

ESERCITAZIONE S2/L2

<Familiarizziamo con la shell Linux>

Come primo passo inseriamo il comando **<top>** per controllare i processi attivi:

```
kali@kali: ~  
File Actions Edit View Help  
top - 12:52:17 up 59 min, 1 user, load average: 0.05, 0.06, 0.08  
Tasks: 157 total, 1 running, 156 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 0.3 us, 0.5 sy, 0.0 ni, 98.7 id, 0.2 wa, 0.0 hi, 0.3 si, 0.0 st  
MiB Mem : 1967.1 total, 727.2 free, 732.3 used, 657.2 buff/cache  
MiB Swap: 975.0 total, 975.0 free, 0.0 used. 1234.7 avail Mem  


| PID   | USER | PR | NI | VIRT   | RES    | SHR   | S | %CPU | %MEM | TIME+   | COMMAND         |
|-------|------|----|----|--------|--------|-------|---|------|------|---------|-----------------|
| 733   | root | 20 | 0  | 385476 | 119592 | 53980 | S | 1.3  | 5.9  | 0:17.19 | Xorg            |
| 30659 | kali | 20 | 0  | 446612 | 103056 | 84172 | S | 0.7  | 5.1  | 0:00.11 | qterminal       |
| 1101  | kali | 20 | 0  | 278000 | 32252  | 19456 | S | 0.3  | 1.6  | 0:03.09 | panel-13-cpugra |
| 1103  | kali | 20 | 0  | 350360 | 27984  | 20772 | S | 0.3  | 1.4  | 0:03.21 | panel-15-genmon |
| 30658 | kali | 20 | 0  | 39504  | 15360  | 13440 | S | 0.3  | 0.8  | 0:00.01 | xfce4-mime-help |
| 1     | root | 20 | 0  | 20820  | 12520  | 9320  | S | 0.0  | 0.6  | 0:00.58 | systemd         |


```

Le colonne che andremo ad analizzare sono:

PID (Process Identifier): Numero identificativo del processo

USER: Utente che ha lanciato il processo, in questo caso ROOT

COMMAND: Il comando utilizzato per lanciare il processo

Andiamo a filtrare con il comando **<grep>** i processi che hanno come user “root” e “kali”, inserendo l’output al comando **<top | grep root>** e **<top | grep kali>**:

```
(kali@kali)-[~]  
$ top | grep root  
1 root 20 0 20820 12520 9320 S 0.0 0.6 0:00.58 systemd  
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd  
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp  
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par+  
5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 slub_fl+  
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 netns  
9 root 20 0 0 0 0 I 0.0 0.0 0:00.72 kworker+  
10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_perc+  
11 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tas+  
12 root 20 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tas+
```

```
(kali@kali)-[~]  
$ top | grep kali  
1093 kali 20 0 488492 60316 36012 S 0.3 3.0 0:00.89 xfdesktop+  
1101 kali 20 0 426516 35900 22592 S 0.3 1.8 0:03.33 panel-1+  
1103 kali 20 0 350360 28368 21156 S 0.3 1.4 0:03.42 panel-1+  
30659 kali 20 0 446752 103184 84172 S 0.3 5.1 0:00.46 qtermin+  
1033 kali 20 0 955388 108284 77420 R 0.3 5.4 0:04.00 xfwm4  
30659 kali 20 0 446752 103184 84172 S 0.3 5.1 0:00.47 qtermin+  
1033 kali 20 0 955388 108284 77420 S 0.3 5.4 0:04.01 xfwm4  
32598 kali 20 0 12116 4992 2944 R 0.3 0.2 0:00.01 top  
1101 kali 20 0 426516 35900 22592 S 0.3 1.8 0:03.34 panel-1+  
977 kali 20 0 283856 3200 2816 S 0.3 0.2 0:02.53 VBoxCli+
```

Di seguito andiamo a creare una cartella col nome “Epicode_lab” e successivamente verifichiamo che il comando sia stato eseguito con **<ls -l>**:

```
(kali㉿kali)-[~]
$ mkdir Epicode_lab

(kali㉿kali)-[~]
$ _l
-l: command not found

(kali㉿kali)-[~]
$ ls -l
Desktop
Documents
Downloads
Epicode_lab
Music
Pictures
Public
Templates
Videos
top.save
```

Spostiamo la cartella “Epicode_lab” nella directory “Desktop”:

```
(kali㉿kali)-[~]
$ ls -l
Desktop
Documents
Downloads
Epicode_lab
Music
Pictures
Public
Templates
Videos
top.save

(kali㉿kali)-[~]
$ mv Epicode_lab Desktop
```

In alternativa avremmo potuto creare la cartella direttamente nel percorso scelto inserendo il comando **<mkdir directory /home/kali/Desktop/Epicode_lab>** saltando il passaggio dello spostamento della directory.

Prima di creare il file di testo all’interno della cartella scelta, accediamoci:

```
(kali㉿kali)-[~]
$ cd /home/kali/Desktop/Epicode_lab

(kali㉿kali)-[~/Desktop/Epicode_lab]
$
```

Ora procediamo con la creazione del file di testo tramite l’editor di testo **<nano>** inserendolo come comando, ci apparirà questo:

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^_ Replace	^U Paste	^J Justify	^_ Go To Line

Salviamo il file con nome “Esercitazione”.

Per leggere a schermo il .txt appena salvato basterà inserire il comando **<cat Esercitazione>**, come segue:

```
(kali@kali)-[~/Desktop/Epicode_lab]
$ cat Esercitazione
Hello World :)
```

Controlliamo i permessi del file:

```
(kali@kali)-[~/Desktop/Epicode_lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 14:40 .
drwxr-xr-x 3 kali kali 4096 Nov 28 14:19 ..
-rw-r--r-- 1 kali kali 15 Nov 28 14:40 Esercitazione
```

Ora andiamo a modificare i privilegi in modo tale che l'utente li abbia tutti (r, w, x), il gruppo (r, w) e gli altri utenti solo lettura (r). Come? Con il comando **<chmod>**.

Nel nostro caso specifico abbiamo bisogno di aggiungere il privilegio dell'esecuzione all'utente e quello della scrittura al gruppo. Nel caso degli altri utenti non abbiamo bisogno di aggiungere o togliere alcun permesso.

I comandi che andremo a utilizzare sono:

<chmod u+x Esercitazione>

<chmod g+w Esercitazione>

Adesso andiamo a controllare se effettivamente i permessi sono stati cambiati:

```
(kali㉿kali)-[~/Desktop/Epicode_lab]
$ chmod u+x Esercitazione

(kali㉿kali)-[~/Desktop/Epicode_lab]
$ chmod g+w Esercitazione

(kali㉿kali)-[~/Desktop/Epicode_lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 14:40 .
drwxr-xr-x 3 kali kali 4096 Nov 28 14:19 ..
-rwxrw-r-- 1 kali kali  15 Nov 28 14:40 Esercitazione
```

Ora creiamo un nuovo utente, che ci tornerà utile più avanti:

```
(kali㉿kali)-[/]
$ sudo useradd Ajeje

(kali㉿kali)-[/]
$ sudo passwd Ajeje
New password:
Retype new password:
passwd: password updated successfully
```

Adesso andiamo a cambiare di nuovo i permessi del file Esercitazione.txt in modo che altri utenti non siano abilitati alla lettura, torniamo quindi ad usare il comando **<chmod>**:

```
(kali㉿kali)-[~/Desktop/Epicode_lab]
$ chmod o-r Esercitazione

(kali㉿kali)-[~/Desktop/Epicode_lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 14:40 .
drwxr-xr-x 3 kali kali 4096 Nov 28 14:19 ..
-rwxrw--- 1 kali kali  15 Nov 28 14:40 Esercitazione

(kali㉿kali)-[~/Desktop/Epicode_lab]
$
```

Ora gli altri utenti non possiedono più alcun privilegio.

Continuiamo spostando il file nella cartella di root “/” e controlliamo che si sia effettivamente spostato:

```
(kali@kali)-[~/Desktop/Epicode_lab]
$ sudo mv Esercitazione /

(kali@kali)-[~/Desktop/Epicode_lab]
$ cd /

(kali@kali)-[/]
$ ls
Esercitazione  dev      initrd.img  lib32      lost+found  opt      run      sys      var
bin            etc      initrd.img.old  lib64      media      proc     sbin     tmp      vmlinuz
boot          home     lib         libx32     mnt        root     srv      usr      vmlinuz.old
```

Adesso cambiamo utente, utilizziamo quello creato in precedenza, utilizzando il comando **<su>**:

```
(kali@kali)-[/]
$ su Ajeje
Password:
$ whoami
Ajeje
```

Se proviamo ad aprire il file Esercitazione.txt con questo utente, tramite editor di testo nano, scopriamo che non abbiamo il permesso per leggerlo:

```
[ Error reading Esercitazione: Permission denied ] ...
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify     ^/ Go To Line
```

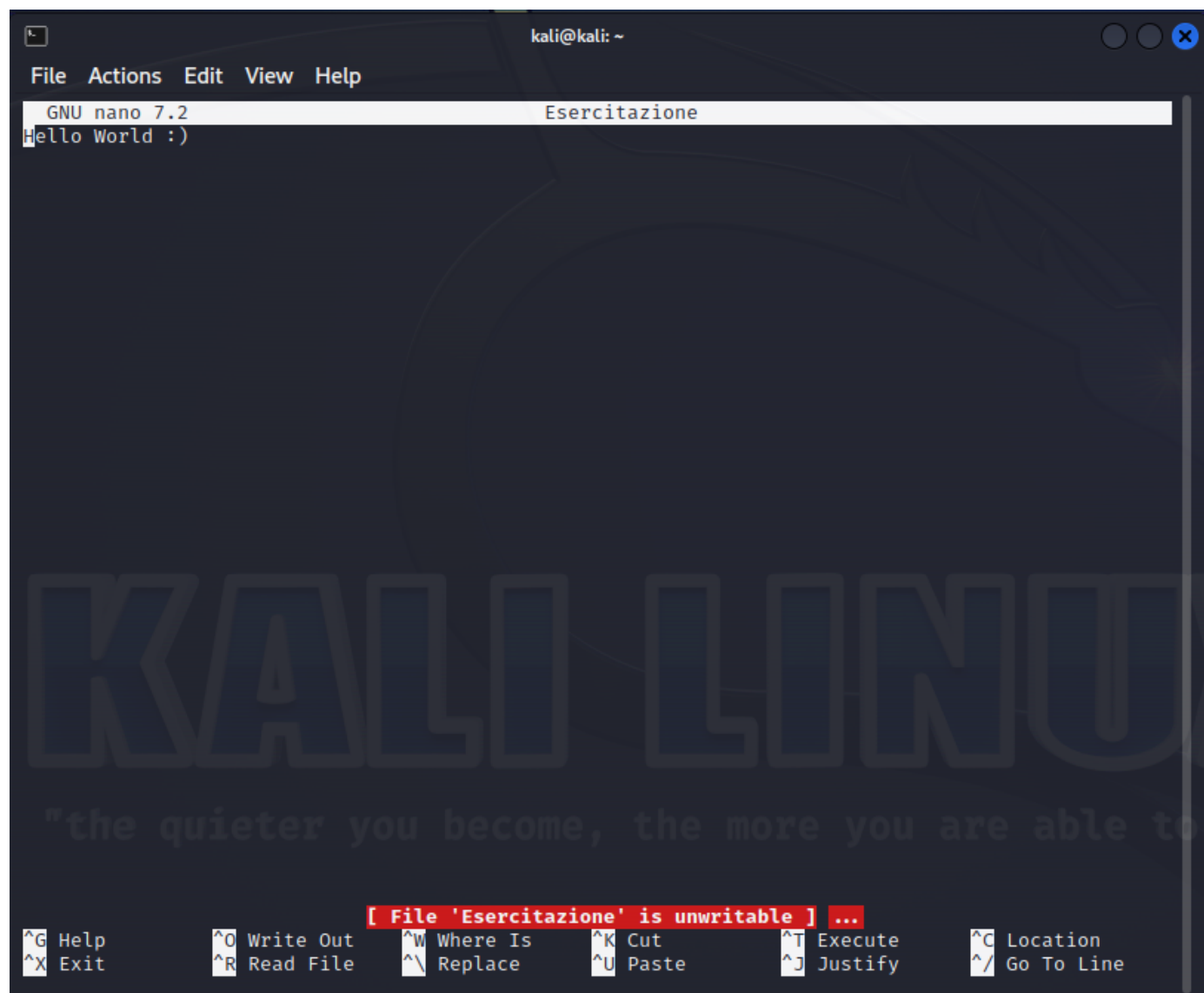
Quindi ora rifacciamo l’accesso con l’utente Kali per permettere al nuovo utente di poter leggere il file di testo, come prima ci torna in aiuto il comando **<chmod>**:

```
(kali@kali)-[/]
$ ls -l Esercitazione
-rwxrw--- 1 kali kali 15 Nov 28 14:40 Esercitazione

(kali@kali)-[/]
$ chmod o+r Esercitazione

(kali@kali)-[/]
$ ls -l Esercitazione
-rwxrw-r-- 1 kali kali 15 Nov 28 14:40 Esercitazione
```

Accediamo nuovamente col secondo user per vedere se ora riusciamo a visualizzare il testo all'interno del file:

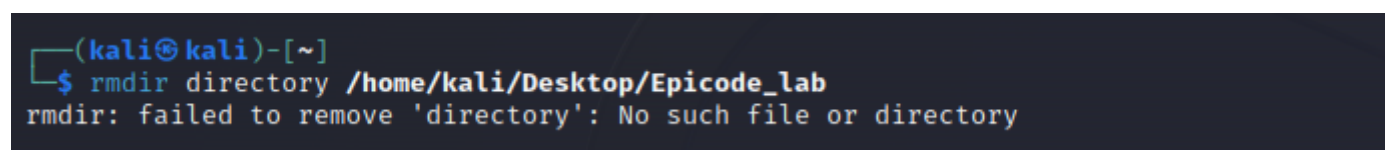


```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 Esercitazione  
Hello World :)  
  
[ File 'Esercitazione' is unwritable ] ...  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location  
^X Exit      ^R Read File  ^\ Replace    ^U Paste       ^J Justify    ^_ Go To Line
```

Come vediamo ora possiamo leggerlo ma ci specifica anche non possiamo scrivere al suo interno, come giusto che sia dandosi che il permesso di scrivere glielo abbiamo negato.

Ora rimuoviamo il file, la cartella e l'utente creato, per riportare tutto allo stato iniziale.

Eliminazione cartella:



```
(kali@kali)-[~]  
$ rm -r directory /home/kali/Desktop/Epicode_lab  
rm: failed to remove 'directory': No such file or directory
```

Nel nostro caso anche se ci segnala l'errore, la cartella è stata eliminata.

Eliminazione file:

```
(kali㉿kali)-[/]  
$ sudo rm Esercitazione  
[sudo] password for kali:
```

Eliminazione utente aggiuntivo:

```
(kali㉿kali)-[/]  
$ sudo userdel Ajeje  
  
(kali㉿kali)-[/]  
$ su Ajeje  
su: user Ajeje does not exist or the user entry does not contain all the required fields  
  
(kali㉿kali)-[/]  
$
```