

Tema 2: Organización de un sistema operativo tipo GNU/Linux (Ejercicios)

Programación y Administración de Sistemas (2023-2024)

Javier Sánchez Monedero

8 de marzo de 2024

Tabla de contenidos

1 Algunos ejercicios	1
----------------------	---

1 Algunos ejercicios

Usuarios y grupos de ejemplo

Crea tres usuarios, dos de ellos tendrán un grupo común. Suponiendo que nuestro usuario de administración es `pas`, lo añadimos al grupo `sudo` como `root`:

```
/sbin/usermod -aG sudo pas
```

Creamos un grupo para la clase y tres usuarios de ejemplo, los dos primeros tendrá como grupo principal `clase` y el tercero no:

```
sudo addgroup clase
sudo adduser usuario1 --ingroup clase
sudo adduser usuario2 --ingroup clase
sudo adduser usuario3
```

Permisos

Con `usuario1` Crear un archivo con el contenido `HOLA!`, utilizando la orden `echo`, y asignarle permisos para que solo puede ser consultado por su propietario y por los miembros del grupo `clase`.

NOTA: Puede ser una buena idea tener varios terminales abiertos con cada usuario del sistema para probar que los permisos son efectivos.

Permisos

Modifica los permisos por defecto con `umask` para que los ficheros creados:

- no puedan ser leídos por el resto de usuarios y los directorios no puedan ser listados.
- puedan ser leídos y escritos por el grupo.

Comprueba que tienen efecto creando ficheros y directorios de ejemplo.

Busca cómo hacer permanentes en cada usuario los permisos `umask`.

Algunos ejercicios de permisos

- Transformar los siguientes permisos simbólicos en absolutos:

`rwxr-xr-x` `r-xr--r--` `rw-r-----` `r-x--x--x`

- Transformar los siguientes permisos absolutos en simbólicos:

`644` `755` `610` `631`

- Fijar, en modo simbólico, los permisos de `arch1` en modo `754`.
- Fijar, en modo absoluto, los permisos de `arch1` en modo `rwxr-x--x`.
- Fijar los permisos del directorio `dir1` de modo que todos lo puedan leer y entrar, pero sólo el dueño pueda modificar sus archivos: 1) en modo simbólico; 2) en modo absoluto.
- Modificar para que el grupo también pueda modificar archivos.
- Fijar en modo simbólico los permisos del archivo ejecutable `exec.tar` para que sea ejecutable por todos, legible por el dueño y el grupo, y modificable solo por el dueño. Repetir en modo absoluto.
- Fijar en modo absoluto los permisos del directorio `dir1` de modo que sólo el dueño y el grupo lo puedan recorrer y leer, y sólo el dueño pueda grabar y borrar en él. Repetir en modo simbólico.

Interpretar salida `ls -l`

Sea la siguiente salida del comando `ls -l`:

```
-rwSr-xr-x 1 pagutierrez docentes 29024 ene 1 16:29 controlar
-rw-rw-r-- 1 pagutierrez docentes 2300 may 18 09:37 borrador.txt
-rw-r--r-- 1 pagutierrez docentes 5895 may 15 12:08 index.htm
-rwxr-xr-x 1 pagutierrez docentes 29024 ene 1 16:29 revisar
-rwxr--r-- 1 pagutierrez docentes 29024 ene 1 16:29 mostrar
drwxrwxrwt 2 pagutierrez tecnicos 1024 may 1 17:23 trabajos
drwxr-xr-x 2 pagutierrez tecnicos 1024 oct 16 1998 netscape3
drwxrwx--x 2 pagutierrez tecnicos 1024 may 11 7:29 finanzas
drwxrwxr-x 2 pagutierrez tecnicos 1024 jul 7 6:54 redes
drwxr-xr-x 2 jsanchezm docentes 1024 jun 17 19:35 corporacion
```

El usuario `jsanchezm`, del grupo `docentes`, tiene acceso al presente directorio. Indicar, si los hay:

1. Archivos de los que puede mostrar contenido.
2. Archivos que puede ejecutar como programa.
3. Archivos en los que puede modificar contenido.
4. Subdirectorios en los que puede ingresar.
5. Subdirectorios en que puede crear/eliminar ficheros propios.
6. Subdirectorios en los que puede borrar archivos de otros.
7. Subdirectorios en los que puede entrar y ejecutar programas contenidos en ellos, pero no ver nombres de archivos.
8. Archivos que puede ejecutar como programa con permisos del usuario `pagutierrez`.

Interpretar salida `ls -l`

Sea la siguiente salida del comando `ls -l` (suponemos que `pagutierrez` pertenece a `staff`):

```
-rw-r--r-- 1 root root 33280 jun 12 19:40 Carta.doc
drwxrwxrwx 5 pagutierrez staff 1024 dic 4 1999 step
drwxrwxr-x 22 pagutierrez staff 1024 nov 20 1999 Office51
drwxr-x--- 6 pagutierrez staff 1024 may 7 16:43 argos
drwxrwxr-- 21 pagutierrez staff 1024 jul 11 18:22 bajados
-rw-rw---- 3 root root 542 jul 13 11:26 boor.exe
```

```

drwxrwxrwt 3 pagutierrez staff      1024 may 25 10:02 borrador
-rwSrWsr-x 1 root          root      9218 jun 12 19:41 pph3
drwxrwx--x 2 pagutierrez pagutierrez 1024 may 7  16:47 cdir
-rw-rw-r-- 3 root          root      542 jul 13 11:26 mysql-doc
-rw-r-xr-- 3 pagutierrez staff      1084 ago 1  10:01 ver.exe
-rwxr-xr-x 3 pagutierrez staff      1084 ago 1  10:01 ver
drwxr-xr-x 7 pagutierrez pagutierrez 1024 jul 25 11:48 lit

```

Indicar, si los hay:

1. directorios públicos (todo el mundo puede entrar, listar y borrar archivos);
2. archivos que tienen enlaces hard o físicos;
3. archivos ejecutables por el usuario **pagutierrez**;
4. directorios navegables por todo el mundo;
5. directorios donde miembros del grupo **staff** puede borrar archivos;
6. archivos que son enlaces simbólicos.
7. archivos ejecutables que adquieren permisos de usuario **root**.

Enlaces

Marca todos los tipos de enlace que pueden establecerse en los siguientes casos (físico, simbólico o ambos).

- enlace hacia un archivo en el mismo directorio.
- enlace hacia un archivo en otro sistema de archivos.
- enlace hacia un directorio en el mismo sistema de archivos.
- enlace hacia un directorio en otro sistema de archivos.