

Gestione dei Permessi in Linux

L'esercizio si è concentrato sulla gestione dei permessi di lettura, scrittura ed esecuzione su file e directory in un ambiente Linux. L'obiettivo era comprendere il significato dei permessi e la loro modifica tramite comandi specifici.

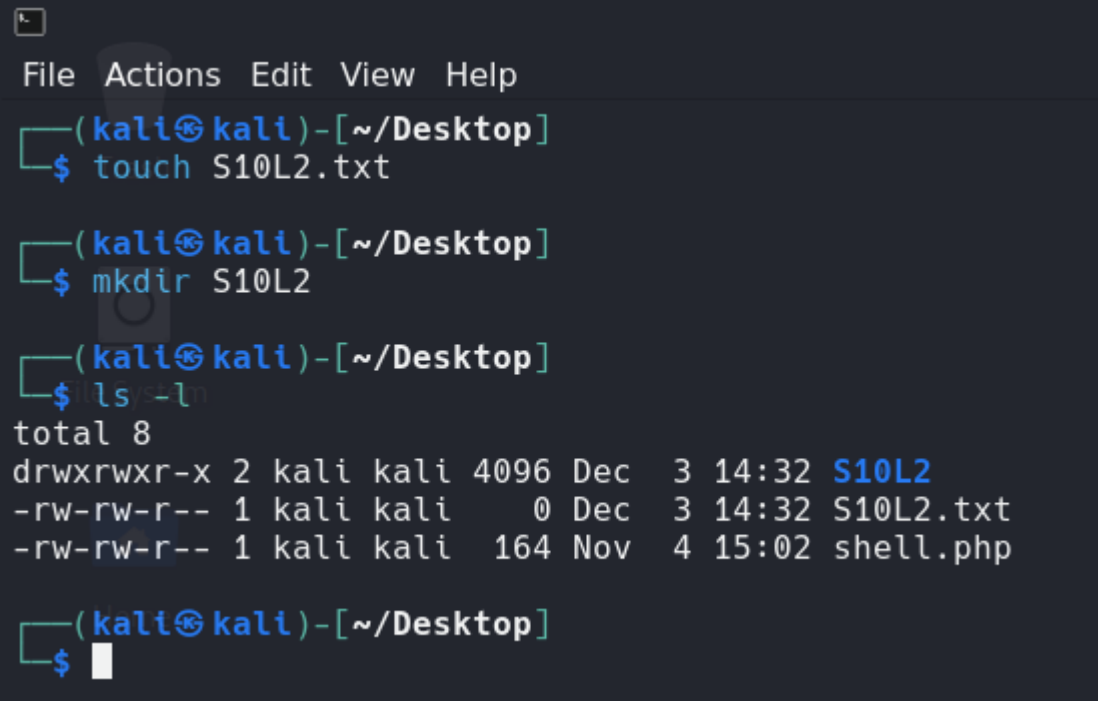
Ho creato un file di testo chiamato S10L2.txt utilizzando il comando:

touch S10L2.txt

Ho creato una directory chiamata S10L2 con il comando:

mkdir S10L2

Una volta creata la cartella e il file ne ho verificato i permessi con il comando **ls -l**



```
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ touch S10L2.txt

(kali㉿kali)-[~/Desktop]
$ mkdir S10L2

(kali㉿kali)-[~/Desktop]
$ ls -l
total 8
drwxrwxr-x 2 kali kali 4096 Dec  3 14:32 S10L2
-rw-rw-r-- 1 kali kali    0 Dec  3 14:32 S10L2.txt
-rw-rw-r-- 1 kali kali  164 Nov  4 15:02 shell.php

(kali㉿kali)-[~/Desktop]
$
```

L'output ha mostrato i permessi iniziali assegnati dal sistema.

I file in Linux riportano le autorizzazioni per l'utente corrente «u», il gruppo «g» e gli altri utenti «o» e il «-» è utilizzato in mancanza di quel particolare permesso.

-Il Permesso di lettura è indicato con la lettera «r», che sta per read. E' il permesso che consente agli utenti di vedere il contenuto del file o di una directory.

-Il Permesso di scrittura è indicato con la lettera «w», che sta per write. E' il permesso che consente agli utenti di scrivere o modificare il contenuto di un file. Il permesso write consente anche di eliminare un file.

-Il Permesso di esecuzione è indicato con la lettera «x», che sta per execute. E' il permesso che consente agli utenti eseguire un file – in questo caso si parla di file eseguibili. Non si troverà mai un permesso «x» su un file di testo.

Ho modificato i permessi del file S10L2.txt, rimuovendo i diritti di lettura e scrittura per l'utente (proprietario) con il comando:

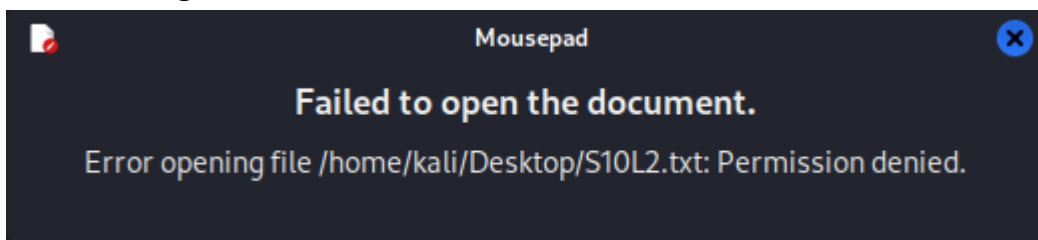
chmod u-rw S10L2.txt

Successivamente verificato che i diritti fossero stati cambiati, come infatti possiamo vedere nella foto.

```
(kali㉿kali)-[~/Desktop]
$ chmod u-rw S10L2.txt

(kali㉿kali)-[~/Desktop]
$ ls -l
total 8
drwxrwxr-x 2 kali kali 4096 Dec  3 14:32 S10L2
----rw-r-- 1 kali kali    0 Dec  3 14:32 S10L2.txt
-rw-rw-r-- 1 kali kali  164 Nov  4 15:02 shell.php
```

L'output ha confermato che i permessi di lettura e scrittura per l'utente erano stati rimossi, infatti se si prova ad aprire il file ci verrà mostrato a schermo un errore con **accesso negato**.



Conclusione

Questo esercizio ha dimostrato come i permessi possano essere gestiti in modo preciso su file e directory, controllando l'accesso in base alle esigenze. La rimozione dei diritti di lettura e scrittura all'utente dimostra come si possano implementare restrizioni di sicurezza. L'utilizzo di comandi come **chmod** e **ls -l** è essenziale per monitorare e modificare i permessi in un ambiente Linux.