AMATO SARA

S10 L2

**Gestione dei Permessi di Lettura, Scrittura ed Esecuzione in Linux**

L’obiettivo dell’esercizio è stato configurare e gestire i permessi su file e directory in un sistema Linux, utilizzando strumenti nativi come chmod e testando i permessi configurati con un secondo utente. I permessi in Linux permettono di definire chi può leggere, scrivere o eseguire file e directory, offrendo un controllo granulare per garantire la sicurezza del sistema.

**Passaggi Svolti:**

1. Creazione del file e della directory

Ho iniziato creando un file (esempio.txt) e una directory (esempio\_dir) all’interno della home directory dell’utente kali:

touch esempio.txt

mkdir esempio\_dir

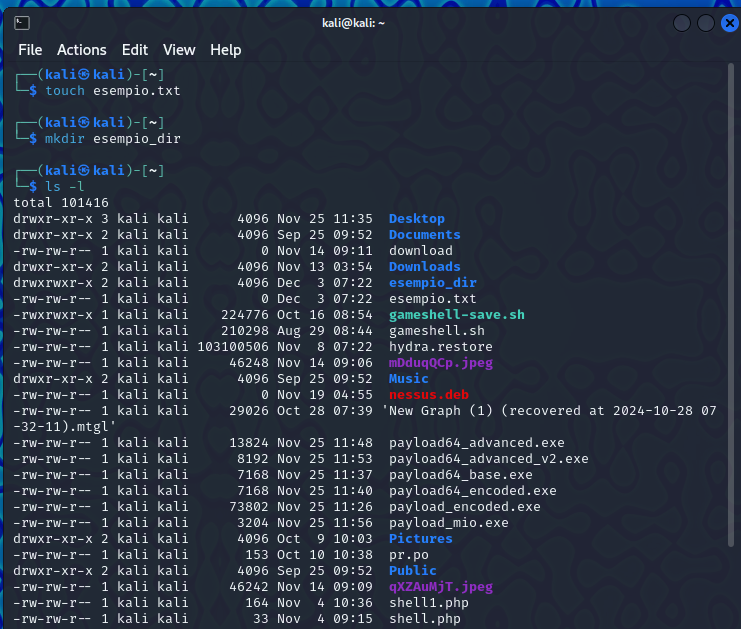
Ho quindi verificato i permessi di default utilizzando il comando:

ls -l

L'output ha mostrato:

-rw-rw-r-- 1 kali kali 0 Dec 3 07:22 esempio.txt

drwxrwxr-x 2 kali kali 4096 Dec 3 07:22 esempio\_dir



Analisi:

Il file esempio.txt ha i permessi -rw-rw-r--, indicando che il proprietario e il gruppo possono leggere e scrivere, mentre gli altri possono solo leggere.

La directory esempio\_dir ha i permessi drwxrwxr-x, che permettono al proprietario e al gruppo di leggere, scrivere ed eseguire, mentre gli altri possono solo leggere ed eseguire.

2. Modifica dei permessi del file

Per restringere l’accesso al file, ho modificato i permessi utilizzando:

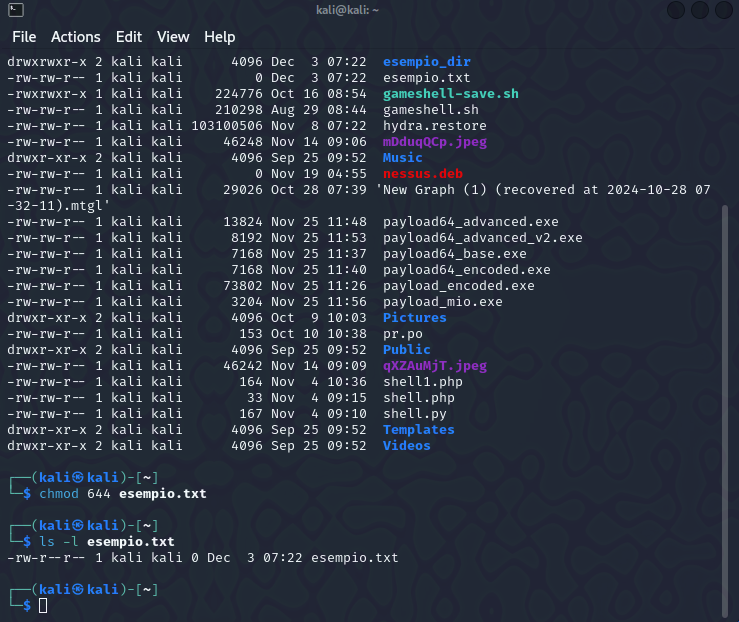
chmod 644 esempio.txt

Successivamente, ho verificato nuovamente i permessi:

ls -l esempio.txt

L'output è stato:

-rw-r--r-- 1 kali kali 0 Dec 3 07:22 esempio.txt



Interpretazione:

Ora, solo il proprietario (kali) può leggere e scrivere.

Gli altri utenti, inclusi quelli appartenenti al gruppo, possono solo leggere.

3. Scrittura nel file

Ho verificato che l’utente kali potesse ancora scrivere nel file:

echo "prova" > esempio.txt

L'operazione è riuscita senza errori, confermando che i permessi rw- per il proprietario erano corretti.

4. Creazione di un nuovo utente

Per testare i permessi configurati, ho creato un nuovo utente chiamato testuser:

sudo useradd -m testuser

sudo passwd testuser

Dopo essermi autenticato come testuser, ho cercato di accedere al file esempio.txt.

5. Test dei permessi con testuser

Tentativo di scrittura nel file:

echo "test di scrittura by testuser" > /home/kali/esempio.txt

Questo comando ha generato l’errore:

sh: 1: cannot create /home/kali/esempio.txt: Permission denied

La scrittura è stata bloccata dai permessi del file (-rw-r--r--), che consentono solo al proprietario di scrivere.

Tentativo di lettura del file:

cat /home/kali/esempio.txt

Anche la lettura ha fallito con il messaggio:

cat: /home/kali/esempio.txt: Permission denied

Questo è dovuto ai permessi della directory /home/kali:

drwx------ 23 kali kali 4096 Dec 3 07:22 /home/kali

Poiché la directory personale di kali è completamente chiusa agli altri utenti (------), testuser non può nemmeno accedere al file.

Analisi delle Scelte sui Permessi

Permessi sul file (esempio.txt):

L'uso del comando chmod 644 ha reso il file leggibile da tutti, ma modificabile solo dal proprietario. Questo è ideale in contesti in cui si desidera condividere informazioni senza permettere modifiche non autorizzate.

Permessi sulla directory /home/kali:

I permessi predefiniti drwx------ proteggono la directory personale dell'utente kali, impedendo ad altri utenti di accedere ai file al suo interno, anche se i permessi del file lo consentirebbero.

Esclusione di modifiche alla directory:

Non ho modificato i permessi della directory /home/kali, poiché in un sistema reale ciò rappresenterebbe un rischio per la sicurezza.

**Conclusioni**

Questo esercizio ha mostrato come i permessi in Linux si combinano per determinare l'accesso ai file e alle directory. In particolare:

* I permessi dei file (chmod) regolano chi può leggere, scrivere o eseguire un file.
* I permessi delle directory prevalgono sui file al loro interno, bloccando o consentendo l'accesso.
* Per garantire sicurezza e privacy, è fondamentale configurare correttamente sia i permessi delle directory che quelli dei file.

**Proposte di Miglioramento**

Utilizzo di una directory condivisa: Per testare in modo più efficace i permessi, sarebbe stato utile creare una directory condivisa, con permessi configurati esplicitamente per consentire l'accesso a più utenti.

Gestione dei gruppi: L’aggiunta di entrambi gli utenti (kali e testuser) a un gruppo comune avrebbe permesso di sperimentare con i permessi di gruppo.

Utilizzo di ACL: Per un controllo più granulare, le ACL (Access Control Lists) offrono un livello superiore di gestione rispetto ai tradizionali permessi.