S10L2

**Relazione: Gestione dei Permessi in Linux**

**Obiettivo**

Configurare e gestire i permessi di lettura, scrittura ed esecuzione per file o directory in un sistema Linux, documentando i passaggi con screenshot e analizzando i risultati.

**1. Creazione del File o della Directory**

**Comando Eseguito:**

* Per creare un file:

touch file.txt

* Per creare una directory:

mkdir directory\_dir

**Risultati:**



**2. Verifica dei Permessi Attuali**

**Comandi Eseguiti:**

* Per verificare i permessi attuali:

ls -l file.txt

ls -l directory\_dir

**Risultati:**



**3. Modifica dei Permessi**

**Comandi Eseguiti:**

* Per cambiare i permessi del file per consentire la scrittura a tutti gli utenti:

chmod u=rw,g=r,o=r file.txt

* Per cambiare i permessi della directory per consentire l'accesso completo solo al proprietario:

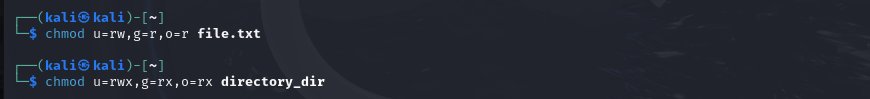
chmod u=rwx,g=rx,o=rx directory\_dir

**Verifica:**

* Dopo le modifiche, verifica i permessi con:
* ls -l file.txt

ls -l directory\_dir

**Risultati:**



**4. Test dei Permessi**

**Test del File:**

* Comando per verificare la scrittura nel file:

echo "prova scrittura su file" >> esempio.txt

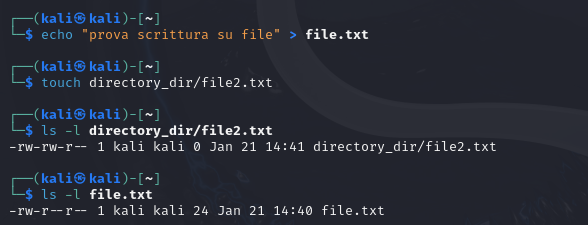
* Risultato Atteso:
  + Se i permessi sono corretti, il comando aggiungerà il testo al file senza errori.

**Test della Directory:**

* Comando per creare un file nella directory:

touch esempio\_dir/file2.txt

* Risultato Atteso:
  + Solo il proprietario può creare nuovi file nella directory. Altri utenti otterranno un errore di "Permission denied".



**5. Scelte dei permessi**

1. **File:** Ho configurato i permessi per consentire la lettura e scrittura a tutti gli utenti, rendendo il file accessibile e modificabile da chiunque.
2. **Directory :** Ho impostato i permessi per garantire che solo il proprietario possa accedere, modificare e creare file nella directory, proteggendo i dati sensibili.