# INFORME DE ENTREGA: TRABAJO PRÁCTICO 4

## (Monitorización de accesos)

### Componentes del grupo:

Sergio

Alejandro

Ana

### Funcionamiento del script:

El script acepta un único parámetro. Este parámetro, *threshold,* es el valor límite de intentos de acceso fallidos que vamos a considerar. Si un usuario ha tenido un número de accesos fallidos superior a ese valor en el espacio de tiempo desde la ejecución anterior del script al momento de ejecución actual, ese usuario (junto al número exacto de intentos fallidos que ha tenido) será almacenado en el fichero de salida */var/log/login\_unsuccessful.*

Para discernir si nos encontramos en la primera ejecución del script o si nos encontramos en la segunda, o posterior ejecución, comprobamos si existe o no éste fichero de salida. Si existe, la fecha de la última ejecución se tomará de la última línea del fichero de salida, y si no, le damos un valor de -1, ya que en este caso nos encontramos en la primera ejecución del script y necesitamos tratar todos los intentos registrados en */var/log/secure* sin importar su fecha, y cualquier fecha, al compararse con -1, será superior y entrará en la condición establecida en el script.

Los usuarios con intentos cuya fecha caiga en esta condición serán recogidos en un fichero auxiliar, */var/ultimosAccesosUsuarios.*

Si este fichero existe, es decir, si ha ocurrido algún intento de acceso fallido desde la última ejecución del script, procedemos a ordenar y contar el número de intentos de cada usuario mediante *sort* y *uniq –c*. Entonces, tratando este fichero por líneas, podemos comprobar fácilmente si el campo de “ocurrencias” es mayor que nuestro *threshold,* para cada usuario.

En el caso de que lo sea, se comprueba:

* Que el nombre de usuario no sea un intento de acceso con un nombre en vacío
* Que el UID del usuario sea mayor que el UID\_MIN definido para el sistema, de manera que nos aseguremos que se trata de un usuario y no una cuenta de servicio.
* Que la cuenta *root* también se incluya, comprobando también el caso del UID = 0

Si se llegan a estas condiciones, se añade al fichero de salida */var/log/login\_unsuccessful* una línea por ese usuario concreto, con el formato:

*usuario* (fallos = *número\_intentos*)

Una vez tratados todos los usuarios marcados en el fichero auxiliar */var/ultimosAccesosUsuarios*, borramos este fichero.

Con esto se termina la ejecución del script, de manera que añadimos como última línea al fichero de salida la fecha actual, en el mismo formato con el que se representan las fechas en el fichero */var/log/secure.*

### Opción adicional:

En el momento de añadir el usuario que cumple las condiciones al fichero de salida, consultamos con *chage –l usuario* la información de caducidad de su cuenta y su contraseña*.*

Si la cuenta o contraseña (o ambas) de este usuario no tienen caducidad, se indica en la línea dedicada al usuario en el fichero de salida, con el formato:

*usuario* (fallos = *número\_intentos*) (cuenta nunca expira/contraseña nunca expira)