Level 3 Hardening

Perform all of the procedures listed in the Level 1 & 2 Hardening Baselines

Remove SUID bits from the following applications

1. chmod a-s /bin/mount
2. chmod a-s /bin/umount
3. chmod a-s /bin/ping
4. chmod a-s /usr/bin/at
5. chmod a-s /usr/sbin/traceroute

Remove permissions from lpd for anyone but root

- chmod 500 /usr/bin/lpr
- chmod 500 /usr/bin/lprm

The following chattr steps are recommended for L3 hardening, but NOT required. These steps may not be compatible with most applications as it effectively locks the system from being able to modify these files at all. Therefore, to modify the password file, you must remove the immutable bit, make your changes and then set it back. This applies not only to adding/modifying users, but anything that attempts to modify the password file for you (i.e. dselect if it is adding a service which creates a new user, etc).

Set /etc/passwd, shadow, group and gshadow immutable

```
chattr +i /etc/passwd
chattr +i /etc/shadow
chattr +i /etc/group
chattr +i /etc/gshadow
```

configure /etc/security/limits.conf

```
# to not allow core dumps;
* hard core 0
```

to limit the number of process per user (that logins via the login program)

```
# to limit all users to 100 soft and 150 hard process
* soft nproc 100
* hard nproc 150
# to limit ftp to 40 process
ftp hard nproc 40
# to limit usera to 2 logins
usera – maxlogins 2
(etc)
```

(note none of the above applies to uid 0 accounts)

edit /etc/pam.d/login and uncomment ;
session required pam_limits.so

edit /etc/pam.d/ssh and uncomment
session required pam_limits.so

add to sysctl.conf values;
net/ipv4/tcp_syncookies = 1

tighten up login defaults even further
/etc/login.defs
FAIL_DELAY = 60
LOG_UNKFAIL_ENAB = yes
LOG_OK_LOGINS = yes

build a monolithic kernel
apt-get install libncurses5-dev
retrieve approved kernel source
in kernel config;
- set Local version M-L3 (if 2.6.9)
- be sure that sysctl is enabled
- turn off module loading
- turn off un needed features
- configure all needed features to be built in static
- turn on ext3 security labels

add kernel to grub (the following examples assumes that it is 2.6.9 and that the kernel is /boot/linux-2.6.9, adjust root as needed)

```
title          M-L3, kernel 2.6.9
root           (hd0,1)
kernel         /boot/linux-2.6.9 root=/dev/sda2 ro
savedefault
boot

title          M-L3, kernel 2.6.9 (recovery mode)
root           (hd0,1)
kernel         /boot/linux-2.6.9 root=/dev/sda2 ro single
savedefault
boot
```

review /etc/SekHost.conf and tighten if possible

- greater restrictions on open services
- log drops
- DI[0]="-p tcp --tcp-flags ALL SYN,FIN"
- DI[1]="-p tcp --tcp-flags ALL SYN,FIN,RST"
- DI[2]="-p tcp --tcp-flags ALL SYN,FIN,URG"
- DI[3]="-p tcp --tcp-flags ALL SYN,FIN,RST,URG"
- DI[4]="-p tcp --tcp-flags ALL SYN,FIN,ACK,URG"
- DI[5]="-p tcp --tcp-flags ALL SYN,FIN,PSH"
- DI[6]="-p tcp --tcp-flags ALL SYN,FIN,PSH,URG"
- DI[7]="-p tcp --tcp-flags ALL SYN,FIN,PSH,RST"
- DI[8]="-p tcp --tcp-flags ALL SYN,FIN,PSH,RST"
- DI[9]="-p tcp ! --syn -m state --state NEW"

rerun tripwire to update to new values
store trip wire db in a secure location and review during each patch management cycle

If running apache and the TRACE/TRACK methods are not needed add the following rewrite rules;

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* -[F]
```