

S10L2 - Permessi su Kali Linux

L'esercizio mira a comprendere la gestione dei permessi in Linux, focalizzandosi su come configurare i privilegi di lettura, scrittura ed esecuzione. L'attenzione si è concentrata su un file sensibile, dove era necessario limitare le modifiche al solo proprietario, consentendo agli altri di leggerlo. Questo approccio garantisce sicurezza e integrità dei dati aziendali.

Inizialmente, abbiamo creato un file rappresentante dati aziendali sensibili tramite il comando `touch`. Questo passaggio ha mostrato come partire da un file neutro per configurare in seguito i permessi adeguati. Tale configurazione di base è essenziale per organizzare il controllo degli accessi fin dalle prime fasi di gestione dei dati. Il comando `ls -l` ci ha permesso di analizzare i permessi iniziali del file. Abbiamo osservato che, per default, il proprietario disponeva di lettura e scrittura, mentre gruppo e altri potevano solo leggere. Questo ha fornito la base per personalizzare i permessi secondo le necessità di sicurezza aziendale.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd Desktop

(kali㉿kali)-[~/Desktop]
$ touch risultati_azienza.txt

(kali㉿kali)-[~/Desktop]
$ ls -l risultati_azienza.txt
-rw-rw-r-- 1 kali kali 0 Dec  3 09:31 risultati_azienza.txt

(kali㉿kali)-[~/Desktop]
$
```

Usando il comando `chmod`, abbiamo impostato i permessi a `644`, permettendo solo al proprietario di scrivere e a tutti gli altri di leggere. Questa configurazione assicura che i dati restino accessibili per consultazione ma non modificabili da utenti non autorizzati. Il comando `ls -l` ha confermato la corretta applicazione dei permessi modificati.

```
(kali㉿kali)-[~/Desktop]
$ chmod 644 risultati_azienza.txt

(kali㉿kali)-[~/Desktop]
$ ls -l risultati_azienza.txt
-rw-r--r-- 1 kali kali 0 Dec  3 09:31 risultati_azienza.txt
```

Abbiamo verificato il funzionamento dei permessi simulando accessi differenti. Il proprietario ha potuto scrivere e leggere il file, mentre un altro utente ha ricevuto un errore nel tentativo di modifica. Questo test ha validato la configurazione, dimostrando che i permessi erano stati applicati correttamente.

```
(kali㉿kali)-[~/Desktop]
$ sudo adduser nuovo_utente
[sudo] password for kali:
info: Adding user `nuovo_utente' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `nuovo_utente' (1002) ...
info: Adding new user `nuovo_utente' (1002) with group `nuovo_utente (1002)' ...
info: Creating home directory `/home/nuovo_utente' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for nuovo_utente
Enter the new value, or press ENTER for the default
  Full Name []: Impiegato
  Room Number []: Incompetente
  Work Phone []: 1234567
  Home Phone []: 12345678
  Other []: 1111
Is the information correct? [Y/n] Y
info: Adding new user `nuovo_utente' to supplemental / extra groups `users' ...
info: Adding user `nuovo_utente' to group `users' ...
```

```
(kali㉿kali)-[~/Desktop]
$ echo "Dati sensibili del fine anno" > risultati_azienza.txt

(kali㉿kali)-[~/Desktop]
$ cat risultati_azienza.txt
Dati sensibili del fine anno
```

```
(kali㉿kali)-[~/Desktop]
$ su nuovo_utente
Password:
(nuovo_utente㉿kali)-[/home/kali/Desktop]
$ echo "Test di modifica" >> /percorso/completo/a/risultati_azienza.txt
bash: /percorso/completo/a/risultati_azienza.txt: No such file or directory

(nuovo_utente㉿kali)-[/home/kali/Desktop]
$
```

L'esercizio ha mostrato come configurare e verificare i permessi in un ambiente Linux, dimostrando l'importanza di un controllo preciso per proteggere i dati sensibili.