

Tercer Problema (Admon)

Muchas labores administrativas precisan la intervención del superusuario, pero existen otras labores que cualquier usuario puede realizar libremente para configurar su cuenta.

Para cada labor listada a continuación indique en qué consistiría y justifique porqué es imprescindible que sea realizada por el superusuario o, por el contrario, porqué puede ser realizada libremente por cualquier usuario.

- a) Crear una nueva cuenta de usuario.
- b) Instalar un nuevo software para que lo use cualquier usuario.
- c) Proteger mi cuenta: evitando que otros usuarios vean su contenido y estableciendo, de manera permanente, una máscara que impida que futuros archivos sean accesibles por otros usuarios.
- d) Instalar un determinado software para ser usado por mí y por usuarios de mi grupo.

El superusuario también puede delegar...

- e) Explique cómo se consigue que cualquier usuario pueda libremente cambiar, por ejemplo, la palabra clave de su cuenta o el intérprete de mandatos asociado a la misma, usando mandatos como `passwd` y `chsh` respectivamente.

Solución

- a) Crear una nueva cuenta de usuario sólo lo puede realizar el superusuario o administrador.
1. Crear un directorio que será el home del usuario.
 2. Crear una nueva entrada en el fichero `/etc/passwd` con los datos del nuevo usuario: `loginname`, `UID`, `GID`, `Nombre` y `shell` que utilizará.
 3. Crear una nueva entrada en el fichero `/etc/shadow` con los mismos datos y con la versión cifrada de la palabra clave que se le ponga por defecto.
 4. Regalarle el directorio `home` al usuario.
 5. Copiar la versión por defecto de ciertos ficheros de configuración en la cuenta del usuario y regalárselos. Configuración del `shell` y del correo electrónico).

Todas las acciones anteriores exigen alterar ficheros o directorios globales que deben ser propiedad del superusuario, luego sólo él podrá realizar dichas operaciones.

- b) Instalar globalmente un nuevo software sólo lo puede realizar el superusuario o administrador.
1. Descargar el software en cuestión y extraerlo.
 2. Ejecutar algún script de instalación que copiará los diferentes ficheros (ejecutables, bibliotecas, ficheros de configuración, etc.) en su correspondiente directorio del sistema, para que la herramienta software pueda ser utilizada por cualquier usuario.
 3. Borrar el software de la zona de descarga.

Todas las acciones anteriores exigen alterar ficheros o directorios globales que deben ser propiedad del superusuario, luego sólo él podrá realizar dichas operaciones.

- c) Proteger la propia mi cuenta lo puede hacer el propio usuario.
1. Cambiar los permisos de nuestro directorio `HOME`: `chmod . 0750`
 2. Indicar en el fichero de configuración del `shell` (`.profile`) el establecimiento de la máscara de creación de ficheros que queramos: `umask 027`

Todas las acciones anteriores exigen alterar ficheros o directorios propiedad del propio usuario, luego no se precisa la intervención del administrador.

- d) Instalar un determinado software en la propia cuenta exige realizar las mismas operaciones que en el caso b) de instalación global en el sistema, a diferencia de que se realizará sobre directorios locales propios y situados dentro de la propia cuenta. Usuarios de mi grupo que deseen usar dicho software deberán tener acceso al interior de mi cuenta. Para ello se podrá jugar con los permisos de acceso a gente del mismo grupo de usuarios.

Todas las acciones anteriores alterarán sólo elementos propiedad del propio usuario, luego no se precisa la intervención del administrador.

- e) El mecanismo de delegación mediante el cual es posible que el administrador facilite que cada usuario pueda cambiar ciertos aspectos de configuración de su propia cuenta sin por ello comprometer la seguridad del sistema es el bit `SETUID`. Ciertos mandatos de administración como `passwd` y `chsh` son propiedad de `root` y tienen activo el bit `SETUID`. Con ello se consigue que, durante su ejecución, el proceso sea, de manera efectiva, del superusuario, y por lo tanto pueda hacer las cosas que el superusuario puede y el usuario, por sí mismo, no.