3. Usuarios y Grupos.

3.1. Introducción.

Actualmente, la mayoría de los sistemas operativos existentes son multiusuario y multitarea. Ello implica que más de un usuario puede trabajar en el sistema de forma simultánea a otros, ejecutando una o más tareas a la vez. Por este motivo, es muy importante que el mismo sistema operativo incorpore mecanismos para manipular y controlar correctamente a los usuarios: el sistema de entrada e identificación (*login*), los programas que puede ejecutar cada uno, mecanismos de seguridad para proteger el hardware del ordenador, protección para los ficheros de los usuarios, etc.

Los sistemas operativos basados en UNIX organizan toda esta información por usuarios y grupos. Al entrar en el sistema, debemos identificarnos con un *login* y una contraseña. El *login* suele ser un nombre que identifica de forma inequívoca al usuario. En sistemas donde hay más que unos pocos usuarios, es importante disponer de una buena política de nombres para poderlos identificar a todos de forma clara. La contraseña debe ser una combinación de letras, números y caracteres especiales. No debe estar formada por ninguna palabra de diccionario o similares porque puede representar un problema de seguridad importante. El sistema de contraseñas es de tipo unidireccional. Esto quiere decir que nuestra contraseña no es almacenada como texto, sino que es cifrada y guardada tal como es. Cuando entramos en el sistema y escribimos nuestra contraseña, ésta es cifrada y comparada con la que está almacenada. Si coinciden, la identificación es positiva, si no coinciden, no hay identificación. Lo importante de todo este sistema es que a partir del cifrado no podemos conseguir, de ninguna manera, la clave original. Los programas que intentan romper las contraseñas de los usuarios lo único que pueden hacer es cifrar palabras a partir de diccionarios (con sistemas automáticos para derivarlas y buscar variantes) y probar si coinciden con el cifrado de alguna de las contraseñas de usuario. Es por este motivo por lo que debemos escoger cuidadosamente nuestras contraseñas; de otra forma comprometeremos toda la seguridad del sistema.

Actualmente, en los sistemas GNU/Linux podemos escoger dos tipos de cifrado posibles para las contraseñas de usuario. El que se viene usando desde los inicios de UNIX es el 3DES. El único inconveniente de este tipo de cifrado es que sólo nos permite contraseñas de 8 letras (si escribimos más, se ignoran), a diferencia del otro tipo de cifrado, llamado MD5, con el que podemos usar contraseñas de la longitud que queramos. Cuanto más larga sea la contraseña, más segura resulta, con lo cual, se recomienda utilizar el segundo tipo de cifrado. De todos modos debemos considerar que, si necesitamos usar algunos programas especiales para la gestión de usuarios, como el NIS, puede que no sean compatibles con MD5.

Si bien un usuario es un individuo particular que puede entrar en el sistema, un grupo es un conjunto de usuarios con acceso al sistema que comparten unas mismas características, de forma que nos es útil agruparlos para poder darles una serie de permisos especiales en el sistema. Un usuario debe pertenecer, al menos, a un grupo, aunque puede ser de más de uno. El sistema también utiliza todo este mecanismo de usuarios y grupos para gestionar los servidores de aplicaciones instalados y otros mecanismos. Por esta razón, además de los usuarios reales, en un sistema habrá muchos otros vinculados a otras tareas que se deben realizar en el operativo. Generalmente, este tipo de usuario no podrá entrar (con un *login* normal) al sistema.

En todo sistema operativo debe haber un superusuario (*root*). Éste será el usuario que contará con todos los permisos, el que tendrá los privilegios máximos que le permitirán efectuar cualquier operación sobre el sistema. Es necesario que éste exista, ya que será quien se encargará de toda la administración y gestión de

servidores, grupos, etc. Esta cuenta no debe utilizarse para trabajar normalmente en el sistema. Sólo deberíamos entrar como *root* cuando sea realmente necesario, utilizando otras cuentas para el trabajo normal de los usuarios. De este modo nunca podremos dañar el sistema con operaciones erróneas o con la prueba de programas maliciosos, etc.

Toda la información de usuarios y grupos se guarda en los siguientes archivos:

- `/etc/passwd`: información (nombre, directorio *home*, . . .) del usuario.
- `/etc/group`: información sobre los grupos de usuarios.
- `/etc/shadow`: contraseñas cifradas de los usuarios y configuración para su validez, cambio, etc.

Utilizar el archivo de `shadow` es opcional. En un principio, las contraseñas cifradas de los usuarios se guardaban en el mismo fichero de `passwd`, pero, por razones de seguridad (muchos mecanismos deben poder leer este fichero, con lo cual era muy fácil hacerse con él e intentar "crackear" las contraseñas) se optó por cambiar este mecanismo para hacer que el fichero de `shadow` sólo fuera accesible para algunos usuarios con privilegios especiales en el sistema. Esta opción es configurable en el proceso de instalación del sistema y suele ser recomendable utilizarla. Todos estos ficheros están organizados por líneas, donde cada una de ellas identifica a un usuario o grupo (dependiendo del fichero). En cada línea hay diversos campos separados por el carácter ":". En tareas de administración, es importante saber qué son estos campos, por lo que vamos a explorarlos con un poco más de detalle:

- passwd

1) *Login*: el nombre del usuario. No puede haber dos nombres iguales, aunque sí alguno que coincida con un grupo del sistema.

2) *Contraseña cifrada*: si no se utiliza el fichero de `shadow`, las contraseñas cifradas se almacenan en este campo. Si utilizamos el fichero de `shadow`, todos los usuarios existentes en este fichero deben existir también en el de `shadow` y en este campo se pone el carácter "`x`".

3) *User* ID: número de identificación del usuario. Es el número con el cual el sistema identifica al usuario. El 0 es el único que está reservado para el *root.*

4) *Group* ID: el número de grupo al cual pertenece el usuario. Como un usuario puede pertenecer a más de un grupo, este grupo se denomina *primario*.

5) Comentarios: campo reservado para introducir los comentarios que queramos sobre el usuario. Se suele utilizar para poner el nombre completo o algún tipo de identificación personal.

6) Directorio *home*: el directorio *home* del usuario es donde éste podrá guardar todos sus ficheros. Suelen ponerse todos en alguna carpeta del sistema (generalmente `/home/)` y organizados por grupos.

7) *Intérprete de comandos*: un intérprete de comandos (*shell*) es un programa que se encarga de leer todo lo que escribimos en el teclado y ejecutar los programas o comandos que le indiquemos. Hay decenas de ellos, aunque el más utilizado es, sin duda, el bash (*GNU Bourne-Again SHell*). Si en este campo escribimos `/bin/false` no permitiremos que el usuario ejecute ningún comando en el sistema, aunque esté dado de alta en el mismo.

• group

1) Nombre del grupo.

2) Contraseña cifrada: la contraseña de un grupo se utiliza para permitir que los usuarios de un determinado grupo se puedan cambiar a otro o para ejecutar algunos programas con permisos de otro grupo (siempre que se disponga de la contraseña).

3) *Group* ID: número de identificación del grupo. Es el número con el cual el sistema identifica internamente a los grupos. El 0 es el único que está reservado para el grupo del *root* (los administradores).

4) Lista de usuarios: los nombres de los usuarios que pertenecen al grupo, separados por comas. Aunque todos los usuarios deben pertenecer a un determinado grupo (especificado en el cuarto campo del fichero de `passwd`), este campo se puede utilizar para que usuarios de otros grupos también dispongan de los mismos permisos que tiene el que se está referenciando.

• shadow

1) *Login*: debe ser el mismo nombre que se utiliza en el fichero de `passwd`.

2) Contraseña cifrada.

3) Días que han pasado, desde el 1 de enero de 1970, hasta que la contraseña ha sido cambiada por última vez.

4) Días que deben pasar hasta que la contraseña pueda ser cambiada.

5) Días que han de pasar hasta que la contraseña deba ser cambiada.

6) Días antes de caducar la contraseña en el que se avisará al usuario de que debe cambiarla.

7) Días que pueden pasar después de que la contraseña caduque, antes de deshabilitar la cuenta del usuario (si no se cambia la contraseña).

8) Días, desde el 1 de enero de 1970, desde que la cuenta está deshabilitada.

9) Campo reservado.

Cuando un usuario entra en el sistema, se le sitúa en su directorio *home* y se ejecuta el intérprete de comandos (*shell*) configurado. De este modo ya puede empezar a trabajar. Sólo el *root* del sistema (o los usuarios de su grupo) tienen permiso para manipular la información de los usuarios y grupos, darlos de alta, de baja, etc. Existen muchos comandos para manipular todo esto. Cada uno de ellos tiene, además, varios parámetros diferentes para gestionar todos los campos que hemos visto anteriormente de forma amena. A continuación mostramos algunos de estos comandos:

- `adduser`: nos sirve para añadir un nuevo usuario al sistema. La forma como éste se añade (si no le especificamos nada) se puede configurar en el fichero `/etc/adduser.conf`. Se le pueden pasar multitud de opciones diferentes para especificar el directorio home, el shell que hay que utilizar, etc.
- `useradd`: crea un nuevo usuario o cambia la configuración por defecto de los mismos. Este comando y el anterior nos pueden servir para realizar las mismas acciones.
- `usermod`: con este comando podemos modificar la mayoría de los campos que se encuentran en el fichero de `passwd` y `shadow`, como el directorio *home*, el *shell*, la expiración de la contraseña, etc.
- `chfn`: cambia la información personal del usuario, contenida en el campo de comentarios del fichero de `passwd`.
- `chsh`: cambia el s*hell* del usuario.
- `deluser`: elimina un usuario del sistema, borrando o guardando todos sus ficheros según los parámetros que le pasemos, haciendo copia de seguridad de los mismos o no, etc. La configuración que se utilizará por defecto con este comando está especificada en el fichero `/etc/deluser.conf`.
- `userdel`: comando con las mismas posibilidades que el anterior.
- `passwd`: nos sirve para cambiar la contraseña de un usuario, la información de expiración de las mismas o para bloquear o desbloquear una determinada cuenta.
- `addgroup`: permite añadir un grupo al sistema.
- `groupadd`: lo mismo que el comando anterior, pero con diferentes parámetros.
- `groupmod`: nos permite modificar la información (nombre y GID) de un determinado grupo.
- `delgroup`: elimina un determinado grupo. Si algún usuario todavía lo tiene como primario, no se podrá eliminar.
- `groupdel`: igual que en el caso anterior.
- `gpasswd`: nos sirve para cambiar la contraseña del grupo.

Para saber qué usuario somos, podemos utilizar el comando `whoami`, que nos mostrará nuestro *login*. `groups` nos sirve para saber a qué grupos pertenecemos e `id` nos mostrará usuario y grupos. También es interesante poder convertirnos en otro usuario sin tener que salir de la sesión (comando `login` o `su`) o cambiarnos de grupo con el comando `newgrp`. Este último comando debemos utilizarlo sólo cuando no pertenecemos al grupo en cuestión y sabemos su contraseña (que debe estar activada en el fichero de `group`). Si sólo necesitamos los permisos del grupo en cuestión para ejecutar un determinado comando, también podemos utilizar `sg`.

Tal como decíamos anteriormente, GNU/Linux es un sistema operativo multiusuario, por lo que en un mismo momento puede haber varios usuarios conectados al sistema de forma simultánea. Para saber qué usuarios hay en un determinado momento, podemos utilizar el comando `who`, que nos muestra la lista de usuarios dentro

del sistema. `w`, además, nos muestra qué es lo que están haciendo. Nos podemos comunicar con ellos utilizando el comando `write`, con el cual aparece el mensaje que hayamos escrito en la pantalla del usuario indicada o `wall`, que escribe el contenido del fichero que hayamos especificado a todos los usuarios dentro del sistema. Para activar o desactivar la opción de recibir mensajes tenemos el comando `mesg`. También podemos hacer un *chat* personal con algún usuario a partir del comando `talk`.