Grado en Ingeniería Informática

Seguridad y Riesgos en Sistemas de Información

Práctica 3 - Logs

Laboratorio

Contenidos

Introducción

Uno de los pilares clave para asegurar un sistema es la de tener la posibilidad de ver qué acciones han realizado sus usuarios sobre el sistema de archivos.

Para ello existen numerosas herramientas, como la gestión de *logs* o registros del sistema. Los sistemas *Linux* cuentan con un robusto sistema de *logs* donde se puede consultar valiosa información del sistema, p.ej. en el directorio */var/log*.

En esta práctica se va a realizar un sistema para registrar y visualizar las acciones que realizan los usuarios en el sistema.

Al terminar la práctica se habrán trabajado los siguientes puntos:

- ☐ Gestión de *logs* usando herramientas propias del sistema *Linux*
- ☐ Gestión y visualización personalizada de logs
- ☐ Desarrollo de scripts en *bash script*

Temporización

3 semanas (ver cronograma de la asignatura).

- Semana 1: planteamiento
- Semana 2: dudas
- Semana 3: entrega y evaluación

Entorno

Herramientas

Los comandos propuestos para realizar el sistema de gestión de registro son los siguientes:

- cut
- echo
- grep
- logger
- printf
- readlink

También se puede utilizar cualquier estructura de control.

Ejecutables

Para el desarrollo de la práctica los comandos de utilidad del sistema se crearán en la carpeta /usr/bin (se necesitan permisos de *root*).

Registro de Acciones

La responsabilidad sobre las acciones de los usuarios sobre el sistema de archivos (*accountability*) es un aspecto fundamental para una correcta gestión de la seguridad en un sistema *linux*. Algunos de los comandos básicos a registrar serían el listado de archivos, los directorios visitados o los archivos borrados. Por ello se propone el registro de las siguientes acciones en el sistema.

- Entrar en un directorio (comando *cd*)
- Listar un archivo o directorio (comando *ls*)
- Borrar un archivo o directorio (comando *rm*)

Para realizar el registro se va a utilizar una utilidad existente en los sistemas *linux*, *logger*. Esta utilidad permite añadir registros al log del sistema. Estos, en un sistema *Ubuntu* consisten en un fichero de texto que está ubicado en la ruta */var/log/syslog*. El formato del registro se puede observar editando/visualizando el fichero. Básicamente contiene la fecha, el equipo, una etiqueta, y a continuación el mensaje de registro.

Para añadir registros utilizando la utilidad *logger* sólo hay que invocar el comando seguido del mensaje de registro. También se puede cambiar la etiqueta utilizando el modificador *-t*. Consultar la ayuda del comando *logger* para mayor información.

Formato del Registro

Para gestionar los eventos que se generan en el *log* se va a utilizar el siguiente formato:

- Se añade como etiqueta un *string* que identifica nuestro sitema de log y permite diferenciar nuestros logs. Este identificador es *customlog*
- Como mensaje se genera un *string* formado por 4 campos separados por comas. Los campos son los siguientes:
  1. Identificador del usuario (*UID*)
  2. Nombre del usuario
  3. Acción realizada (*cd*,*rm* o *ls*)
  4. Archivo sobre el que se ha realizado la acción (ruta absoluta)

Un ejemplo de acción registrada en el *log* del sistema con este formato sería el siguiente:

```
Feb 5 18:45:52 laptop customlog: 1000,user1,cd,/home/user1/downloads
```

Comandos Implementados

A efectos prácticos, no se van a sustituir los comandos originales que realizan las acciones indicadas. En su lugar, se van a implementar unos comandos que se utilizarán en su lugar y nos servirán para ilustrar su uso e implementar el

sistema de registro. Estos comandos son *ccd*, *crm* y *cls*. Junto a estos comandos, el sistema consta también de otros scripts, *clog* y *cview*. *Clog* se encarga de realizar el registro de las acciones. Será utilizado por los comandos para realizar ese registro.

Cada uno de estos comandos es un *script* en *bash* que realiza las siguientes acciones:

- Invoca *clog* con dos parámetros:
  1. El comando que se utiliza (*cd*, *rm*, o *ls*)
  2. El fichero sobre el que se va a realizar la acción (ruta absoluta)
- Invoca al comando original para que realice las acciones pertinentes
  - *ccd* invoca a *cd*
  - *crm* invoca a *rm*
  - *cls* invoca a *ls*

El comando *clog* realiza las siguientes acciones:

- A partir de sus parámetros genera la entrada en el registro utilizando el comando *logger*

Visualización del Registro

El registro se puede visualizar directamente listando/editando el fichero de registro, */var/log/syslog*. Pero para una más cómoda gestión y para que sirva para los propósitos de este ejercicio se va a crear el *bash script* denominado *cview*.

Este script sólo muestra los eventos de nuestro sistema teniendo en cuenta las siguientes consideraciones:

- Sólo muestra los eventos que se han realizado en el directorio actual o, de forma recursiva, en uno de sus directorios hijo
- Si no recibe ningún parámetro muestras los eventos asociados a todas las acciones (*ls*, *rm*, o *cd*)
- Si recibe un parámetro, este se corresponderá con una de las acciones definidas (*ls*, *rm*, o *cd*), sirviendo esta como filtro (sólo muestra las acciones de ese tipo)

El formato de visualización consta de 4 columnas tabuladas con los encabezados y formato que se muestra en el ejemplo siguiente:

```
id     user   action path
 1000  user1  rm     /home/user1/folder1/folder2/fileA.txt
 1001  user2  ls     /home/user2/fileC
 1000  user1  rm     /home/user1/folder1/folder2/fileB.txt
```

Consideraciones

- Los comandos implementados (*cls*, *crm*, o *ccd*), de cara al usuario, realizan las mismas acciones que los comandos a los que invocan (*ls*, *rm*, o *cd*). No se produce ninguna salida adicional
- Los comandos implementados (*cls*, *crm*, o *ccd*) soportan las mismas funcionalidades que los comandos a los que invocan (*ls*, *rm*, o *cd*)

Entrega

La entrega de la práctica tiene como fecha límite el 05 de Mayo de 2024 a las 23:59 horas.

Los artefactos a entregar serán los ficheros ejecutables que constituyen el sistema de registro (*cls*, *crm*, *ccd*, *clog* y *cview*).