educación IT
CODE YOUR FUTURE

Introducción a Linux

Módulo 4

Permisos especiales

Permisos especiales

Es típico de los sistemas Unix emplear **tres permisos o modos adicionales** que se asignan a archivos o directorios en conjunto, **no a cada clase de forma separada** (como sucedía con los permisos básicos).

Estos tres permisos -especificables de forma independiente-, un bit por cada uno de ellos, permiten 8 combinaciones posibles que se expresan con un dígito en base 8 (del 0 al 7, uno por cada combinación posible) que se antepone al modo de permisos. Así, el modo se amplía ahora del **0000** al **7777.**

Aparte de los siempre aplicables de lectura, escritura y ejecución, algunas veces es necesario algo más para un archivo o directorio. Estos permisos especiales son los siguientes:

- **Asignar ID de usuario (set user ID) (SUID).**
- **Asignar ID de grupo (set group ID) (SGID).**
- **Sticky bit.**

SUID

Permiso ***set user ID, setuid o SUID:*** cuando un archivo tiene este permiso asignado y es ejecutado, el proceso resultante asumirá el ID de usuario efectivo del propietario del archivo.

El ejemplo típico es el cambio de una clave de usuario: ningún usuario debería poder modificar **`/etc/shadow`** directamente. La única forma de poder modificarlo debería ser a través del comando correspondiente, que necesariamente tendrá que tener asignado el **`setuid`**.

Es decir, el comando **`/usr/bin/passwd`** ejecutado por un usuario se ejecutará como si lo hubiese invocado el root, de manera que puede modificar **`/etc/shadow.`**

En la siguiente slide veremos ejemplos de su uso.

Ejemplo:

Se puede ver que en los permisos del usuario aparece una “s” en vez de una “x”

```
# ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 45396 May 25  2012 /usr/bin/passwd
```

Este permiso se puede setear con:

```
# chmod 4655 archivo
# chmod u+s archivo
```

Para ver todos los archivos que tienen este permiso en el sistema:

```
# find / -perm -4000  2>/dev/null
```

SGID

Permiso set group ID, setgid o SGID: cuando un archivo que tiene este permiso asignado se ejecuta, el proceso resultante asumirá el ID de grupo efectivo definido en el archivo. Cuando el **`setgid`** le es asignado a un directorio, archivos nuevos o directorios creados debajo de ese directorio heredarán el grupo de ese directorio, a diferencia del comportamiento por defecto, que es usar el grupo primario del usuario efectivo al asignar el grupo de archivos nuevos y directorios.

En la siguiente slide veremos ejemplos de su uso.

Ejemplo:

```
$ ls -ld /test
drwxr-sr-x 241 educacionit educacionit 4096 Sep 12 19:29 /test
$ sudo mkdir /test/prueba
$ ls -ld /test
drwxr-sr-x 2 root  educacionit 4096 Sep 12 19:35 prueba
```

Este permiso se puede setear con:

```
# chmod 2755 directorio (o un archivo)
# chmod g+s directorio (o un archivo)
```

Para ver todos los archivos que tienen este permiso en el sistema:

```
# find / -perm -2000  2>/dev/null
```

Sticky Bit

Este permiso no trabaja como los otros permisos especiales. Con un valor numérico de 1000, sus operaciones difieren cuando están aplicadas a un directorio o a un archivo.

Cuando está aplicado a un directorio: evita que los usuarios borren archivos de las carpetas que les conceden el permiso de escritura, a menos que sean el propietario del archivo. Por defecto, cualquier usuario que tenga permiso de escritura en un directorio puede borrar archivos dentro de ese directorio, incluso si no tiene el permiso de escritura de ese archivo.

Cuando se aplica sobre un archivo: el archivo se convierte en *"sticky"* (bloqueado). Si el archivo no es ejecutable, el último bit de permiso se convierte en "**T**". Si el archivo es un fichero ejecutable, o el permiso se aplica a un directorio, el bit pasado se convierte en una "**t**". Cuando se aplica el permiso **`chmod`** y las letras, aparece "**t**" de todos modos (sea archivo o directorio).

El directorio /tmp cuenta con este permiso activo porque **todos los usuarios tienen permiso de escritura, pero nadie podrá borrar ningún archivo que no le pertenezca.**

Ejemplo:

Este permiso se puede setear con:

```
# chmod 1755 directorio (o un archivo)
# chmod o+t directorio (o un archivo)
```

```
$ ls -ld /tmp
drwxrwxrwt 26 root root 36864 Sep 15 23:17 /tmp
```

Para ver todos los archivos que tienen este permiso en el sistema:

```
# find / -perm -1000  2>/dev/null
```

educación IT
CODE YOUR FUTURE

¡Sigamos trabajando!