

# **Guía breve Tripwire**

**V0.50 - 17/01/2002**

**Diego Bravo Estrada**

Esta es una guía breve para utilizar Tripwire en Linux. Se desarrolló en ambiente RedHat 7.1; sin embargo, debe ser útil en cualquier otro OS compatible.

## **Tabla de contenidos**

<b>1. Introducción .....</b>	<b>3</b>
<b>2. Configuración de Tripwire.....</b>	<b>3</b>
<b>3. Configuración permanente de Tripwire .....</b>	<b>7</b>
<b>4. Eliminación de archivos de texto .....</b>	<b>9</b>



# 1. Introducción

## 1.1. ¿Por qué usar Tripwire?

Para mejorar la seguridad de su sistema.

No existen los sistemas computacionales perfectos e invulnerables que desearíamos, y siempre estaremos expuestos a ataques. Más allá de todas las medidas preventivas que tomemos (firewalls, patches, políticas, etc.) siempre cabe la posibilidad de ser alcanzados por un hacker. Los ataques exitosos a través de la red típicamente involucran la modificación parcial del sistema mediante la alteración o reemplazo de ciertos archivos, lo cual suele ser empleado por el atacante para posteriormente tomar el control total del sistema.

Tripwire asume que todos los controles de seguridad han fallado, y que nuestro sistema ya ha sido alterado; al menos, parcialmente. Sin embargo, parte del arte de los atacantes consiste en no ser descubiertos, y para esto emplean diversas técnicas relativamente sofisticadas. Tripwire servirá para alertar al administrador de estos cambios (los cuales de otro modo podrían pasar desapercibidos por semanas o meses) a fin de tomar acciones con rapidez.

Para esto, Tripwire monitorea rutinariamente la integridad de una gran cantidad de archivos que tienden a ser blanco de los atacantes. Sin embargo, este proceso es pesado, y se suele ejecutar a intervalos; por ejemplo, diarios o interdiarios, aunque no hay ninguna restricción (salvo de recursos) para no lanzarlo cada media hora.

## 1.2. Instalar Tripwire

Descargue la versión open source de Tripwire del site [www.tripwire.org](http://www.tripwire.org) (<http://www.tripwire.org>). Elija la versión que corresponda mejor a su sistema operativo.

Tripwire normalmente se distribuye en un archivo RPM que viene empacado en formato TAR comprimido. En este último caso, usar:

```
# tar xvzf tripwire.tar.gz
```

Lo cual debería generar el archivo `tripwire-2.3-47.i386.rpm` (el nombre exacto dependerá de su versión.)

Ahora instálelo:

```
# rpm -ivh tripwire-2.3-47.i386.rpm
```

## 2. Configuración de Tripwire

### 2.1. Definir las claves de Tripwire

Tripwire utiliza dos claves (que pueden ser palabras u oraciones) para almacenar su información. Una de ellas, la "site key" o "clave del site", se emplea para encriptar los archivos de configuración y de las políticas. La otra - la "local key" o "clave local", se usa para encriptar la información referida al estado de los archivos del sistema que se monitorean.

Ud. necesita estas dos claves para las tareas de administración de Tripwire. Estas se deben introducir tan pronto como se ha instalado Tripwire mediante el comando:

```
# /etc/tripwire/twinstall.sh
```

Recuérdelas bien, o anótelas en un lugar seguro.

### 2.2. Configurar el archivo de políticas

La configuración de los archivos que van a ser monitoreados por Tripwire se mantiene en un gran archivo conocido como "archivo de políticas" (policy file.) Su manipulación es algo tediosa dada su extensión. Tripwire viene con un archivo que sirve de "plantilla" para ser modificado. Este archivo es: `/etc/tripwire/twpol.txt`.

Ud. puede modificarlo directamente con un editor de texto (aunque le aconsejo que guarde una copia sin modificar del mismo.)

Ahora haremos una observación de orden práctico y didáctico: Tripwire por lo general toma varios minutos en cada una de sus ejecuciones, y si Ud. nunca lo ha usado, probablemente le resultará desesperante aguardar mucho tiempo sin saber si las cosas están yendo bien o mal. Por este motivo yo sugiero que empecemos con una versión reducida (y casi inútil) del archivo de políticas. Una vez que Ud. comprenda el proceso completo, podrá retomar el archivo original y aprovecharlo.

Nuevamente va la advertencia: haga una copia de seguridad del archivo `twpol.txt`.

Para recortar el archivo proporcionado, simplemente use un editor de texto (como vi) y busque la sección "File System and Disk Administration Programs" (que en el archivo que yo tengo, se ubica a partir de la línea 185.) Un extracto de esa sección es presentado aquí:

```
...
##### #
# File System and Disk Administration Programs # #
##### #
(
```

```

    rulename = "File System and Disk Administration 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) ;
    ...

```

Como Ud. ya se imaginará, esto corresponde a un conjunto de archivos que se monitorean por Tripwire. Nosotros reduciremos la extensa lista recortando el archivo en esta sección. Por ejemplo, haciendo que termine en **/sbin/e2fsck**:

```

...
##### #
# File System and Disk Administration Programs # #
##### #
(
    rulename = "File System and Disk Administration Programs",
    severity = $(SIG_HI)
)
{
    /sbin/accton                -> $(SEC_CRIT) ;
    /sbin/badblocks            -> $(SEC_CRIT) ;
    /sbin/dosfsck              -> $(SEC_CRIT) ;
    /sbin/e2fsck               -> $(SEC_CRIT) ;
}
# AHORA AQUI TERMINA EL ARCHIVO. OBSERVE LA LLAVE DE CIERRE.

```

Como se ve, hemos recortado la parte que estaba más abajo de **/sbin/e2fsck**, y hemos tenido cuidado de añadir una llave de cierre (}) para mantener la sintaxis del archivo. A fin de ver los posibles errores con que nos podemos encontrar, sugiero al lector que añada un archivo inexistente a la lista:

```

...
##### #
# File System and Disk Administration Programs # #
##### #
(
    rulename = "File System and Disk Administration Programs",
    severity = $(SIG_HI)
)
{
    /sbin/accton                -> $(SEC_CRIT) ;
    /sbin/badblocks            -> $(SEC_CRIT) ;
    /sbin/dosfsck              -> $(SEC_CRIT) ;
    /sbin/e2fsck               -> $(SEC_CRIT) ;
}

```

```
# ARCHIVO DE PRUEBA INEXISTENTE AÑADIDO. OBSERVE QUE ESTA
# UBICADO ANTES DE LA LLAVE DE CIERRE
  /sbin/lechuga                                -> $(SEC_CRIT) ;
}
# AHORA AQUI TERMINA EL ARCHIVO
```

Tenga cuidado de no insertar este archivo por debajo de la llave de cierre del grupo. Recuerde que más tarde deberá vérselas con el archivo original que contiene (en mi caso) 452 entradas.

## 2.3. Instalar el archivo de políticas

Cuando el archivo de políticas contiene todo lo que pretendemos monitorear, es menester "instalarlo". En realidad Tripwire usa una versión compilada y encriptada de este archivo, que se almacena en `/etc/tripwire/tw.pol`. Para generarlo (y regenerarlo cuantas veces se necesite), usar:

```
# twadmin -m P /etc/tripwire/twpol.txt
```

## 2.4. Construir la base de datos Tripwire

Una vez configurado e instalado el archivo de políticas, Tripwire necesita recolectar la información actual de los archivos que debe monitorear. Dicha información se almacena en una base de datos especial generada mediante el comando:

```
# tripwire -m i 2> /tmp/mensajes
```

Hemos redirigido parte de la salida de este comando al archivo `/tmp/mensajes`. Es muy probable que hayan archivos especificados en las políticas (`twpol.txt`) que no existen o están incorrectamente escritos (como **lechuga**.) Esto quedará registrado en `/tmp/mensajes`. Los errores deberán corregirse en `twpol.txt`, el cual se deberá reinstalar, para proceder a reconstruir la base de datos Tripwire. Este procedimiento se repetirá mientras subsistan errores en el archivo de políticas.

Borre el archivo `/tmp/mensajes` cuando hayan desaparecido todos los errores.

## 2.5. Verificación del filesystem

Ahora que Tripwire está correctamente configurado con su base de datos, es el momento de verificar la integridad del filesystem. Esto

se consigue con el comando:

```
# tripwire -m c
```

Este comando se usará cada vez que deseamos saber que nuestro sistema no ha sido alterado.

Si por algún motivo algunos de los archivos monitoreados son modificados (por ejemplo, por una actualización en el software) entonces debemos reconstruir la base de datos como se vió en el paso anterior, a fin de que no aparezcan discrepancias con el estado actual del filesystem en las próximas verificaciones.

Si deseamos dejar de monitorear ciertos archivos o iniciar el monitoreo de otros, entonces debemos configurar el archivo de políticas (`twpol.txt`) como se vió anteriormente, y reinstalarlo. Después, se volverá a generar la base de datos del filesystem. Este proceso lamentablemente puede ser muy tedioso cuando hay muchos archivos por monitorear.

## 3. Configuración permanente de Tripwire

### 3.1. Automatización

Ahora que Ud. ha probado la correcta ejecución de Tripwire, debemos programar su ejecución automática. Se aconseja una frecuencia diaria, aunque el administrador es libre de usar otro esquema. En RedHat 7.1, la ejecución diaria de tripwire se efectúa fácilmente creando un archivo en el directorio `/etc/cron.daily` (por ejemplo, `/etc/cron.daily/tripwire` con el siguiente contenido:

```
/usr/sbin/tripwire -m c | mail root@localhost
```

Donde Ud. deberá modificar la dirección "root@localhost" por lo que más le convenga. No olvide asegurarse de que el servicio **cron** esté operativo.

Asegúrese de que este archivo para cron sea ejecutable:

```
# chmod 755 /etc/cron.daily/tripwire
```

### 3.2. Notificación vía email

Esta funcionalidad proporciona un control más flexible con respecto a los reportes vía email. Tripwire es capaz de notificar por email sin necesidad de que el administrador invoque a un cliente de correo

como en el ejemplo anterior (en que invocamos a **mail**. Para esto, en el archivo de políticas debemos insertar la directiva:

```
emailto = user@host.domain
```

Esta directiva debe insertarse en la configuración de cada grupo de archivos que vamos a monitorear. Cuando alguno de estos archivos es modificado, Tripwire notifica al destinatario especificado. Por ejemplo, si queremos ser alertados cuando hubieren modificaciones de los archivos de administración del kernel, debemos modificar la sección correspondiente:

```
...
# Kernel Administration Programs # #
(
  rulename = "Kernel Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin/depmod                -> $(SEC_CRIT) ;
  /sbin/adjtimex              -> $(SEC_CRIT) ;
  /sbin/ctrlaltdel           -> $(SEC_CRIT) ;
  /sbin/instrmod              -> $(SEC_CRIT) ;
  ...
```

e insertar **emailto**:

```
...
# Kernel Administration Programs # #
(
  rulename = "Kernel Administration Programs",
  severity = $(SIG_HI), emailto = root@localhost
)
{
  /sbin/depmod                -> $(SEC_CRIT) ;
  /sbin/adjtimex              -> $(SEC_CRIT) ;
  /sbin/ctrlaltdel           -> $(SEC_CRIT) ;
  /sbin/instrmod              -> $(SEC_CRIT) ;
  ...
```

Tripwire normalmente invoca para esto a **sendmail**.

Si Ud. usa **vi**, puede insertar automáticamente la directiva **emailto** en todas las secciones del archivo con el siguiente comando "de última línea":

```
:1,$s/severity =.*/&,emailto = root@localhost/
```

Asegúrese de respetar todos los espacios y los signos de puntuación.

Finalmente, el archivo `/etc/cron.daily/tripwire` debe ser modificado del siguiente modo:

```
/usr/sbin/tripwire -m c -email-report
```

El archivo de configuración `twcfg.txt` contiene algunos parámetros adicionales para la configuración del sistema de notificación de email. Por ejemplo, es posible configurar si se deben enviar reportes aún si no han habido problemas (ver directiva **MAILNOVIOLATIONS** de `twcfg.txt`.) También se puede seleccionar el agente de mensajería (ver directiva **MAILPROGRAM**) a fin de no usar **sendmail** y generar una conexión directa SMTP hacia otro host.

Consulte el manual de `twconfig(4)` y `twpolicy(4)` para más opciones y ejemplos.

## 4. Eliminación de archivos de texto

Tripwire guarda su configuración y la política del filesystem en dos archivos encriptados con la "clave del site". Estos son: `/etc/tripwire/tw.cfg` y `/etc/tripwire/tw.pol`, respectivamente. El primero se generó a partir de `/etc/tripwire/twcfg.txt` cuando se configuraron las claves, y el segundo ha sido regenerado cada vez que Ud. modificó su archivo de políticas `/etc/tripwire/twpol.txt`. Por seguridad, Ud. no debería mantenerlos en el sistema hasta que se vuelvan a necesitar, así que proceda a borrarlos:

```
# rm /etc/tripwire/twcfg.txt /etc/tripwire/twpol.txt
```

Cuando Ud. necesite hacer una modificación de la política, puede regenerar el archivo `twpol.txt` del siguiente modo:

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

Y el de configuración mediante:

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

