# File permissions in Linux

## Project description

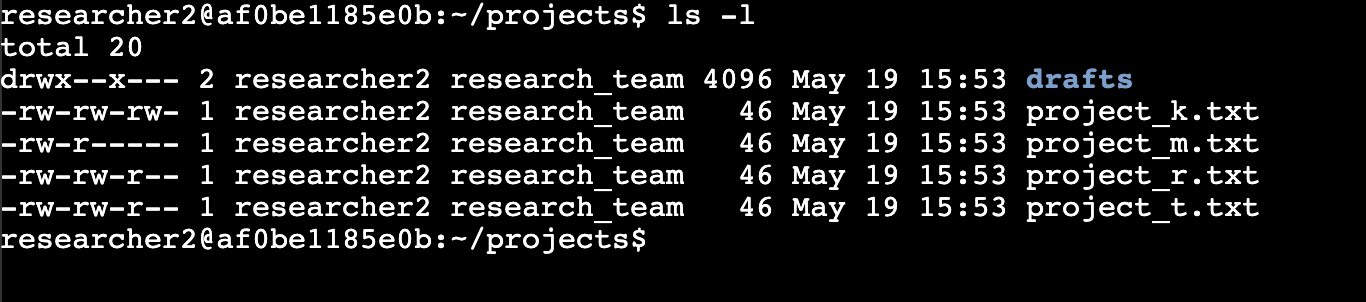
En este proyecto estaremos revisando una serie de modificaciones de permisos que se han solicitado al departamento de análisis de seguridad. Después de realizar una serie de investigaciones y comprobaciones hemos llegado a la conclusión que varios usuarios de la organización no están cumpliendo con el principio de permisos mínimos.

## Check file and directory details

Primero hemos comenzado analizando la carpeta de proyectos de la organización llamada “Projects”.

Como véis esta es la estructura que nos encontramos de manera detallada por; permisos, usuario, departamento, fecha de los archivos y nombre de los archivos.

El comando ls -l en Linux muestra una lista detallada de los archivos y directorios en el directorio actual.



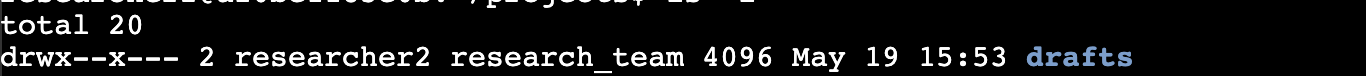
La cadena de 10 caracteres **"drwxrwxrwx" significa que:**

* Es un **directorio**.
* El **propietario** tiene permisos de lectura, escritura y ejecución.
* Los miembros del **grupo** tienen permisos de lectura, escritura y ejecución.
* **Otros usuarios** tienen permisos de lectura, escritura y ejecución.

En este caso todos los archivos tienen un acceso por parte del “research\_team” de la organización.

## Describe the permissions string

En cada uno de los objetos dentro de la carpeta projects el equipo tiene algún tipo de permiso, el más alto es el directorio “drafts” ya que el usuario “researcher2” tiene permisos de lectura, escritura y ejecución. Se representa como algo tal que así “drwx--x---”



El permiso drwx--x--- describe los permisos de un directorio con las siguientes características:

d: Indica que se trata de un directorio.

rwx (para el propietario): El propietario del directorio tiene los siguientes permisos:

r: Permiso de lectura, lo que significa que puede listar el contenido del directorio.

w: Permiso de escritura, lo que le permite crear, eliminar y renombrar archivos dentro del directorio.

x: Permiso de ejecución, que le permite acceder al directorio y, por lo tanto, a sus contenidos.

--x (para el grupo): Los miembros del grupo al que pertenece el directorio tienen el siguiente permiso:

- : Sin permiso de lectura, por lo que no pueden listar el contenido del directorio.

- : Sin permiso de escritura, por lo que no pueden crear, eliminar ni renombrar archivos dentro del directorio.

x: Permiso de ejecución, lo que les permite acceder al directorio y a sus contenidos, siempre y cuando conozcan los nombres de los archivos o subdirectorios.

--- (para otros): Otros usuarios que no son el propietario ni pertenecen al grupo no tienen ningún permiso para este directorio. No pueden leer su contenido, escribir en él ni acceder a él.

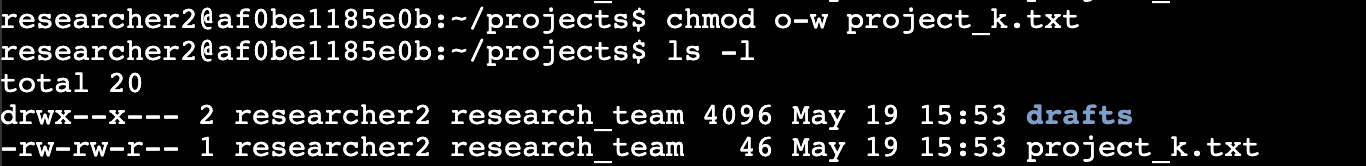
## Change file permissions

A continuación, vamos a revisar uno de los archivos que tenemos en el listado antes analizado para retirar uno de los permisos que pueden ser algo peligrosos para la seguridad del departamento.

Si nos fijamos en el archivo “project\_k.txt”, tiene permisos por parte del grupo “otros” de lectura y también escritura. Esto provoca que un usuario conectado como la sección “otros”, es decir, del exterior puede realizar cambios en los archivos gracias a ese permiso que tiene habilitado.

Con el comando “chmod o-w project\_k.txt” desactivaremos los permisos de escritura del archivo “project\_k.txt”.

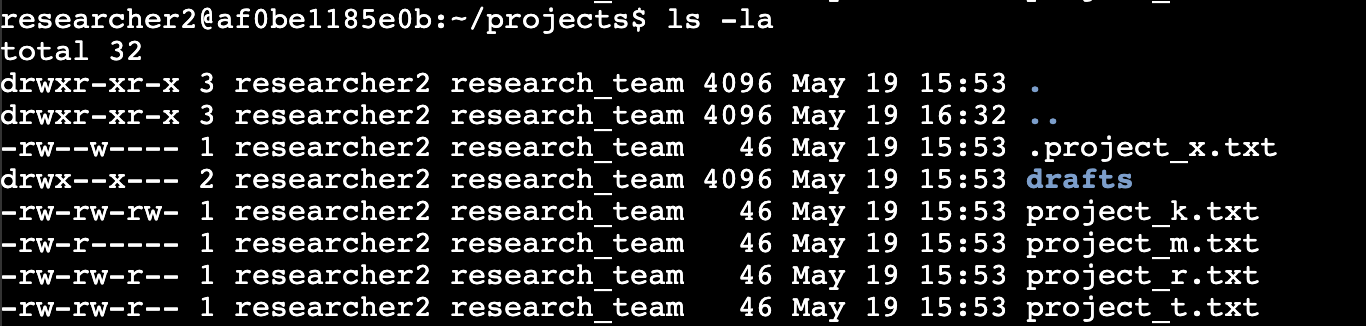
Como véis en la siguiente captura el estado de los permisos del archivo ha cambiado de forma inmediata:



Ya no tenemos la letra “w” marcada en la cadena de caracteres de permisos del archivo.

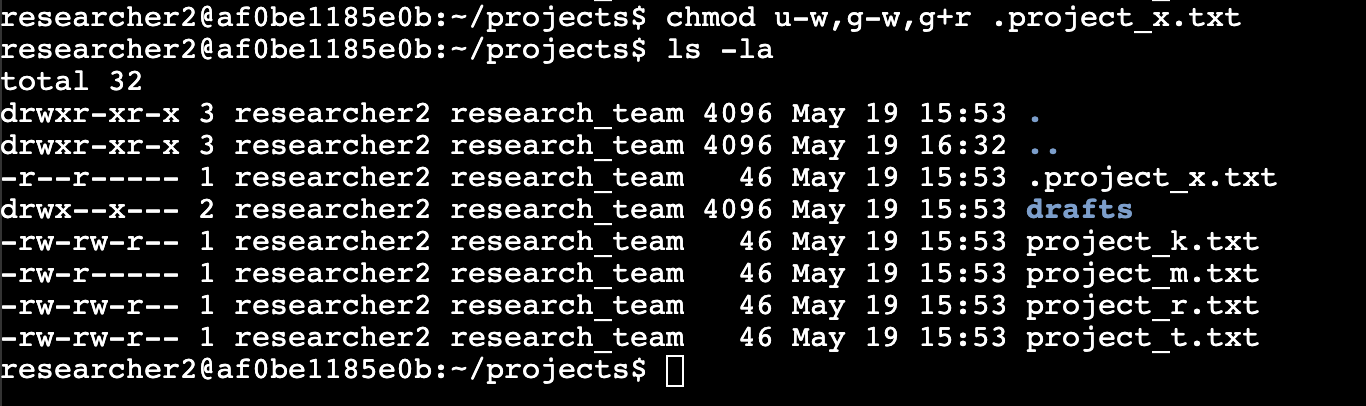
## Change file permissions on a hidden file

Hemos descubierto un archivo oculto con unos permisos incorrectos, estamos hablando del archivo “.project\_x.txt”, mediante el comando ls -la hemos descubierto que se encontraba dentro del directorio.



Este archivo no debería tener permisos de escritura para nadie, pero el usuario y el grupo tendrían que poder leer el archivo.

Para asignar estos permisos usaremos el comando “chmod u-w, g-w, g+r .project\_x.txt”:



Nuestros permisos deberían quedar de la siguiente manera que se presenta, cuando, ejecutamos de nuevo el comando “ls -la” para listar los archivos ocultos.

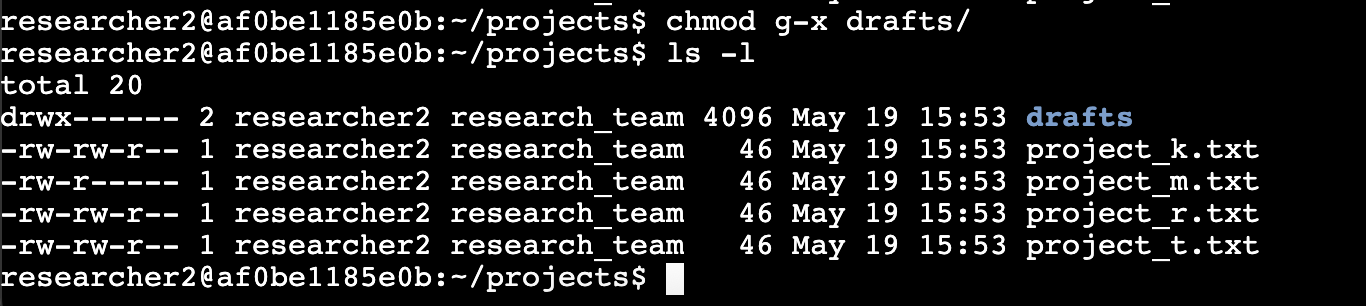
## Change directory permissions

Para finalizar editaremos los permisos del directorio “drafts”, que como hemos comentado anteriormente deberemos definir correctamente los permisos de los usuarios.

Para ello, desde el directorio “projects” que nos encontramos, realizaremos el cambio de permisos a la carpeta de manera que únicamente el usuario “researcher2” tenga acceso a ejecución del directorio, en otras palabras para que solo él pueda acceder al directorio.

Así estaremos cumpliendo también con el principio mínimo de permisos.

El comando es el siguiente “chmod g-x drafts”:



Como vemos se han realizado los cambios satisfactoriamente.

El comando chmod g-x drafts se ejecuta desde el directorio "projects" para modificar los permisos del directorio "drafts". Su objetivo es **restringir el acceso** a este directorio, específicamente **quitando el permiso de ejecución (x) al grupo (g) propietario de "drafts"**.

El permiso de ejecución en un directorio es necesario para poder **acceder a su contenido** (usar cd). Al eliminar este permiso al grupo, se busca que **solo el propietario (que idealmente sería "researcher2") pueda entrar en el directorio**.

La efectividad de que solo "researcher2" pueda acceder depende de cómo estén configurados los usuarios y grupos del sistema. Se asume que "researcher2" es el propietario o el único miembro relevante del grupo propietario que necesita acceder a "drafts".

## Summary

El documento aborda las permisiones de archivos en Linux, explicando su estructura, importancia y comandos relacionados con la gestión de derechos de acceso.

- Linux utiliza un sistema de permisos de archivos para mejorar la seguridad y gestionar el acceso de los usuarios.

- Cada archivo tiene tres tipos de permisos: lectura, escritura y ejecución, aplicables a tres categorías de usuarios: propietario, grupo y otros.

- El comando 'chmod' se emplea para cambiar los permisos de archivo, permitiendo a los usuarios otorgar o revocar acceso según sea necesario.

- Los usuarios pueden visualizar los permisos de archivo utilizando el comando 'ls -l', que muestra la configuración de permisos junto con detalles del archivo.

- Comprender y gestionar eficazmente los permisos de archivos es fundamental para mantener la seguridad del sistema y la integridad de los datos.

Principales conclusiones:

- Aprender a manipular los permisos de archivos es esencial para la administración de sistemas Linux.

- Los permisos adecuados ayudan a prevenir accesos no autorizados y a proteger datos sensibles.