```
##############################################################################
 #                                                                          ##
############################################################################## #
#                                                                          # #
#                     Policy file for RedHat Linux 7.0                     # #
#                               V1.0.0                                     # #
#                            July 18, 2000                                 # #
#                                                                          ##
##############################################################################
  ############################################################################
 #                                                                           ##
############################################################################## #
#                                                                          # #
# This is the example Tripwire Policy file.  It is intended as a place to  # #
# start creating your own custom Tripwire Policy file.  Referring to it as # #
# well as the Tripwire Policy Guide should give you enough information to  # #
# make a good custom Tripwire Policy file that better covers your          # #
# configuration and security needs.  A text version of this policy file is # #
# called twpol.txt.                                                        # #
#                                                                          # #
# Note that this file is tuned to an 'everything' install of RedHat Linux  # #
# 7.0.  If run unmodified, this file should create no errors on database   # #
# creation, or violations on a subsiquent integrity check.  However, it is # #
# impossible for there to be one policy file for all machines, so this     # #
# existing one errs on the side of security.  Your Linux configuration will # #
# most likey differ from the one our policy file was tuned to, and will    # #
# therefore require some editing of the default Tripwire Policy file.      # #
#                                                                          # #
# The example policy file is best run with 'Loose Directory Checking'      # #
# enabled. Set LOOSEDIRECTORYCHECKING=TRUE in the Tripwire Configuration   # #
# file.                                                                    # #
#                                                                          # #
# Email support is not included and must be added to this file.            # #
# Add the 'emailto=' to the rule directive section of each rule (add a comma # #
# after the 'severity=' line and add an 'emailto=' and include the email   # #
# addresses you want the violation reports to go to).  Addresses are       # #
# semi-colon delimited.                                                    # #
#                                                                          ##
##############################################################################
  ############################################################################
 #                                                                           ##
############################################################################## #
#                                                                          # #
# Global Variable Definitions                                              # #
#                                                                          # #
# These are defined at install time by the installation script.  You may   # #
# Manually edit these if you are using this file directly and not from the # #
# installation script itself.                                              # #
#                                                                          ##
##############################################################################
@@section GLOBAL
TWDOCS="/usr/doc/tripwire";
TWBIN="/usr/sbin";
TWPOL="/etc/tripwire";
TWDB="/var/lib/tripwire";
TWSKEY="/etc/tripwire";
TWLKEY="/etc/tripwire";
TWREPORT="/var/lib/tripwire/report";
HOSTNAME=fedora.elpiso.es;
@@section FS
SEC_CRIT      = $(IgnoreNone)-SHa ;# Critical files that cannot change
SEC_SUID      = $(IgnoreNone)-SHa ;# Binaries with the SUID or SGID flags set
SEC_BIN       = $(ReadOnly) ;      # Binaries that should not change
SEC_CONFIG    = $(Dynamic) ;       # Config files that are changed infrequently but acces-
sed often
SEC_LOG       = $(Growing) ;       # Files that grow, but that should never change owners-
```

```
hip
SEC_INVARIANT = +tpug ;            # Directories that should never change permission or ow-
nership
SIG_LOW       = 33 ;               # Non-critical files that are of minimal security impact
SIG_MED       = 66 ;               # Non-
critical files that are of significant security impact
SIG_HI        = 100 ;              # Critical files that are significant points of vulnera-
bility
# Tripwire Binaries
(
  rulename = "Tripwire Binaries",
  severity = $(SIG_HI)
)
{
  $(TWBIN)/siggen                     -> $(SEC_BIN) ;
  $(TWBIN)/tripwire                   -> $(SEC_BIN) ;
  $(TWBIN)/twadmin                    -> $(SEC_BIN) ;
  $(TWBIN)/twprint                    -> $(SEC_BIN) ;
}
# Tripwire Data Files - Configuration Files, Policy Files, Keys, Reports, Databases
(
  rulename = "Tripwire Data Files",
  severity = $(SIG_HI)
)
{
  # NOTE: We remove the inode attribute because when Tripwire creates a backup,
  # it does so by renaming the old file and creating a new one (which will
  # have a new inode number).  Inode is left turned on for keys, which shouldn't
  # ever change.
  # NOTE: The first integrity check triggers this rule and each integrity check
  # afterward triggers this rule until a database update is run, since the
  # database file does not exist before that point.
  $(TWDB)                             -> $(SEC_CONFIG) -i ;
  $(TWPOL)/tw.pol                     -> $(SEC_BIN) -i ;
  $(TWPOL)/tw.cfg                     -> $(SEC_BIN) -i ;
  $(TWLKEY)/$(HOSTNAME)-local.key     -> $(SEC_BIN) ;
  $(TWSKEY)/site.key                  -> $(SEC_BIN) ;
  #don't scan the individual reports
  $(TWREPORT)                         -> $(SEC_CONFIG) (recurse=0) ;
}
# Tripwire HQ Connector Binaries
#(
#  rulename = "Tripwire HQ Connector Binaries",
#  severity = $(SIG_HI)
#)
#{
#  $(TWBIN)/hqagent                    -> $(SEC_BIN) ;
#}
#
# Tripwire HQ Connector - Configuration Files, Keys, and Logs
  ##############################################################################
 #                                                                             ##
############################################################################## #
#                                                                            # #
# Note: File locations here are different than in a stock HQ Connector       # #
# installation.  This is because Tripwire 2.3 uses a different path          # #
# structure than Tripwire 2.2.1.                                             # #
#                                                                            # #
# You may need to update your HQ Agent configuation file (or this policy     # #
# file) to correct the paths.  We have attempted to support the FHS standard # #
# here by placing the HQ Agent files similarly to the way Tripwire 2.3       # #
# places them.                                                               # #
#                                                                            ##
##############################################################################
#(
#  rulename = "Tripwire HQ Connector Data Files",
```

```
#  severity = $(SIG_HI)
#)
#{
#   ##############################################################################
#  ##############################################################################
#  # NOTE: Removing the inode attribute because when Tripwire creates a backup ##
#  # it does so by renaming the old file and creating a new one (which will    ##
#  # have a new inode number).  Leaving inode turned on for keys, which        ##
#  # shouldn't ever change.                                                    ##
#  ##############################################################################
#
#  $(TWBIN)/agent.cfg                   -> $(SEC_BIN) -i ;
#  $(TWLKEY)/authentication.key         -> $(SEC_BIN) ;
#  $(TWDB)/tasks.dat                    -> $(SEC_CONFIG) ;
#  $(TWDB)/schedule.dat                 -> $(SEC_CONFIG) ;
#
#  # Uncomment if you have agent logging enabled.
#  #/var/log/tripwire/agent.log      -> $(SEC_LOG) ;
#}
# Commonly accessed directories that should remain static with regards to owner and group
(
  rulename = "Invariant Directories",
  severity = $(SIG_MED)
)
{
  /                                   -> $(SEC_INVARIANT) (recurse = 0) ;
  /home                               -> $(SEC_INVARIANT) (recurse = 0) ;
  /etc                                -> $(SEC_INVARIANT) (recurse = 0) ;
}
  ################################################
 #                                               ##
################################################ #
#                                               # #
# File System and Disk Administration Programs # #
#                                               ##
################################################
(
  rulename = "File System and Disk Administraton Programs",
  severity = $(SIG_HI)
)
{
  /sbin/accton                        -> $(SEC_CRIT) ;
  /sbin/badblocks                     -> $(SEC_CRIT) ;
  /sbin/dosfsck                       -> $(SEC_CRIT) ;
  /sbin/e2fsck                        -> $(SEC_CRIT) ;
  /sbin/debugfs                       -> $(SEC_CRIT) ;
  /sbin/dumpe2fs                      -> $(SEC_CRIT) ;
  /sbin/dump                          -> $(SEC_CRIT) ;
  /sbin/dump.static                   -> $(SEC_CRIT) ;
  /sbin/e2label                       -> $(SEC_CRIT) ;
  /sbin/fdisk                         -> $(SEC_CRIT) ;
  /sbin/fsck                          -> $(SEC_CRIT) ;
  /sbin/fsck.ext2                     -> $(SEC_CRIT) ;
  /sbin/fsck.minix                    -> $(SEC_CRIT) ;
  /sbin/fsck.msdos                    -> $(SEC_CRIT) ;
  /sbin/ftl_check                     -> $(SEC_CRIT) ;
  /sbin/ftl_format                    -> $(SEC_CRIT) ;
  /sbin/hdparm                        -> $(SEC_CRIT) ;
  /sbin/mkbootdisk                    -> $(SEC_CRIT) ;
  /sbin/mkdosfs                       -> $(SEC_CRIT) ;
  /sbin/mke2fs                        -> $(SEC_CRIT) ;
  /sbin/mkfs                          -> $(SEC_CRIT) ;
  /sbin/mkfs.ext2                     -> $(SEC_CRIT) ;
  /sbin/mkfs.minix                    -> $(SEC_CRIT) ;
  /sbin/mkfs.msdos                    -> $(SEC_CRIT) ;
  /sbin/mkinitrd                      -> $(SEC_CRIT) ;
```

```
  /sbin/mkpv                            -> $(SEC_CRIT) ;
  /sbin/mkraid                          -> $(SEC_CRIT) ;
  /sbin/mkswap                          -> $(SEC_CRIT) ;
  /sbin/mtx                             -> $(SEC_CRIT) ;
  /sbin/parted                          -> $(SEC_CRIT) ;
  /sbin/pcinitrd                        -> $(SEC_CRIT) ;
  /sbin/quotacheck                      -> $(SEC_CRIT) ;
  /sbin/quotaon                         -> $(SEC_CRIT) ;
  /sbin/raidstart                       -> $(SEC_CRIT) ;
  /sbin/resize2fs                       -> $(SEC_CRIT) ;
  /sbin/restore                         -> $(SEC_CRIT) ;
  /sbin/restore.static                  -> $(SEC_CRIT) ;
  /sbin/scsi_info                       -> $(SEC_CRIT) ;
  /sbin/sfdisk                          -> $(SEC_CRIT) ;
  /sbin/tapeinfo                        -> $(SEC_CRIT) ;
  /sbin/tune2fs                         -> $(SEC_CRIT) ;
  /sbin/update                          -> $(SEC_CRIT) ;
  /bin/mount                            -> $(SEC_CRIT) ;
  /bin/umount                           -> $(SEC_CRIT) ;
  /bin/touch                            -> $(SEC_CRIT) ;
  /bin/mkdir                            -> $(SEC_CRIT) ;
  /bin/mknod                            -> $(SEC_CRIT) ;
  /bin/mktemp                           -> $(SEC_CRIT) ;
  /bin/rm                               -> $(SEC_CRIT) ;
  /bin/rmdir                            -> $(SEC_CRIT) ;
  /bin/chgrp                            -> $(SEC_CRIT) ;
  /bin/chmod                            -> $(SEC_CRIT) ;
  /bin/chown                            -> $(SEC_CRIT) ;
  /bin/cp                               -> $(SEC_CRIT) ;
  /bin/cpio                             -> $(SEC_CRIT) ;
}
  ###################################
 #                                 ##
################################### #
#                                 # #
# Kernel Administration Programs # #
#                                 ##
###################################
(
  rulename = "Kernel Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin/depmod                          -> $(SEC_CRIT) ;
  /sbin/adjtimex                        -> $(SEC_CRIT) ;
  /sbin/ctrlaltdel                      -> $(SEC_CRIT) ;
  /sbin/insmod                          -> $(SEC_CRIT) ;
  /sbin/insmod.static                   -> $(SEC_CRIT) ;
  /sbin/insmod_ksymoops_clean           -> $(SEC_CRIT) ;
  /sbin/klogd                           -> $(SEC_CRIT) ;
  /sbin/ldconfig                        -> $(SEC_CRIT) ;
  /sbin/minilogd                        -> $(SEC_CRIT) ;
  /sbin/modinfo                         -> $(SEC_CRIT) ;
  /sbin/sysctl                          -> $(SEC_CRIT) ;
}
  ########################
 #                      ##
######################## #
#                      # #
# Networking Programs # #
#                      ##
########################
(
  rulename = "Networking Programs",
  severity = $(SIG_HI)
)
```

```
{
  /sbin/arp                             -> $(SEC_CRIT) ;
  /sbin/dhcpcd                          -> $(SEC_CRIT) ;
  /sbin/getty                           -> $(SEC_CRIT) ;
  /sbin/ifcfg                           -> $(SEC_CRIT) ;
  /sbin/ifconfig                        -> $(SEC_CRIT) ;
  /sbin/ifdown                          -> $(SEC_CRIT) ;
  /sbin/ifenslave                       -> $(SEC_CRIT) ;
  /sbin/ifport                          -> $(SEC_CRIT) ;
  /sbin/ifup                            -> $(SEC_CRIT) ;
  /sbin/ifuser                          -> $(SEC_CRIT) ;
  /sbin/ip                              -> $(SEC_CRIT) ;
  /sbin/ipchains                        -> $(SEC_CRIT) ;
  /sbin/ipchains-restore                -> $(SEC_CRIT) ;
  /sbin/ipchains-save                   -> $(SEC_CRIT) ;
  /sbin/ipfwadm                         -> $(SEC_CRIT) ;
  /sbin/ipmaddr                         -> $(SEC_CRIT) ;
  /sbin/iptables                        -> $(SEC_CRIT) ;
  /sbin/iptunnel                        -> $(SEC_CRIT) ;
  /sbin/ipx_configure                   -> $(SEC_CRIT) ;
  /sbin/ipx_interface                   -> $(SEC_CRIT) ;
  /sbin/ipx_internal_net                -> $(SEC_CRIT) ;
  /sbin/iwconfig                        -> $(SEC_CRIT) ;
  /sbin/iwpriv                          -> $(SEC_CRIT) ;
  /sbin/iwspy                           -> $(SEC_CRIT) ;
  /sbin/netreport                       -> $(SEC_CRIT) ;
  /sbin/plipconfig                      -> $(SEC_CRIT) ;
  /sbin/portmap                         -> $(SEC_CRIT) ;
  /sbin/ppp-watch                       -> $(SEC_CRIT) ;
  /sbin/rarp                            -> $(SEC_CRIT) ;
  /sbin/route                           -> $(SEC_CRIT) ;
  /sbin/slattach                        -> $(SEC_CRIT) ;
  /sbin/uugetty                         -> $(SEC_CRIT) ;
  /sbin/vgetty                          -> $(SEC_CRIT) ;
  /sbin/ypbind                          -> $(SEC_CRIT) ;
  /bin/ping                             -> $(SEC_CRIT) ;
}
  ###################################
 #                                  ##
################################### #
#                                  # #
# System Administration Programs # #
#                                  ##
###################################
(
  rulename = "System Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin/chkconfig                       -> $(SEC_CRIT) ;
  /sbin/fuser                           -> $(SEC_CRIT) ;
  /sbin/halt                            -> $(SEC_CRIT) ;
  /sbin/init                            -> $(SEC_CRIT) ;
  /sbin/initlog                         -> $(SEC_CRIT) ;
  /sbin/killall5                        -> $(SEC_CRIT) ;
  /sbin/linuxconf                       -> $(SEC_CRIT) ;
  /sbin/linuxconf-auth                  -> $(SEC_CRIT) ;
  /sbin/pwdb_chkpwd                     -> $(SEC_CRIT) ;
  /sbin/remadmin                        -> $(SEC_CRIT) ;
  /sbin/rescuept                        -> $(SEC_CRIT) ;
  /sbin/rmt                             -> $(SEC_CRIT) ;
  /sbin/rpc.lockd                       -> $(SEC_CRIT) ;
  /sbin/rpc.statd                       -> $(SEC_CRIT) ;
  /sbin/rpcdebug                        -> $(SEC_CRIT) ;
  /sbin/service                         -> $(SEC_CRIT) ;
  /sbin/setsysfont                      -> $(SEC_CRIT) ;
```

```
  /sbin/shutdown                        -> $(SEC_CRIT) ;
  /sbin/sulogin                         -> $(SEC_CRIT) ;
  /sbin/swapon                          -> $(SEC_CRIT) ;
  /sbin/syslogd                         -> $(SEC_CRIT) ;
  /sbin/unix_chkpwd                     -> $(SEC_CRIT) ;
  /bin/pwd                              -> $(SEC_CRIT) ;
  /bin/uname                            -> $(SEC_CRIT) ;
}
  ########################################
 #                                       ##
######################################## #
#                                      # #
# Hardware and Device Control Programs # #
#                                      ##
########################################
(
  rulename = "Hardware and Device Control Programs",
  severity = $(SIG_HI)
)
{
  /sbin/cardctl                         -> $(SEC_CRIT) ;
  /sbin/cardmgr                         -> $(SEC_CRIT) ;
  /sbin/hwclock                         -> $(SEC_CRIT) ;
  /sbin/isapnp                          -> $(SEC_CRIT) ;
  /sbin/kbdrate                         -> $(SEC_CRIT) ;
  /sbin/losetup                         -> $(SEC_CRIT) ;
  /sbin/lspci                           -> $(SEC_CRIT) ;
  /sbin/pnpdump                         -> $(SEC_CRIT) ;
  /sbin/probe                           -> $(SEC_CRIT) ;
  /sbin/pump                            -> $(SEC_CRIT) ;
  /sbin/setpci                          -> $(SEC_CRIT) ;
  /sbin/shapecfg                        -> $(SEC_CRIT) ;
}
  ################################
 #                              ##
################################ #
#                              # #
# System Information Programs # #
#                              ##
################################
(
  rulename = "System Information Programs",
  severity = $(SIG_HI)
)
{
  /sbin/consoletype                     -> $(SEC_CRIT) ;
  /sbin/kernelversion                   -> $(SEC_CRIT) ;
  /sbin/runlevel                        -> $(SEC_CRIT) ;
}
  ####################################
 #                                  ##
#################################### #
#                                  # #
# Application Information Programs # #
#                                  ##
####################################
(
  rulename = "Application Information Programs",
  severity = $(SIG_HI)
)
{
  /sbin/genksyms                        -> $(SEC_CRIT) ;
  /sbin/rtmon                           -> $(SEC_CRIT) ;
  /sbin/sln                             -> $(SEC_CRIT) ;
}
  ##########################
```

```
 #                        ##
########################## #
#                       # #
# Shell Related Programs # #
#                       ##
##########################
(
  rulename = "Shell Releated Programs",
  severity = $(SIG_HI)
)
{
  /sbin/getkey                          -> $(SEC_CRIT) ;
  /sbin/sash                            -> $(SEC_CRIT) ;
}
  ################
 #              ##
################ #
#              # #
# OS Utilities # #
#              ##
################
(
  rulename = "Operating System Utilities",
  severity = $(SIG_HI)
)
{
  /bin/cat                              -> $(SEC_CRIT) ;
  /bin/date                             -> $(SEC_CRIT) ;
  /bin/dd                               -> $(SEC_CRIT) ;
  /bin/df                               -> $(SEC_CRIT) ;
  /bin/echo                             -> $(SEC_CRIT) ;
  /bin/egrep                            -> $(SEC_CRIT) ;
  /bin/false                            -> $(SEC_CRIT) ;
  /bin/fgrep                            -> $(SEC_CRIT) ;
  /bin/gawk                             -> $(SEC_CRIT) ;
  /bin/gawk-3.0.4                       -> $(SEC_CRIT) ;
  /bin/grep                             -> $(SEC_CRIT) ;
  /bin/true                             -> $(SEC_CRIT) ;
  /bin/arch                             -> $(SEC_CRIT) ;
  /bin/ash                              -> $(SEC_CRIT) ;
  /bin/ash.static                       -> $(SEC_CRIT) ;
  /bin/aumix-minimal                    -> $(SEC_CRIT) ;
  /bin/basename                         -> $(SEC_CRIT) ;
  /bin/consolechars                     -> $(SEC_CRIT) ;
  /bin/dmesg                            -> $(SEC_CRIT) ;
  /bin/doexec                           -> $(SEC_CRIT) ;
  /bin/ed                               -> $(SEC_CRIT) ;
  /bin/gunzip                           -> $(SEC_CRIT) ;
  /bin/gzip                             -> $(SEC_CRIT) ;
  /bin/hostname                         -> $(SEC_CRIT) ;
  /bin/igawk                            -> $(SEC_CRIT) ;
  /bin/ipcalc                           -> $(SEC_CRIT) ;
  /bin/kill                             -> $(SEC_CRIT) ;
  /bin/ln                               -> $(SEC_CRIT) ;
  /bin/loadkeys                         -> $(SEC_CRIT) ;
  /bin/login                            -> $(SEC_CRIT) ;
  /bin/ls                               -> $(SEC_CRIT) ;
  /bin/mail                             -> $(SEC_CRIT) ;
  /bin/more                             -> $(SEC_CRIT) ;
  /bin/mt                               -> $(SEC_CRIT) ;
  /bin/mv                               -> $(SEC_CRIT) ;
  /bin/netstat                          -> $(SEC_CRIT) ;
  /bin/nice                             -> $(SEC_CRIT) ;
  /bin/ps                               -> $(SEC_CRIT) ;
  /bin/rpm                              -> $(SEC_CRIT) ;
  /bin/sed                              -> $(SEC_CRIT) ;
```

```
  /bin/setserial                        -> $(SEC_CRIT) ;
  /bin/sfxload                          -> $(SEC_CRIT) ;
  /bin/sleep                            -> $(SEC_CRIT) ;
  /bin/sort                             -> $(SEC_CRIT) ;
  /bin/stty                             -> $(SEC_CRIT) ;
  /bin/su                               -> $(SEC_CRIT) ;
  /bin/sync                             -> $(SEC_CRIT) ;
  /bin/tar                              -> $(SEC_CRIT) ;
  /bin/usleep                           -> $(SEC_CRIT) ;
  /bin/vi                               -> $(SEC_CRIT) ;
  /bin/vimtutor                         -> $(SEC_CRIT) ;
  /bin/zcat                             -> $(SEC_CRIT) ;
  /bin/zsh                              -> $(SEC_CRIT) ;
  /bin/zsh-3.0.8                        -> $(SEC_CRIT) ;
}
  ##############################
 #                             ##
############################### #
#                             # #
# Critical Utility Sym-Links # #
#                             ##
##############################
(
  rulename = "Critical Utility Sym-Links",
  severity = $(SIG_HI)
)
{
  /sbin/askrunlevel                     -> $(SEC_CRIT) ;
  /sbin/clock                           -> $(SEC_CRIT) ;
  /sbin/dnsconf                         -> $(SEC_CRIT) ;
  /sbin/fixperm                         -> $(SEC_CRIT) ;
  /sbin/fsconf                          -> $(SEC_CRIT) ;
  /sbin/ipfwadm-wrapper                 -> $(SEC_CRIT) ;
  /sbin/kallsyms                        -> $(SEC_CRIT) ;
  /sbin/ksyms                           -> $(SEC_CRIT) ;
  /sbin/mailconf                        -> $(SEC_CRIT) ;
  /sbin/managerpm                       -> $(SEC_CRIT) ;
  /sbin/modemconf                       -> $(SEC_CRIT) ;
  /sbin/lsmod                           -> $(SEC_CRIT) ;
  /sbin/modprobe                        -> $(SEC_CRIT) ;
  /sbin/mount.ncp                       -> $(SEC_CRIT) ;
  /sbin/mount.ncpfs                     -> $(SEC_CRIT) ;
  /sbin/mount.smb                       -> $(SEC_CRIT) ;
  /sbin/mount.smbfs                     -> $(SEC_CRIT) ;
  /sbin/netconf                         -> $(SEC_CRIT) ;
  /sbin/pidof                           -> $(SEC_CRIT) ;
  /sbin/poweroff                        -> $(SEC_CRIT) ;
  /sbin/quotaoff                        -> $(SEC_CRIT) ;
  /sbin/raid0run                        -> $(SEC_CRIT) ;
  /sbin/raidhotadd                      -> $(SEC_CRIT) ;
  /sbin/raidhotremove                   -> $(SEC_CRIT) ;
  /sbin/raidstop                        -> $(SEC_CRIT) ;
  /sbin/rdump.static                    -> $(SEC_CRIT) ;
  /sbin/rrestore                        -> $(SEC_CRIT) ;
  /sbin/rrestore.static                 -> $(SEC_CRIT) ;
  /sbin/swapoff                         -> $(SEC_CRIT) ;
  /sbin/rdump                           -> $(SEC_CRIT) ;
  /sbin/reboot                          -> $(SEC_CRIT) ;
  /sbin/rmmod                           -> $(SEC_CRIT) ;
  /sbin/telinit                         -> $(SEC_CRIT) ;
  /sbin/userconf                        -> $(SEC_CRIT) ;
  /sbin/uucpconf                        -> $(SEC_CRIT) ;
  /bin/awk                              -> $(SEC_CRIT) ;
  /bin/dnsdomainname                    -> $(SEC_CRIT) ;
  /bin/domainname                       -> $(SEC_CRIT) ;
  /bin/ex                               -> $(SEC_CRIT) ;
```

```
  /bin/gtar                             -> $(SEC_CRIT) ;
  /bin/nisdomainname                    -> $(SEC_CRIT) ;
  /bin/red                              -> $(SEC_CRIT) ;
  /bin/rvi                              -> $(SEC_CRIT) ;
  /bin/rview                            -> $(SEC_CRIT) ;
  /bin/view                             -> $(SEC_CRIT) ;
  /bin/xnmap                            -> $(SEC_CRIT) ;
  /bin/ypdomainname                     -> $(SEC_CRIT) ;
}
  ##########################
 #                         ##
########################## #
#                        # #
# Temporary directories # #
#                        ##
##########################
(
  rulename = "Temporary directories",
  recurse = false,
  severity = $(SIG_LOW)
)
{
  /usr/tmp                              -> $(SEC_INVARIANT) ;
  /var/tmp                              -> $(SEC_INVARIANT) ;
  /tmp                                  -> $(SEC_INVARIANT) ;
}
  ###############
 #             ##
############### #
#             # #
# Local files # #
#             ##
###############
(
  rulename = "User binaries",
  severity = $(SIG_MED)
)
{
  /sbin                                 -> $(SEC_BIN) (recurse = 1) ;
  /usr/local/bin                        -> $(SEC_BIN) (recurse = 1) ;
  /usr/sbin                             -> $(SEC_BIN) (recurse = 1) ;
  /usr/bin                              -> $(SEC_BIN) (recurse = 1) ;
}
(
  rulename = "Shell Binaries",
  severity = $(SIG_HI)
)
{
  /bin/bsh                              -> $(SEC_BIN) ;
  /bin/csh                              -> $(SEC_BIN) ;
  /bin/ksh                              -> $(SEC_BIN) ;
  # /bin/psh                              -> $(SEC_BIN) ; # No longer used?
  /usr/kerberos/bin/rsh                -> $(SEC_SUID) ;
  # /bin/Rsh                              -> $(SEC_BIN) ; # No longer used?
  /bin/sh                               -> $(SEC_BIN) ;
  # /bin/shell                            -> $(SEC_SUID) ; # No longer used?
  # /bin/tsh                              -> $(SEC_BIN) ; # No longer used?
  /bin/bash                             -> $(SEC_BIN) ;
  /bin/tcsh                             -> $(SEC_BIN) ;
  /bin/bash2                            -> $(SEC_BIN) ;
}
(
  rulename = "Security Control",
  severity = $(SIG_HI)
)
{
```

```
  /etc/group                            -> $(SEC_CRIT) ;
  /etc/security/                        -> $(SEC_CRIT) ;
  #/var/spool/cron/crontabs              -> $(SEC_CRIT) ; # Uncomment when this file exists
}
#(
#  rulename = "Boot Scripts",
#  severity = $(SIG_HI)
#)
#{
#  /etc/rc                              -> $(SEC_CONFIG) ;
#  /etc/rc.bsdnet                       -> $(SEC_CONFIG) ;
#  /etc/rc.dt                           -> $(SEC_CONFIG) ;
#  /etc/rc.net                          -> $(SEC_CONFIG) ;
#  /etc/rc.net.serial                   -> $(SEC_CONFIG) ;
#  /etc/rc.nfs                          -> $(SEC_CONFIG) ;
#  /etc/rc.powerfail                    -> $(SEC_CONFIG) ;
#  /etc/rc.tcpip                        -> $(SEC_CONFIG) ;
#  /etc/trcfmt.Z                        -> $(SEC_CONFIG) ;
#}
(
  rulename = "Login Scripts",
  severity = $(SIG_HI)
)
{
  /etc/csh.cshrc                        -> $(SEC_CONFIG) ;
  /etc/csh.login                        -> $(SEC_CONFIG) ;
  # /etc/tsh_profile                     -
> $(SEC_CONFIG) ; #Uncomment when this file exists
  /etc/profile                          -> $(SEC_CONFIG) ;
}
# Libraries
(
  rulename = "Libraries",
  severity = $(SIG_MED)
)
{
  /usr/lib                              -> $(SEC_BIN) ;
  /usr/local/lib                        -> $(SEC_BIN) ;
}
  ########################################################
 #                                                       ##
######################################################## #
#                                                      # #
# Critical System Boot Files                           # #
# These files are critical to a correct system boot. # #
#                                                      ##
########################################################
(
  rulename = "Critical system boot files",
  severity = $(SIG_HI)
)
{
     /boot                              -> $(SEC_CRIT) ;
     /sbin/lilo                         -> $(SEC_CRIT) ;
     !/boot/System.map ;
     !/boot/module-info ;
     # other boot files may exist.  Look for:
     #/ufsboot                           -> $(SEC_CRIT) ;
}
   ##################################################
  ##################################################
  # These files change every time the system boots ##
  ##################################################
(
  rulename = "System boot changes",
  severity = $(SIG_HI)
```

```
)
{
    !/var/run/ftp.pids-all ; # Comes and goes on reboot.
    !/root/.enlightenment ;
    /dev/log                        -> $(SEC_CONFIG) ;
    /dev/cua0                       -> $(SEC_CONFIG) ;
    # /dev/printer                  -
> $(SEC_CONFIG) ; # Uncomment if you have a printer device
    /dev/console                    -> $(SEC_CONFIG) -
u;#User ID may change on console login/logout.
    #/dev/tty2                      -> $(SEC_CONFIG) ; # tty devices
    /dev/tty3                       -> $(SEC_CONFIG) ; # are extremely
    /dev/tty4                       -> $(SEC_CONFIG) ; # variable
    /dev/tty5                       -> $(SEC_CONFIG) ;
    /dev/tty6                       -> $(SEC_CONFIG) ;
    /dev/urandom                    -> $(SEC_CONFIG) ;
    /dev/initctl                    -> $(SEC_CONFIG) ;
    /var/lock/subsys                -> $(SEC_CONFIG) ;
    /var/lock/subsys/random         -> $(SEC_CONFIG) ;
    /var/lock/subsys/network        -> $(SEC_CONFIG) ;
    /var/lock/subsys/portmap        -> $(SEC_CONFIG) ;
    # /var/lock/subsys/nfsfs         -> $(SEC_CONFIG) ; #Uncomment when this file exists
    /var/lock/subsys/nfslock        -> $(SEC_CONFIG) ;
    /var/lock/subsys/syslog         -> $(SEC_CONFIG) ;
    /var/lock/subsys/atd            -> $(SEC_CONFIG) ;
    /var/lock/subsys/crond          -> $(SEC_CONFIG) ;
    # /var/lock/subsys/inet          -> $(SEC_CONFIG) ; #Uncomment when this file exists
    # /var/lock/subsys/named         -> $(SEC_CONFIG) ; #Uncomment when this file exists
    /var/lock/subsys/lpd            -> $(SEC_CONFIG) ;
    # /var/lock/subsys/nfs           -> $(SEC_CONFIG) ; #Uncomment when this file exists
    /var/lock/subsys/sendmail       -> $(SEC_CONFIG) ;
    /var/lock/subsys/gpm            -> $(SEC_CONFIG) ;
    /var/lock/subsys/httpd          -> $(SEC_CONFIG) ;
    # /var/lock/subsys/sound         -> $(SEC_CONFIG) ; #Uncomment when this file exists
    # /var/lock/subsys/smb           -> $(SEC_CONFIG) ; #Uncomment when this file exists
    /var/lock/subsys/anacron        -> $(SEC_CONFIG) ;
    /var/lock/subsys/autofs         -> $(SEC_CONFIG) ;
    /var/lock/subsys/canna          -> $(SEC_CONFIG) ;
    /var/lock/subsys/firewall       -> $(SEC_CONFIG) ;
    /var/lock/subsys/identd         -> $(SEC_CONFIG) ;
    /var/lock/subsys/jserver        -> $(SEC_CONFIG) ;
    /var/lock/subsys/keytable       -> $(SEC_CONFIG) ;
    /var/lock/subsys/kudzu          -> $(SEC_CONFIG) ;
    /var/lock/subsys/netfs          -> $(SEC_CONFIG) ;
    /var/lock/subsys/reconfig       -> $(SEC_CONFIG) ;
    /var/lock/subsys/xfs            -> $(SEC_CONFIG) ;
    /var/lock/subsys/xinetd         -> $(SEC_CONFIG) ;
    /var/lock/subsys/ypbind         -> $(SEC_CONFIG) ;
    /var/run                        -> $(SEC_CONFIG) ; # daemon PIDs
    #/var/spool/lpd/lpd.lock         -> $(SEC_CONFIG) ; #Uncomment when this file exists
    /var/log                        -> $(SEC_CONFIG) ;
    /etc/issue.net                  -> $(SEC_CONFIG) -i ; # Inode number changes
    /etc/ioctl.save                 -> $(SEC_CONFIG) ;
    /etc/issue                      -> $(SEC_CONFIG) ;
    /etc/.pwd.lock                  -> $(SEC_CONFIG) ;
    /etc/mtab                       -> $(SEC_CONFIG) -
i;#Inode number changes on any mount/unmount
    /lib/modules                    -> $(SEC_CONFIG) ;
    # /lib/modules/preferred         -> $(SEC_CONFIG) ; #Uncomment when this file exists
}
# These files change the behavior of the root account
(
  rulename = "Root config files",
  severity = 100
)
{
```

```
     /root                          -> $(SEC_CRIT) ; # Catch all additions to /root
     /root/mail                     -> $(SEC_CONFIG) ;
     /root/Mail                     -> $(SEC_CONFIG) ;
     /root/.xsession-errors         -> $(SEC_CONFIG) ;
     /root/.xauth                   -> $(SEC_CONFIG) ;
     /root/.tcshrc                  -> $(SEC_CONFIG) ;
     /root/.sawfish                 -> $(SEC_CONFIG) ;
     /root/.pinerc                  -> $(SEC_CONFIG) ;
     /root/.mc                      -> $(SEC_CONFIG) ;
     /root/.gnome_private           -> $(SEC_CONFIG) ;
     /root/.gnome-desktop           -> $(SEC_CONFIG) ;
     /root/.gnome                   -> $(SEC_CONFIG) ;
     /root/.esd_auth                -> $(SEC_CONFIG) ;
     /root/.elm                     -> $(SEC_CONFIG) ;
     /root/.cshrc                   -> $(SEC_CONFIG) ;
     /root/.bashrc                  -> $(SEC_CONFIG) ;
     /root/.bash_profile            -> $(SEC_CONFIG) ;
     /root/.bash_logout             -> $(SEC_CONFIG) ;
     /root/.bash_history            -> $(SEC_CONFIG) ;
     /root/.amandahosts             -> $(SEC_CONFIG) ;
     /root/.addressbook.lu          -> $(SEC_CONFIG) ;
     /root/.addressbook             -> $(SEC_CONFIG) ;
     /root/.Xresources              -> $(SEC_CONFIG) ;
     /root/.Xauthority              -> $(SEC_CONFIG) -
i ; # Changes Inode number on login
     /root/.ICEauthority            -> $(SEC_CONFIG) ;
}
  ################################
 #                              ##
################################ #
#                              # #
# Critical configuration files # #
#                              ##
################################
(
  rulename = "Critical configuration files",
  severity = $(SIG_HI)
)
{
     /etc/conf.linuxconf            -> $(SEC_BIN) ;
     # /etc/conf.modules              -> $(SEC_BIN) ; # No longer used?
     /etc/crontab                   -> $(SEC_BIN) ;
     /etc/cron.hourly               -> $(SEC_BIN) ;
     /etc/cron.daily                -> $(SEC_BIN) ;
     /etc/cron.weekly               -> $(SEC_BIN) ;
     /etc/cron.monthly              -> $(SEC_BIN) ;
     /etc/default                   -> $(SEC_BIN) ;
     /etc/fstab                     -> $(SEC_BIN) ;
     /etc/exports                   -> $(SEC_BIN) ;
     /etc/group-                    -> $(SEC_BIN) ;  # changes should be infrequent
     /etc/host.conf                 -> $(SEC_BIN) ;
     /etc/hosts.allow               -> $(SEC_BIN) ;
     /etc/hosts.deny                -> $(SEC_BIN) ;
     /etc/httpd/conf                -> $(SEC_BIN) ;  # changes should be infrequent
     /etc/protocols                 -> $(SEC_BIN) ;
     /etc/services                  -> $(SEC_BIN) ;
     /etc/rc.d/init.d               -> $(SEC_BIN) ;
     /etc/rc.d                      -> $(SEC_BIN) ;
     /etc/mail.rc                   -> $(SEC_BIN) ;
     /etc/motd                      -> $(SEC_BIN) ;
     # /etc/named.boot               -> $(SEC_BIN) ;
     /etc/passwd                    -> $(SEC_CONFIG) ;
     /etc/passwd-                   -> $(SEC_CONFIG) ;
     /etc/profile.d                 -> $(SEC_BIN) ;
     /var/lib/nfs/rmtab             -> $(SEC_BIN) ;
     /usr/sbin/fixrmtab             -> $(SEC_BIN) ;
```

```
     /etc/rpc                          -> $(SEC_BIN) ;
     /etc/sysconfig                    -> $(SEC_BIN) ;
     /etc/smb.conf                     -> $(SEC_CONFIG) ;
     /etc/gettydefs                    -> $(SEC_BIN) ;
     /etc/nsswitch.conf                -> $(SEC_BIN) ;
     /etc/yp.conf                      -> $(SEC_BIN) ;
     /etc/hosts                        -> $(SEC_CONFIG) ;
     /etc/inetd.conf                   -> $(SEC_CONFIG) ;
     /etc/inittab                      -> $(SEC_CONFIG) ;
     /etc/resolv.conf                  -> $(SEC_CONFIG) ;
     /etc/syslog.conf                  -> $(SEC_CONFIG) ;
}
  ####################
 #                  ##
#################### #
#                  # #
# Critical devices # #
#                  ##
####################
(
  rulename = "Critical devices",
  severity = $(SIG_HI),
  recurse = false
)
{
     /dev/kmem                         -> $(Device) ;
     /dev/mem                          -> $(Device) ;
     /dev/null                         -> $(Device) ;
     /dev/zero                         -> $(Device) ;
     /proc/devices                     -> $(Device) ;
     /proc/net                         -> $(Device) ;
     /proc/sys                         -> $(Device) ;
     /proc/cpuinfo                     -> $(Device) ;
     /proc/modules                     -> $(Device) ;
     /proc/mounts                      -> $(Device) ;
     /proc/dma                         -> $(Device) ;
     /proc/filesystems                 -> $(Device) ;
     /proc/pci                         -> $(Device) ;
     /proc/interrupts                  -> $(Device) ;
     /proc/rtc                         -> $(Device) ;
     /proc/ioports                     -> $(Device) ;
     /proc/scsi                        -> $(Device) ;
     /proc/kcore                       -> $(Device) ;
     /proc/self                        -> $(Device) ;
     /proc/kmsg                        -> $(Device) ;
     /proc/stat                        -> $(Device) ;
     /proc/ksyms                       -> $(Device) ;
     /proc/loadavg                     -> $(Device) ;
     /proc/uptime                      -> $(Device) ;
     /proc/locks                       -> $(Device) ;
     /proc/version                     -> $(Device) ;
     /proc/mdstat                      -> $(Device) ;
     /proc/meminfo                     -> $(Device) ;
     /proc/cmdline                     -> $(Device) ;
     /proc/misc                        -> $(Device) ;
}
# Rest of critical system binaries
(
  rulename = "OS executables and libraries",
  severity = $(SIG_HI)
)
{
     /bin                              -> $(SEC_BIN) ;
     /lib                              -> $(SEC_BIN) ;
}
#============================================================================
```

```
#
# Copyright 2000 Tripwire, Inc. Tripwire is a registered trademark of Tripwire,
# Inc. in the United States and other countries. All rights reserved.
#
# Linux is a registered trademark of Linus Torvalds.
#
# UNIX is a registered trademark of The Open Group.
#
#==============================================================================
#
# Permission is granted to make and distribute verbatim copies of this document
# provided the copyright notice and this permission notice are preserved on all
# copies.
#
# Permission is granted to copy and distribute modified versions of this
# document under the conditions for verbatim copying, provided that the entire
# resulting derived work is distributed under the terms of a permission notice
# identical to this one.
#
# Permission is granted to copy and distribute translations of this document
# into another language, under the above conditions for modified versions,
# except that this permission notice may be stated in a translation approved by
# Tripwire, Inc.
#
# DCM
```