Bits SUID, SGID i "Sticky"

Existen una serie de permisos especiales que se pueden utilizar sobre cualquier sistema de archivos nativo de Linux y que pueden resultarnos útiles para determinadas tareas.

Bit SUID

El bit SUID activo en un archivo ejecutable significa que cuando se ejecute lo va a hacer como si lo hubiera ejecutado su propietario (es decir, con los permisos que este tenga sobre el sistema) y no del usuario que lo haya ejecutado. Esto puede llegar a ser muy util en algunas situaciones (por ejemplo, fijarse en el comando *passwd*, por ejemplo, cuyo propietario es el usuario root y necesita el bit SUID para que cualquier usuario pueda cambiarse su propia contraseña modificando el archivo "/etc/passwd") pero hay que utilizarlo con cuidado, dado que puede generar grandes problemas de seguridad.

Para activarlo basta con ejecutar *chmod u+s archivo* (o *chmod 4nnn archivo*). Al hacer un *ls -l* veremos cómo en el lugar del permiso de ejecución del usuario-propietario aparece una "s" en vez de una "x". Hay que tener en cuenta, no obstante, que para que el bit SUID sea efectivo el archivo debe tener permisos de ejecución: si a un archivo con dicho bit se le quita el permiso de ejecución, al hacer un *ls -l* veremos que aparece una "S" en vez de la "s" y en este caso no el bit no tendrá efecto.

Para encontrar los ficheros de nuestro sistema que tienen el bit SUID activado se puede ejecutar *find / -perm -4000* (notar el guión delante de los números para indicar un "como mínimo")

Bit SGID

El SGID se suele activar en directorios para hacerlos compartidos: cualquier archivo (ejecutable o no) creado en un directorio con este bit activado, tendrá asignado como grupo-propietario no el del usuario que lo haya creado sino el del grupo-propietario del directorio que lo contiene.

Para activarlo basta con ejecutar *chmod g+s carpeta* (o *chmod 2nnn carpeta*). Al hacer un *ls -l* veremos cómo en el lugar del permiso de ejecución del grupo del propietario aparece una "s" en vez de una "x". Se puede comprobar el efecto de este bit si, una vez asignado a un determinado directorio, iniciamos sesión con otro usuario y creamos dentro de ese directorio un fichero nuevo: comprobaremos como el grupo-propietario de ese fichero no es el del nuevo usuario sino del grupo-propietario del directorio con el bit SGID activado.

Para encontrar los ficheros de nuestro sistema que tienen el bit SGID activado se puede ejecutar *find / -perm -2000*. Para encontrar los ficheros que tengan tanto el SUID como el SGID activado, bastaría con hacer *find / -perm -6000*

"Sticky" bit

El "sticky" bit se suele activar en directorios para permitir que si cualquier usuario puede añadir o renombrar ficheros de su interior indistintamente (porque tiene permisos para ello), solo el propietario (o root) pueda eliminar el fichero en cuestión. Un ejemplo de uso es asignarlo al directorio "/tmp", ya que debe poder ser utilizado por cualquier proceso pero solo el dueño o root puede eliminar los archivos que cree.

Para activarlo basta con ejecutar *chmod o+t carpeta* (o *chmod 1nnn carpeta*). Al hacer un *ls -l* veremos cómo en el lugar del permiso de ejecución de "los otros" aparece una "t" en vez de una "x".

Para encontrar los ficheros de nuestro sistema que tienen el bit "sticky" activado se puede ejecutar *find / -perm -1000*