Control de la integridad de ficheros y directorios.

Autor: Enrique V. Bonet Esteban

Introducción.

El control de integridad de ficheros y directorios se realiza mediante un programa que permite obtener el estado inicial de los ficheros y directorios del sistema y comparar, con posterioridad, el estado con este estado actual.

El programa más conocido de todos los existentes es tripwire, propiedad en la actualidad de Tripwire Inc. (http://www.tripwire.com). Sin embargo, este programa en sus orígenes en el año 1992 fue desarrollado en la universidad de Purdue y era software libre, manteniéndose en esta situación durante un buen número de años.

A partir de su comercialización por una compañía surgieron dos líneas de desarrollo dentro del software libre:

- Aide: Desarrollado inicialmente como una iniciativa de software libre con el objetivo de cubrir el hueco dejado por tripwire al pasar a ser una iniciativa comercial. Puede descargarse la última versión del mismo en la URL http://sourceforge.net/projects/aide

- Tripwire: Iniciativa de software surgida con posterioridad a aide y que, partiendo de la última versión de software libre de tripwire, continuó su desarrollo con el objetivo de seguir proporcionando la herramienta inicial tal y como se conocía. Puede descargarse desde la URL http://sourceforge.net/projects/tripwire.

De las dos elecciones posibles nos centraremos en el estudio de tripwire.

Tripwire.

Tripwire es un programa para asegurar la integridad de los archivos y directorios de los sistemas críticos de un ordenador. Tripwire identifica los cambios realizados en los mismos, mediante un proceso automático que se ejecuta en intervalos regulares, e informa de los cambios detectados al administrador mediante un correo electrónico[1].

El uso de tripwire sirve no solo para detectar la integridad de los archivos y directorios, sino también minimiza el impacto de una intrusión en el sistema, pues al informar de los archivos modificados permite conocer los archivos que deben ser restaurados.

Tripwire funciona generando, cuando el sistema acaba de ser instalado, una base de datos inicial, conocida como base de datos de fundamentos, que contiene información sobre los archivos y directorios, y genera periódicamente una nueva base

[1] La persona a informar por tripwire de los cambios puede ser configurada, por lo que no tiene porque ser necesariamente el usuario root del sistema.

de datos con el estado actual, comparando ambas bases de datos e informando de cualquier modificación, adición o eliminación.

Configuración inicial de tripwire.

Una vez instalado el software de tripwire, y aunque no es necesario pues ambos archivos de configuración pueden funcionar con las valores por defecto, es recomendable modificar los dos archivos de configuración de tripwire. Estos dos archivos */etc/tripwire/twcfg.txt* y */etc/tripwire/twpol.txt* indican la localización de la base de datos de tripwire y de los archivos y directorios a comprobar, respectivamente.

Configuración del archivo twcfg.txt.

El archivo *twcfg.txt* contiene dos tipos de variables, las de configuración obligatoria en caso de que se modifique cualquier valor del archivo *twcfg.txt* que por defecto se instala, pues en caso de no especificar los valores de alguna de estas variables, aunque el valor deseado sea el valor por defecto, tripwire mostrará un mensaje de error y terminará su ejecución, y las de configuración optativa, pues no es necesario especificar su valor, pudiendo tomar sus valores por defecto.

Las variables de configuración obligatoria son:

- *ROOT*: Contiene el directorio donde se encuentran los ejecutables de tripwire. Por defecto su valor es */usr/sbin*.

- *POLFILE*: Contiene la ubicación del archivo de políticas. Su valor por defecto es */etc/tripwire/tw.pol*.

- *DBFILE*: Indica la localización del archivo de la base de datos. Su valor por defecto es */var/lib/tripwire/$(HOSTNAME).twd*.

- *REPORTFILE*: Contiene la ubicación de los archivos de informes. Su valor por defecto es */var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr*.

- *SITEKEYFILE*: Especifica la localización del archivo de la llave del sitio. Su valor por defecto es */etc/tripwire/site.key*.

- *LOCALKEYFILE*: Especifica la ubicación del archivo de la llave local. Su valor por defecto es */etc/tripwire/$(HOSTNAME)-local.key*.

El resto de variables, cuya configuración es opcional son:

- *EDITOR*: Indica el editor de texto que ejecutará tripwire. Su valor por defecto */bin/vi*.

- *LATEPROMPTING*: Puede tomar los valores *true* ó *false* tomando por defecto el valor *false*. Indica a tripwire que espere tanto como sea posible antes de preguntar una contraseña al usuario, minimizando el tiempo que la contraseña permanece en la memoria del ordenador.

- *LOOSEDIRECTORYCHECKING*: Puede tomar los valores *true* ó *false*, siendo el valor por defecto *false*. Configura tripwire para que informe sobre los cambios que se han realizado en un archivo de un directorio y no sobre los cambios propios del directorio, reduciendo la redundancia en los informes generados.

- *SYSLOGREPORTING*: Toma los valores *true* ó *false*, e indica a tripwire que informe al demonio de syslog de los cambios. El valor por defecto es *false*.

- *MAILNOVIOLATIONS*: Puede tomar los valores *true* ó *false* e indica a tripwire que mande un correo electrónico de forma periódica aún en el caso de que no se haya producido ninguna intrusión en el sistema. El valor por defecto es *true*.

- *EMAILREPORTLEVEL*: Indica el nivel de detalle para los informes enviados por correo electrónico. Los valores válidos son de 0 a 4, siendo el valor por defecto de 3.

- *REPORTLEVEL*: Indica el nivel de detalle para los informes generado por el comando *twprint*[2]. Sus valores válidos son de 0 a 4 y su valor predeterminado es 3.

- *MAILMETHOD*: Especifica el protocolo de correo que usará tripwire. Los valores válidos son *SMTP* ó *SENDMAIL*, siendo este último el valor por defecto.

- *MAILPROGRAM*: Especifica que programa de correo usará tripwire. El valor por defecto es */usr/sbin/sendmail –oi –t*.

  Un ejemplo de archivo de configuración es el siguiente:

```
ROOT                    =/usr/sbin
POLFILE                 =/etc/tripwire/tw.pol
DBFILE                  =/var/lib/tripwire/$(HOSTNAME).twd
REPORTFILE              =/var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr
SITEKEYFILE             =/etc/tripwire/site.key
LOCALKEYFILE            =/etc/tripwire/$(HOSTNAME)-local.key
EDITOR                  =/bin/vi
LATEPROMPTING           =false
LOOSEDIRECTORYCHECKING =false
MAILNOVIOLATIONS        =true
EMAILREPORTLEVEL        =3
REPORTLEVEL             =3
MAILMETHOD              =SENDMAIL
SYSLOGREPORTING         =false
MAILPROGRAM             =/usr/sbin/sendmail -oi -t
```

Configuración del archivo twpol.txt.

El archivo *twpol.txt* contiene la política sobre que archivos y directorios son supervisados por tripwire, indicando que datos de los mismos son almacenados en la base de datos, así como la severidad del chequeo que realizará tripwire sobre cada archivo o directorio. Además, permite activar el envío de un correo electrónico si la integridad del sistema ha sido alterada.

[2] El comando twprint lo veremos con posterioridad.

El fichero *twpol.txt* esta formado por cuatro tipos de elementos: Comentarios, reglas, directivas y variables.

Los comentarios son todo el texto que se encuentra en una línea detrás del carácter # y hasta el final de la misma.

Las reglas determinan como y con que severidad tripwrite chequeará los ficheros y directorios. Existen dos tipos de reglas:

- Reglas normales, que definen que propiedades de un fichero o directorio serán analizadas.
- Reglas de parada, que son utilizadas para especificar ficheros o directorios donde tripwire no debe analizar.

Las directivas son un conjunto pequeño de órdenes que permiten condicionar la interpretación de la política de tripwire, así como ciertos diagnósticos y operaciones de depuración[3].

Las variables permiten al usuario definir cadenas de texto para su sustitución en el fichero.

Procederemos a continuación a examinar más detenidamente como especificar las reglas, directivas y variables.

Especificación de las reglas.

Como hemos indicado, existen dos tipos de reglas, reglas normales y reglas de parada. La sintaxis de las reglas normales es:

```
nombre_del_objeto -> mascara_de_propiedades;
```

Donde *nombre_del_objeto* es el camino completo del fichero o directorio, no permitiéndose el uso de variables de ambiente, pero si de variables de tripwire, como todo o parte del camino, y *mascara_de_propiedades* especifica que propiedades del objeto serán examinadas o ignoradas. Si el objeto especificado es un directorio, el directorio y todos sus descendientes, tanto ficheros como directorios, son analizados de acuerdo a la mascara indicada. Si por el contrario el objeto es un fichero, solo ese fichero es analizado de acuerdo a la máscara indicada.

A cada objeto solo puede asociarse una única máscara, de forma que si un objeto tiene asociada más de una máscara se produce un error y tripwire no realiza el análisis de ningún fichero o directorio.

La máscara de propiedades está formada por una serie de caracteres que pueden ir precedidos de un signo + ó -. Cada carácter indica una propiedad particular que tripwire debe examinar durante la comprobación de integridad. Si el carácter es

[3] Una utilidad básica de las directivas es permitir compartir un fichero con la política de seguridad para varios ordenadores.

precedido del signo +, la propiedad es comprobada, ignorándose si va precedida del signo -. En caso de que no se preceda la propiedad de un signo + ó -, se supone que va precedida del signo +.

La siguiente tabla muestra los caracteres que pueden ser utilizados en la especificación de las propiedades a comprobar o ignorar:

Carácter	**Propiedad a comprobar o ignorar**
a	Fecha y hora de acceso.
b	Número de bloques utilizados.
c	Fecha y hora de creación o modificación de los inodos.
d	Identificador del dispositivo donde los inodos se encuentran.
g	Identificador del grupo del fichero.
i	Número de inodos.
l	El fichero ha aumentado su tamaño
m	Fecha y hora de modificación.
n	Número de enlaces (contador de referencias del inodo).
p	Permisos y bits de modo del fichero.
r	Identificador del dispositivo apuntado por el inodo (valido solo para objetos que se refieran a un dispositivo).
s	Tamaño del fichero.
t	Tipo del fichero.
u	Identificador del dueño del fichero.
C	Valor hash del CRC-32 del fichero.
H	Valor hash de Haval (firma de 128 bits) del fichero.
M	Valor hash del MD5 del fichero.
S	Valor hash del SHA del fichero.

Por su parte, las reglas de parada permiten especificar ficheros o directorios que tripwire no debe analizar. Su sintaxis es:

```
! nombre_del_objeto;
```

Donde *nombre_del_objeto* es, igual que en las reglas normales, el camino completo del fichero o directorio, no estando permitido el uso de variables de ambiente como todo o parte del camino, pero si de variables de tripwire.

Además, las reglas anteriores pueden tener atributos que modifican su comportamiento o proporcionan información adicional. A cada regla se le pueden aplicar todos los atributos que se deseen, siendo los atributos no sensitivos al contexto. La sintaxis de los atributos de las reglas se puede especificar para una regla con la siguiente sintaxis:

```
nombre_del_objeto -> mascara_de_propiedades (atributo_de_la_regla = valor);
```

O para un grupo de reglas mediante la sintaxis:

```
(lista de atributos)
{
      lista de reglas;
```

```
}
```

Tripwire posee cuatro atributos para las reglas, estos atributos son:

- *rulename*, que asocia la regla o conjunto de reglas con un nombre específico, de forma que en el fichero de información este nombre es asociado a las violaciones de las reglas especificadas. Esta propiedad suele usarse para facilitar la búsqueda de determinadas violaciones de seguridad, pues permite realizar una búsqueda u ordenación para obtener todas las violaciones de seguridad asociadas a esta regla o conjunto de reglas.

- *emailto*, que asocia uno o más direcciones de correo electrónico[4] con una regla o conjunto de reglas, de forma que si una regla es ejecutada con la opción --email-report[5] y es violada, es enviado un correo electrónico a todas las direcciones de correo especificadas.

- *severity*, que asocia un nivel numérico de severidad con una regla, de forma que cuando tripwire se ejecuta en el modo de "chequeo de integridad", es posible indicarle que solo las reglas cuyo nivel de severidad sea mayor que un valor especificado sean utilizadas. El valor por defecto es 0 y los valores pueden ir desde 0 hasta 1.000.000.

- *recurse*, que especifica como debe analizar una regla un directorio. Los valores validos son *true*, *false* ó un valor númerico entre -1 y 1.000.000. Si el valor es *true* ó -1, el directorio y todos sus ficheros y subdirectorios son analizados. Si el valor es *false* ó 0, el directorio es analizado, pero sus ficheros y subdirectorios no son analizados. Por último, si el valor es N, mayor que 0, el directorio y sus subdirectorios son analizados hasta una profundidad de N niveles. El valor por defecto es *true*. Este atributo no puede aplicarse a los ficheros.

Especificación de las directivas.

Tripwire soporta un pequeño número de directivas que permiten una interpretación condicional del fichero con la política de reglas y unas ciertas operaciones de diagnóstico y depuración. Las sintaxis de las directivas es la siguiente:

```
@@nombre_de_la_directiva   [argumentos]
```

Donde *nombre_de_la_directiva* es uno de los siguientes valores:

- *section*: Permite designar una sección del fichero de políticas que son específicas de un sistema operativo. Los valores posibles para los argumentos son *FS*, *NTFS*, *NTREG* y *GLOBAL*, asumiéndose el valor *FS* por defecto si no se especifica en una sección. El valor *GLOBAL* se utiliza para indicar variables utilizadas, mientras que el valor *FS* se utiliza para indicar las propiedades que se utilizarán. Los valores *NTFS* y *NTREG* son utilizados por los sistemas Windows NT, 2000 y XP.

[4] La especificación de varias direcciones de correo se realiza separando las mismas mediante el símbolo ; (punto y coma).
[5] Con posterioridad veremos como ejecutar una regla con esta opción.

- *ifhost…else…endif*: Permiten una interpretación condicional del fichero de las reglas de política. Esta directiva permite utilizar como argumentos el nombre de un ordenador o de varios ordenadores separados por || (OR lógico).

- *print*: Es utilizada para diagnostico y depuración. Imprime un texto en la salida estándar.

- *error*: Es similar a la anterior, solo que además de escribir un texto en la salida estándar detiene la ejecución del programa con un código de retorno distinto de cero.

- *end*: Indica el final del fichero de políticas. Cualquier texto que aparezca después de la directiva *end* es ignorado por tripwire.

Especificación de las variables.

Las variables son permitidas por tripwire para comodidad de los usuarios. Las variables pueden ser definidas en cualquier lugar entre las reglas. Su sintaxis es:

```
variable = valor;
```

El uso de la variable es legal en cualquier lugar donde una cadena de caracteres pueda aparecer. Su sintaxis es:

```
$(variable)
```

Tripwire posee un número predefinido de variables cuyo valor no puede ser modificado. Estas variables representan diferentes maneras en que los ficheros y directorios pueden ser analizados. Estas variables predefinidas son:

Variable	Descripción	Valor
ReadOnly	Ficheros que son disponibles a todo el mundo pero solo para lectura	+pinugtsdbmCM-rlacSH
Dynamic	Directorios y ficheros que cambian de forma dinámica.	+pinugtd-srlbamcCMSH
Growing	Ficheros que deben solo incrementar su tamaño.	+pinugtdl-srbamcCMSH
Device	Dispositivos u otros ficheros que tripwire no puede abrir.	+pugsdr-intlbamcCMSH
IgnoreAll	Comprueba la presencia o ausencia de un fichero, pero no chequea ninguna propiedad.	-pinugtsdrlbamcCMSH
IgnoreNone	Activa todas las propiedades que es posible comprobar.[6]	+pinugtsdrbamcCMSH-l

Un fragmento de un fichero de configuración de la política de tripwire es el siguiente:

[6] Se suele utilizar como punto de partida para que un usuario defina sus propias máscaras de propiedades, como por ejemplo mimascars = $(IgnoreNone) -ar;

```
@@section GLOBAL
TWROOT=/usr/sbin;
TWBIN=/usr/sbin;
TWPOL="/etc/tripwire";
TWDB="/var/lib/tripwire";
TWSKEY="/etc/tripwire";
TWLKEY="/etc/tripwire";
TWREPORT="/var/lib/tripwire/report";
HOSTNAME=glup;

@@section FS
SEC_CRIT      = $(IgnoreNone)-SHa ;
SEC_SUID      = $(IgnoreNone)-SHa ;
SEC_BIN       = $(ReadOnly) ;
SEC_CONFIG    = $(Dynamic) ;
SEC_LOG       = $(Growing) ;
SEC_INVARIANT = +tpug ;
SIG_LOW       = 33 ;
SIG_MED       = 66 ;
SIG_HI        = 100 ;

# Tripwire Binaries
(
  rulename = "Tripwire Binaries",
  severity = $(SIG_HI)
)
{
  $(TWBIN)/siggen                    -> $(SEC_BIN) ;
  $(TWBIN)/tripwire                  -> $(SEC_BIN) ;
  $(TWBIN)/twadmin                   -> $(SEC_BIN) ;
  $(TWBIN)/twprint                   -> $(SEC_BIN) ;
}
...
```

De forma general, el archivo de especificación de la política de seguridad debe ser modificado para adaptarse a la configuración de nuestro ordenador, pues no todos los ficheros, directorios, etc., que existen por defecto pueden existir en nuestro ordenador y, de igual forma, podemos tener otros instalados cuya seguridad no sea considerada en la configuración por defecto de la política de seguridad.

Generación de la política inicial de seguridad.

Una vez han sido configurados los archivos *twcfg.txt* y *twpol.txt*, estos deben ser convertidos en los archivos de configuración y de política que utiliza tripwire, esto es, los archivos */etc/tripwire/tw.cfg* y */etc/tripwire/tw.pol* respectivamente.

Para ello, debemos ejecutar el script */usr/sbin/tripwire-setup-keyfiles*, el cual realiza la conversión, solicitando las contraseñas del sitio y local. Estas contraseñas se utilizan para generar claves criptográficas con las que se protegen los archivos de tripwire[7]. La contraseña del sitio protege los archivos de configuración y de política de

[7] Las contraseñas del sitio y local deben ser como mínimo de 8 caracteres y la suma de sus longitudes no debe exceder de 1023 caracteres. Además, no deberían corresponder a la contraseña de root ni a ninguna otra contraseña utilizada en el sistema.

tripwire, mientras que la contraseña local protege la base de datos de tripwire y los archivos de informes que se generen con posterioridad, siendo almacenadas, por defecto, en los archivos */etc/tripwire/site.key* y */etc/tripwire/$(HOSTNAME)-local.key*, respectivamente, tal y como se indico en el fichero de configuración.

La encriptación de los archivos anteriores es necesaria para proteger a tripwire de un intruso, pues aunque un intruso logrará acceder al sistema como usuario root, si no conoce las contraseñas anteriores, no pude modificar los archivos de tripwire y alterar su configuración, etc., con el propósito de ocultar sus acciones sobre el sistema.

Tanto los archivos *twcfg.txt* como *twpol.txt* deben ser borrados o copiados a un lugar seguro una vez se haya terminado de configurar tripwire. Otra opción, menos segura, es cambiar sus permisos de forma que no puedan ser leídos, aunque si un intruso obtiene los privilegios de root, podría leerlos en cualquier caso[8].

Una vez creados los archivos de configuración y de política de tripwire, debemos inicializar la base de datos de tripwire. Para ello, ejecutaremos el comando[9]:

```
/usr/sbin/tripwire --init
```

Este comando generará la base de datos de fundamentos, a partir de la cual tripwire podrá comprobar si se producen cambios en los archivos que se están supervisando. Una vez generada la base de datos inicial, es conveniente ejecutar una primera verificación de la integridad del sistema, pues ello nos permitirá comprobar que no obtendremos informes erróneos, pues en este momento la verificación de integridad debe informarnos de que no se ha modificado ningún archivo o directorio de los supervisados[10].

La ejecución del control de integridad de forma manual se realiza mediante el comando:

```
/usr/sbin/tripwire --check
```

Que generará su salida en un fichero dentro del directorio */var/lib/tripwire/report*. De forma general, estos ficheros tienen la extensión *.twr*.

Además de su ejecución manual, tripwire debería ejecutarse de forma periódica, por ejemplo una vez al día, para asegurar la integridad del sistema. Para ello, puede colocarse un script de ejecución de tripwire dentro del directorio */etc/cron.daily*, que es ejecutado por el sistema diariamente[11].

[8] Esta acción es necesaria pues un intruso podría, mirando los archivos, averiguar nuestra política de seguridad e intentar encontrar alguna debilidad en la misma.
[9] Este comando puede tardar algunos minutos en ejecutarse completamente.
[10] Si en este primer informe se obtiene información sobre la modificación de archivos, etc., de los supervisados, esto suele indicar una incorrecta configuración de la política de supervisión y la necesidad de modificación de la misma.
[11] Por defecto, la instalación de tripwire coloca un script, de nombre tripwire-check, dentro del directorio /etc/cron.daily para chequear el sistema todos los días. Si se desea ejecutar tripwire más de una vez al día puede instarse mediante un proceso del cron, para lo que se recomienda se consulten los manuales del sistema de cron y crontab.

Comprobación de los informes y base de datos de tripwire.

Tripwire genera sus informes de forma cifrada, por lo que estos no pueden ser vistos directamente por los usuarios autorizados. Para ver un informe es necesario ejecutar el comando:

```
/usr/sbin/twprint –m r -r /var/lib/tripwire/report/<nombre>.twr
```

Donde la opción *-m r* indica a tripwire que descifre el informe y *-r* indica el nombre del informe a descifrar. Un ejemplo de informe generado por tripwire es el siguiente:

```
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            lun 25 abr 2005 16:56:47 CEST
Database last updated on:     Never

===============================================================================
Report Summary:
===============================================================================

Host name:                    glup
Host IP address:              147.156.222.65
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/glup.twd
Command line used:            tripwire --check

===============================================================================
Rule Summary:
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  --------
  Invariant Directories           66                0        0        0
  Temporary directories           33                0        0        0
* Tripwire Data Files             100               1        0        0
  Critical devices                100               0        0        0
  User binaries                   66                0        0        0
  Tripwire Binaries               100               0        0        0
  Critical configuration files    100               0        0        0
  Libraries                       66                0        0        0
  Operating System Utilities      100               0        0        0
  File System and Disk Administration Programs
                                  100               0        0        0
  Kernel Administration Programs  100               0        0        0
  Networking Programs             100               0        0        0
  System Administration Programs  100               0        0        0
  Hardware and Device Control Programs
                                  100               0        0        0
  System Information Programs     100               0        0        0
  Application Information Programs
                                  100               0        0        0
  Shell Related Programs          100               0        0        0
  Critical Utility Sym-Links      100               0        0        0
  Shell Binaries                  100               0        0        0
  Critical system boot files      100               0        0        0
  System boot changes             100               0        0        0
  OS executables and libraries    100               0        0        0
  Security Control                100               0        0        0
  Login Scripts                   100               0        0        0
  Root config files               100               0        0        0

Total objects scanned:  48406
```

```
Total violations found:  1

===============================================================================
Object Summary:
===============================================================================

-------------------------------------------------------------------------------
# Section: Unix File System
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Rule Name: Tripwire Data Files (/var/lib/tripwire)
Severity Level: 100
-------------------------------------------------------------------------------

Added:
"/var/lib/tripwire/glup.twd"

===============================================================================
Error Report:
===============================================================================

No Errors

-------------------------------------------------------------------------------
*** End of report ***
```

Además de los informes, el comando twprint permite ver el contenido de una base de datos de tripwire. Para ello, el comando a ejecutar es:

```
/usr/sbin/twprint -m d –d /var/lib/tripwire/<nombre>.twd
```

Que mostrará la salida de toda la base de datos de tripwrite especificada por *<nombre>*. Si nos interesa ver tan solo la información de un fichero de la base de datos, se puede especificar este fichero en el comando con tan solo añadirlo detrás:

```
/usr/sbin/twprint -m d -d /var/lib/tripwire/<nombre>.twd <fichero>
```

Generándose como salida un informe como el siguiente, en el que hemos preguntado por el fichero */bin/bash*:

```
Object name:  /bin/bash

Property:               Value:
-------------           -----------
Object Type             Regular File
Device Number           771
Inode Number            721259
Mode                    -rwxr-xr-x
Num Links               1
UID                     root (0)
GID                     root (0)
Size                    626124
Modify Time             mié 09 abr 2003 14:59:51 CEST
Blocks                  1232
CRC32                   CkQtai
MD5                     CNABlAO+m08l4V9ma8K5yS
```

De forma general, los informes de tripwire indicarán, si no se ha desactivado esa opción, que no se ha producido ningún cambio en los ficheros y directorios supervisados por la política del sistema. Sin embargo, en ciertas ocasiones se informará

de que se han producido modificaciones. En este caso, necesitamos saber si dichas modificaciones son el resultado de una intrusión en el sistema aprovechando un fallo en la seguridad del mismo, o bien son el producto de alguna modificación autorizada, como puede ser, por ejemplo, la instalación de una nueva versión de un programa. En el primer caso, obviamente, deberemos tomar las medidas necesarias para mejorar la seguridad del sistema y arreglar todas las modificaciones, etc., no autorizadas que se hayan realizado. En el segundo caso, debemos actualizar la base de datos de tripwire con el fin de que estas presuntas "modificaciones no autorizadas" sigan apareciendo en los informes y conviertan estos en algo tedioso e inútil de analizar.

La actualización de la base de datos de tripwire de modo que acepte las modificaciones encontradas en un informe se basa en especificar el informe que se desea utilizar para actualizar la base de datos. El comando para realizarlo es:

```
/usr/sbin/tripwire --update --twrfile /var/lib/tripwire/report/<nombre>.twr
```

Donde <*nombre*> es el nombre del fichero de informe que se desea utilizar[12].

Al ejecutar este comando, tripwire cruza las referencias entre el archivo del informe y la base de datos, y luego muestra en el editor definido por defecto las diferencias entre ambos. Esto nos permite quitar los archivos que no deseamos que se actualicen en la base de datos de tripwire y dejar que el resto de cambios sean actualizados en la base de datos de tripwire. Un ejemplo de esto es el siguiente[13]:

```
Added:
[x] "/var/lib/tripwire/glup.twd"
```

Si se desea excluir que una modificación valida sea añadida a la base de datos de tripwire basta con quitar el símbolo x que se encuentra antes del archivo. Una vez hemos terminado de indicar que modificaciones deseamos que sean introducidas en la base de datos, salimos del editor de texto grabando los cambios y dejamos que tripwire ejecute los cambios que hemos dejado seleccionados.

Actualización de los archivos de configuración y de políticas de tripwire.

Como hemos indicado con anterioridad, una vez generados los ficheros de configuración y de políticas de tripwire lo correcto es borrar los archivos existentes en texto plano, esto es, los archivos */etc/tripwire/twcfg.txt* y */etc/tripwire/twpol.txt*.

Sin embargo, en ciertas ocasiones puede ser necesario modificar alguno de estos archivos para cambiar la configuración o la política de seguridad del sistema. Para ello, existe una herramienta, */usr/sbin/twadmin*, que permite generar los archivos de texto a partir de sus correspondientes archivos generados al instalar tripwire.

[12] Generalmente el informe a utilizar será el más reciente, pues es el que contendrá el mayor número de modificaciones autorizadas que deseamos incluir en la base de datos de tripwire.

[13] Hemos utilizado el error que aparece en el informe inicial en el cual se nos indica que en el directorio /var/lib/tripwire ha aparecido un fichero de nombre glup.twd que corresponde, obviamente, a la base de datos de tripwire que ha sido creada después de realizar todo el análisis del sistema.

Actualización del archivo de configuración de tripwire.

Para poder actualizar el archivo de configuración de tripwire, podemos regenerarlo a partir del archivo de configuración mediante la ejecución del comando:

```
/usr/sbin/twadmin -m f > /etc/tripwire/twcfg.txt
```

Una vez regenerado el fichero, podemos realizar los cambios deseados, debiendo convertir, una vez realizados los cambios, el nuevo fichero a su formato de tripwire mediante el comando:

```
/usr/sbin/twadmin -m F -S site.key /etc/tripwire/twcfg.txt
```

Como el archivo de configuración no altera la política de tripwire o los archivos comprobados por el programa, no es necesario regenerar la base de datos de tripwire al modificar el archivo de configuración.

Actualización del archivo de políticas de tripwire.

Igual que en el caso anterior, para poder modificar el archivo de políticas de tripwire, necesitamos regenerar el archivo de políticas. Para ello, utilizaremos el comando:

```
/usr/sbin/twadmin -m p > /etc/tripwire/twpol.txt
```

Una vez obtenido el fichero de texto con la política de seguridad del sistema, podemos modificar la política de seguridad, debiendo, una vez terminada su modificación, generar el archivo de política de tripwire mediante el comando:

```
/usr/sbin/twadmin -m P -S site.key /etc/tripwire/twpol.txt
```

Una vez actualizada la política de seguridad de tripwire, debemos crear una nueva base de datos de tripwire que refleje los cambios realizados. Para ello, lo más sencillo consiste en borrar la base de datos existente en la actualidad y generar una nueva, tal y como se explicó con anterioridad.

Envío de avisos de tripwire mediante correo electrónico.

Como se indicó con anterioridad, es posible configurar tripwire para que envíe un correo electrónico a uno o varios usuarios si una regla, que contiene la opción de enviar un correo electrónico, ha sido violada.

Para ello, en la sección de atributos de una regla o conjunto de reglas, debe añadirse la directiva *emailto = <dirección de correo>[;<otra dirección de correo>]*, que permite enviar un correo electrónico a todas las direcciones especificadas si alguna de las reglas ha sido violada.

Por ejemplo, en el archivo de política de tripwire que vimos como ejemplo, podemos añadir que se envíe correo electrónico a dos usuarios modificando el archivo de la siguiente manera:

```
# Tripwire Binaries
(
  rulename = "Tripwire Binaries",
  severity = $(SIG_HI),
  emailto = root@glup.uv.es;enrique.bonet@uv.es
)
{
  $(TWBIN)/siggen                       -> $(SEC_BIN) ;
  $(TWBIN)/tripwire                     -> $(SEC_BIN) ;
  $(TWBIN)/twadmin                      -> $(SEC_BIN) ;
  $(TWBIN)/twprint                      -> $(SEC_BIN) ;
}
```

Una vez realizado este cambio, debemos generar un nuevo archivo de política de tripwire tal y como vimos en el punto anterior.

Indicar por último, que es posible comprobar que la configuración de los avisos de correo electrónico por parte de tripwire es correcta mediante la ejecución del comando:

```
/usr/sbin/tripwire -m t -e <dirección de correo>
```

De forma que se envía un mensaje de correo de prueba a la dirección especificada utilizando la configuración que posee tripwire en su archivo de configuración, de forma que si el correo es enviado, la configuración es correcta, debiendo revisarse en caso contrario.