# Relazione: Gestione dei Permessi di Lettura, Scrittura ed Esecuzione in Linux

## Motivazione delle Scelte sui Permessi Configurati

### File: esempio.txt

Per il file esempio.txt, ho utilizzato il comando:  
chmod u=rw,g=r,o=r esempio.txt  
Questa configurazione assegna:  
- al proprietario (u): i permessi di lettura e scrittura;  
- al gruppo (g): solo il permesso di lettura;  
- agli altri utenti (o): solo il permesso di lettura.  
  
Motivazione:  
- La decisione di consentire al proprietario di leggere e scrivere garantisce la piena gestione del file da parte dell'utente che lo ha creato.  
- I membri del gruppo possono solo leggere il contenuto del file, il che è utile per la condivisione delle informazioni senza rischi di modifica accidentale.  
- Gli altri utenti hanno accesso in sola lettura per favorire la consultazione del file senza compromettere la sicurezza o l’integrità dei dati.  
  
Questa configurazione bilancia la necessità di gestione esclusiva del file da parte del proprietario con l’esigenza di accesso controllato da parte di altri utenti.

### Directory: esempio\_dir

Per la directory esempio\_dir, ho utilizzato il comando:  
chmod u=rwx,g=rx,o=rx esempio\_dir  
Questa configurazione assegna:  
- al proprietario (u): i permessi di lettura, scrittura ed esecuzione;  
- al gruppo (g): i permessi di lettura ed esecuzione;  
- agli altri utenti (o): i permessi di lettura ed esecuzione.  
  
Motivazione:  
- Il proprietario ha pieni permessi (rwx), permettendo di creare, eliminare e modificare i file all’interno della directory, oltre a poter accedere ai contenuti.  
- I membri del gruppo e gli altri utenti hanno permessi di lettura ed esecuzione (rx), il che consente di accedere al contenuto della directory e aprire i file, senza tuttavia modificarne la struttura o crearne di nuovi.  
- Questa configurazione è adatta per condividere i file contenuti nella directory senza compromettere la sua organizzazione o sicurezza.  
  
La scelta di includere il permesso di esecuzione (“x”) per il gruppo e gli altri utenti è fondamentale, poiché senza di esso non sarebbe possibile accedere ai file all’interno della directory.

## Analisi dei Risultati dei Test sui Permessi

### File: esempio.txt

- Scrittura: Il proprietario è stato in grado di modificare il file senza problemi, confermando la corretta assegnazione dei permessi di scrittura.  
- Lettura: I membri del gruppo e gli altri utenti hanno potuto leggere il file, ma non modificarlo, come previsto.  
- Esecuzione: Tentativi di eseguire il file (non necessario per un file di testo) hanno restituito un errore, confermando l’assenza del permesso di esecuzione.

### Directory: esempio\_dir

- Creazione di file: Solo il proprietario è stato in grado di creare nuovi file all’interno della directory.  
- Accesso ai file: I membri del gruppo e gli altri utenti hanno potuto elencare e aprire i file nella directory, ma non modificarli o crearne di nuovi.  
- Rimozione di file: Solo il proprietario è riuscito a rimuovere file dalla directory, come previsto.

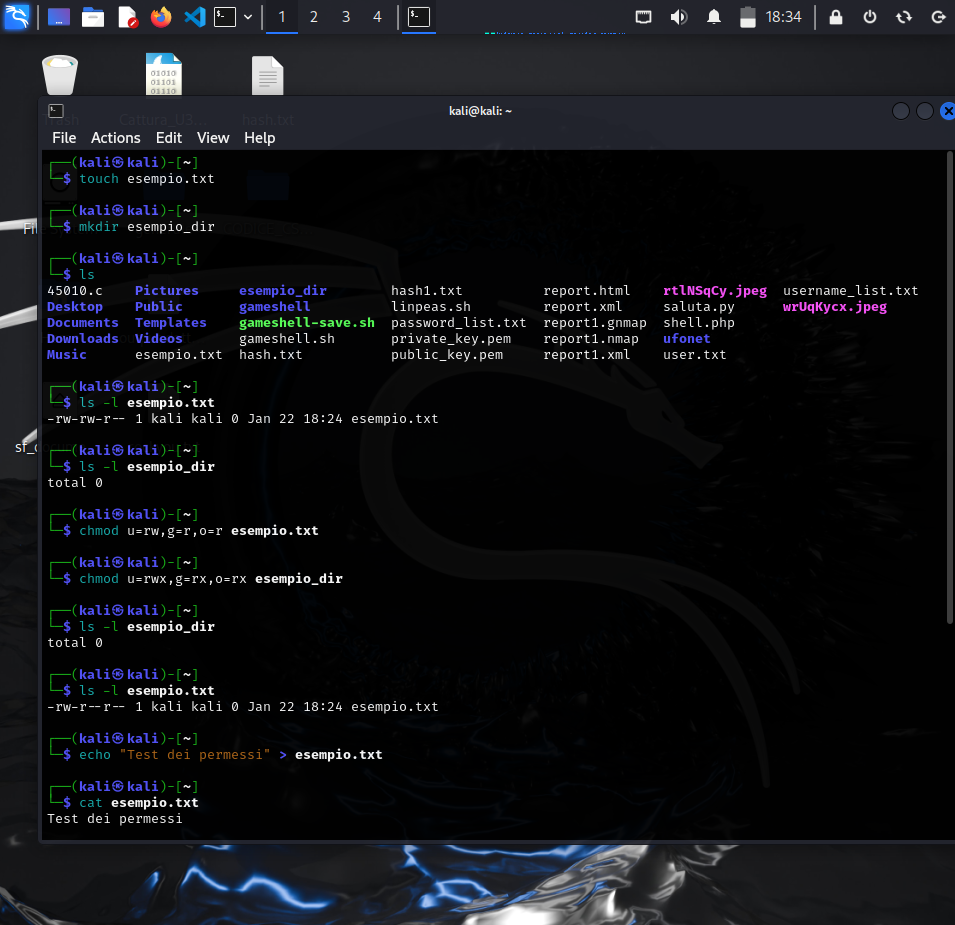
## Conclusione

Le scelte effettuate per la configurazione dei permessi hanno dimostrato di essere adeguate alle esigenze. Hanno garantito:  
- La sicurezza e l’integrità dei file e della directory;  
- Un accesso controllato per i membri del gruppo e gli altri utenti;  
- La piena gestione da parte del proprietario.  
  
Questa configurazione è particolarmente utile in contesti in cui il proprietario deve mantenere il controllo completo sui file e sulla directory, ma è necessaria una condivisione sicura delle risorse con altri utenti.

## Screenshot della Creazione e Test dei Permessi

Di seguito sono riportati i due screenshot che mostrano la creazione dei file e i test relativi ai permessi configurati:

Screenshot 1: Creazione del file e modifica dei permessi



Screenshot 2: Test dei permessi configurati

