Asegurando la integridad del sistema

Imobach González Sosa (imobachgs@softhome.net)
Manolo Padrón Martínez (manolopm@cip.es)

Ampliación de Sistemas Operativos

Contenidos

Contenidos

Contenidos

Un poco de historia

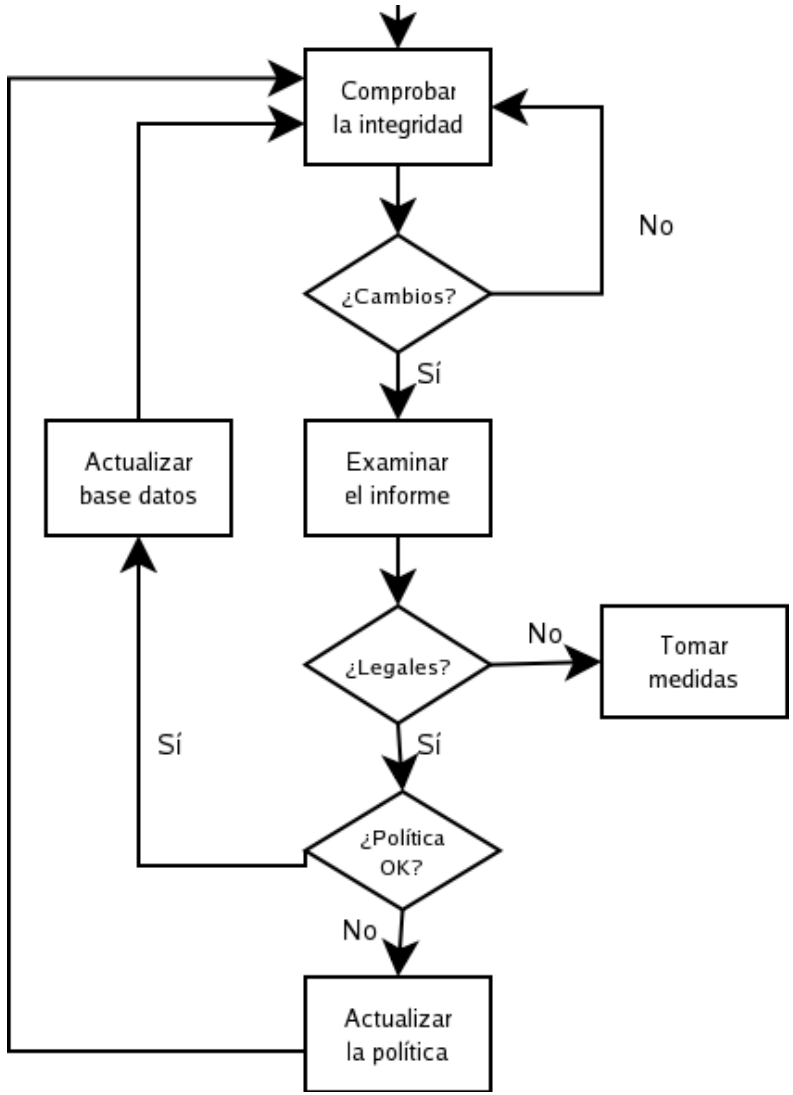
- La primera versión, 1992 en la Universidad de Purdue, era propietaria.
- El código estaba accesible mediante una licencia que permitía un uso restringido.
- En 1997 se funda Tripwire, Inc., que adquiere los derechos del software.
- Tripwire, Inc. reescribe el código y lo lanza como producto propietario y cerrado.
- Actualmente existen dos ramas, una de ellas libre (sólo para Linux).

Fundamentos

- Diseñada para ayudar al administrador a mantener la integridad del sistema.
- Tripwire monitoriza objetos —ficheros y directorios— detectando cambios en sus atributos.
- Mantiene una base de datos donde almacena los atributos de los objetos.
- El administrador fija la **política** que determinará qué objetos —y qué atributos— han de vigilarse.
- Tripwire usa criptografía asimétrica (de clave pública).

Flujo de trabajo habitual

1. Instalar y configurar.
2. Inicializar la base de datos.
3. Comprobar la integridad.
4. Examinar el informe.
5. Sincronizar la base de datos.
6. Actualizar la política.



Instalar y configurar

Proceso sencillo

- Ajustar la configuración —fichero `twcfg.txt`—.
- Diseñar y escribir la política —fichero `twpol.txt`—.
- Ejecutar el script `twinstall.sh`.

Criptografía asimétrica en Tripwire

- Tripwire usa dos pares de llaves para proteger los ficheros.
- Una general (`site.key` compartida entre varias máquinas que protege los ficheros de configuración y política).
- Otra local (`hostname-local.key`) que protege la base de datos y los informes.

Inicializar la base de datos

Orden

`/usr/sbin/tripwire --init`

- Tripwire construye la base de datos de objetos y atributos.
- La almacena en `/var/lib/tripwire` con un nombre que suele seguir el patrón `máquina.twd`.

```
# twadmin --examine /var/lib/tripwire/echeyde.twd
File: "/var/lib/tripwire/echeyde.twd"
File Type: Tripwire Database (Ver 2.2.0.0)
Encoding: Asymmetric Encryption
The following keys decrypt this file:
Local Keyfile: /etc/tripwire/echeyde-local.key
```

Comprobar la integridad

Orden

`/usr/sbin/tripwire --check`

- Tripwire genera un informe con los cambios producidos.
- El informe se guarda en `/var/lib/tripwire/report` con un nombre que suele seguir el patrón `máquina-fecha-hora.twd`.

```
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
The object: "/dev/pts" is on a different file system...ignoring.
The object: "/dev/shm" is on a different file system...ignoring.
Wrote report file: /var/lib/tripwire/report/echeyde-20040520-151340.twr
```

Examinar el informe

Orden

```
twprint --print-report --twrfile \
/var/lib/tripwire/report/echeyde-20040520-11:23.twr
```

Un informe de Tripwire está dividido en cinco partes:

1. Preámbulo.
2. Resumen del informe.
3. Resumen de reglas.
4. Detalle de objetos.
5. Errores.

Examinar el informe :: Preámbulo

Ofrece información general acerca del informe: autor, fecha de creación y última actualización de la base de datos.

```
Note: Report is not encrypted.
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:              root
Report created on:                jue 20 may 2004 15:13:40 WEST
Database last updated on:         jue 20 may 2004 00:48:54 WEST
```

Examinar el informe :: Resumen del informe

Información más concreta acerca del informe.

- Nombre e IP de la máquina.
- Ficheros de política y configuración.
- Base de datos.

```
Host name:                    echeyde
Host IP address:              192.168.1.30
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/echeyde.twd
Command line used:            tripwire --check
```

Examinar el informe :: Resumen de reglas

Estadísticas acerca de violaciones de reglas agrupadas por sección.

```
-------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------
  Rule Name                  Severity Level  Added    Removed  Modified
  ---------                  --------------  -----    -------  --------
  Invariant Directories      66              0        0        0
  Tripwire Data Files        100             0        0        0
  Other binaries             66              0        0        0
  Tripwire Binaries          100             0        0        0
* Other libraries            66              0        0        2
  ...

Total objects scanned: 13676
Total violations found: 26
```

Examinar el informe :: Detalle de objetos

- Es la parte “intensiva” del informe.
- Se detallan los datos resumidos en las tres partes anteriores.
- Se agrupan por sección y regla todos los cambios, mostrando los valores obtenidos y los esperados.

```
-------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------
-------------------------------------------------------------------
Rule Name: Other libraries (/usr/lib)
Severity Level: 66
-------------------------------------------------------------------
  ---------------------------------
  Modified Objects: 2
  ---------------------------------
```

Examinar el informe :: Detalle de objetos

```
Modified object name: /usr/lib/cgi-bin
  Property:            Expected                      Observed
  ------------         -----------                   -----------
* Modify Time          jue 20 may 2004 00:00:25 WEST
                                                     jue 20 may 2004 08:00:28
WEST
Modified object name: /usr/lib/cgi-bin/awstats052004.irq.homeunix.org.txt
  Property:            Expected                      Observed
  ------------         -----------                   -----------
* Size                 15352                         15963
* Modify Time          jue 20 may 2004 00:00:25 WEST
                                                     jue 20 may 2004 08:00:28
WEST
* CRC32                CLfMqg                        AtKlqz
* MD5                  AN4POmxeEcrksJXp+KoWGB        CQbxtYkH4v+QnR33vf+84K
```

Examinar el informe :: Errores

- Destinada a notificar errores durante el chequeo.
- Notar que errores y violaciones no son lo mismo.
- En el ejemplo, sin problemas.

```
No Errors
------------------------------------------------------------------------
*** End of report ***
```

Sincronizar la base de datos

Orden

```
tripwire --update --twrfile \
/var/lib/tripwire/report/echeyde-20040520-11:23.twr
```

- Es el administrador quien determina qué cambios son naturales y cuáles constituyen una amenaza.
- Los cambios “normales” habrá que incorporarlos a la base de datos.
- Podría regenerarse desde cero, pero no tendría sentido.

Sincronizar la base de datos

Extracto del formulario de sincronización: se marcan sólo los cambios a incorporar.

```
-------------------------------------------------------------------------
Rule Name: Other configuration files (/etc)
Severity Level: 66
-------------------------------------------------------------------------
Remove the "x" from the adjacent box to prevent updating the database
with the new values for this object.
Modified:
[x] "/etc"
[x] "/etc/adjtime"
[x] "/etc/awstats"
[ ] "/etc/awstats/awstats.irq.homeunix.org.conf"
[ ] "/etc/motd"
[x] "/etc/mtab"
[x] "/etc/network/ifstate"
```

Actualizar la política

Órdenes

```
twadmin --print-polfile > /etc/tripwire/twpol.txt
twadmin --create-polfile -S site.key \
/etc/tripwire/twpol.txt
rm /etc/tripwire/twpol.txt
```

- En ocasiones la política puede generar problemas o, simplemente, no ajustarse a las necesidades.
- El administrador puede cambiarla siempre que lo crea oportuno.
- Debe obtener un fichero en texto plano con la política, modificarla y aplicarla nuevamente.

Componentes de las políticas

Una política está formada por cinco clases de componentes:

Reglas Componente básico, especifica objetos/atributos a monitorizar.

Stop points Especifica objetos que no tienen que vigilarse.

Atributos Modifican el comporamiento de las reglas.

Directivas Agrupan reglas y permiten ejecución condicional.

Variables Permiten modificar información.

Componentes :: Reglas

```
objeto -> máscara;
```

objeto Fichero/directorio (UNIX) a monitorizar.

máscara Propiedades a tener en cuenta.

Limitaciones

- Sólo una regla por objeto.
- Si el objeto es un directorio, recursividad controlada.

Componentes :: Reglas

Nombres de objetos

- Rutas completas de ficheros y directorios.
- Se ignoran los espacios y las comillas dobles*.

Ejemplos

- `/usr/local`
- `/usr /local`
- `"/usr" "/local"`

Componentes :: Reglas

Máscaras de propiedades

`[+-]*[pinugtsldbamcrCMSH])+`

- Indican qué atributos examinar.
- Un + habilita; un - deshabilita.
- No son válidas máscaras vacías.
- El + es el símbolo por defecto.
- Símbolos contradictorios o duplicados: el último manda.

Ejemplos

- `+pinugsmtdbCM-raclSH`
- `+pinugtd-rsacmblCMSH`

Componentes :: Stop points

`! objeto;`

- Especifican objetos que no deben monitorizarse.
- Su utilidad está en indicar excepciones.

Ejemplo

```
/etc/     -> $(ReadOnly);
! /etc/mtab;
```

Componentes :: Atributos

```
objeto -> máscara (atributo1=valor1,atributo2=valor2,...);

(atributo1=valor1,atributo2=valor2)
{
  objeto1 -> máscara1;
  objeto2 -> máscara2;
  objeto3 -> máscara3;
  ...
}
```

- Modifican el comportamiento de las reglas u ofrece información adicional.
- Pares `atributo=valor`.
- Pueden referirse a reglas individuales o a grupos de ellas.

Componentes :: Atributos

rulename Nombre de la regla (o del grupo). Pueden ejecutarse comprobaciones que sólo procesen a una regla.

emailto Dirección de correo-e a quien avisar en caso de violación de la regla.

severity Nivel de gravedad. Tripwire permite ejecuciones basadas en este nivel.

recurse Control de recursividad. Ninguna (0), ilimitada (-1) o limitada a *n* niveles (*n*).

Ejemplo

```
(emailto=hostmaster@dis.ulpgc.es,severity=90)
{
  /etc        -> $(ReadOnly)
  /etc/apache -> $(ReadOnly) (emailto=webmaster@dis.ulpgc.es)
}
```

Componentes :: Directivas

¿Qué son?

- Conjunto de elementos preprocesados.
- Permiten compartir políticas entre diferentes máquinas.

@@section

- Etiqueta de secciones (FS, NTFS, NTREG, GLOBAL).
- FS es el valor por defecto.

@@end

- Final lógico del fichero.

Componentes :: Directivas

@@ifhost, @@else, @@endif

Generación de información de diagnóstico y depuración.

```
@@ifhost skywalker || solo
    /bin -> $(ReadOnly);
    /usr/bin -> $(IgnoreNone) -ar;
@@else
    @@ifhost c3po || r2d2
        /bin -> $(IgnoreNone) -ar;
    @@endif
@@endif
```

Componentes :: Directivas

@@print y @@error

Interpretación condicional según el nombre de la máquina.

```
@@ifhost romeo
    /bin          ->      $(ReadOnly);
@@else
    @@ifhost juliet
        @@print "Scanning projects on juliet"
        /projects       ->      $(ReadOnly) +H;
    @@else
        @@error "This policy file not written for this mach
    @@endif
@@endif
```

Componentes :: Variables

Dos tipos

- Locales
- Globales (@@section GLOBAL)

Definición

```
variable = valor;
```

Sustitución

```
$(variable);
```

Componentes :: Variables

Ejemplo

```
# Definición de variables
src = /usr/src ;
mask1 = +pinguC-a ;

# Ejemplo de uso a derecha e izquierda
$(src) -> $(mask1)
```

Componentes :: Variables

Variables predefinidas

Variable	Equivale a
ReadOnly	+pinugsmtdbCM-raclSH
Dynamic	+pinugtd-rsacmblCMSH
Growing	+pinugtdl-rsacmbCMSH
IgnoreAll	-pinusgamctdrblCMSH
IgnoreNone	+pinusgamctdrbCMSH-l
Device	-pugsdr-intlbamcCMSH

Contenidos

Contenidos

Contenidos

Contenidos

Un poco de historia

- Comienza como proyecto de fin de carrera en la universidad de Texas.
- En 1994 se congela el proyecto.
- Se divide en 4 partes, 2 propietarias, 1 de H.P. y 1 de Debian.
- En el 2002 se vuelven a unir como un solo proyecto.

¿Qué es Tiger?

- Tiger es una utilidad para la comprobar la configuración de las aplicaciones y de los usuarios existentes en el sistema.

¿Cómo esta hecho Tiger?

- Scripts en *Bash*.
- Pequeños programas en *C*.
- Ficheros de datos.

tiger

- Es el lanzador en batería de los scripts.
- /etc/tiger/tigerrc

tigercron

- Programador de tareas para *Tiger*.
- /etc/tiger/tigercron

tigerexp

- Muestra información de los errores.
- Se puede lanzar con el parámetro -f para indicar un fichero de entrada.

Módulos locales

check_accounts

- Comprueba el estado de las cuentas.
- Avisa de las cuentas desactivadas que aún conservan algún fichero que permite seguir usando la cuenta en cuestión.

check_logfiles

- Comprueba la existencia y permisos de logs relacionados con la autenticación de usuarios.

crack_run

- Lanza un `brute force`.
- Por defecto es el *crack*.
- `Tiger_CRACKDIR_LOC_OVERRIDE` permite cambiar el `brute`.

Módulos de red

check_anonftp

- Comprueba el acceso vía *ftp* anónimo a una máquina.
- Avisa de los problemas de permisos y propietarios asociados al usuario *ftp*.

check_listeningprocs

- Comprueba los puertos que están abiertos y notifica que programa es el que abre dichos puertos.

check_ssh

- Verifica que no se autentique por el método de compatibilidad con ssh v.1 , es decir el fichero `.rhost`.

Detección de intrusos.

check_know

- Se encarga de buscar las huellas dejadas por ciertos ataques conocidos.

tripwire_run

- Lanza al *tripwire*.

Ejemplos de salida: Tiger y tigercron.

```
/var/log/debian-installer/cdebconf/templates/

# Performing check of embedded pathnames...
--WARN-- [embed001w] Path ‘/usr/share/mysql/echo_stderr’ contains
‘/usr/share/mysql’ which is not owned by root (owned by mysql).
Embedded references in: /usr/bin/mysql_fix_privilege_tables->
/default(PATH)
--WARN-- [embed002w] Path ‘/usr/share/mysql/echo_stderr’ is not owned
by root (owned by mysql).
Embedded references in: /usr/bin/mysql_fix_privilege_tables->
/default(PATH)
10:34> Security report completed for ppro.
```

Ejemplos de salida:Tigerexp.

```
>./tigexp sum001
Message ID: sum001

The system does not appear to require a password
during single-user mode boot.  Either add a
password to your boot loader or add the line:
~~:S:wait:/sbin/sulogin to your /etc/inittab file.
This line should be added immeditaly before the
line containing "rc 0".
```