

FAMILIARIZZAZIONE CON SHELL LINUX

1. CONTROLLARE I PROCESSI ATTIVI SULLA MACCHINA LINUX CON IL COMANDO "TOP" E DESCRIVERE IL SIGNIFICATO DELLE COLONNE PID, USER, COMMAND

Eseguendo il comando top sul terminale di linux appare a video la lista completa dei processi attivi, divisi in colonne. Prendendo in esame lo stesso comando top utilizzato dal nostro utente (kali), nello specifico possiamo riconoscere:

- il PID (Process IDentifier) è l'identificativo univoco del processo in esecuzione
- USER identifica l'utente che ha avviato il processo
- COMMAND non è altro che il nome del processo o applicativo in esecuzione

```
File Actions Edit View Help
top - 08:28:53 up 11 min, 1 user, load average: 0.16, 0.17, 0.18
Tasks: 139 total, 1 running, 138 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.5 us, 0.5 sy, 0.0 ni, 99.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1972.4 total, 950.7 free, 752.1 used, 425.9 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used, 1220.4 avail Mem

  PID USER   PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 555 root    20   0   358412 2812 2436 S   0.7   0.1   0:00.12 VBoxService
5955 kali    20   0   444368 107584 87940 S   0.7   5.3   0:00.78 qterminal
 626 root    20   0   723064 122876 63820 S   0.3   6.1   0:07.58 Xorg
 897 kali    20   0   217956 2460 2116 S   0.3   0.1   0:01.39 VBoxClient
 955 kali    20   0   875024 101652 77536 S   0.3   5.0   0:02.25 xfwm4
1005 kali    20   0   204028 31892 18560 S   0.3   1.6   0:01.48 panel-13-cougra
1007 kali    20   0   358544 30656 20756 S   0.3   1.5   0:01.46 panel-15-genmon
6010 kali    20   0   11736 5304 3164 R   0.3   0.3   0:00.10 top
  1 root    20   0   167780 12108 9020 S   0.0   0.6   0:01.16 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_gp
  5 root    0 -20   0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
  6 root    0 -20   0      0      0 I   0.0   0.0   0:00.00 netns
  8 root    0 -20   0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
  9 root    20   0      0      0      0 I   0.0   0.0   0:01.04 kworker/u4:0-flush-8:0
10 root    0 -20   0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
11 root    20   0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
12 root    20   0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
13 root    20   0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
14 root    20   0      0      0      0 S   0.0   0.0   0:00.00 ksoftirqd/0
15 root    20   0      0      0      0 I   0.0   0.0   0:00.32 rcu_preempt
16 root    rt  0      0      0      0 S   0.0   0.0   0:00.00 migration/0
17 root    20   0      0      0      0 I   0.0   0.0   0:00.02 kworker/0:1-l-events
18 root    20   0      0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
19 root    20   0      0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
20 root    rt  0      0      0      0 S   0.0   0.0   0:00.11 migration/1
21 root    20   0      0      0      0 S   0.0   0.0   0:00.05 ksoftirqd/1
26 root    20   0      0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
27 root    0 -20   0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
```

2. FILTRARE I RISULTATI DEL COMANDO TOP INVIANDO L'OUTPUT AL COMANDO GREP

Utilizzando il comando grep root concatenato a top, il terminale restituirà di nuovo la lista dei processi, ma filtrando solo quelli per l'user indicato (root).

```
(kali@kali)-[~]
$ top | grep root
626 root      20    0  728688 136780  67052 S   6.7   6.8   0:17.84 Xorg
  1 root      20    0  167780  12108   9020 S   0.0   0.6   0:01.18 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
  8 root       0 -20         0         0         0 I   0.0   0.0   0:00.00 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+
13 root      20    0         0         0         0 I   0.0   0.0   0:00.00 rcu_tas+
14 root      20    0         0         0         0 S   0.0   0.0   0:00.08 ksoftir+
15 root      20    0         0         0         0 I   0.0   0.0   0:00.73 rcu_pre+
16 root      rt    0         0         0         0 S   0.0   0.0   0:00.01 migrati+
17 root      20    0         0         0         0 I   0.0   0.0   0:00.02 kworker+
```

Eseguendo la stessa operazione per l'utente kali, il risultato sarà il seguente:

```
(kali@kali)-[~]
$ top | grep kali
955 kali      20    0  875832 106528  77556 S   0.7   5.3   0:05.47 xfwm4
15039 kali    20    0  444204 108044  88464 S   0.7   5.3   0:01.37 qtermin+
897 kali      20    0  217956  2460   2116 S   0.3   0.1   0:04.18 VBoxCli+
1005 kali     20    0  204028  31892  18560 S   0.3   1.6   0:03.82 panel-1+
16942 kali    20    0   11580   4972   3072 R   0.3   0.2   0:00.01 top
```

3. CREARE UNA NUOVA DIRECTORY CHIAMATA "EPICODE_LAB" NELLA DIRECTORY /HOME/KALI/DESKTOP, CREARE UN NUOVO FILE, MODIFICARLO E SALVARLO

Per creare una nuova directory, dobbiamo prima spostarci nella cartella in cui intendiamo creare quella nuova. Con il comando "cd /home/kali/Desktop" ci spostiamo quindi nella directory e successivamente con il comando "mkdir Epicode_Lab" creiamo la nuova cartella. Possiamo vedere l'effettiva creazione della directory con il comando "ls" dalla cartella in cui ci troviamo (/home/kali/Desktop). Epicode_Lab è qui.

```
(kali@kali)-[~]
$ cd /home/kali/desktop
cd: no such file or directory: /home/kali/desktop

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

(kali@kali)-[~/Desktop]
$ mkdir Epicode_Lab

(kali@kali)-[~/Desktop]
$ ls
Epicode_Lab

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

A questo punto ci spostiamo nella nuova cartella appena creata e andiamo a creare il file “Esercizio.txt” tramite il comando “touch Esercizio.txt”

```
(kali@kali)~[~/Desktop]
$ ls
Epicode_Lab

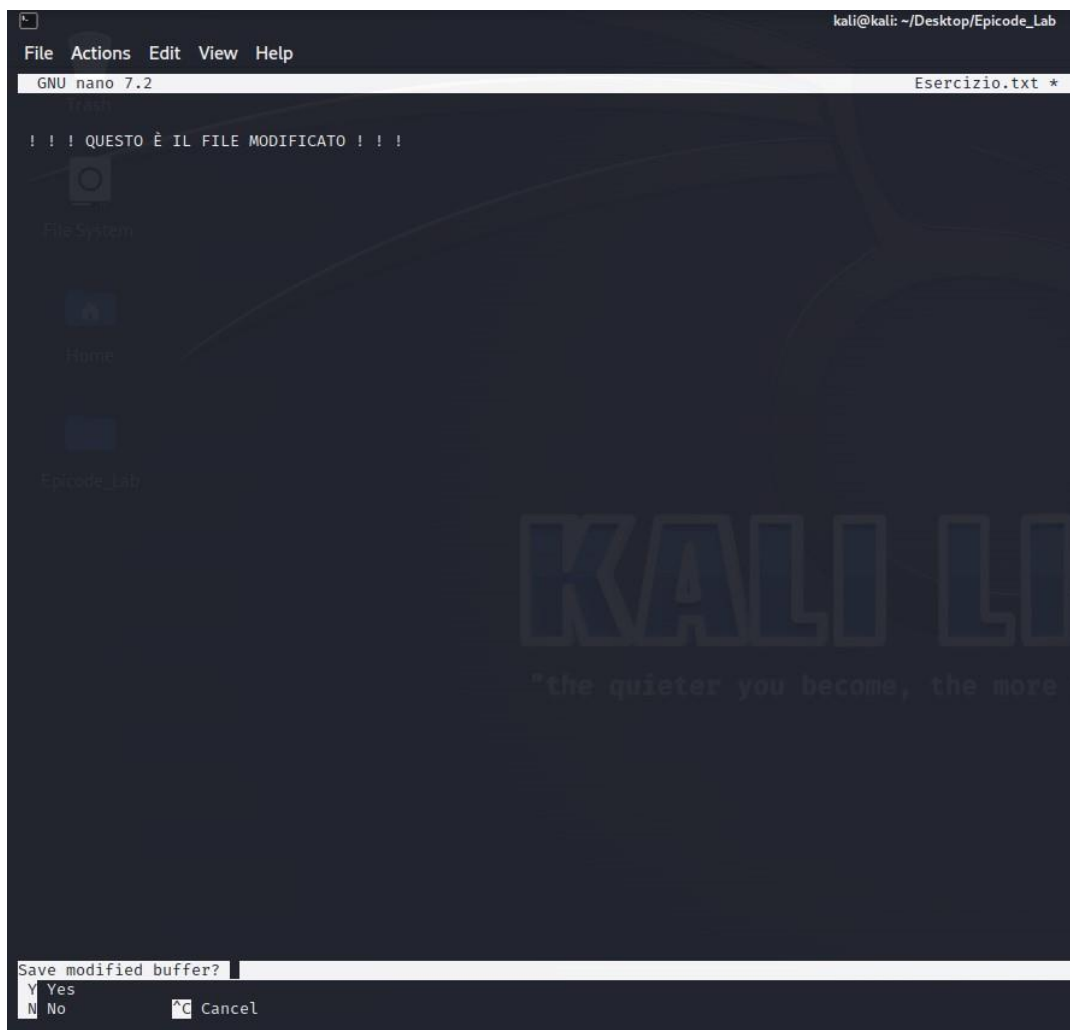
(kali@kali)~[~/Desktop]
$ cd /home/kali/Desktop/Epicode_Lab

(kali@kali)~[~/Desktop/Epicode_Lab]
$ touch Esercizio.txt

(kali@kali)~[~/Desktop/Epicode_Lab]
$ ls
Esercizio.txt

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

Andiamo ad aprirlo e visualizzarlo con “nano”, lo modifichiamo e salviamo la modifica con CTRL+X e Y alla domanda.



4. UTILIZZARE COMANDO “CAT” PER LEGGERE A SCHERMO IL FILE.TXT APPENA MODIFICATO

Con il comando “cat” possiamo eseguire direttamente a schermo il file txt e leggere la modifica effettuata.

```
(kali@kali)-[~/Desktop/Epicode_Lab]
$ cat Esercizio.txt

! ! ! QUESTO È IL FILE MODIFICATO ! ! !

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

5. CONTROLLARE I PERMESSI DEL FILE E MODIFICARNE I PRIVILEGI

Andando ad eseguire il comando “ls -la” andiamo a verificare i permessi che il nostro utente kali ha sul file. Il terminale ci restituisce i seguenti valori:

```
(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -la Esercizio.txt
-rw-r--r-- 1 kali kali 46 May  9 09:12 Esercizio.txt

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

Queste diciture indicano che il file attualmente è leggibile e modificabile (r e w) dal nostro user, ed è solo leggibile (r) dal gruppo e dagli altri utenti. Vogliamo cambiare queste regole per fare in modo che l’utente corrente abbia tutti i privilegi (r, w, x), il gruppo abbia solo i privilegi di lettura e modifica (r, w) e gli altri utenti solo lettura (r).

Per poter eseguire questo passaggio dobbiamo aggiungere il privilegio x allo user e il privilegio w al gruppo: eseguiamo quindi il comando “chmod u+x Esercizio.txt” per aggiungere (+) all’utente kali (u) il permesso di esecuzione (x) sul file txt. Successivamente con il comando “chmod g+w Esercizio.txt” aggiungiamo (+) al gruppo (g) il permesso di scrittura (w). Infine riscrivendo il comando “ls -la Esercizio.txt” possiamo verificare l’avvenuta modifica.

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la Esercizio.txt
-rw-r--r-- 1 kali kali 46 May  9 09:12 Esercizio.txt

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ chmod u+x Esercizio.txt

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ chmod g+w Esercizio.txt

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la Esercizio.txt
-rwxrw-r-- 1 kali kali 46 May  9 09:12 Esercizio.txt

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

6. CREARE NUOVO UTENTE E CAMBIARE I PRIVILEGI DEL FILE PER MODIFICARE I PERMESSI DI LETTURA PER GLI ALTRI UTENTI

Per creare un nuovo utente eseguiamo il comando “sudo useradd” e “sudo passwd + nome utente” per assegnare una password.

```
(kali㉿kali)-[~]
$ sudo useradd RiccBrun

(kali㉿kali)-[~]
$ sudo passwd RiccBrun
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$
```

Modifichiamo i privilegi di Esercizio.txt in modo che altri utenti (o) non abbiano i permessi di lettura (r) con il comando “chmod o-r Esercizio.txt” sempre dalla cartella di Epicode_Lab

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ chmod o-r Esercizio.txt

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la Esercizio.txt
-rwxrw----- 1 kali kali 46 May  9 09:12 Esercizio.txt

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


7. SPOSTARE IL FILE NELLA DIRECTORY DI ROOT E CAMBIARE UTENTE PER PROVARE AD APRIRE IL FILE .TXT CON NANO

Spostiamo il file nella cartella di root con il comando “mv Esercizio.txt /” all’interno della directory Epicode_Lab per spostare il file in root (/). Verifichiamo con “ls” che Epicode_Lab adesso è vuota e sempre con “ls” che invece la directory di root contiene il nostro .txt

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

Cambiamo l’utente corrente con quello creato con il comando “su” e proviamo ad aprire il file appena spostato con “nano”.

```
(kali@kali)-[~]
$ su RiccBrun
Password:
$ nano Esercizio.txt
```

Il terminale aprirà il file con un messaggio di errore: permesso negato. Avendo cambiato i permessi da user kali per disabilitare tutti i privilegi per gli altri utenti (compreso il nostro nuovo utente), non è possibile neanche leggere il file.



The screenshot shows the nano text editor interface. At the bottom, a red error message is displayed: "Error reading Esercizio.txt: Permission denied". The message is circled in red. The nano editor's status bar at the bottom shows various keyboard shortcuts like Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Location, Go To Line, Undo, Redo, Set Mark, Copy, To Bracket, Where Was, Previous, Next, Back, and Forward.

8. MODIFICARE I PERMESSI DEL FILE PER FARE IN MODO CHE IL NUOVO UTENTE POSSA LEGGERLO, CAMBIARE UTENTE E RIPROVARE AD APRIRLO

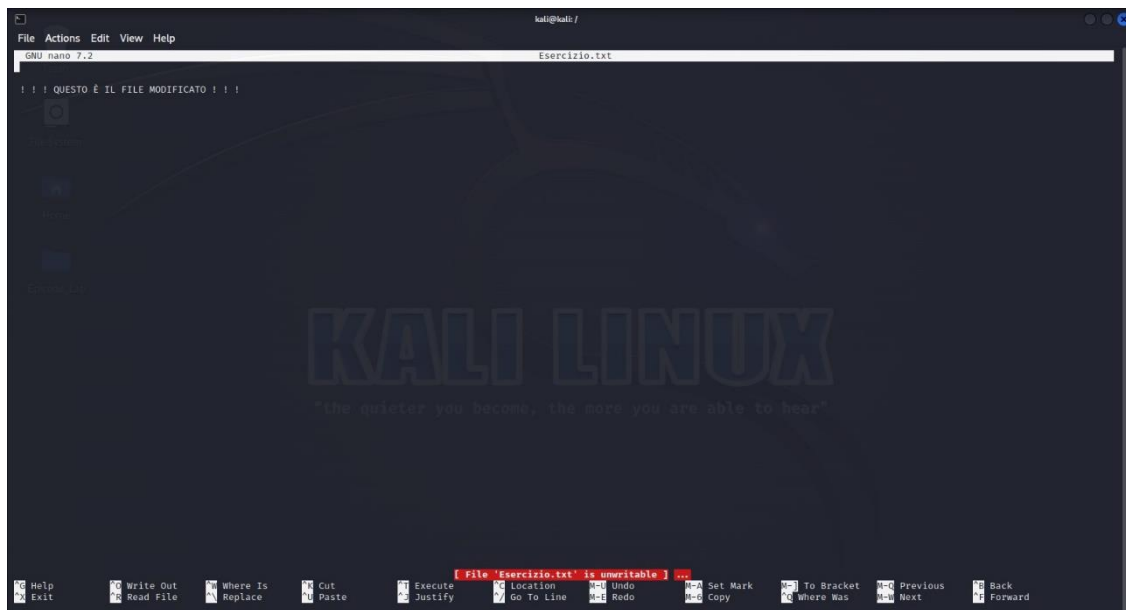
Torniamo all'user kali sempre con il comando "su" e modifichiamo i privilegi cosicché gli altri utenti (o) possano leggere il nostro file. Da terminale siamo già nella cartella root (/) dove si trova il file, quindi eseguiamo "chmod o+r Esercizio.txt". Verifichiamo come al solito con "ls -la Esercizio.txt" che i permessi sono stati applicati

```
$ su kali Lab
Password:
(kali@kali)-[/]
$ chmod o+r Esercizio.txt

(kali@kali)-[/]
$ ls -la Esercizio.txt
-rwxr--r-- 1 kali kali 46 May  9 09:12 Esercizio.txt

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

Torniamo al nuovo utente e verifichiamo che stavolta il file con il comando "nano Esercizio.txt" si può aprire senza errori di lettura (persiste un errore, ma riguarda la scrittura poiché il permesso w è disabilitato)



9. RIMUOVERE FILE, CARTELLE E UTENTE CREATI

Per rimuovere tutto e riportare il sistema allo stato iniziale, torniamo allo user kali ed eseguiamo il comando "sudo deluser + nomeutente" seguito dalla password per cancellare il nuovo utente. Poi ci spostiamo nella directory /home/Desktop/ eseguiamo "rmdir Epicode_Lab" per rimuovere la cartella creata. Infine spostandoci nella directory di root /

eseguiamo “rm Esercizio.txt” per eliminare il file. Con “ls” all’interno delle rispettive cartelle possiamo verificare l’avvenuta eliminazione.

```
(kali@kali)-[~]  
$ sudo deluser RiccBrun  
[sudo] password for kali:  
Removing crontab ...  
Removing user `RiccBrun' ...  
Done.
```

```
(kali@kali)-[~/Desktop/Epicode_Lab]  
$ cd /home/kali/Desktop/  
  
(kali@kali)-[~/Desktop]  
$ rmdir Epicode_Lab  
  
(kali@kali)-[~/Desktop]  
$ ls  
  
(kali@kali)-[~/Desktop]  
$
```

```
(kali@kali)-[~/Desktop]  
$ cd /  
  
(kali@kali)-[/]  
$ rm Esercizio.txt  
  
(kali@kali)-[/]  
$ ls  
bin boot dev 32 home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found media mnt opt proc root run/sbin srv swapfile sys tmp usr var vmlinuz vmlinuz.old  
  
(kali@kali)-[/]  
$
```

A questo punto abbiamo eliminato tutto, tornando allo scenario di partenza.