

Task 21/01/25: Permessi di Linux

Traccia

Obiettivo dell'Esercizio:

Abbiamo visto come si gestiscono i permessi in Linux.

Obiettivo: 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 mostrano i passaggi effettuati e scrivere una relazione spiegando le scelte fatte riguardo ai permessi.

Passaggi da Seguire:

Consegna:

1. Screenshot della Creazione del File o della Directory:
 - a. Fornisci uno screenshot che mostri i comandi utilizzati per creare il file o la directory.
2. Screenshot della Verifica dei Permessi Attuali:
 - a. Fornisci uno screenshot che mostri i comandi `ls -l` e l'output prima della modifica dei permessi.
3. Screenshot della Modifica dei Permessi:
 - a. Fornisci uno screenshot che mostri i comandi `chmod` utilizzati e l'output successivo con `ls -l`.
4. Screenshot del Test dei Permessi:
 - a. Fornisci uno screenshot che mostri i tentativi di scrivere nel file o di creare un nuovo file nella directory, insieme ai comandi e agli output.
5. Relazione:
 - a. Scrivi una relazione spiegando le scelte fatte riguardo ai permessi configurati. La relazione deve includere:
 - i. La motivazione delle scelte fatte per i permessi di lettura, scrittura ed esecuzione.
 - ii. Un'analisi dei risultati ottenuti durante i test dei permessi.

Task21/01/25: Permessi di Linux

Report

Introduzione:

L'obiettivo di questo esercizio è stato quello di configurare e gestire i permessi di lettura, scrittura ed esecuzione per un file specifico in un sistema Linux. Ho creato un nuovo utente senza privilegi di root, gestito i permessi di un file "SuperSegreto.txt" e verificato il comportamento dei permessi da parte dell'utente Kali.

1. Creazione del Nuovo Utente

Comando utilizzato: `sudo adduser utente_segreto`

1. Questo comando crea un nuovo utente chiamato `utente_segreto` con una directory home dedicata.

```
(kali㉿kali)-[~]
$ whoami
kali

(kali㉿kali)-[~]
$ sudo adduser utente_segreto

[sudo] password for kali:
info: Adding user `utente_segreto' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `utente_segreto' (1001) ...
info: Adding new user `utente_segreto' (1001) with group `utente_segreto (1001)' ...
info: Creating home directory `/home/utente_segreto' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for utente_segreto
Enter the new value, or press ENTER for the default
  Full Name []: Utente Segreto
   Room Number []:
   Work Phone []:
   Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user `utente_segreto' to supplemental / extra groups `users' ...
info: Adding user `utente_segreto' to group `users' ...
```

2. Login con il Nuovo Utente e Creazione del File

Comandi utilizzati: `su - utente_segreto`, `echo "Questo è un file super segreto!" > SuperSegreto.txt` e `ls -l`

1. Il primo comando consente di accedere come l'utente "utente_segreto".
2. Il secondo comando crea il file SuperSegreto.txt con il contenuto specificato.
3. Il terzo comando verifica i permessi predefiniti del file.

```

(kali㉿kali)-[~]
$ su - utente_segreto

Password:
(kali㉿kali)-[~]
$ whoami
utente_segreto

(kali㉿kali)-[~]
$ echo "Questo è un file super segreto!" > SuperSegreto.txt

(kali㉿kali)-[~]
$ ls -l
total 4
-rw-rw-r-- 1 utente_segreto utente_segreto 33 Jan 21 08:32 SuperSegreto.txt

```

3. Modifica dei Permessi del File

Comandi utilizzati: `chmod 600 SuperSegreto.txt` e `ls -l`

1. Il primo comando imposta i permessi del file in modo che solo il proprietario possa leggerlo e scriverlo.
2. Il secondo comando conferma i permessi aggiornati.

```

(kali㉿kali)-[~]
$ chmod 600 SuperSegreto.txt

(kali㉿kali)-[~]
$ ls -l
total 4
-rw----- 1 utente_segreto utente_segreto 33 Jan 21 08:32 SuperSegreto.txt

(kali㉿kali)-[~]
$ cat SuperSegreto.txt
Questo è un file super segreto!

```

4. Test dei Permessi

Comandi utilizzati: `exit`, `whoami`, `cat /home/utente_segreto/SuperSegreto.txt`

1. Il primo comando consente di uscire dall'utente "utente_segreto".
2. Il secondo comando conferma l'utente corrente.
3. Il terzo comando tenta di leggere il file con un utente diverso, verificando che venga restituito un errore di "Permission Denied".

```
(utente_segreto@kali)-[~]
$ exit
logout

(kali@kali)-[~]
$ whomai
Command 'whomai' not found, did you mean:
  command 'whoami' from deb coreutils
Try: sudo apt install <deb name>

(kali@kali)-[~]
$ whoami
kali

(kali@kali)-[~]
$ cat /home/utente_segreto/SuperSegreto.txt
cat: /home/utente_segreto/SuperSegreto.txt: Permission denied
```

Motivazione delle Scelte

1. **Creazione del Nuovo Utente**, La creazione di un utente dedicato garantisce che il file sia isolato da altri utenti nel sistema. Questo approccio incrementa la sicurezza dei dati sensibili.
2. **Permessi 600**, l'utilizzo di `chmod 600` limita l'accesso al file esclusivamente al proprietario. Nessun altro utente può leggerlo, scriverlo o eseguirlo, garantendo la massima protezione.
3. **Test dei Permessi**, la verifica pratica con un altro utente permette di dimostrare che i permessi siano stati configurati correttamente.

Analisi dei Risultati

1. Il file `SuperSegreto.txt` è stato creato con successo dall'utente "utente_segreto".
2. I permessi sono stati modificati correttamente, come confermato dall'output del comando `ls -l`.
3. Tentativi di accesso al file da parte di altri utenti hanno restituito un errore di "Permission Denied", dimostrando che la configurazione dei permessi ha funzionato come previsto.

Conclusione

Questo esercizio ha dimostrato come configurare e testare i permessi su un file specifico in Linux, utilizzando un approccio pratico e sicuro. La gestione corretta dei permessi è essenziale per proteggere i dati sensibili in ambienti multi-utente.