Appendix D – Tripwire Sample Configuration
Session # 115

```
# tripwire.config
#
# Modified from original (generic) sample created by:
#       Joe Polcari <jpolcari@galaxy.prime.com>
#
# This file contains a list of files and directories that System
# Preener will scan.  Information collected from these files will be
# stored in the tripwire.database file.
#
# Format:       [!|=] entry [ignore-flags]
#
# where:        '!' signifies the entry is to be pruned (inclusive) from
#                       the list of files to be scanned.
#               '=' signifies the entry is to be added, but if it is
#                       a directory, then all its contents are pruned
#                       (useful for /tmp).
#
# where:        entry is the absolute pathname of a file or a directory
#
# where ignore-flags are in the format:
#               [template][ [+|-][pinugsam12] ... ]
#
#       - :  ignore the following atributes
#       + :  do not ignore the following attributes
#
#       p :  permission and file mode bits      a: access timestamp
#       i :  inode number                       m: modification timestamp
#       n :  number of links (ref count)        c: inode creation timestamp
#       u :  user id of owner                   1: signature 1
#       g :  group id of owner                  2: signature 2
#       s :  size of file
#
#
# Ex:   The following entry will scan all the files in /etc, and report
#       any changes in mode bits, inode number, reference count, uid,
#       gid, modification and creation timestamp, and the signatures.
#       However, it will ignore any changes in the access timestamp.
#
#       /etc    +pinugsm12-a
#
# The following templates have been pre-defined to make these long ignore
# mask descriptions unecessary.
#
# Templates:    (default)       R :  [R]ead-only (+pinugsm12-a)
```

```
#                       L :  [L]og file (+pinug-sam12)
#                       N :  ignore [N]othing (+pinusgsamc12)
#                       E :  ignore [E]verything (-pinusgsamc12)
#
# By default, Tripwire uses the R-c2 template -- it ignores
# only the access timestamp.
#
# You can use templates with modifiers, like:
#       Ex:  /etc/lp    E+ug
#
#       Example configuration file:
#               /etc            R       # all system files
#               !/etc/lp        R       # ...but not those logs
#               =/tmp           N       # just the directory, not its files
#
# Note the difference between pruning (via "!") and ignoring everything
# (via "E" template):  Ignoring everything in a directory still monitors
# for added and deleted files.  Pruning a directory will prevent Tripwire
# from even looking in the specified directory.
#
#
# Tripwire running slowly?  Modify your tripwire.config entries to
# ignore the (signature 2) attribute when this computationally-exorbitant
# protection is not needed.  (See README and design document for further
# details.)
#
# ---------------------------------------------------------------------------
#
#       970612  bs      Modified sample to better meet HP-UX 10.20 and CTC
#                       usage
#
# ---------------------------------------------------------------------------
#
# First, the root directory and root's "home"
=/                      R-c2
=/root                  L-c2
/root/.Xauthority       R-c2
/root/.elm              L-c2
/root/.profile          R-c2
/root/.secure           R-c2
=/root/.sw              L-c2

# Unix (kernel) files themself
/stand                  R-c2

# Now, some critical directories and files
```

```
#  Some exceptions are noted further down
/etc                          R-c2
/etc/hpC2400/hparray.map        L-c2
/etc/shutdownlog                L-c2
/etc/mail/sendmail.pid          L-c2
/etc/mail/aliases.db            L-c2
/etc/mail/aliases               L-c2
/etc/xtab                       L-c2
/etc/.ad                        L-c2
/etc/hpC2400/hparray.addr       L-c2
/etc/hpC2400/hparray.devs       L-c2
/etc/hpC2400/hparray.luns       L-c2
/etc/hpC2400/monitor.lock       L-c2
/etc/hpC2400/pscan.lock         L-c2
/etc/rmtab                      L-c2
/etc/ifconfig.muxids            L-c2
/etc/auto_parms.log             L-c2i
/etc/auto_parms.log.old         L-c2
/etc/hpC2400/HPARRAY.INFO       L-c2
/etc/rc.log                     L-c2
/etc/rc.log.old                 L-c2
/etc/mnttab                     L-c2
/etc/eisa/config.err            L-c2
/etc/SnmpAgent.d/snmpd.conf     L-c2
/etc/SnmpAgent.d                L-c2
/etc/group                      L-c2i
/etc/pam_user.conf              L-c2
/etc/#pam_user.conf             L-c2
/etc/profile                    L-c2
/etc/passwd                     L-c2i
/etc/utmp                       L-c2
/etc/utmpx                      L-c2
/etc/inetd.conf                 R-c

!/cdrom
!/net

/tcb                          R-c
=/tcb/files/auth                R-c2
/tcb/files/auth/system/default  R-c2

=/var                         R-c2
=/var/X11                       L-c2
=/var/adm                       R-c2
/var/adm/inetd.sec              R-c
/var/adm/btmp                   L-c2i
```

```
/var/adm/wtmp                 L-c2i
/var/adm/sulog                L-c2i
=/var/adm/syslog              L-c2i
=/var/adm/cron                R-c2
/var/adm/cron/at.allow        L-c2i
/var/adm/cron/cron.allow      L-c2i
=/var/dt                      R-c2
=/var/mail                    R-c2
=/var/news                    R-c2
=/var/opt                     R-c2
=/var/preserve                R-c2
=/var/rbootd                  R-c2
=/var/run                     R-c2
=/var/sam                     R-c2
=/var/spool                   R-c2
=/var/statmon                 R-c2
=/var/tmp                     R-c2i
=/var/uucp                    R-c2
=/var/yp                      R-c2
=/dev                         R-c2
/dev                          E
/dev/vg00                     R-c2
/dev/vg01                     R-c2
=/usr                         R-c2
/usr/bin                      R-c2
/usr/bin/ccs                  R-c2
/usr/conf                     R-c2
/usr/contrib                  R-c2
/usr/dt                       R-c2
/usr/etc                      R-c2
=/usr/examples                R-c2
/usr/hpC2400                  E
/usr/include                  R-c2
/usr/lbin                     R-c2
/usr/lib                      R-c2
/usr/local                    R-c2i
/usr/newconfig                R-c2i
/usr/obam                     E
/usr/old                      R-c2
/usr/sam                      R-c2
/usr/sbin                     R-c2
/usr/share                    R-c2
/usr/tsm                      E
/usr/vue                      R-c2
=/opt                         R-c
/opt/tripwire/tripwire-1.2    R-c
```

```
# Checksumming the following is not so critical.  However,
#  setuid/setgid files are special-c2ased further down.

=/lib                R-c2
=/bin                 R-c2
/sbin                 R-c2

=/tmp                 L-c2

#  Here are entries for setuid/setgid files.  On these, we use
#  both signatures just to be sure. (From /etc /sbin /bin /lib
#  /opt)


#  Here are entries for setuid/setgid files.  On these, we use
#  both signatures just to be sure.
#
#  You may want/need to edit this list.  Batteries not inc.

/etc/wall       R-c
/etc/vgscan     R-c
/etc/vgremove   R-c
/etc/vgreduce   R-c
/etc/vgimport   R-c
/etc/vgextend   R-c
/etc/vgexport   R-c
/etc/vgdisplay  R-c
/etc/vgcreate   R-c
/etc/vgchange   R-c
/etc/vgcfgrestore       R-c
/etc/vgcfgbackup        R-c
/etc/sysdef     R-c
/etc/pvmove     R-c
/etc/pvdisplay  R-c
/etc/pvcreate   R-c
/etc/pvchange   R-c
/etc/ping       R-c
/etc/mediainit  R-c
/etc/lvrmboot   R-c
/etc/lvremove   R-c
/etc/lvreduce   R-c
/etc/lvlnboot   R-c
/etc/lvextend   R-c
/etc/lvdisplay  R-c
/etc/lvcreate   R-c
```

```
/etc/lvchange   R-c
/etc/lanscan    R-c
/etc/arp        R-c
/usr/bin/mediainit      R-c
/usr/bin/bdf    R-c
/usr/bin/rcp    R-c
/usr/bin/remsh  R-c
/usr/bin/at     R-c
/usr/bin/crontab        R-c
/usr/bin/mail   R-c
#
#
#
```