Sistemas informáticos. Gestión de usuarios y procesos.

# Actividades propuestas

4.1.- Muestra el contenido del fichero /etc/passwd, mediante cat /etc/passwd. Analiza los campos de cada fila.

Texto

Descripción generada automáticamente

El archivo /etc/passwd es un archivo de texto plano que se utiliza para almacenar información sobre las cuentas de usuario en un sistema operativo Unix o Linux. Cada línea en el archivo representa una cuenta de usuario y contiene siete campos separados por dos puntos (:). Los campos son los siguientes:

* Nombre de usuario (username): Es el nombre que utiliza el usuario para iniciar sesión en el sistema.
* Contraseña (password): Aunque el archivo /etc/passwd almacena contraseñas, en la mayoría de los sistemas modernos, las contraseñas se almacenan en el archivo /etc/shadow para aumentar la seguridad. La entrada de la contraseña en el archivo /etc/passwd se muestra como una cadena de caracteres aleatorios.
* UID (User ID): Es el identificador numérico del usuario en el sistema. Este número es utilizado por el sistema para identificar de forma única al usuario.
* GID (Group ID): Es el identificador numérico del grupo principal al que pertenece el usuario.
* Comentario (comment): Es un campo opcional que se utiliza para proporcionar información adicional sobre la cuenta de usuario.
* Directorio de inicio (home directory): Es el directorio inicial que se asigna al usuario cuando inicia sesión en el sistema.
* Shell de inicio (login shell): Es la shell que se utiliza por defecto cuando el usuario inicia sesión en el sistema.

4.2.- Muestra el contenido del fichero /etc/group, mediante cat /etc/group. Analiza los campos de cada fila.

Texto

Descripción generada automáticamente

El archivo /etc/group es otro archivo de texto plano que se utiliza para almacenar información sobre los grupos de usuarios en un sistema operativo Unix o Linux. Cada línea en el archivo representa un grupo y contiene cuatro campos separados por dos puntos (:). Los campos son los siguientes:

* Nombre de grupo (groupname): Es el nombre del grupo.
* Contraseña de grupo (password): Este campo solía almacenar contraseñas de grupo en versiones antiguas del sistema operativo, pero en sistemas modernos, este campo se utiliza para indicar si se requiere o no una contraseña de grupo para acceder a los recursos compartidos del grupo.
* GID (Group ID): Es el identificador numérico del grupo en el sistema.
* Lista de usuarios (user list): Es una lista separada por comas de los nombres de usuario que pertenecen a este grupo.

4.3.- Analiza el contenido del fichero /etc/sudores. Averigua cómo se puede editar su contenido. ¿Es necesario editarlo para que un usuario pueda realizar acciones en nombre de otros usuarios?

Texto

Descripción generada automáticamente

El archivo /etc/sudoers es un archivo de configuración en sistemas operativos Unix y Linux que define las reglas y permisos de sudo, un programa que permite a los usuarios ejecutar comandos con los permisos de otro usuario (generalmente el usuario root) en un sistema.

El contenido del archivo /etc/sudoers está escrito en un lenguaje específico de sudo que se parece a una sintaxis de archivo de configuración. El archivo contiene reglas y permisos que definen qué usuarios pueden realizar ciertas acciones y qué acciones pueden realizar. El archivo también puede contener otras opciones de configuración para el programa sudo.

Es importante tener en cuenta que la edición manual del archivo /etc/sudoers puede ser riesgoso, ya que incluso un error tipográfico puede impedir que los usuarios realicen tareas importantes o dañar el sistema. Por esta razón, la mayoría de los sistemas operativos Unix y Linux incluyen utilidades de edición de sudoers, como visudo, que realizan una verificación sintáctica antes de guardar el archivo.

Para permitir que un usuario pueda realizar acciones en nombre de otros usuarios, se puede agregar una regla específica en el archivo /etc/sudoers. Por ejemplo, si se desea permitir que el usuario "usuario1" ejecute el comando "apt-get" con permisos de superusuario, la línea de regla correspondiente podría verse así:

alberto ALL=(ALL:ALL) NOPASSWD:/usr/bin/apt-get

4.4.- Crea dos usuarios con los archivos de configuración del /etc/skel. Elimina un usuario, manteniendo sus archivos. Elimina totalmente el otro usuario. Comprueba las acciones.

Texto

Descripción generada automáticamente

4.5.- Muestra el contenido del directorio /etc/skel, mediante ls -la /etc/skel. Presta atención a cada fichero.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

4.6.- Crea un usuario con un GID propio. Crea varios archivos con dicho usuario. Modifica el GID del usuario. Asigna los ficheros anteriores al nuevo GID.

Para crear un usuario con un GID específico se usa el comando:

sudo useradd -g (Número del GID) nombreusuario.

Nos metemos en el usuario con el comando su:

sudo su nombresusuario

Una vez dentro, creamos dos archivos. Ahora cambiamos el GID del usuario:

sudo usermod -g (Número del GID) nombreusuario

Finalmente, asignamos los archivos creados al nuevo GID, con el comando “chgrp”, que sirve para cambiar la propiedad de los grupos.

Sudo chgrp (Número del GID) archivo archivo2

4.7 Modifica la contraseña de un usuario mediante: sudo passwd usuario:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

4.8 Ejecuta ls -l /usr/bin/passwd. Observa quién es el propietario y si se encuentra activo el set-uid en dicho archivo.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

4.9 Ejecuta ls -ld/tmp. Observa quién es el propietario, el grupo y si se encuentra activo el sticky-bit del directorio.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente