S10 – L2

Gestione dei permessi in Linux (Kali Linux)

Introduzione

In questo esercizio ho configurato e **verificato i permessi di accesso su file e directory in ambiente Linux (Kali).**
L'obiettivo è stato applicare concretamente i c**oncetti di autorizzazione basati su utente, gruppo e altri (others)**, utilizzando i comandi **`chmod`, `chgrp`, `useradd`, `ls -l`** e verificando il corretto funzionamento attraverso test pratici.

Preparazione ambiente

Per eseguire test realistici sui permessi ho creato utenti e un gruppo dedicato.

1. Creo un gruppo di laboratorio

```
sudo groupadd labgrp
```

2. Creo due utenti

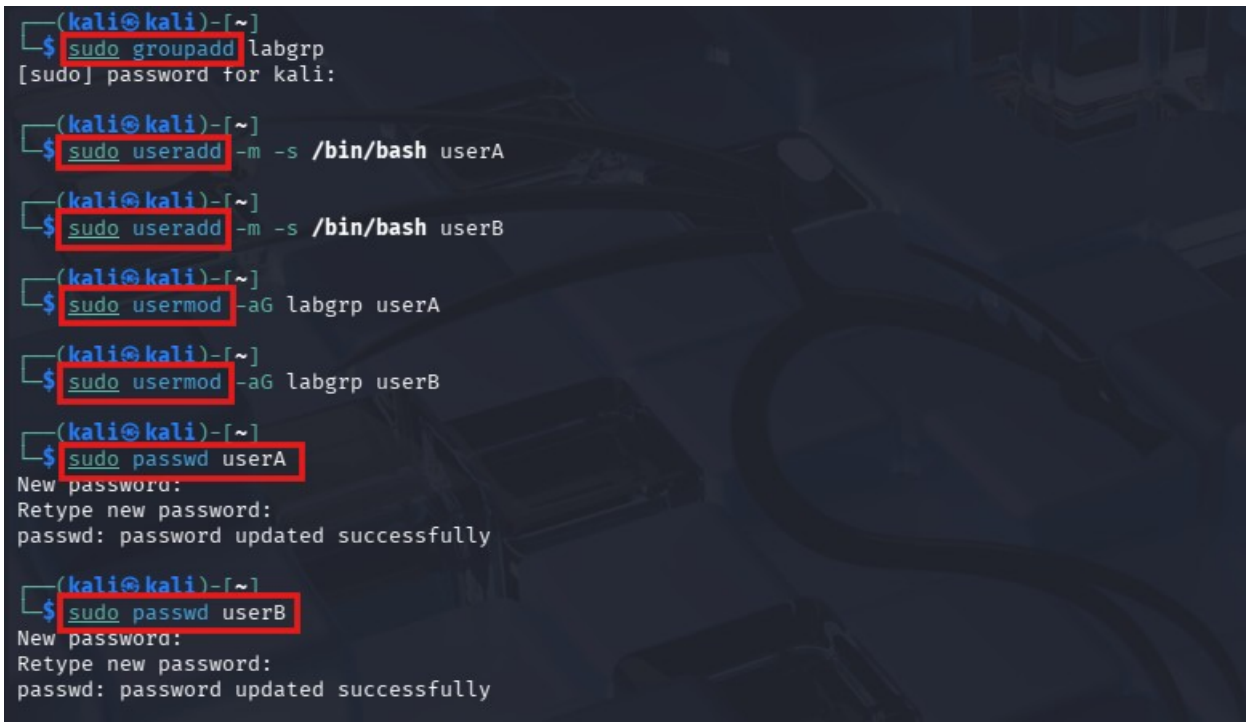
```
sudo useradd -m -s /bin/bash userA
sudo useradd -m -s /bin/bash userB
```

3. Inserisco gli utenti nel gruppo

```
sudo usermod -aG labgrp userA
sudo usermod -aG labgrp userB
```

4. Imposto le password

```
sudo passwd userA (userA123)
sudo passwd userB (userB123)
```

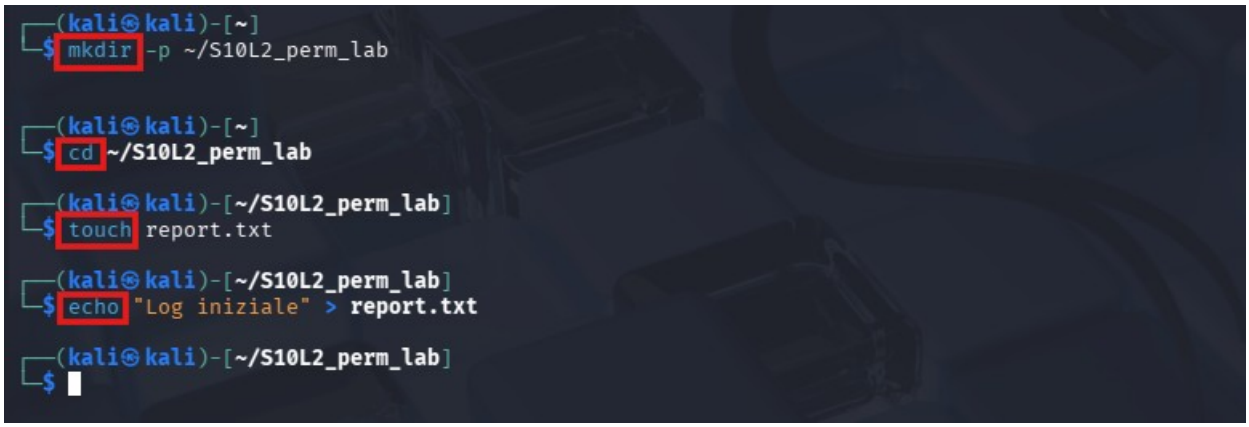


Output comandi di creazione utenti/gruppo, password

FASE 1 — Creazione directory e file

Creo una directory di laboratorio e un file al suo interno.

```
mkdir -p ~/S10L2_perm_lab
cd ~/S10L2_perm_lab
touch report.txt
echo "Log iniziale" > report.txt
```



Terminale con mkdir/touch/echo e output

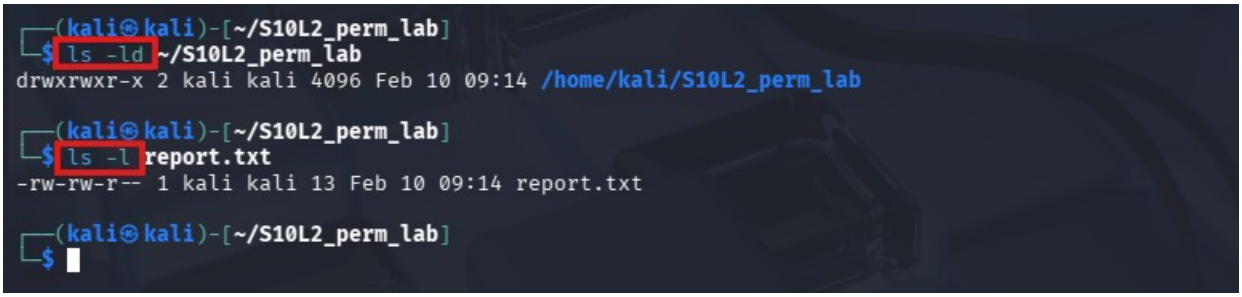
Con questi comandi:

- Creo la cartella `S10L2_perm_lab`
- Creo il file `report.txt`
- Inserisco un contenuto iniziale

FASE 2 — Verifica permessi iniziali

Controllo i permessi attuali prima di modificarli.

```
ls -ld ~/S10L2_perm_lab
ls -l report.txt
```



Output di `ls -ld` e `ls -l` *prima* di qualsiasi modifica.

Osservo:

- Proprietario (owner)
- Gruppo
- Stringa dei permessi (es. `drwxr-xr-x`, `-rw-r--r--`)

FASE 3 — Modifica permessi e gruppo

1. Assegno il gruppo alla directory e al file

```
sudo chgrp labgrp ~/S10L2_perm_lab
sudo chgrp labgrp report.txt
```

2. Modifico i permessi

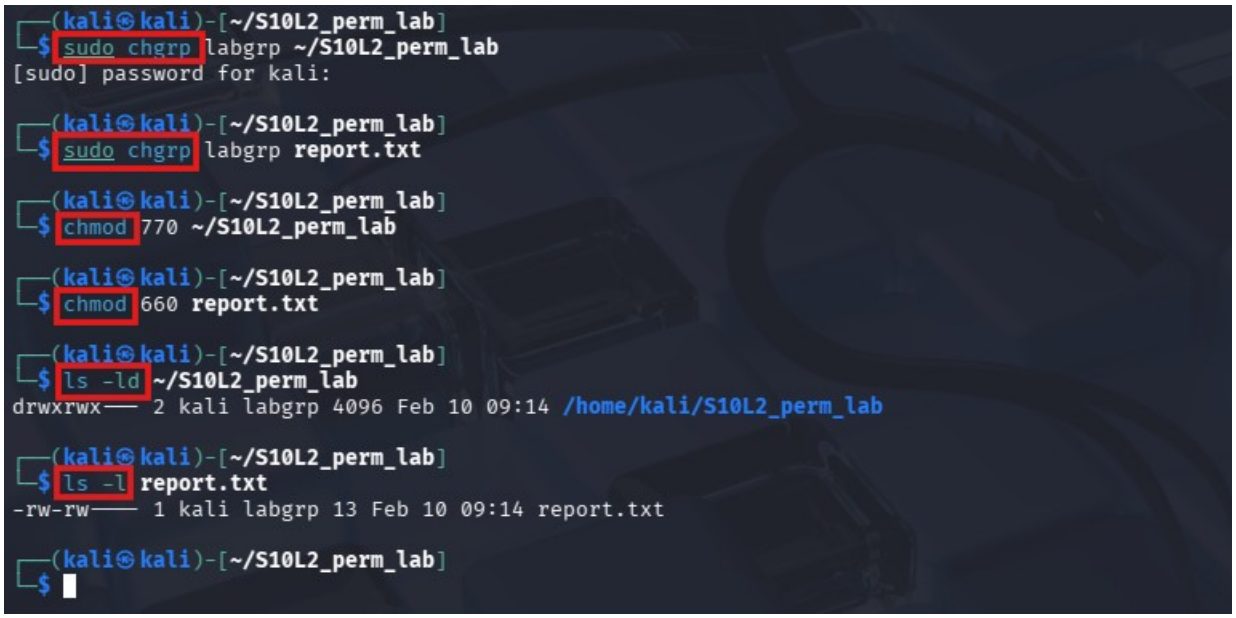
Imposto:

- Directory → 770
- File → 660

```
chmod 770 ~/S10L2_perm_lab
chmod 660 report.txt
```

Verifico:

```
ls -ld ~/S10L2_perm_lab
ls -l report.txt
```



Comandi chmod + output ls -l/ls -ld *dopo* la modifica.

Significato dei permessi:

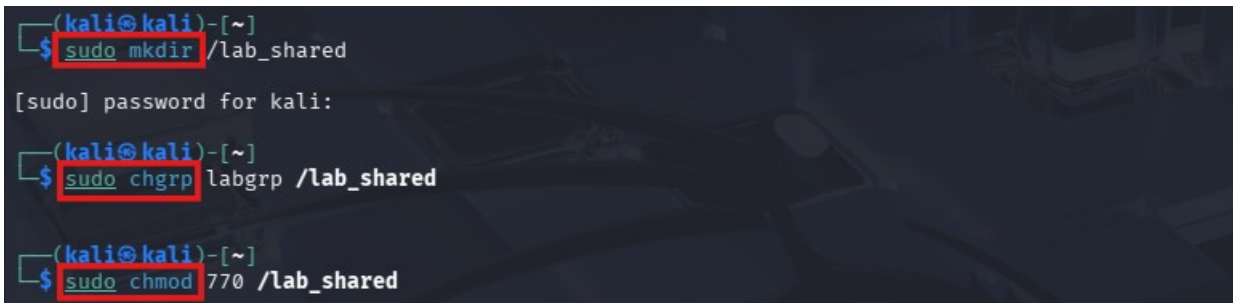
- 7 = lettura + scrittura + esecuzione
- 6 = lettura + scrittura
- 0 = nessun permesso

Ho quindi configurato:

- Accesso completo per owner e gruppo
- Nessun accesso per altri utenti

Creo directory condivisa fuori dalla home

```
sudo mkdir /lab_shared
sudo chgrp labgrp /lab_shared
sudo chmod 770 /lab_shared
```



Creo il file

```
sudo touch /lab_shared/report.txt
sudo chgrp labgrp /lab_shared/report.txt
sudo chmod 660 /lab_shared/report.txt
```

FASE 4 — Test pratico dei permessi: Test come userA (membro del gruppo come userB)

```
su - userA
cd /lab_shared
pwd
echo "Scrittura da userA" >> report.txt
touch creato_da_userA.txt
ls -l
exit
```

Output test permessi userA

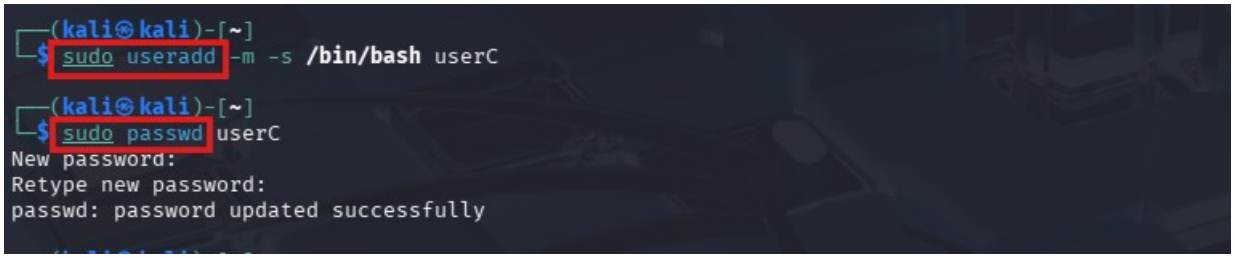
Risultato:

- La scrittura nel file riesce
- La creazione di un nuovo file riesce

Test con utente NON autorizzato

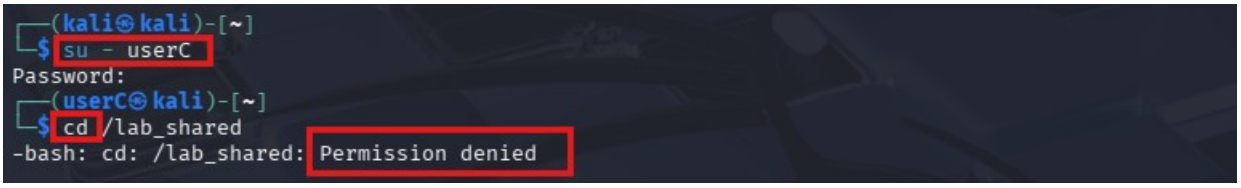
Creo un terzo utente non appartenente al gruppo.

```
sudo useradd -m -s /bin/bash userC
sudo passwd userC (userC123)
```



Test:

```
su - userC
cd /lab_shared
```



Output del terminale che mostra l'errore "Permission denied" durante il tentativo di accesso alla directory condivisa da parte di un utente non appartenente al gruppo autorizzato.

Risultato atteso:

- Permission denied
- Nessuna creazione o modifica consentita

Analisi dei risultati

Dai test effettuati ho verificato che:

- Gli utenti appartenenti al gruppo `labgrp` possono modificare il file e creare nuovi file nella directory.
- Un utente esterno al gruppo non può accedere né scrivere.
- I permessi configurati con **`chmod`** e **`chgrp`** funzionano correttamente.

Questo dimostra che il controllo degli accessi basato su utente e gruppo è stato applicato in modo efficace.

Conclusioni

Attraverso questo esercizio ho **configurato e verificato** con test pratici la **gestione dei permessi in Linux**. Ho applicato il **principio del privilegio minimo**, consentendo operazioni solo agli utenti autorizzati e bloccando gli altri.

Ho applicato in modo pratico la gestione dei permessi in ambiente Linux, configurando correttamente **accessi basati su utente e gruppo.**

Ho creato una directory condivisa e un file associato, impostando permessi specifici (770 per la directory e 660 per il file) e assegnando il gruppo autorizzato tramite `chgrp`.

I test effettuati hanno dimostrato che:

- **Gli utenti appartenenti al gruppo `labgrp` possono accedere alla directory, modificare il file e creare nuovi file.**
- **Un utente non appartenente al gruppo riceve correttamente l’errore “Permission denied”, confermando l’efficacia delle restrizioni applicate.**

L’esercizio ha quindi permesso di verificare concretamente il funzionamento del modello di autorizzazione Linux (owner, group, others) e l’applicazione del principio del privilegio minimo, garantendo accesso solo ai soggetti autorizzati.