# File permissions in Linux

## Project description

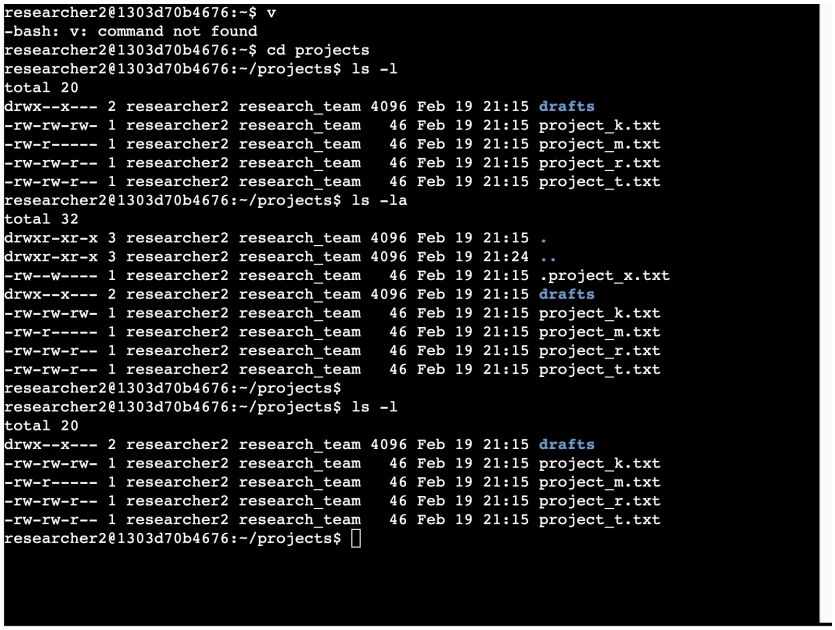
Como profesional de seguridad, mi objetivo en este proyecto fue auditar y actualizar los permisos del sistema de archivos para el equipo de investigación de la organización. Utilicé comandos de Linux para identificar vulnerabilidades de acceso y aplicar el principio de menor privilegio, asegurando que solo los usuarios autorizados tengan los permisos de lectura, escritura o ejecución necesarios para sus funciones.

## Check file and directory details

Para revisar los permisos actuales de todos los archivos y directorios, incluyendo archivos ocultos, utilicé el comando:

`ls -la`.

Fig 1




## Describe the permissions string

La cuerda de permisos funciona de la siguiente manera:
Empieza con una letra d o un guión que nos dice si es un directorio o un archivo común.
Los 3 caracteres siguientes corresponden a permiso de WRX, escritura W, lectura R y ejecución X. Para el perfil de usuario.
Los siguientes 3, corresponden al perfil de grupo y los últimos 3 caracteres son para el perfil de Otros.
Luce de la siguiente manera: dwrxwrxwrx.
Si en la posición de la letra encontramos un guión, eso quiere decir que ese perfil carece de autorización para la acción que describe.

Se solicitó buscar que archivos tenían permiso de escribir “w”, para el perfil de “others”,
Se identificó el archivo project_k.txt (Fig 1)

Usando el comando chmod se retiró el permiso de escritura “w” para el perfil de “others” en el archivo project_k.txt (Fig 2)

```
researcher2@1303d70b4676:~/projects$ chmod o-w project_k.txt
researcher2@1303d70b4676:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb 19 21:15 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb 19 21:24 ..
-rw--w---- 1 researcher2 research_team   46 Feb 19 21:15 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb 19 21:15 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb 19 21:15 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_t.txt
researcher2@1303d70b4676:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Feb 19 21:15 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb 19 21:15 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_t.txt
researcher2@1303d70b4676:~/projects$
```

Fig 2

Con esto se aseguró el contenido del archivo project_k.txt
También se modificó el permiso del archivo project_m.txt, con el comando **chmod g-r project_m.txt** se le quitó el permiso de lectura al perfil de “group”

## Change file permissions on a hidden file

Posteriormente se solicitó saber si existían archivos escondidos, para esto se usó el comando **ls -la**

Se encontraron 2 directorios escondidos y un archivo, con el nombre .project_x.txt (Es importante señalar que los archivos escondidos empiezan con el caracter . Antes del nombre.)

```
drwxr-xr-x 3 researcher2 research_team 4096 Feb 19 21:15 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb 19 21:24 ..
-rw--w---- 1 researcher2 research_team   46 Feb 19 21:15 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb 19 21:15 drafts
```

El archivo oculto project_x.txt tenía permisos de escritura para el perfil usuario y grupo.
Para endurecer la seguridad se deseaba retirar el permiso para escribir en este archivo para todos los perfiles.
Usando el comando **chmod u-w, g-w, g+r project_x.txt** se removieron los permisos de escritura y se agregó el permiso de lectura g+r al perfil de “group”.

```
researcher2@1303d70b4676:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb 19 21:15 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb 19 21:24 ..
-rw--w---- 1 researcher2 research_team   46 Feb 19 21:15 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb 19 21:15 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_k.txt
-rw------- 1 researcher2 research_team   46 Feb 19 21:15 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_t.txt
researcher2@1303d70b4676:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@1303d70b4676:~/projects$ ls-la
-bash: ls-la: command not found
researcher2@1303d70b4676:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb 19 21:15 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb 19 21:24 ..
-r--r----- 1 researcher2 research_team   46 Feb 19 21:15 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb 19 21:15 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_k.txt
-rw------- 1 researcher2 research_team   46 Feb 19 21:15 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_t.txt
researcher2@1303d70b4676:~/projects$
```

## Change directory permissions

La siguiente acción fue cambiar los permisos de un directorio.
Para identificar un directorio en el bash, se usa el comando ls -l y los directorios son los que comienzan con la letra d, seguida de los guiones que representan los permisos de diferentes perfiles. En este caso encontramos un directorio que se llama drafts. Fue identificado que el perfil group tenía permiso para ejecutar “x” y se determinó retirar el permiso, usando el comando: **chmod g-x drafts .**

```
researcher2@1303d70b4676:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Feb 19 21:15 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_k.txt
-rw------- 1 researcher2 research_team   46 Feb 19 21:15 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_t.txt
researcher2@1303d70b4676:~/projects$ chmod g-x drafts
researcher2@1303d70b4676:~/projects$ la -l
-bash: la: command not found
researcher2@1303d70b4676:~/projects$ ls -l
total 20
drwx------ 2 researcher2 research_team 4096 Feb 19 21:15 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_k.txt
-rw------- 1 researcher2 research_team   46 Feb 19 21:15 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb 19 21:15 project_t.txt
```

## Summary

En resumen en este documento se muestran los comandos para administrar los permisos para los 3 perfiles de owners que permite Linux. User, Group y Others.
Se aprendió a revelar los permisos, a identificar los tipos de archivos, ya sea directorios o archivos de texto y revelar archivos ocultos.
También se revisaron los comandos para hacer las modificaciones de estos permisos.
Este conocimiento resulta de gran utilidad para endurecer la seguridad en Linux.