Permisos de usuario en Linux y permisos especiales

Laila Fernandez Santamaria 1ºDAW

# Introducción

Los permisos en Linux son unos de los más fundamentales de la seguridad y la administración en un sistema operativo. Este sistema, que es heredado de UNIX, está basado en tres entidades, que son, el propietario del archivo, al grupo al que pertenece y todos los demás usuarios.

Linux utiliza el sistema numérico octal para representar los permisos básicos de lectura, escritura y ejecución (r, w, x), que también se puede representar de forma numérica (4, 2, 1), Esta estructura permite desarrollar mucho más detalladamente el acceso a archivos y directorios, facilitando el poder usar la política de seguridad en entornos multiusuario.

Además de los permisos básicos, Linux nos da también algunos permisos especiales como SUID, SGID y Sticky Bit, estos amplían mucho las capacidades del sistema. El permiso SUID nos permiten ejecutar archivos con los privilegios del propietario, el permiso SGID nos mantiene la pertenencia a grupos en subdirectorios y el Sticky Bit restringe la eliminación de archivos a sus propietarios.

El dominio de este sistema de permisos es esencial para los administradores de sistemas, desarrolladores y cualquier usuario que quera entender el funcionamiento de la protección en entornos Linux, siendo una base muy importante para agregar estrategias de seguridad que sean buenas.

# ¿Qué son los permisos y que importancia tienen?

Los permisos de Linux son un sistema para controlar quien puede hacer qué con cada archivo y carpeta en un ordenador. Linux divide a los tres tipos de usuarios en tres categorías:

* **El propietario** – Persona que creo el archivo y/o lo posee.
* **El grupo** – Personas cercanas al archivo que comparten algunos de los privilegios.
* **Otros** – Resto de usuarios que pueden ver y leer el archivo, pero no pueden hacer nada con él.

Los permisos tienen mucha importancia ya que si tienes los permisos correctos puedes proteger tu información personal, evitar que alguien borre cosas que no se deberían borrar, puedes compartir un archivo con tus compañeros de trabajo de manera segura y aprendes cómo funciona los sistemas de seguridad informática.

# Permisos básicos

Linux tiene tres tipos básicos de permisos que son muy fáciles de entender y muy efectivos:

* **Permisos de lectura (r)** -- Nos da la facilidad de poder ver el contenido de un archivo y de listar el contenido de un directorio
* **Permisos de escritura (w)** – Nos deja modificar el contenido de un archivo.
* **Permisos de ejecución (x)** – Nos permite ejecutar un Script o un programa, acceder al contenido de un directorio y crear o eliminar archivos dentro de un directorio.

En directorios, el permiso de ejecución es súper importante. Sin él no podrías ver absolutamente ningún archivo y no podrías realizar nada.

# Comprensión visual de los permisos

Al abrir una terminal Linux y escribir ls –l aparece una línea de código así:

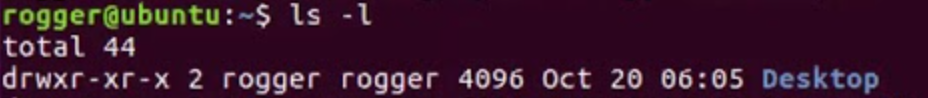


Figura 3.1 LS –L

https://i.ytimg.com/vi/K7n5RqEfVWA/maxresdefault.jpg [enlaces] [propietario] [grupo] [tamaño] [fecha] [nombre]

* **d** – tipo (en este caso es un directorio)
* **rwxr-xr-x** 🡪 Amarillo – Permisos del propietario

Verde – Permisos del grupo

Azul – Permisos de otros usuarios