tmp/ on install which is a requirement for making it difficult on hackers to jump to different partitions. This configuration will prevent hard link breaches or escalations.

• Add a bios password to a server so hackers cannot modify the bios. Boot your server to a bios prompt and add a password. Also, move removable devices down the ladder of the boot order.

Update your Distro before proceeding with a “yum install updates” or “apt-get install updates”, this will get your current fixes, updates, patches as needed.

• Sync your NTP with an install of time service, type “apt-get install NTP” or ”yum install NTP” then start the service with “service NTPD start” or check status with “service NTPD status”

• Password security, set expire dates, “vi /etc/default/useradd” and set the expired days to your company’s policy.

• Set passwords as non-reusable “vi /etc/default/useradd” look for line ”password sufficient” at the end of that line add “remember=8” and save. 8 means times you may use the same passwords. You can add a line if it’s not there “password sufficient pam_unix.so use_authtok md5 shadow remember=8”

• To check for SUID bit, which allows programs executed with root privileges: find / -perm -04000

• Check that no users have a UID as zero; the only root should have a zero. “grep 'x:0:' /etc/passwd” or “getent passwd 0”

• ssh to connect to other servers use”ssh-keygen –t rsa” this creates both private and public keys.

• To export your public key use “scp .ssh/ida_rsa.pub x.x.x.x: .ssh/authorized_keys2” use an IP or hostname to replace x.

• Put a padlock on the server if possible.

• Lock down cron as Root only

Check the file of who names have access to open crontab or create one.

“vi /etc/cron.allow” add the name “root” if empty. This will allow the only root to modify cron jobs.

• Lock down USB sticks installs vi /etc/modprobe.d/no-usb.

• Add a line “install usb-storage /bin/true” reboot, test an usb stick and it should not install anything.

• Remove FTP service if installed with “yum remove –y ftp” or “apt-get remove ftp”.

• Use sftp instead and this will encrypt your password.

• Check ports that are open: netstat –lnptu and close the wrong ports that are not needed.

• Download selinux if you really know how to run with it. “aptitude install selinux-basics selinux-policy-default”

• Turn on SELinux if off, check with “getenforce” or turn on with “setenforce enforcing” this is a strict mode for users trying to do other non-permissive commands. The file is located at /etc/selinux/config check to see if it is set to “SELINUX=enforcing”.

• Shutdown all graphical interfaces if you have multiple machines (Xwindows) GNOME if installed.

• Setting to run level 3 “cat /etc/inittab” look for a hard link (ln –s) that points to runlevel5 and remove it.

• Remove the path to runlevel5, my command looks like this “rm /etc/system/system/default.target” runlevel5 is the GNOME or KDE level.

• Set to runlevel3 mine looks like this:

• “ln –s /lib/systemd/system/runlevel3.target /etc/systemd/system/default.target”

• Now check and remove all GNOME and KDE, locate with “yum grouplist |egrep “GNOME|KDE”.

```
# yum grouplist | egrep "GNOME|KDE"
   GNOME Desktop Environment
   GNOME Software Development
   KDE Software Compilation
   KDE Software Development
                # yum groupremove "GNOME Desktop Environment" -y;yum groupremove "GNOME So
tware Development" -y; yum groupremove "KDE Software Compilation" -y; yum groupremove "KDE
 Software Development" -y
```

REBOOT and all should be good and use command line only moving forward.