Manual TripWire

17/11/23

Jose Almirón Lopez

Índice

¿Qué es TripWire?

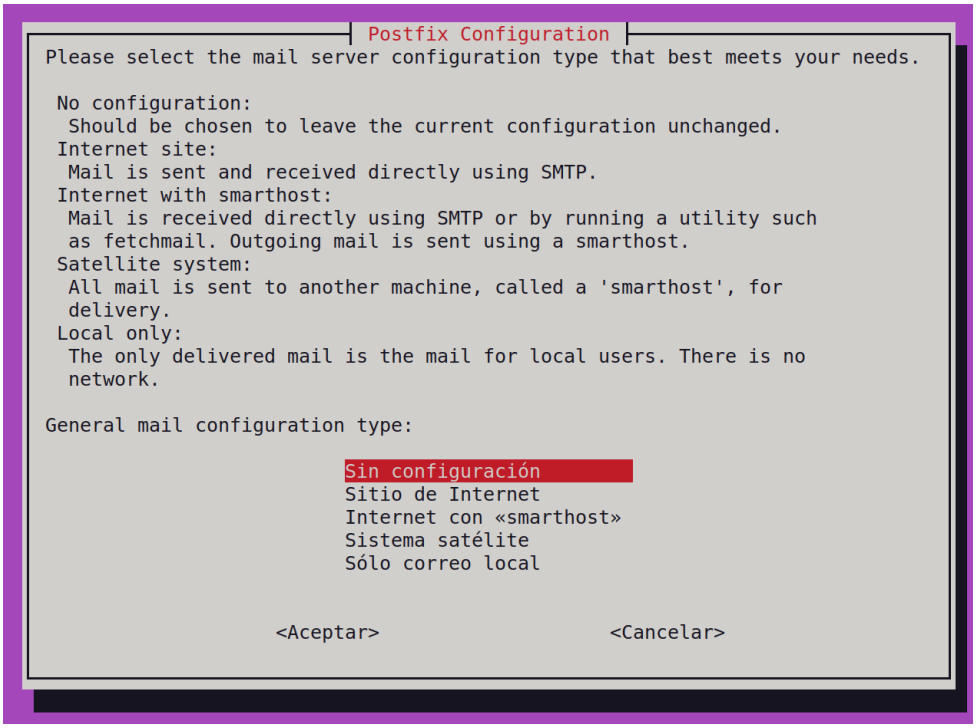
Tripwire es un software de detección de intrusos que monitoriza cambios en archivos y directorios en un sistema informático. Compara el estado actual de los archivos con un estado conocido, emitiendo alertas si se detectan cambios no autorizados.

Instalación del servicio

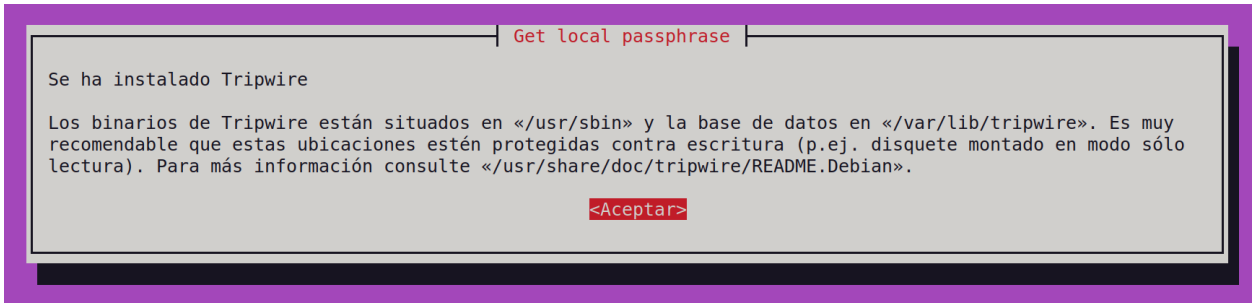
Obtenemos el paquete Tripwire descargándolo de los repositorios de Ubuntu.

```
jose@jose-almiron:~$ sudo apt install tripwire
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  postfix
Paquetes sugeridos:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin | dovecot-common
  resolvconf postfix-cdb postfix-mta-sts-resolver postfix-doc
Se instalarán los siguientes paquetes NUEVOS:
  postfix tripwire
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 2 no actualizados.
Se necesita descargar 3.095 kB de archivos.
Se utilizarán 15,9 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Se abrirá un entorno gráfico de instalación, donde elegiremos la opción de instalación sin configuración



Aceptamos todas las opciones predeterminadas y se nos solicitará ingresar una contraseña en cuatro ocasiones



Inicialización y configuración básica del servicio

Para inicializar la base de datos, utilizaremos el comando "**tripwire --init**". Es posible que se generen varios errores en este momento, pero los abordaremos y solucionaremos en los pasos siguientes.

```
jose@jose-almiron:~$ sudo tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
### Warning: File system error.
### Filename: /var/lib/tripwire/jose-almiron.twd
### No existe el archivo o el directorio
### Continuing...
### Warning: File system error.
### Filename: /etc/rc.boot
### No existe el archivo o el directorio
### Continuing...
The object: "/boot/efi" is on a different file system...ignoring.
### Warning: File system error.
### Filename: /root/mail
### No existe el archivo o el directorio
### Continuing...
### Warning: File system error.
### Filename: /root/Mail
### No existe el archivo o el directorio
### Continuing...
### Warning: File system error.
### Filename: /root/.xsession-errors
### No existe el archivo o el directorio
### Continuing...
### Warning: File system error.
### Filename: /root/.xauth
### No existe el archivo o el directorio
```

Configuramos el archivo "**/etc/tripwire/twpol.txt**" y comentaremos algunos archivos.

- /etc/rc.boot
- todos los que empiezan por /root
- /proc

```
  severity = $(SIG_HI)
)
{
        /etc/init.d             -> $(SEC_BIN) ;
#       /etc/rc.boot            -> $(SEC_BIN) ;
        /etc/rcS.d              -> $(SEC_BIN) ;
        /etc/rc0.d              -> $(SEC_BIN) ;
```

```
  GNU nano 6.2                                  /etc/tripwire/twpol.txt *
  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) ;
}
```

```
  severity = $(SIG_HI),
)
{
        /dev            -> $(Device) ;
#       /proc           -> $(Device) ;
}
```

Aplicamos las políticas con el comando "**sudo twadmin -m P twoo.txt**" para implementar los cambios realizados.

```
jose@jose-almiron:/etc/tripwire$ sudo twadmin -m P twpol.txt
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
jose@jose-almiron:/etc/tripwire$
```

Ahora podemos reiniciar el servicio y esta vez debería iniciarse sin problemas.

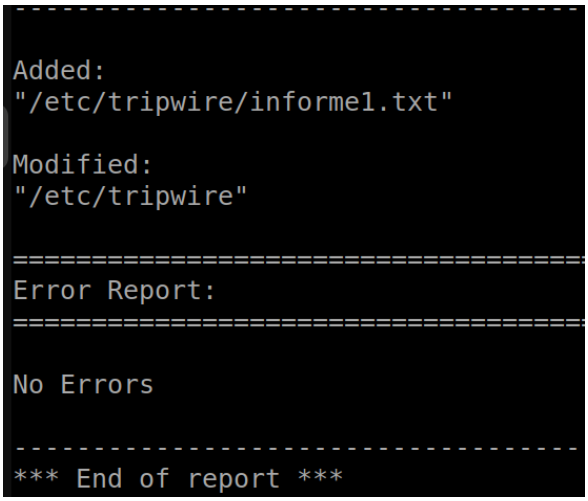
```
jose@jose-almiron:/etc/tripwire$ sudo tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
The object: "/boot/efi" is on a different file system...ignoring.
The object: "/dev/hugepages" is on a different file system...ignoring.
The object: "/dev/mqueue" is on a different file system...ignoring.
The object: "/dev/pts" is on a different file system...ignoring.
The object: "/dev/shm" is on a different file system...ignoring.
Wrote database file: /var/lib/tripwire/jose-almiron.twd
The database was successfully generated.
jose@jose-almiron:/etc/tripwire$
```

Funcionamiento del servicio

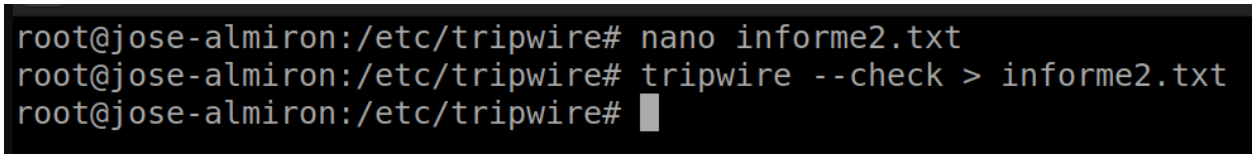
Podemos generar informes utilizando el comando "sudo tripwire --check > informe1.txt", redirigiendo la salida a un archivo que hayamos creado previamente, donde se almacenará el informe.

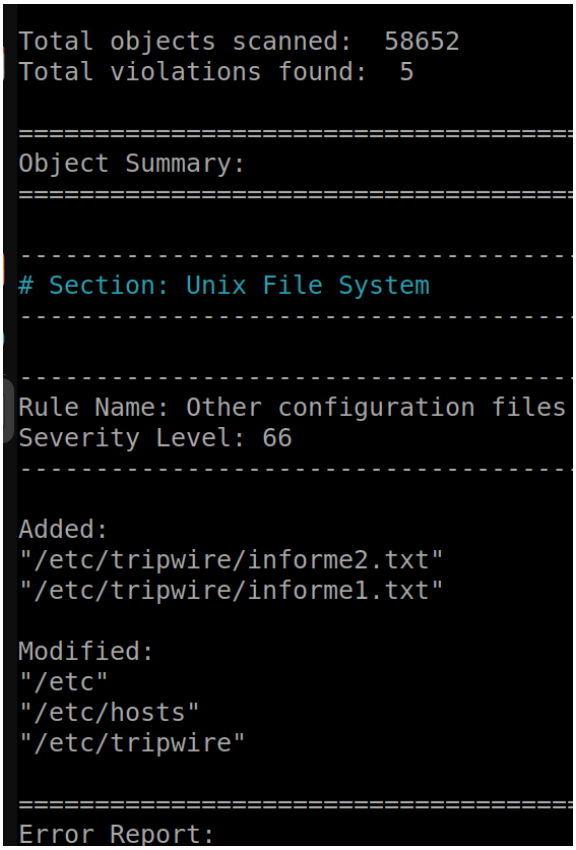
```
root@jose-almiron:/etc/tripwire# nano informe1.txt
root@jose-almiron:/etc/tripwire# tripwire --check > informe1.txt
root@jose-almiron:/etc/tripwire#
```

Podemos examinar el informe con herramientas como "nano" o "cat", aunque lo común es utilizar un comando específico proporcionado por Tripwire, el cual explicaremos más adelante.

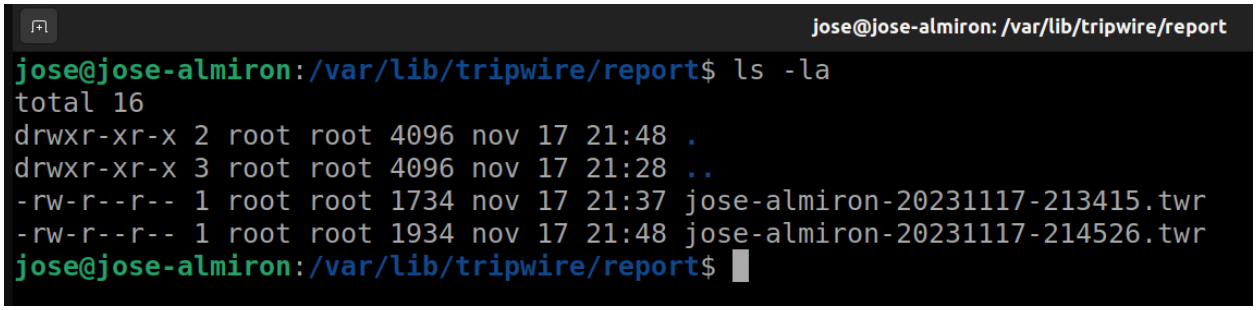


Vamos a editar un archivo del sistema, en este caso, "/etc/hosts". Después de hacer esta modificación, generamos otro informe para observar el proceso de monitorización con Tripwire. En este segundo informe, podremos identificar qué archivo hemos modificado.





Al dirigirnos a la ruta "**/var/lib/tripwire/report**", podremos comprobar que todos nuestros informes están almacenados en ese directorio



Para visualizar los informes de manera detallada, utilizaremos el comando "**sudo twprint -m r --twrfile informe.twr**". Esto nos proporcionará una vista más completa del informe generado