

# **Informe de realización de la práctica 6: Monitorización cambios en ficheros**



## **Administración de Sistemas Operativos**

Nombre:

- **José María Amusquívar Poppe**
- **Prashant Jeswani Tejawani**
- **Eduardo Maldonado Fernández**

Curso: **3º (Grupo 44)**

Practica: 6º- Administración de dispositivos y archivos

# Índice

- a)** Implementación en scripts de la monitorización de los cambios en fichero
- b)** Opciones adicionales
- c)** Pruebas y funcionamiento correcto de los scripts
- d)** Fallos o incidencias

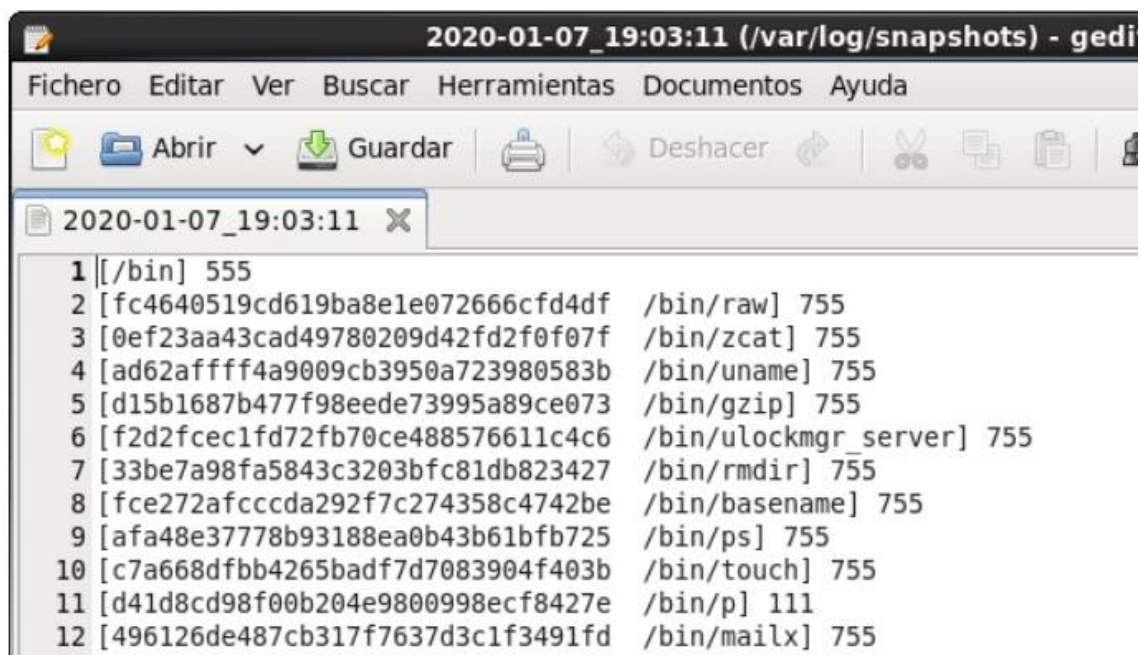
### a) Implementación en scripts de la monitorización de los cambios en fichero

Implementamos la función con dos scripts: **snapshot.sh** y **compare\_snapshot.sh**. Primero, en **snapshot.sh**, hacemos un control de errores para evitar el uso de argumentos por parámetros. Para hacer la ‘foto’ actual de los ficheros y archivos de los directorios /bin,/usr/bin,/sbin,/usr/sbin utilizaremos dos vectores: “files” y el vector asociativo “map”, es asociativo debido a que podemos encontrar a los ficheros según su suma de control. Mediante una función ‘functionFind()’ se le pasa como parámetro uno de los cuatros directorios (mediante un bucle ‘for’ en el main), y se va recorriendo todos los ficheros, directorios, se va guardando en “map” la clave es el checksum y el valor guardado para esta clave son los permisos del fichero y su ruta o en caso de ser un directorio, la clave es la ruta del directorio. En otra función ‘executeSnapshot()’ la ‘foto’ se guardará en el directorio /var/log/snapshots. Por último, al terminar de ejecutarse el script snapshot.sh se escribe “FIN” para conocer que la ejecución no se ha interrumpido.

Ejemplo de Fichero y directorio:

[4748498jdlfjfi73393 /bin/A] 755 – [‘Checksum’ ‘Ruta del fichero’] ‘Permisos’

[/bin/directorio/] 555 – [‘Ruta del directorio’] ‘Permisos’



The screenshot shows a Gedit window titled "2020-01-07\_19:03:11 (/var/log/snapshots) - gedit". The window contains a list of files and their checksums, permissions, and paths. The list is as follows:

Checksum	Path	Permissions
[/bin]	/bin	555
[fc4640519cd619ba8e1e072666cfd4df]	/bin/raw	755
[0ef23aa43cad49780209d42fd2f0f07f]	/bin/zcat	755
[ad62affff4a9009cb3950a723980583b]	/bin/uname	755
[d15b1687b477f98eede73995a89ce073]	/bin/gzip	755
[f2d2fcec1fd72fb70ce488576611c4c6]	/bin/ulockmgr_server	755
[33be7a98fa5843c3203bfc81db823427]	/bin/rmdir	755
[fce272afcccda292f7c274358c4742be]	/bin/basename	755
[afa48e37778b93188ea0b43b61bfb725]	/bin/ps	755
[c7a668dfbb4265badf7d7083904f403b]	/bin/touch	755
[d41d8cd98f00b204e9800998ecf8427e]	/bin/p	111
[496126de487cb317f7637d3c1f3491fd]	/bin/mailx	755

En el segundo script **compare\_snapshot.sh** se realiza diversos controles de errores para poder ejecutar la comparación de la foto actual con respecto la primera foto realizada (Existe otra opción -l que se explicará en el apartado b)). Mediante la variable 'snapshotOld' recuperamos la 'foto' original.

Se ejecuta dos funciones;

La primera 'executeComparison()' se ejecutará el script snapshot.sh para conseguir foto actual de los directorios guardando el fichero obtenido de dicha ejecución en 'snapshotNow'. Mediante la instrucción 'diff' se retorna todas las diferencias presentes en ambos ficheros usando los símbolos de mayor o menor para especificar dichos cambios. El resultado obtenido del 'diff' se normaliza los espacios y elimina corchetes con el programa 'tr'. Ahora, con un bucle while y la ayuda del IFS lo organizamos en 'sign' que es el símbolo del 'diff' '<','>', en 'hashcode' es la suma de control del fichero, 'direc' la ruta del fichero y 'perm' son los permisos de dicho fichero. En caso de ser un directorio el campo 'hashcode' equivale a la ruta del directorio, moviéndose todos los campos a la derecha.

La segunda función 'crontabOption()' comprueba si ya existe una configuración antigua en el fichero crontab para poder ejecutar este script en un tiempo especificado por el usuario y sino ofrece la opción de establecer dicha configuración.

#### **b) Opciones adicionales**

En el script **compare\_snapshot.sh** existe una opción '-l' si se le pasa como argumento. La opción '-l' compara el estado actual con el último snapshot realizado, en cambio, la opción por defecto compara el estado actual con el primer snapshot realizado.

Existe la opción '-h' en ambos scripts para mostrar un mensaje de ayuda del uso correcto.

#### **c) Pruebas y funcionamiento correcto de los scripts**

Para comprobar que se cumple las especificaciones de la monitorización de los cambios en un fichero o directorio, se ha creado un script **tests.sh** que se adjuntará en el archivo comprimido.

En este script creamos 2 ficheros y 2 directorios en /bin /sbin /usr/bin /usr/sbin. A partir de aquí, se modificará el contenido y los permisos de estos archivos para comprobar las funcionalidades básicas correctamente.

También, se ha ejecutado pruebas más estrictas, como detectar los cambios de permisos en caso de que sea el SUID, si hay alguna interrupción del snapshot.sh.

#### **d) Fallos e incidencias**

A lo largo del desarrollo y funcionamiento de los scripts hemos encontrados algunos errores, pero se han solucionado en gran medida.