Permisos y privilegios en Linux

Dentro de Linux hay un aspecto que destaca de otros sistemas operativos como Windows por ejemplo y es la seguridad en directorios y ficheros

no solo hablando de vulnerabilidades y privacidad sino de la forma en la que se gestionan los archivos personales de sus usuarios, cada fichero y cada directorio cuenta con unos permisos definidos sin los cuales nadie podría acceder al archivo en cuestión.

En Linux, los permisos y privilegios son mecanismos de seguridad utilizados para controlar el acceso a los archivos y directorios del sistema. Cada archivo o directorio tiene un usuario dueño y un grupo dueño, y se pueden establecer diferentes niveles de acceso para el usuario dueño, el grupo dueño y otros usuarios.

Los permisos se dividen en tres categorías: lectura (r), escritura (w) y ejecución (x). Estos permisos se pueden asignar de manera individual para el dueño del archivo, el grupo dueño y otros usuarios.

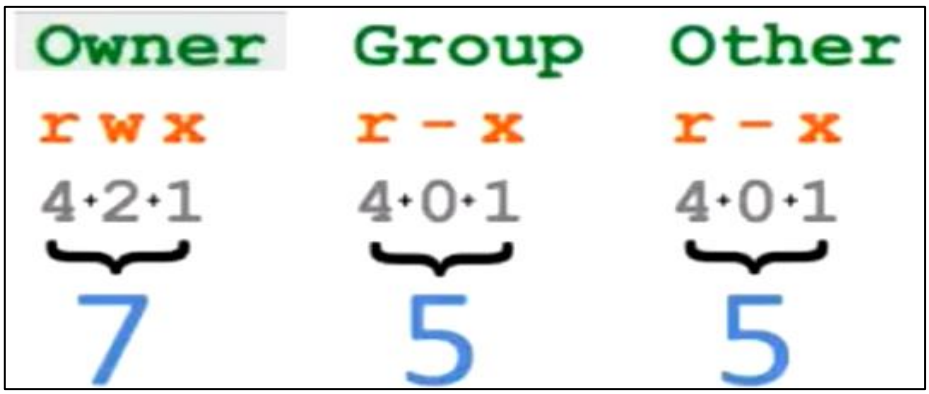
- Lectura (read) 'r':
  Permite leer, abrir, copiar el contenido del archivo o listar el contenido del directorio.

- Escritura (write) 'w':
  Permite modificar el contenido del archivo o añadir y/o eliminar archivos del directorio.

- Ejecución (execute) 'x':
  Permite ejecutar un archivo como un programa o script, o acceder a un directorio.

Adicionalmente también tenemos la relación numeral que tiene cada una de estas iniciales para dar permisos de forma avanzada

- x = 1
- w = 2
- r = 4



En un entorno de producción, es importante establecer permisos y privilegios adecuados para garantizar la seguridad del sistema.

Por ejemplo, es recomendable que los archivos críticos del sistema, como los archivos de configuración, solo sean accesibles por el usuario root o por un usuario específico con privilegios de administrador.

También es recomendable establecer permisos de lectura y escritura solo para el usuario dueño o para un grupo seleccionado de usuarios, y evitar dar permisos de ejecución a archivos que no necesiten ser ejecutados.

En resumen, configurar correctamente los permisos y privilegios en un entorno de producción es fundamental para garantizar la seguridad del sistema, y es importante establecer políticas claras para la gestión de usuarios, contraseñas y acceso al sistema.

1. Comando “chmod”
   El comando chmod se usa para cambiar los permisos de archivos o directorios. En Linux hay un conjunto de reglas para cada archivo que define quién puede acceder a ese archivo, y cómo se puede acceder a él. Estas reglas se llaman permisos de archivo o modos de archivo. El nombre de comando chmod significa “change mode” y se usa para definir la forma en que se puede acceder a un archivo.

   `sudo chmod -R 777 /Directorio` -> Brinda todos los permisos para todos los usuarios y grupos que existan en el sistema para el directorio objetivo y todos los ficheros que existan dentro de él.

   `sudo chmod 777 fichero.ext` -> Brinda todos los permisos para todos los usuarios y grupos que existan en el sistema para el fichero objetivo.

2. Comando “chown”

El comando chown en Linux (change owner) nos permite cambiar de propietario en archivos y directorios de Linux.

```
sudo chown -R NuevoPropietario /Directorio
```

Cambia de propietario a un directorio y todo lo que este dentro de el al nuevo propietario

```
sudo chown -R :NuevoGrupo /Directorio
```

cambia de grupo dueño a un directorio y todo lo que este dentro de el a un nuevo grupo

```
sudo chown -R NuevoPropietario:NuevoGrupo /Directorio
```

Cambia de propietario y grupo dueño a un directorio y todo lo que este dentro de el