

PERMESSI DI LINUX

Traccia: Configurare e gestire i permessi di lettura, scrittura ed esecuzione per file o directory in un sistema Linux.

La scelta dei file o delle directory da configurare spetta allo studente.

Infine, lo studente dovrà creare degli screenshot che mostrino i passaggi effettuati e scrivere una relazione spiegando le scelte fatte riguardo ai permessi.

Indice:

- **Introduzione**
- **Descrizione dei permessi in Linux**
- **Creazione di Directory e File**
- **Verifica dei permessi**
- **Modifica dei permessi**
- **Test di scrittura con l'utente corrente**
- **Secondo test di scrittura**
- **Conclusioni**

Introduzione

Nell'esercitazione odierna si chiede di configurare e gestire i permessi di lettura, scrittura ed esecuzione per file o directory in un sistema Linux, le modalità sono a discrezione dello studente.

Si tratta di una funzione di Linux fondamentale per garantire sicurezza e controllo sull'accesso ed utilizzo delle risorse.

I permessi in Linux si dividono in 3 categorie:

- Lettura (consente la sola lettura);
- Scrittura (consente la scrittura, quindi modifica o cancellazione);
- Esecuzione (non valida per i file di solo testo).

Creazione Directory e File

Il primo passaggio per l'esecuzione dell'esercizio sarà la creazione di una nuova Directory ed un file da utilizzare come test. Per comodità e praticità andremo a realizzare una cartella sul Desktop chiamata *cartella_prova*, ed al suo interno inseriremo un file fittizio di testo che chiameremo *testo.txt*.

```
(kali㉿kali)-[~]  
$ cd Desktop  
  
(kali㉿kali)-[~/Desktop]  
$ mkdir cartella_prova  
  
(kali㉿kali)-[~/Desktop]  
$ cd cartella_prova  
  
(kali㉿kali)-[~/Desktop/cartella_prova]  
$ touch testo.txt  
  
(kali㉿kali)-[~/Desktop/cartella_prova]  
$
```

Nello screenshot appena allegato potremo vedere i comandi utilizzati per la creazione della directory e del file.

Verifica dei permessi

Come passo successivo andremo a verificare i permessi presenti per il file appena creato tramite il comando `ls -lA`.

```
(kali㉿kali)-[~/Desktop/cartella_prova]  
$ ls -lA  
total 0  
-rw-rw-r-- 1 kali kali 0 Dec  3 08:49 testo.txt
```

Andando ad interpretare possiamo verificare che:

- l'utente corrente possiede i permessi di lettura e scrittura;
- il gruppo di utenti possiede i permessi di lettura e scrittura;
- il permesso degli altri utenti esterni possiede il permesso di sola lettura.

Modifica dei permessi

Per fare delle prove, andremo ad utilizzare il comando *chmod* per modificare i permessi per tale file, andremo a rimuovere i permessi di scrittura all'utente corrente ed al gruppo, ed eseguiremo nuovamente *ls -lA* per verificare che siano stati rimossi correttamente.

```
(kali㉿kali)-[~/Desktop/cartella_prova]
$ chmod u-w testo.txt

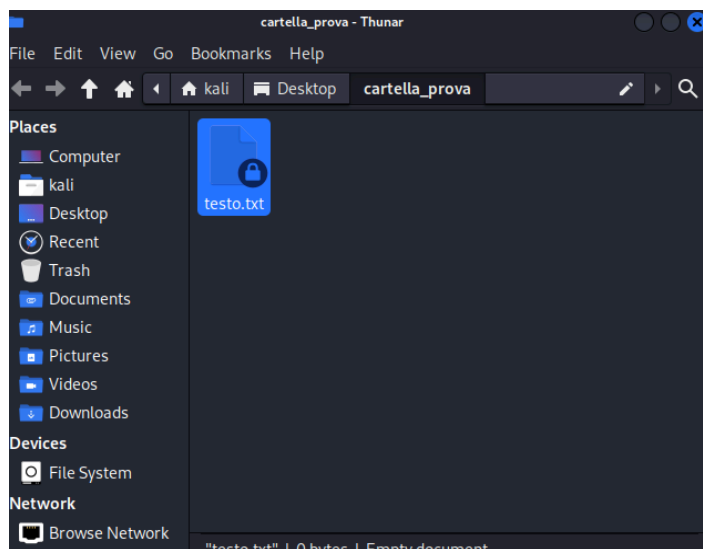
(kali㉿kali)-[~/Desktop/cartella_prova]
$ ls -lA
total 0
-r--r--r-- 1 kali kali 0 Dec  3 08:49 testo.txt
```

Per “u” si intende l'utente corrente. Precedentemente è stato modificato anche su “g” ovvero il gruppo. Per rimuovere i permessi si utilizza il simbolo “-”, per aggiungerli il simbolo “+”.

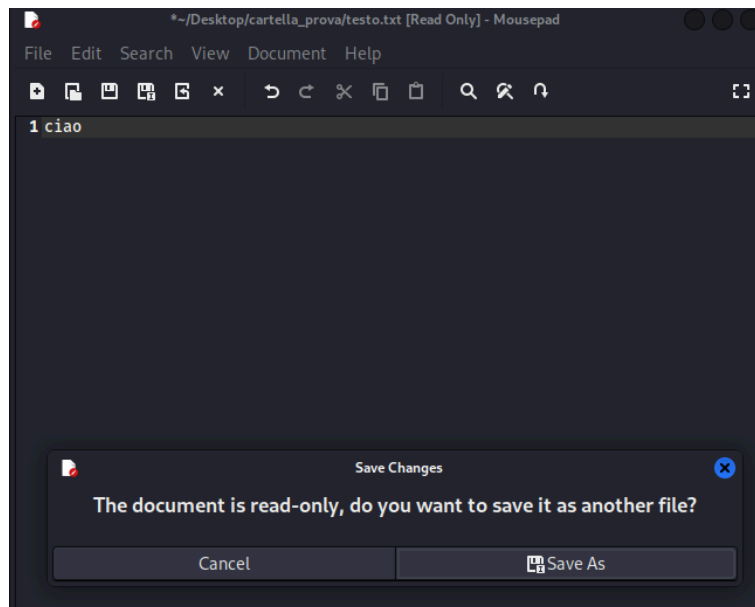
Come possiamo vedere, i permessi sono stati correttamente modificati.

Test di scrittura con utente corrente

Per verificare che realmente l'utente corrente non possa scrivere sul file, andremo a provare a modificarlo fisicamente. L'output che ci restituirà sarà il seguente:



Possiamo notare la presenza del lucchetto, il quale sta a significare che si tratta di un file con permesso di sola lettura, infatti potremo tranquillamente aprirlo, ma non ci consentirà la modifica, ma al massimo la creazione di un file separato, contenente le modifiche apportate, senza intaccare il file originale.



Secondo test di scrittura

Per fare una seconda prova, si andrà a restituire all'utente corrente il permesso di scrittura come da screenshot che segue:

```
(kali㉿kali)-[~/Desktop/cartella_prova]
$ chmod g-w testo.txt

(kali㉿kali)-[~/Desktop/cartella_prova]
$ ls -lA
total 0
-rw-r--r-- 1 kali kali 0 Dec  3 08:49 testo.txt
```

Andando a guardare il file, potremo notare che sarà possibile aprire e modificare il file a piacimento, in quanto il lucchetto che ne bloccava la modifica, non sarà più presente ed all'utente corrente è stata appena restituita la possibilità di modificare quello specifico file.

Tali permessi possono essere applicati anche alle Directory.

Conclusioni

L'esercitazione ha permesso di comprendere l'importanza della corretta gestione dei permessi di lettura, scrittura ed esecuzione in un sistema Linux.

Attraverso la creazione di una directory e di un file di test, è stato possibile verificare come i permessi influenzano l'accesso e le operazioni che gli utenti possono eseguire.

L'utilizzo del comando *chmod* ha dimostrato la flessibilità con cui è possibile configurare i permessi, garantendo il controllo sull'utilizzo dei file e delle directory da parte di diversi utenti o gruppi.

In particolare, i test di scrittura hanno evidenziato come la rimozione o l'aggiunta dei permessi di scrittura influenzi la possibilità di modificare un file. La gestione accurata di questi permessi è cruciale per garantire la sicurezza e il corretto funzionamento del sistema, evitando modifiche accidentali o accessi non autorizzati.

*Progetto a cura di
Sonia Laterza*