Gestión de usuarios y grupos

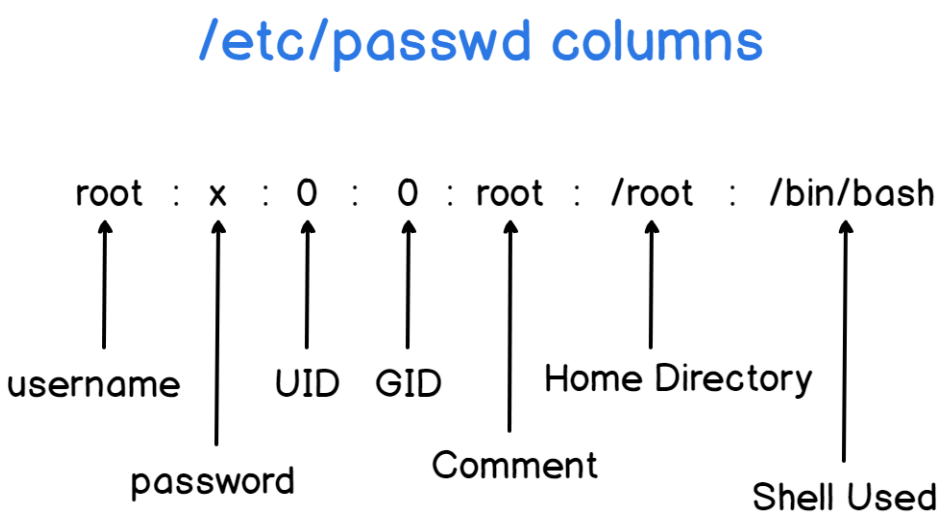
Gestión de usuarios y procesos

Introducción

- Todo sistema operativo ha de ofrecer soporte para que los usuarios puedan hacer uso del sistema de forma segura, con privacidad y con las herramientas necesarias para gestionar usuarios.
- Los usuarios administradores se encargan de la supervisión y gestión de los procesos del sistema.
- La gestión de usuarios determina en gran medida la seguridad del sistema.
- Los sistemas GNU/Linux gestionan los usuarios mediante archivos de configuración. Para poder acceder a estos archivos hay el usuario debe tener permisos de administrador.
- En algunos casos la edición de estos archivos puede ser directa, mientras que en otros resulta recomendable que la modificación se haga a través de comandos, evitando así errores.

Configuración de usuarios y grupos

- Los usuarios y grupos se gestionan a través de los archivos **/etc/passwd** y **/etc/group**, principalmente.
- El fichero **/etc/passwd** almacena las cuentas de los usuarios del sistema. Cada fila es un usuario que consta de siete campos separados por ":"



Campos de /etc/passwd

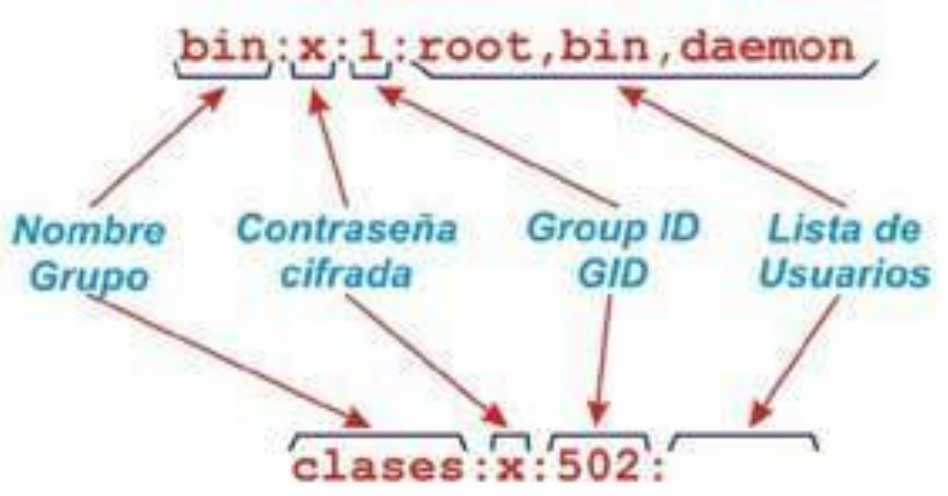
- **Login** de usuario: nombre que se emplea para acceder al sistema
- **Password**: aparece una "x" indicando que la contraseña se encuentra encriptada en el fichero de configuración /etc/shadow
- **UID**: número de identificación del usuario único.
- **GID**: número de identificación del grupo principal del usuario
- **Comment**: Se suele incluir información personal del usuario
- **Home**: directorio inicial del usuario
- **Shell**: intérprete de comandos empelado por el usuario cuando inicia el sistema.

Configuración de usuarios y grupos

- Por usuario administrador entendemos aquel que tiene capacidad de gestión en el sistema, sin ser necesariamente el superusuario (root). Esta capacidad se habilita utilizando el comando **sudo**.
- Los **grupos** en Linux son muy empleados, ya que facilitan la administración de privilegios en el sistema. Se emplean cuando se desea que algunos ususarios tengan permisso sobre archivos o carpetas sin ser los propietarios de los mismos.
- Los grupos se configuran en el fichero **/etc/group**

Campos de /etc/group

- **Nombre** del grupo.
- **Contraseña**: no se suele utilizar, si aparece una "x" indica que la contraseña está encriptada en el fichero **/etc/gshadow**



- **GID**: identificador único del grupo
- **Lista de usuarios**: usuarios pertenecientes al grupo. Un usuario puede pertenecer a varios grupos

Creación de usuarios - useradd

useradd [-g <grupo>] [-G <grupo>[,<grupo> ...]] [-d <home_dir>] [-m] [-p <contraseña>] [-s <shell>] <login>

Opción	Descripción	Ejemplo
-g <grupo>	Asignación del grupo principal del usuario. En caso de no especificar esta opción, se creará un grupo con el nombre del usuario	useradd –g alumnos alumno
-G <grupos>	Lista de grupos secundarios separados por comas y sin espacios	useradd –G grupo1,grupo2 alumno
-d <dir>	Establece el directorio de trabajo del usuario. Si no se especifica el directorio de trabajo será /home/<login>	useradd –d /home/otro alumno
-m	Crea el directorio de trabajo si no existe	useradd -m alumno
-p <password>	Contraseña encripatada del usuario, si no se especifica el usuario no podra hacer login.	useradd –p j.8UTsa0lxF0U alumno
-s <shell>	Establece el intérprete de comandos del usuario. Por defecto emplea /bin/bash	useradd –s /bin/s alumno

Modificación de usuarios - usermod

usermod [-g <grupo>] [-G <grupo>[,<grupo> ...]] [-d <home_dir>] [-m] [-p <contraseña>] [-s <shell>] [-c <comentario>] [-e <fecha>] [-f <dias>] [-l <nuevo_login>] [-L] [-U] <login>

Opción	Descripción	Ejemplo
-c <comentario>	Establece valores asociados al quinto campo del fichero /etc/passwd	usermod –c "Alguna info" alumno
-e <fecha>	Establece la fecha de expiración de la cuenta	usermod –e 2021-01-31 alumno
-f <dias>	Establece los días tras los cuales el password quedará inactivo	usermod –f 100 alumno
-l <nuevo_login>	Modifica el login del usuario	usermod –l alumno2 alumno
-L	Bloquea una cuenta de usuario	usermod –L alumno
-U	Desbloquea una cuenta de usuario	usermod –U alumno

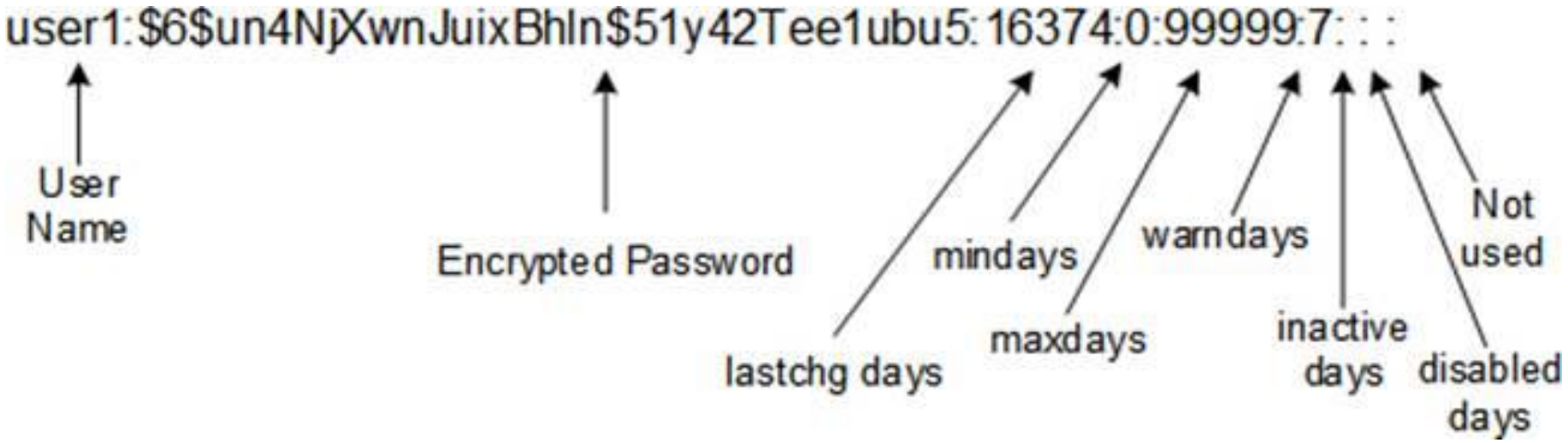
Eliminación de usuarios - userdel

userdel [-r] <login>

- Elimina el usuario del sistema
- Si se incluye la opción -r, se elimina la carpeta de usuario asociada

Seguridad de usuarios y contraseñas

- Linux emplea un sistema centralizado de autenticación de usuarios llamado **Linux-PAM**.
- Como ya hemos visto, la seguridad de usuarios se basa en contraseñas, las cuales se almacenan en /**etc/shadow**. Cada fila en este fichero se corresponde con un usuario.



Almacenamiento de contraseñas

- Las contraseñas se almacenan después de haberles aplicado una función de **hashing criptográfico** que generan una cadena de tamaño fijo.
- Almacenar las contraseñas en texto plano supondría un gran agujero de seguridad ya que, de ser así, cualquier usuario administrador podría ver las contraseñas de otros usuarios quedando estos completamente expuestos.
- Teóricamente, el proceso de digestión de las contraseñas utilizando un algoritmo de hashing criptográfico es **irreversible** matemáticamente. Esto quiere decir que no hay un método matemático que pueda revertir el proceso en un tiempo razonable.
- Sin embargo, es posible crackear una contraseña a través de los denominados **ataques de diccionario**, que prueban la generación de hashes con palabras comunes de un diccionario hasta que encuentran una que coincida.

Almacenamiento de contraseñas

- Existen bases de datos con hashes precalculados para millones de contraseñas, gracias a esto es posible crackear muchas contraseñas casi instantáneamente.
- Para paliar este problema, es fundamental realizar modificaciones aleatorias a las contraseñas antes de aplicarles el algoritmo criptográfico, de forma que los atacantes se vean obligados a recomputar los hashes aplicando esta modificación a todas las combinaciones. Este proceso modificación de la contraseña se denomina **salting**.
- A cada contraseña se le aplica una modificación diferente generando un valor aleatorio que es almacenado junto con el hash de la contraseña

Almacenamiento de contraseñas

- El campo de la contraseña se divide en tres partes separadas por el símbolo $: **$id$salt$hashed**
- El primer campo de la contraseña identifica el algoritmo de hashing criptográfico que se ha utilizado:
  - **1:** MD5 (hash de 128 bits)
  - **$2a$** y **$2y$**: Blowfish
  - **5**: SHA-256 (hash de 256 bits)
  - **6:** SHA-512 (hash de 512 bits)
- El segundo campo es el valor de la salt aplicada a la contraseña antes de hashearla (hash SALT + PASSWORD)
- Por último, tenemos el hash resultante de aplicar el salting y el hashing a la contraseña

Almacenamiento de contraseñas

- Gracias al salting, conseguimos que los atacantes se vean obligados a recomputar todas las combinaciones de palabras añadiéndoles el salt, lo que implica una gran cantidad de recursos computacionales.
- Sin embargo, sigue siendo posible crackear un password aunque se le haya aplicado un salting si el atacante dispone de los recursos computacionales necesarios.
- Para evitar esta posibilidad se deben utilizar contraseñas de tipo passphrase, es decir una frase codificada con caracteres especiales. Por ejemplo: "$0yM1k3!ElPr0f3"

Administración de grupos

groupadd [-g <GID>] <nombre_grupo>

groupmod [-g <GID>] [-n <nuevo_nombre>] <nombre_grupo>

groupdel <nombre_grupo>

Opción	Descripción	Ejemplo
-g <GID>	Asigna un identificador del grupo. El valor debe ser superior a 1000 y debe ser único por grupo	groupadd –g 1001 alumnos
-n <nuevo_nombre>	Lista de grupos secundarios separados por comas y sin espacios	groupmod –n alumnos2 alumnos

groups <login>

adduser <login> <grupo>

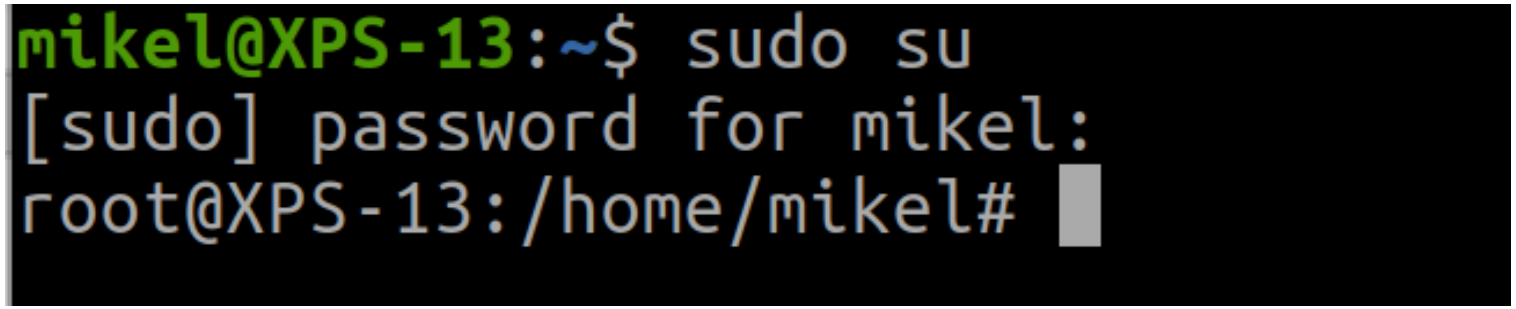
deluser <login> <grupo>

Grupos predeterminados

Grupo	Descripción
adm	Grupo de administración que permite accesos a logs del sistema y comandos como **sudo** y **su**
users	Grupo de usuarios estándar
nobody	Sin privilegios
root	Administración sin restricciones sobre todo el sistema
tty	Aporta privilegios sobre algunos dispositivos, como /dev/tty
lpadmin	Confiere privilegios sobre dispositivos de puerto paralelo
sudo	Grupo de usuarios que pueden hacer sudo

Usuarios administradores

- Existe un usuario administrador conocido como superusuario y cuyo login es **root**.
- Es un usuario de especial relevancia por su capacidad de administración.
- Si un usuario es administrador puede convertirse en root ejecutando el comando **sudo su**



Usuarios administradores

- La contraseña del usuario root se encuentra bloqueada por defecto, por lo que no se puede hacer login directamente con este usuario.
- Para que otros usuarios tengan permisos de administración deben estar configurados en el fichero **/etc/sudoers**
- Un usuario puede ejecutar comandos con permisos de administración poniendo **sudo** antes del comando.
- También es posible ejecutar comandos en nombre de otros usuarios: **sudo –u <otro_usuario> <comando>**

Usuarios administradores

- El superusuario puede editar el fichero /etc/passwd, modificar valores de campos, eliminar filas... El campo de la contraseña, al estar encriptada, se debe modificar usando el comando **passwd**
- Es posible cambiar de un usuario a otro ejecutando el comando **su - <otro_usuario>**
- Para hacer que un usuario sea administrador basta con añadirlo al grupo sudo ejecutando el comando

sudo useradd <login> sudo

Otros comandos

Comando	Descripción	Uso
who	Muestra los usuarios conectados al sistema	**am i**: muestra al usuario actual **-u**: muestra información de los usuarios conectados **-H**: imprime cabeceras **-q**: muestra solamente los logins y el número de usuarios conectados
passwd	Permite modificar la contraseña de un usuario.	passwd <usuario>
openssl passwd	Herramienta criptográfica que permite generar contraseñas hash encriptadas	openssl passwd [opcion] <contraseña_a_encriptar> Opciones: **-1**: Se genera usando el algoritmo MD5 **-2**: Se genera usando el algoritmo SHA-256 **-3**: Se genera usando el algoritmo SHA-512
chage	Permite establecer políticas de caducidad de las contraseñas de los usuarios	chage [opciones] <login> **-d**: establece la fecha cuando la contraseña fue modificada **-E**: establece la fecha de expiración de la contraseña **-I**: número de días que la cuenta permanece inactiva después de la expiración del password, una vez superado se bloquea la cuenta.