Introducción

- El control de integridad se realiza mediante un programa que:
  - Crea un estado inicial de los ficheros y directorios.
  - Compara el estado inicial con el actual e informa de los cambios.
- El programa más conocido es tripwire:
  - Desarrollado inicialmente en 1992 por la universidad de Purdue.
  - Actualmente es código propietario.
- Iniciativas de software libre:
  - Aide: Desarrollado para cubrir el hueco dejado por tripwire al pasar a ser código propietario.
  - Tripwire: Desarrollado a partir de la última versión libre del programa, es un desarrollo independiente del comercial.

Tripwire

- Asegura la integridad de los archivos y directorios críticos de un ordenador.
- Identifica los cambios realizados de forma automática e informa de los mismos.
- Permite minimizar el impacto de una intrusión en el sistema.
- Funciona generando, al instalar el sistema, una base de datos inicial (base de datos de fundamentos) y comparándola con una base de datos generada periódicamente.

Configuración inicial de tripwire

- Inicialmente, tripwire posee una configuración por defecto que puede ser usada.
  - Sin embargo, es recomendable modificar dicha configuración por defecto.
- Los archivos de configuración son:
  - /etc/tripwire/twcfg.txt
  - /etc/tripwire/twpol.txt

Configuración del archivo twcfg.txt (I)

- El archivo /etc/tripwire/twcfg.txt indica la localización de tripwire, su base de datos, etc.
- Posee dos tipos de variables:
  - De configuración obligatoria: Si se modifica el valor por defecto de una de ellas debe especificarse el valor de todas ellas, aunque se deseen sus valores por defecto.
  - De configuración optativa: No es necesario especificar su valor, pudiendo tomar el valor por defecto.

Configuración del archivo twcfg.txt (II)

- Las variables de configuración obligatoria son:
  - ROOT: Directorio con los ejecutables de tripwire (/usr/sbin).
  - POLFILE: Archivo de políticas (/etc/tripwire/tw.pol).
  - DBFILE: Archivo de la base de datos (/var/lib/tripwire/$(HOSTNAME).twd).
  - REPORTFILE: Archivo de los informes (/var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr).
  - SITEKEYFILE: Archivo de la llave del sitio (/etc/tripwire/site.key).
  - LOCALKEYFILE: Archivo de la llave local (/etc/tripwire/$(HOSTNAME)-local.key).

Configuración del archivo twcfg.txt (III)

- Las variables de configuración optativa son:
  - EDITOR: Editor de texto a utilizar (/bin/vi).
  - LATEPROMPTING: Minimizar el tiempo de permanencia de una contraseña en memoria (valor true) o no (valor por defecto false).
  - LOOSEDIRECTORYCHECKING: Informar solo sobre los cambios de un fichero y no los del directorio (valor true) o no (valor por defecto false).
  - SYSLOGREPORTING: Informar al demonio de syslog de los cambios (valor true) o no (valor por defecto false).
  - MAILNOVIOLATIONS: Mandar un correo electrónico aunque no se hayan producido modificaciones (valor por defecto true) o no (valor false).
  - EMAILREPORTLEVEL: Nivel de detalle de los informes enviados por correo, puede tomar valores de 0 a 4 siendo el valor por defecto 3.
  - REPORTLEVEL: Nivel de detalle de los informes generados por el comando twprint. Puede tomar valores de 0 a 4 siendo el valor por defecto 3.
  - MAILMETHOD: Protocolo de correo utilizado, puede tomar como valores SMTP o SENDMAIL (valor por defecto).
  - MAILPROGRAM: Programa de correo utilizado. Por defecto es /usr/sbin/sendmail –oi –t.

Configuración del archivo twcfg.txt (IV)

- Ejemplo de archivo twcfg.txt:

```
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

- Contiene que archivos y directorios son supervisados y la severidad de su supervisión.
- Esta formado por cuatro tipos de elementos:
  - Comentarios: Todo el texto de una línea que se encuentra detrás del carácter #.
  - Reglas: Indican como y con que severidad chequea tripwire los ficheros.
    - Reglas normales: Define que propiedades de un fichero o directorio serán analizadas.
    - Reglas de parada: Indican ficheros o directorios que no deben analizarse.
  - Directivas: Ordenes que condicionan la interpretación de la política en función, por ejemplo, del ordenador.
  - Variables: Permiten definir cadenas de texto para su sustitución en el fichero.

Especificación de las reglas (I)

- La sintaxis de las reglas normales es:

```
nombre_del_objeto -> mascara_de_propiedades;
```

  - Nombre del objeto: Camino completo hasta el fichero o directorio.
    - No se permiten variables de ambiente.
    - Se permiten variables de tripwire.
  - Máscara de propiedades: Propiedades del objeto a examinar o ignorar.
    - Si el objeto es un directorio, el directorio y todos sus subdirectorios son examinados con esas propiedades.
    - Si el objeto es un fichero, solo ese fichero es analizado con esas propiedades.
    - Cada objeto solo puede tener asociada una máscara, en caso contrario se produce un error.

Especificación de las reglas (II)

- La máscara de propiedades se especifica como una serie de caracteres que pueden ir precedidos de + o -.
- Cada carácter indica una propiedad que tripwire debe:
  - Comprobar si va precedida de +.
  - No debe comprobar si va precedida de -.

Especificación de las reglas (III)

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.

Especificación de las reglas (IV)

- La sintaxis de las reglas de parada es:

```
! nombre_del_objeto;
```

  - Nombre del objeto: Similar a nombre del objeto de las reglas normales.

- Las reglas normales pueden tener atributos para:
  - Modificar su comportamiento.
  - Proporcionar información adicional.
- Su sintaxis es para una regla:

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

- O para un grupo de reglas:

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

Especificación de las reglas (V)

- Los atributos posibles son cuatro:
  - rulename: Asocia una regla o conjunto de reglas con un nombre.
  - emailto: Asocia una o más direcciones de correo con una regla.
  - severity: Nivel numérico de severidad de una regla. El valor puede ir de 0 a 1.000.000, siendo el valor por defecto 0.
  - recurse: Indica como debe analizar una regla un directorio:
    - Valor true o -1: Se analizan todos los ficheros y subdirectorios.
    - Valor false o 0: Se analiza solo el directorio, pero no sus ficheros y subdirectorios.
    - Valor N entre 1 y 1.000.000: Se analizan los ficheros y subdirectorios hasta la profundidad N.

Especificación de las directivas

- Las directivas se especifican con la sintaxis:

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

- Donde nombre de la directiva puede tomar uno de los valores:
  - section: Sección de políticas específicas para un sistema operativo.
  - ifhost ... else ... endif: Interpretación del fichero según el ordenador (u ordenadores separados por ||).
  - print: Imprime un texto a la salida estándar.
  - error: Imprime un texto y detiene la ejecución.
  - end: Final de la política de directivas.

Especificación de las variables

- Las variables se especifican como:

```
variable = valor;
```

- El uso de una variable es legal en cualquier lugar donde pueda aparecer una cadena de caracteres.
- Existen un número predefinido de variables:

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.	+pinugtsdrbamcCMSH-l

Ejemplo de archivo twpol.txt

```
@@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) ;
}
…
```

Generación de la política de seguridad (I)

- Los archivos twcfg.txt y twpol.txt deben convertirse a formato de tripwire:
  - /etc/tripwire/twcfg.txt -> /etc/tripwire/tw.cfg
  - /etc/tripwire/twpol.txt -> /etc/tripwire/tw.pol
- Para ello se utiliza el script:
  - /usr/sbin/tripwire-setup-keyfiles.
- Solicita las contraseñas del sitio y local:
  - La contraseña del sitio protege los archivos de configuración y política (/etc/tripwire/site.key)..
  - La contraseña local protege la base de datos y los archivos de informes (/etc/tripwire/$(HOSTNAME)-local.key).
- Una vez generados los archivos, deben borrarse o copiarse los archivos .txt.

Generación de la política de seguridad (II)

- La base de datos inicial de tripwire se crea con el comando:

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

- Y podemos ejecutar el comando:

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

- Para comprobar la integridad del sistema respecto a la base de datos inicial.
  - Se genera un fichero dentro de /var/lib/tripwire/report con extensión .twr.
- Debe ejecutarse de forma periódica la comprobación.

Comprobación de los informes (I)

- Tripwire genera sus informes de forma cifrada. Para verlos hemos de ejecutar el informe:

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

- Donde:
  - -m r: Descifrar el informe.
  - -r Informe a descifrar.
- Siendo solicitada la contraseña local para poder acceder al informe.

Comprobación de los informes (II)

- Ejemplo de informe:

```
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 Administraton 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
```

Comprobación de los informes (III)

- Ejemplo de informe (continuación):

```
  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 ***
```

Comprobación de los informes (IV)

- Tripwire permite ver el contenido de la base de datos:

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

- O obtener datos de un fichero:

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

- Generando el informe:

```
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
```

Comprobación de los informes (V)

- Los informes de tripwire indican las modificaciones realizadas.
  - Mientras no se indique nada estas modificaciones no son introducidas en la base de fundamentos de tripwire y aparecen en todos los informes.
- Para introducir una modificación detectada por tripwire en la base de fundamentos ejecutamos:

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

  - Donde <nombre> es el fichero de informe a utilizar.
- Tripwire cruza la base de fundamentos con el fichero de informe indicado y abre un editor en el que se muestran los cambios:

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

- Si se desean aceptar las modificaciones se dejan con la [x], bastando ponerlas como [ ] para que no sean incluidas en la base de fundamentos.

Actualización del archivo de configuración

- El archivo de configuración puede regenerarse como:

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

  - Siendo solicita la contraseña del sitio.

- Y una vez modificado, generar el nuevo archivo de configuración con el comando:

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

- No siendo necesario regenerar la base de datos de tripwire.

Actualización del archivo de políticas

- El archivo de políticas puede regenerarse como:

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

  - Siendo solicita la contraseña del sitio.

- Y una vez modificado, generar el nuevo archivo de configuración con el comando:

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

- Siendo necesario regenerar la base de datos de tripwire.

Envío de avisos de correo electrónico (I)

- Tripwire puede enviar un correo electrónico cuando una regla ha sido violada.
- Basta incluir en la sección de atributos de una regla o conjunto de reglas la directiva:

```
emailto = <dirección>[;<dirección>]
```

Envío de avisos de correo electrónico (II)

- Ejemplo:

```
# 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) ;
}
```

- La configuración puede probarse mediante el comando:

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