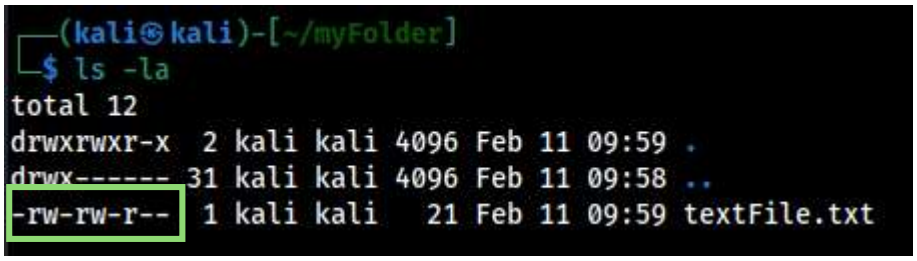
Il primo passaggio è stato quello di creare una cartella chiamata “myFolder” con al suo interno un file chiamato “textFile.txt”.

Successivamente sono andato a visualizzare i permessi della cartella creata

E del file al suo interno



Possiamo notare come, nella directory, sono presenti delle sequenze di lettere che indicano i permessi:

d che indica che si tratta di una cartella

la prima serie di lettere “rwx” è la parte che specifica i permessi del proprietario del file “kali”

r permessi di lettura

w permessi di scrittura

x permessi di esecuzione o accesso alla cartella

la seconda serie di lettere “rwx” indica i permessi del gruppo “kali” proprietario che in questo caso hanno gli stessi diritti del proprietario “kali”

le ultime tre lettere “r-x” indicano i permessi degli altri

r permessi di lettura

- permessi di modifica non presenti

x permessi di esecuzione

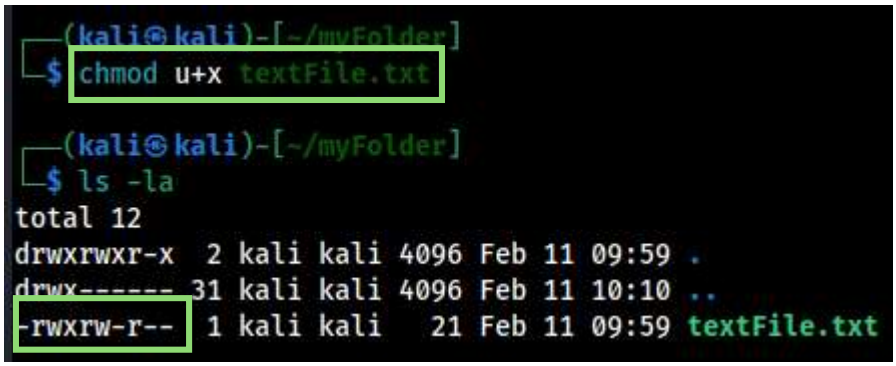
lo stesso discorso vale per il file “textFile.txt” dove però la prima lettera è “-“ e non “d” che indica appunto che si tratta di un file.

La parte dell’utente indica che si tratta di un file scrivibile e leggibile ma non eseguibile, la parte del gruppo è la stessa dell’utente mentre la parte degli altri indica che possono solo leggere e non modificare e eseguire.

Proviamo a dare il permesso di esecuzione all'utente "kali" corrente, usando il comando:

chmod u+x nomeDelFile

dove chmod sta per "CHange MODe" e appunto serve per modificare i permessi, u sta ad indicare l'utente corrente, + sta ad indicare che stiamo aggiungendo permessi e x sta ad indicare i permessi di esecuzione

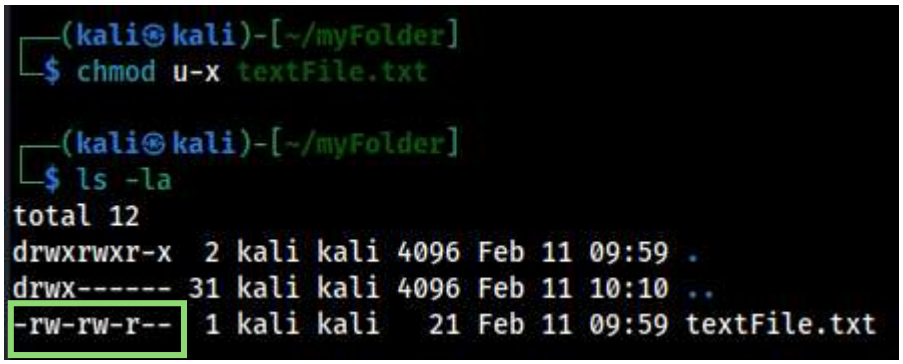


Facendo una visualizzazione dei permessi, possiamo notare come nella sequenza dei permessi è comparsa la lettera "x" nella sezione dedicata all' utente il che sta a significare che l'utente potrebbe eseguire il file.

Per rimuovere questo permesso, uso il comando:

chmod u-x nomeDelFile

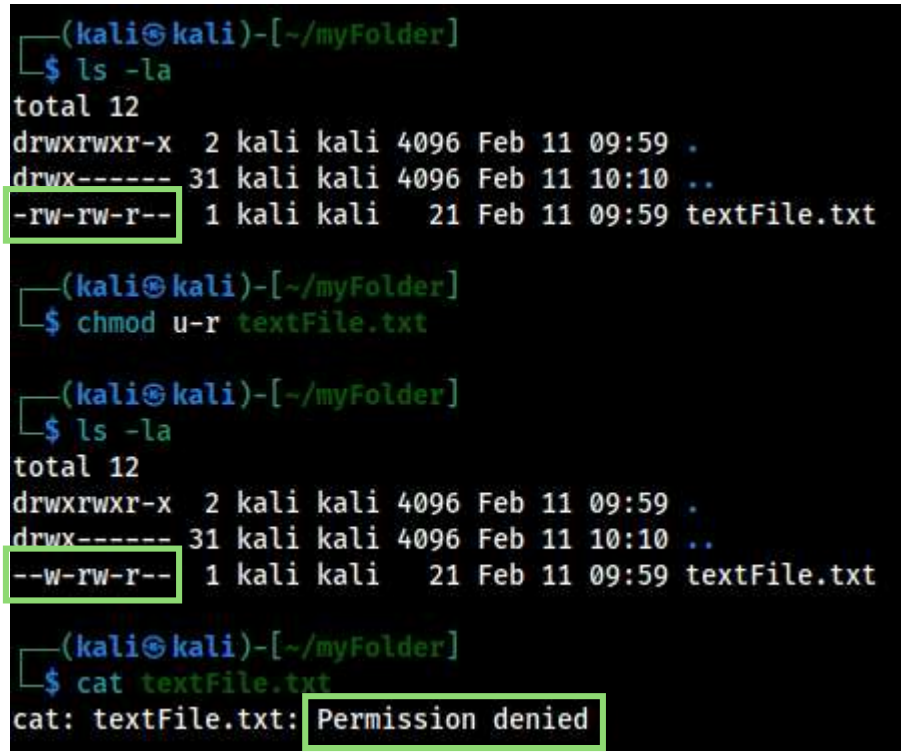
dove appunto "-"sta ad indicare la rimozione del permesso indicato



Per poter testare i permessi, rimuovo la possibilitá di poter leggere il file all'utente corrente usando il comando:

chmod u-r NomeDelFile

dove appunto con "-"rimuovo un permesso e con "r" indico il permesso di lettura.
Possiamo notare dalla successiva immagine come prima della modifica dei permessi, il flag di lettura era presente prima del file e che dopo la modifica con chmod fosse diventato "-" infatti, provando a leggere il file usando il comando cat, viene detto che il permesso è stato negato:



Cambiare i permessi di un file con chmod è essenziale per garantire **sicurezza** e **controllo degli accessi** in un sistema Linux dato che potrebbero essere presenti dei file contenenti passwords o configurazioni che non dovrebbero essere letti da chiunque.
La limitazione dei permessi è utile anche per dire al sistema operativo come deve interpretare un file come, ad esempio, un file .sh dovrebbe essere eseguito e modificato in fase di configurazione solo da un utente root e non da chiunque compromettendone l'integrità.