5.1 Gestión de usuarios

Desde el punto de vista del sistema, un *usuario* es cualquier entidad que puede ejecutar programas o poseer recursos. Ej. Sistema de accounting, pseudo usuarios (poseen un conjunto de ficheros del sistema y ejecutan los procesos requeridos en un determinado subsistema)

? Cada usuario tiene un *username* que lo identifica

? Cuando se añade un usuario, el *administrador* le asigna un número de identificación de usuario (*uid*) ? la credencial del usuario en el sistema

? Cuando se da de alta a un usuario, el administrador lo incluye en 1 o más *grupos* ? Cada grupo se identifica con un *gid*

5.2 Base de datos de usuarios

Los usuarios de un sistema Unix son registrados en un fichero ASCII denominado **/etc/password**

• Tiene permisos de lectura por parte de todos los usuarios pues parte de la información se necesita conocer por parte de los usuarios. Ej. "ls"

• Aunque la clave se encuentra cifrada, ("*crypt*") ? Plantea un problema de seguridad (ataques de diccionario)

• Cada línea corresponde a un usuario y describe los atributos del mismo.

• Cada atributo está separado por ":".

Ejemplo:

usu1:$3tr56n/sdfg233456GY$&aGpLb2YGhqCK1:501:200:Usuario1:/home/usu1:/bin/bash

Elemento	Significado
usu1	Nombre de usuario (sensible mayúsculas)
:$3tr56n/sdfg233456GY$&aGpLb2YGhqCK1	Contraseña cifrada
501	Identificador de usuario (UID)
200	Identificador primario de grupo al que pertenece el usuario (GID)
Usuario 1	Descripción del usuario (hasta 30 caracteres)
/home/usu1	Directorio de conexión inicial del usuario
/bin/bash	Shell de arranque

5.3 Extensión de la base de datos de usuarios

En la mayoría de los sistemas Unix actuales se utiliza otra tablea ? ***/etc/shadow***

- Se almacena información complementaria del usuario a la almacenada en /etc/passwd
- Tiene permisos de sólo lectura por parte del superusuario "*root*" ? soluciona el problema de accesos por parte del usuario
- Cada línea de este fichero se corresponde con una línea del fichero /etc/passwd.
- Añade plazos de mantenimiento y cambio de contraseñas
- Los campos se encuentran separados por ":"

Ejemplo:

La entrada correspondiente a la entrada de usu1 en /etc/passwd podría ser:

usu1:$3tr56n/sdfg233456GY$&aGpLb2YGhqCK1:10989:0:99999:7:-1:-1:134538436

El significado de cada campo es el siguiente:

• Nombre de usuario. Coincide con la entrada correspondiente en /etc/passwd

• Password cifrado. Una entrada en blanco (::) significa que no se requiere contraseña (no aconsejable). Un "*" (:*:) indica que la cuenta está deshabilitada.

• Número de días (desde el 1 de Enero de 1970) desde la última modificación de la contraseña

• *Días mínimos:* Número de días que deben transcurrir para volver a cambiar el password (0 indica que puede ser cambiado inmediatamente)

• *Días máximos*: Número de días que pueden transcurrir sin cambiar la contraseña

• *Días de aviso*: Número de días que se ha de avisar la caducidad de la contraseña

• *Días de inactividad*: La cuenta será desactivada si no se usa durante este número de días.

• Número de días desde el 1 de Enero de 1970 que una cuenta ha estado deshabilitada

• Campo reservado para uso en el futuro.

Cuando el sistema emplea esta tabla, la contraseña almacenada en */etc/passwd* se sustituye por una "*x*".

Puesto que el formato de los campos de caducidad viene expresado en días, es recomendable que para modificar esta información no se haga de forma directa, sino utilizando herramientas administrativas específicas.

Los comandos *pwconv, pwuncov, grpconv y grpuncov* se pueden utilizar para sincronizar ficheros *passwd* y *shadow*.

• Es aconsejable comprobar la integridad de los ficheros antes de ejecutar las aplicaciones anteriores "*pwck*" ? Posible duplicidad de entradas, formatos erróneos,...

5.4 Base de datos de grupos

Los grupos de un sistema Unix son registrados en el fichero /etc/group

Cada línea de este fichero corresponde a un grupo y describe los atributos del mismo.

Los atributos están separados por "*:*".

Ejemplo:

grupo1:f$frjt56RX6l0lhfGFbftRcg/sdf:501:usu1,usu2,usu3

Elemento	**Significado**
grupo1	Nombre del grupo
f$frjt56RX6l0lhfGFbftRcg/sdf	Contraseña cifrada. Permite a un usuario cambiar de grupo primario si se conoce esta contraseña
usu1,usu2,usu3	Lista de usuarios que pertenecen a este grupo

• Un usuario puede aparecer en la lista de varios grupos

• Aquel grupo cuyo GID aparece en la entrada correspondiente de */etc/passwd* se considera **grupo primario**.

• El resto de grupos se denominan **grupos suplementarios**

Comando gpasswd:

• Permite al administrador del sistema nombrar un administrador de grupo

• Le delega las altas y las bajas en el grupo, así como una contraseña para los visitantes

5.5 Comandos para la gestión de usuarios y grupos

En la mayoría de los sistemas Unix System V pueden utilizarse los siguientes comandos:

Comando	Uso
useradd	Añadir un usuario
userdel	Eliminar un usuario
usermod	Modificar los atributos de un usuario
groupadd	Añadir un grupo
groupdel	Eliminar un grupo
groupmod	Modificar los atributos de un grupo
passwd	Cambiar la contraseña de un usuario
chage	Gestionar la caducidad de la contraseáste grupo

Especialmente útiles para automatizar la gestión de usuarios mediante scripts

También existen herramientas gráficas que facilitan la labor del administrador (Ej. . *Linuxconf*)

5.6 Desactivación de cuentas de usuarios

• Es preferible desactivar las cuentas antes que eliminarlas (por lo menos, temporalmente)

• No reutilizar los UID’s (por lo menos durante 1 año ? por si hay que volver a darlo de alta)

- Anteponer un carácter “*” al campo password (no puede ser generado por el algoritmo de cifrado)
- Caducidad de la contraseña
- Cambiar el shell predeterminado a /bin/false ó a algún fichero ejecutable (no un script) que haga al final un exit.
- Eliminar tareas cron y at del usuario así como los procesos que esté ejecutando
- Hacer copia de seguridad del directorio home.

5.7 Protección

5.7.1 Protección de los procesos

Los atributos de protección son asignados al proceso en el momento de su creación.

Se heredan del proceso padre ? *shell*

5.7.1.1 Identificadores del usuario propietario del proceso

• *Identificador real de usuario (rUID):* Corresponde al usuario que creo el proceso.

• *Identificador efectivo de usuario (eUID):* Es el usuario que se utiliza en el mecanismo de protección.

Ambos identificadores suelen ser iguales salvo que se utilice el bit SETUID en el fichero ejecutable

5.7.1.2 Identificadores del grupo propietario del proceso

• *Identificador real de grupo (rGID):* Corresponde al grupo primario al que pertenece el usuario

• *Identificador efectivo de grupo (eGID):* Es el grupo que se utiliza en el mecanismo de protección.

Ambos identificadores suelen ser iguales salvo que se utilice el bit SETUID en el fichero ejecutable.

5.7.1.3 Lista de grupos suplementarios

Lista con los grupos suplementarios del usuario que creó el proceso

Los atributos rUID y rGID se extraen de */etc/passwd*

La lista de grupos suplementarios se extrae de */etc/group*

5.7.2 Protección de los ficheros

Los atributos de ficheros que intervienen en el mecanismo de protección son:

5.7.2.1 OwnerUID

Identificador del usuario propietario del fichero. Comando *chown*

5.7.2.2 OwnerGID

Identificador del grupo propietario del fichero. Comando *chgrp*

5.7.2.3 Bits de permisos

12 bits que fijan las operaciones permitidas sobre el fichero en función del proceso que acceda al mismo

Bit	Significado
11	SEUID
10	SETGID
9	Sticky
8	Lectura para el propietario
7	Escritura para el propietario
6	Ejecución para el propietario
5	Lectura para el grupo propietario
4	Escritura para el grupo propietario
3	Ejecución para el grupo propietario
2	Lectura para el resto de usuarios
1	Escritura para el resto de usuarios
0	Ejecución para el resto de usuarios

Directorios:

Lectura: Puede listarse el contenido del directorio

Escritura: Permite la creación, eliminación o renombrado de ficheros o directorios

Ejecución: Permite utilizar el directorio para formar parte de un nombre de ruta o para realizar un "*cd <directorio>*"

• No existe ningún bit de borrado ? Se controla con los permisos del directorio

• En algunos sistemas, el bit *sticky* se utiliza para modificar la regla de eliminación de ficheros: Un directorio con el bit *sticky* activo, un usuario puede borrar un fichero sólo si es el propietario de dicho fichero.

5.7.2.4 Cambio de atributos de protección

• Bits de permisos: Un proceso puede cambiar los bits de permisos de un fichero si:

  • el eUID del proceso es 0 (Superusuario)

  • el eUID del proceso = ownerID del fichero

• Propietario:

  • Sólo el superusuario

• Cambio de grupo propietario

  • Superusuario

  • El usuario es el propietario del fichero y el nuevo grupo es igual a alguno de los grupos del usuario

5.7.3 Reglas de protección básicas

Cuando un proceso notifica al sistema que desea utilizar un determinado fichero, también notifica la operación que desea realizar: lectura, escritura, ejecución.

• Si eUID = 0 ? Se concede el permiso (superusuario)

• Si eUID = ownerID del fichero ? Se controla la operación en función del valor de los bits 6-8.

• Si eGID del proceso o alguno de los grupos suplementarios del proceso = ownerGID del fichero ? Se controla la operación en función del valor de los bits 3-5.

• En otro caso, se controla la operación en función del valor de los bits 0-2

5.7.4 Bits SETUID y SETGID en ficheros ejecutables

Permiten que un programa se ejecute bajo los privilegios de usuario distinto al que lo ejecuta.

Normalmente estos programas pertenecen al superusuario (Ej. Passwd)

La existencia de estos ficheros debe estar controlada ? agujeros de seguridad

- Si el fichero ejecutable tiene el bit SETUID ? eUID del proceso que ejecuta = ownerID del fichero
- Si el fichero ejecutable tiene el bit SETGID ? eGID del proceso que ejecuta = ownerGID del fichero

5.7.5 Bit SETGID en directorios

La utilización de este bit está orientada a facilitar el trabajo en grupo ? compartición de ficheros y directorios. Si un directorio D tiene el bit SETGID:

- Si se crea un fichero dentro de D ? ownerGID del fichero = ownerGID de D
- Si se crea un directorio dentro de D ? ownerGID del directorio = ownerGID de D y el bit SETGID activo.

  De esta forma, aunque varios usuarios creen ficheros dentro de un directorio, todos ellos pertenecerán al menos al mismo grupo ? una utilización adecuada de los bits de permisos puede hacer que todos ellos puedan compartir ficheros.

5.7.6 Estrategia de grupos privados

Se emplea por defecto en RedHat.

- Se crea un grupo por cada usuario (mismo nombre que el usuario) y se hace que éste sea el grupo primario del usuario.
- Se usan los grupos suplementarios para agrupar usuarios
- Se utiliza el bit SETGID y un grupo suplementario para compartir directorios
- Se utiliza el grupo privado en los directorios HOME
- Se asigna como máscara por defecto 00X

5.8 Control del uso de disco con cuotas.

La escasez de espacio de disco es un problema común en todos los sistemas ? Algunos sistemas Unix permiten limitar el espacio que cada usuario utiliza: **"cuotas"**.

• Cuando se habilitan las cuotas, el sistema mantiene información para cada usuario de la cantidad de disco y el número de inodos utilizados.

• Las cuotas se establecen por sistema de fichero

• Dos tipos de cuotas:

  • *Límite duro:* No se puede sobrepasar bajo ninguna circunstancia. Cuando se alcanza este límite, el sistema muestra un mensaje y rechaza la operación.

  • *Límite blando:* El usuario puede sobrepasar este límite durante un periodo de tiempo limitado. La operación se realiza, pero el usuario recibe un mensaje de aviso cada vez que entra en el sistema hasta que:

    • Reduce la utilización de disco por debajo de este límite

    • Expira el tiempo de gracia ? Necesita reducir el espacio ocupado

• Para habilitar las cuotas, es necesario considerar lo siguiente:

  • Asegurarse que el Kernel las soporta (compilado con esa opción)

  • Indicar que el sistema de ficheros tiene cuotas (opción usrquota en /etc/fstab)

  • Ficheros quota.user y quota.group en el "/" del sistema de ficheros

• Comandos relacionados:

  • quota, (información de cuota del usuario)

  • edquota, (edición de las cuotas de usuarios y grupos)

  • quotacheck, (chequea el sistema de ficheros para observar el uso de disco)

  • repquota, (genera un informe de las cuotas en un sistema de ficheros)

  • quotaon, quotaoff (activar y desactivar el sistema de cuotas)