ADMINISTRACIÓN DE SISTEMAS

Práctica 1. Usuarios y protección en Linux

Introducción

El objetivo de la práctica consiste en la utilización de los mecanismos que implementa Linux para la gestión de usuarios y grupos en un sistema de estas características. Además se pretende familiarizar a los administradores con los mecanismos de protección habilitados en este sistema operativo. En particular, se abordarán los siguientes conceptos:

* Usuarios y grupos primarios
* Grupos suplementarios
* Reglas de protección de ficheros y directorios
* Utilización de los bits SETUID y SETGID en ficheros ejecutables
* Utilización del bit SETGID en directorios
* Utilización del sticky bit

Para ello, se plantea un caso práctico de una organización que utiliza un sistema Linux como soporte informático.

Reglas de seguridad en la Organización

El plan de seguridad de la Organización cubre los siguientes aspectos:

1. **Contraseñas**:
    * Los usuarios deben cambiar sus contraseñas cada 3 meses.
    * Es necesario notificar a los usuarios 1 día antes de que su contraseña caduque
    * Transcurridos 2 días desde la caducidad del password, la cuenta ha de quedar desactivada
    * En la práctica, la contraseña de cada usuario coincidirá con el nombre de usuario
2. **Directorio de cada usuario**
    * Todo usuario del sistema debe poseer un subdirectorio del directorio */home* cuyo nombre debe coincidir con el de la cuenta del usuario
    * En este directorio, el usuario debe poder crear y borrar ficheros y directorios, pero no debe poder modificar los permisos de su directorio de conexión.

* Ningún otro usuario del sistema podrá acceder a dicho directorio y a su contenido

3. Proyectos en ejecución

La Organización tiene varios proyectos en curso. Para estos proyectos, se ha de cumplir:

* Cada proyecto debe tener un directorio bajo el directorio */home/proyectos* donde se almacenará la documentación asociada al mismo.
* Todos los usuarios que participan en un proyecto deben tener la posibilidad de leer, modificar, crear y borrar los archivos que forman parte del proyecto
* Cuando un usuario cree un archivo en el directorio del proyecto, por defecto, éste debe poder ser leído, modificado o borrado por cualquier otro usuario del mismo proyecto
* Ningún otro usuario podrá acceder a estos directorios
* Existirá un directorio */home/proyectos/comun* donde se almacenará información común a todos los proyectos de tal forma que todos los usuarios puedan añadir y modificar información a este directorio, pero sólo el propietario de cada carpeta pueda eliminarla.

4. Ejecutivos

En la empresa existen varios ejecutivos que tienen asignada la evaluación de algunos de los proyectos existentes con las siguientes restricciones:

* Los ejecutivos no deben poder acceder directamente a los directorios de los proyectos
* Para que los ejecutivos puedan controlar el estado de cada proyecto, deben existir en el directorio */usr/local/bin* tantos programas como proyectos existan. Estos programas internamente han de realizar un "*ls*" sobre el directorio del proyecto correspondiente
* El programa que permite evaluar cada proyecto, debe cumplir lo siguiente:
  - Debe poder ser ejectuado únicamente por los ejecutivos asociados a cada proyecto.
  - Debe tener asignado los permisos suficientes para poder ejecutar el "*ls*" sobre el directorio correspondiente.

5. Resto de usuarios

En la organización pueden existir otros usuarios no vinculados con ningún proyecto, que no tendrán acceso a los directorios de los proyectos.

Situación actual de la Organización

Actualmente, se tiene la siguiente situación:

* Existen 3 proyectos: Aeropuerto, Centro Comerical y Parque
* Dos ejecutivos: ejec1 y ejec2
* Existen dos usuarios no relacionados con ningún proyecto: inv1 e inv2.
* La distribución de los usuarios por proyectos es de la siguiente forma:

Usuario	**Proyecto**		
	Aeropuerto	Centro Comerical	Parque
usu1		?	
usu2	?		
usu3	?	?	
usu4	?	?	
usu5	?	?	?
usu6			?

* La asociación de ejecutivos a proyectos es:

Ejecutivo	**Proyecto**		
	Aeropuerto	Centro Comerical	Parque
ejec1	?		?
ejec2	?	?	

Opcional:

Se valorará cualquier aportación extra del alumno: limitación de horas de conexión, acceso restringido a ciertos terminales, creación de scripts para la automatización,…