

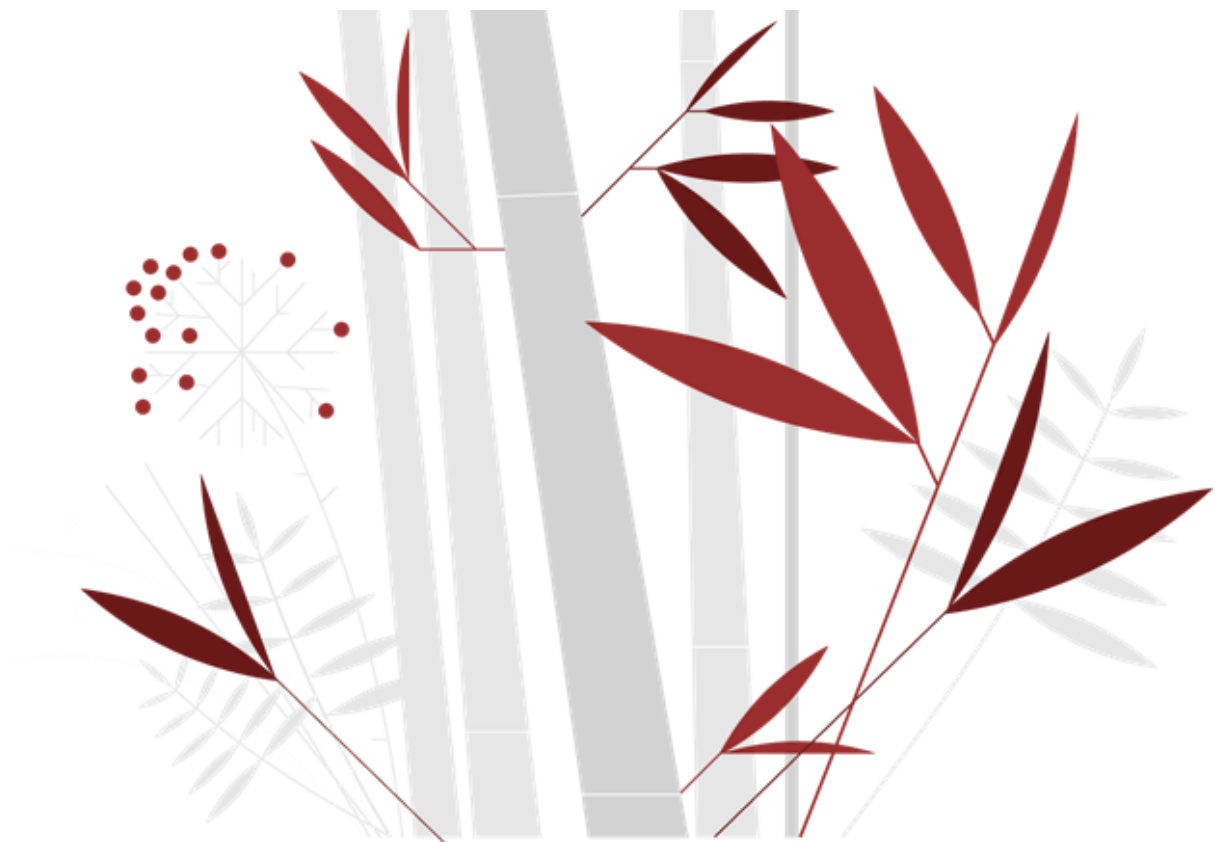
CYBER SECURITY & ETHICAL HACKING

Permessi di Linux

Sara Maimone

S10.L2

03/12/2024



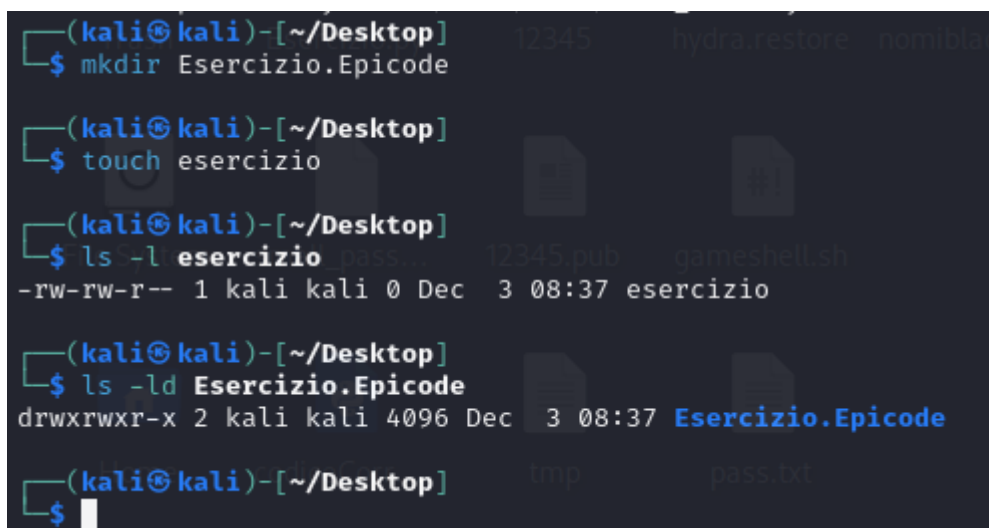
Esercizio di oggi:

Gestione dei Permessi di Lettura, Scrittura ed Esecuzione in Linux 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 mostrino i passaggi effettuati e scrivere una relazione spiegando le scelte fatte riguardo ai permessi.

Svolgimento:

L'esercizio di oggi ci chiedeva di creare un file o una directory su kali e successivamente modificarne i permessi, andiamo su kali e iniziamo a creare la nostra directory chiamata Esercizio.Epicode tramite il comando `mkdir` e il nostro file chiamato esercizio tramite il comando `touch` e ne verifichiamo i permessi tramite il comando `"ls -l"` per il file e `"ls -ld"` per la directory.



```
(kali@kali)-[~/Desktop]
$ mkdir Esercizio.Epicode

(kali@kali)-[~/Desktop]
$ touch esercizio

(kali@kali)-[~/Desktop]
$ ls -l esercizio
-rw-rw-r-- 1 kali kali 0 Dec  3 08:37 esercizio

(kali@kali)-[~/Desktop]
$ ls -ld Esercizio.Epicode
drwxrwxr-x 2 kali kali 4096 Dec  3 08:37 Esercizio.Epicode

(kali@kali)-[~/Desktop]
$
```

Come possiamo vedere dallo screen il file ha i seguenti permessi:

- `-rw-rw-r--`—ovvero:
- Che il proprietario ha il permesso di leggere e scrivere nel file, ma non di eseguirlo.
- Gli utenti appartenenti al gruppo del file hanno gli stessi permessi del proprietario.
- Gli utenti esterni al gruppo possono solo leggere il file, senza poterlo modificare o eseguire.

Mentre la directory ha i seguenti permessi: `drwxrwxr-x` ovvero:

- Il proprietario ha il permesso di leggere il contenuto della directory, creare, rinominare o eliminare file, ed eseguire per accedere alla directory con comandi come cd.
- Gli utenti appartenenti al gruppo della directory hanno gli stessi permessi del proprietario: leggere, scrivere, ed eseguire.
- Gli utenti esterni al gruppo possono leggere il contenuto della directory e accedervi.

Successivamente andiamo a modificare i permessi tramite il comando `chmod`:

Utilizziamo il comando “`chmod 644 esercizio`” che equivale a “`chmod u=rw,g=r,o=r` (permessi UGO) `esercizio`” per modificare i permessi del file (utilizzo il valore 644 poichè è un abbreviazione del comando `u=rw,g=r,o=r`), con questa configurazione il proprietario può modificare il file, mentre gli altri utenti possono solo leggerlo.

Per la directory invece utilizziamo il comando “`chmod 700 Esercizio.Epicode`” che equivale a “`chmod u=rwx,g=,o= Esercizio.Epicode`”

Con questa configurazione Solo il proprietario può accedere, leggere, scrivere e navigare all'interno della directory mentre il gruppo e gli altri utenti non hanno alcun permesso.

Poi andiamo a verificare nuovamente i permessi concessi.

```
(kali@kali)-[~/Desktop]
$ chmod 644 esercizio

(kali@kali)-[~/Desktop]
$ chmod 700 Esercizio.Epicode

(kali@kali)-[~/Desktop]
$ ls -l esercizio
-rw-r--r-- 1 kali kali 0 Dec 3 08:37 esercizio

(kali@kali)-[~/Desktop]
$ ls -ld Esercizio.Epicode
drwx----- 2 kali kali 4096 Dec 3 08:37 Esercizio.Epicode

(kali@kali)-[~/Desktop]
$
```

Successivamente creiamo un nuovo utente per poter verificare la modifica dei permessi.

```

(kali@kali)-[~/Desktop]
$ sudo su
[sudo] password for kali:
(kali@kali)-[~/Desktop]
# adduser Sara
err: Please enter a username matching the regular expression
      configured via the NAME_REGEX configuration variable. Use the
      '--allow-bad-names' option to relax this check or reconfigure
      NAME_REGEX in configuration.

(kali@kali)-[~/Desktop]
# adduser Sara --allow-bad-names
info: Allowing use of questionable username.
info: Adding user `Sara' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `Sara' (1003) ...
info: Adding new user `Sara' (1003) with group `Sara (1003)' ...
info: Creating home directory `/home/Sara' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for Sara
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user `Sara' to supplemental / extra groups `users' ...
info: Adding user `Sara' to group `users' ...

(kali@kali)-[~/Desktop]
# su Sara
(Sara@kali)-[~/Desktop]
$

```

Dopo avere creato il nuovo utente andiamo ad effettuare dei test, così da poter vedere l'avvenuto cambio dei permessi:

```

(kali@kali)-[~/Desktop]
# su Sara
(Sara@kali)-[~/Desktop]
$ cat esercizio
s

(Sara@kali)-[~/Desktop]
$ echo "test" > esercizio
bash: esercizio: Permission denied

(Sara@kali)-[~/Desktop]
$ ls Esercizio.Epicode
ls: cannot open directory 'Esercizio.Epicode': Permission denied

(Sara@kali)-[~/Desktop]
$

```

Con l'utente "Sara" proviamo a leggere il file "esercizio" tramite il comando "cat", come mostrato nello screenshot, l'operazione è riuscita senza problemi, confermando che il permesso di lettura era attivo per gli "altri" utenti, successivamente proviamo a modificare il file tramite

il comando “echo "test" > esercizio” e come possiamo vedere la schermata ci restituisce l’avviso permesso negato, successivamente proviamo ad accedere alla directory Esercizio.Epicode, anche in questo caso, il sistema ha restituito "Permission denied", poiché i permessi 700 assegnati alla directory consentono l’accesso esclusivamente al proprietario. L’utente "Sara", non essendo il proprietario, non ha né il permesso di lettura né quello di esecuzione, necessari per accedere o visualizzare il contenuto della directory.

Conclusione:

L'esercizio ci ha permesso di comprendere a fondo la gestione dei permessi in un sistema Linux, evidenziando come configurazioni specifiche possano influenzare l'accesso e le operazioni sui file e sulle directory, e come i permessi dati con chmod sono fondamentali per proteggere i dati in ambienti multiutente.

Legenda:

UGO => User (u), Group (g), Others (o)

- **r**: Permesso di lettura (Read)
- **w**: Permesso di scrittura (Write)
- **x**: Permesso di esecuzione (Execute)

Permessi numerici:

- **r** (read) = 4
- **w** (write) = 2
- **x** (execute) = 1

Es. 644 equivale a “u=rw,g=r,o=r”

6 (4+2 ovvero r+w) 4 (r) 4 (r)