Tutorial Básico de Administración de Usuarios en Linux

1. **Introducción**

¿Qué es un usuario en Linux?
Un usuario en Linux es una cuenta que permite a una persona o proceso acceder al sistema operativo con permisos y configuraciones específicas. Cada usuario tiene un nombre de usuario, un identificador único (UID), un directorio personal y ciertos privilegios dentro del sistema.

Diferencias entre usuario y root:

- Usuario normal: Tiene permisos restringidos, lo que evita que pueda modificar archivos críticos del sistema. Solo puede acceder y modificar sus propios archivos y aquellos para los que tenga permisos explícitos.
- Usuario root: Es el administrador del sistema y tiene acceso total a todos los archivos y configuraciones. Puede instalar programas, cambiar permisos, modificar configuraciones del sistema y realizar cualquier acción sin restricciones.

¿Por qué es necesario usar usuarios en Linux?

- Seguridad: Restringir el acceso a archivos y procesos críticos evita que los usuarios normales dañen accidentalmente el sistema.
- Organización: Cada usuario tiene su propio entorno, archivos y configuraciones personales.
- Control de permisos: Se pueden asignar permisos específicos a distintos usuarios o grupos para definir qué acciones pueden realizar.
- Protección contra amenazas: Usar cuentas sin privilegios reduce el riesgo de ejecutar malware con acceso total al sistema.

---

2. Comandos de Administración de Usuarios

2.1 Creación y Eliminación de Usuarios

- adduser [usuario] : Crea un nuevo usuario y su directorio personal.
- useradd [usuario] : Crea un nuevo usuario (sin directorio personal por defecto).
- passwd [usuario] : Cambia la contraseña de un usuario.
- deluser [usuario] : Elimina un usuario y su directorio personal.
- userdel [usuario] : Elimina un usuario (sin eliminar su directorio personal por defecto).

2.2 Gestión de Grupos

- groupadd [grupo] : Crea un nuevo grupo.
- groupdel [grupo] : Elimina un grupo.
- usermod -aG [grupo] [usuario] : Agrega un usuario a un grupo.
- gpasswd -d [usuario] [grupo] : Elimina un usuario de un grupo.

2.3 Modificación de Usuarios

- usermod -l [nuevo_nombre] [usuario] : Cambia el nombre de un usuario.
- usermod -d [nuevo_directorio] [usuario] : Cambia el directorio personal de un usuario.
- usermod -L [usuario] : Bloquea una cuenta de usuario.
- usermod -U [usuario] : Desbloquea una cuenta de usuario.

2.4 Información de Usuarios

- id [usuario] : Muestra el UID, GID y grupos de un usuario.
- who : Muestra los usuarios actualmente conectados.
- w : Muestra los usuarios conectados y su actividad.
- last : Muestra el historial de inicios de sesión.

3. Comandos básicos de permisos y privilegios

1. **Ver permisos de archivos y directorios:**

ls -l

Muestra los permisos en formato rwx para usuario, grupo y otros.

2. **Cambiar permisos de archivos o directorios:**

chmod 755 archivo.txt

Permite lectura/escritura/ejecución para el propietario, y solo lectura/ejecución para otros.

3. **Cambiar propietario de un archivo o directorio:**

chown usuario:grupo archivo.txt

Modifica el propietario y grupo de un archivo.

4. **Cambiar grupo de un archivo o directorio:**

chgrp grupo archivo.txt

Cambia solo el grupo propietario del archivo.

5. **Dar permisos especiales (SUID, SGID, Sticky Bit):**
6. chmod u+s archivo # SUID: el archivo se ejecuta con permisos del propietario
7. chmod g+s directorio # SGID: los archivos creados en este directorio heredan el grupo

chmod +t directorio # Sticky Bit: evita que usuarios eliminen archivos de otros

---

4. Comandos avanzados con chage

El comando chage permite **administrar la caducidad y políticas de contraseñas** de usuarios.

1. **Ver información sobre la caducidad de una cuenta:**

chage -l usuario

Muestra la configuración actual de vencimiento de la cuenta.

2. **Forzar el cambio de contraseña en el próximo inicio de sesión:**

chage -d 0 usuario

Obliga al usuario a cambiar su contraseña al iniciar sesión.

3. **Definir una fecha de expiración para la cuenta:**

chage -E 2025-12-31 usuario

La cuenta del usuario expirará en la fecha indicada.

4. **Configurar la caducidad de la contraseña en X días:**

chage -M 90 usuario

Obliga al usuario a cambiar su contraseña cada 90 días.

5. **Definir días de advertencia antes del vencimiento de la contraseña:**

chage -W 7 usuario

El usuario recibirá una advertencia 7 días antes de que su contraseña expire.

6. **Bloquear una cuenta después de X días sin cambiar la contraseña:**

chage -I 30 usuario

Si la contraseña expira y pasan 30 días sin cambiarla, la cuenta se desactiva.