

SHELL Linux

Controllo e filtraggio processi attivi su macchina Linux

Creazione di un file all'interno di una nuova cartella e modifica privilegi

Creazione nuovo utente e nuova modifica privilegi

Spostamento del file nella directory di root (/)

Cambio utente e lettura file con privilegi già impostati e,
successivamente, modificati

Orlando Tangari

Scenario iniziale

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ top
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
top - 15:37:22 up 45 min, 1 user, load average: 0,25, 0,15, 0,10  
Tasks: 151 total, 1 running, 150 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 2,5 us, 1,5 sy, 0,0 ni, 96,0 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0  
MiB Mem : 1981,3 total, 987,1 free, 533,8 used, 460,3 buff/cache  
MiB Swap: 976,0 total, 976,0 free, 0,0 used. 1296,2 avail Mem  


| PID  | USER | PR | NI  | VIRT   | RES    | SHR   | S | %CPU | %MEM | TIME+   |
|------|------|----|-----|--------|--------|-------|---|------|------|---------|
| 888  | kali | 20 | 0   | 353888 | 38100  | 22180 | S | 2,0  | 1,9  | 0:30.75 |
| 514  | root | 20 | 0   | 335880 | 90580  | 54092 | S | 1,7  | 4,5  | 0:24.23 |
| 890  | kali | 20 | 0   | 359848 | 30848  | 20920 | S | 1,0  | 1,5  | 0:12.47 |
| 1124 | kali | 20 | 0   | 432460 | 104088 | 83660 | S | 0,7  | 5,1  | 0:20.75 |
| 1456 | kali | 20 | 0   | 10392  | 3744   | 3200  | R | 0,7  | 0,2  | 0:16.38 |
| 793  | kali | 20 | 0   | 153000 | 2768   | 2288  | S | 0,3  | 0,1  | 0:03.16 |
| 893  | kali | 20 | 0   | 668300 | 46988  | 35416 | S | 0,3  | 2,3  | 0:02.77 |
| 1    | root | 20 | 0   | 102480 | 12104  | 8988  | S | 0,0  | 0,6  | 0:01.42 |
| 2    | root | 20 | 0   | 0      | 0      | 0     | S | 0,0  | 0,0  | 0:00.00 |
| 3    | root | 0  | -20 | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.00 |
| 4    | root | 0  | -20 | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.00 |
| 5    | root | 0  | -20 | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.00 |
| 7    | root | 0  | -20 | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.00 |
| 9    | root | 0  | -20 | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.14 |
| 10   | root | 0  | -20 | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.00 |
| 11   | root | 20 | 0   | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.00 |
| 12   | root | 20 | 0   | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.00 |
| 13   | root | 20 | 0   | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.00 |
| 14   | root | 20 | 0   | 0      | 0      | 0     | S | 0,0  | 0,0  | 0:00.06 |
| 15   | root | 20 | 0   | 0      | 0      | 0     | I | 0,0  | 0,0  | 0:00.84 |


```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
top - 15:45:55 up 54 min, 1 user, load average: 0,02, 0,07, 0,08  
Tasks: 151 total, 1 running, 150 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 2,0 us, 1,5 sy, 0,0 ni, 96,5 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0  
MiB Mem : 1981,3 total, 996,3 free, 524,6 used, 460,4 buff/cache  
MiB Swap: 976,0 total, 976,0 free, 0,0 used. 1305,5 avail Mem  


| COMMAND                     |
|-----------------------------|
| qterminal                   |
| systemd                     |
| kthreadd                    |
| rcu_gp                      |
| rcu_par_gp                  |
| netns                       |
| kworker/0:0H-events_highpri |
| kworker/0:1H-events_highpri |
| mm_percpu_wq                |
| rcu_tasks_kthread           |
| rcu_tasks_rude_kthread      |
| rcu_tasks_trace_kthread     |
| ksoftirqd/0                 |
| rcu_preempt                 |
| migration/0                 |
| cpuhp/0                     |
| cpuhp/1                     |
| migration/1                 |
| ksoftirqd/1                 |
| kworker/1:0H-events_highpri |


```

Processi attivi su macchina Linux

Attraverso il comando: *top*, digitato nel terminale, si controllano i processi attivi.

Nella colonna *PID*, si hanno dei valori di assegnazione secondo l'ordine temporale di creazione dei processi.

Nella colonna *USER*, si hanno gli utenti in cui sono in esecuzione i processi.

Nella colonna *COMMAND*, si hanno i comandi in cui sono in esecuzione i processi.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ top | grep root  
1 root      20   0 102468 12096 8988 S   0,0   0,6 0:01.65  
2 root      20   0      0      0      0 S   0,0   0,0 0:00.00  
3 root       0 -20      0      0      0 I   0,0   0,0 0:00.00  
4 root       0 -20      0      0      0 I   0,0   0,0 0:00.00  
5 root       0 -20      0      0      0 I   0,0   0,0 0:00.00  
7 root       0 -20      0      0      0 I   0,0   0,0 0:00.00  
9 root       0 -20      0      0      0 I   0,0   0,0 0:00.31  
10 root      0 -20      0      0      0 I   0,0   0,0 0:00.00  
11 root      20   0      0      0      0 I   0,0   0,0 0:00.00  
12 root      20   0      0      0      0 I   0,0   0,0 0:00.00  
13 root      20   0      0      0      0 I   0,0   0,0 0:00.00  
14 root      20   0      0      0      0 S   0,0   0,0 0:00.15  
15 root      20   0      0      0      0 I   0,0   0,0 0:04.19  
16 root      rt   0      0      0      0 S   0,0   0,0 0:00.08  
18 root      20   0      0      0      0 S   0,0   0,0 0:00.00  
19 root      20   0      0      0      0 S   0,0   0,0 0:00.00  
20 root      rt   0      0      0      0 S   0,0   0,0 0:00.20  
  
(kali@kali)-[~]  
$
```

Processi attivi su macchina Linux filtrati per utente *root*

Attraverso il comando: `top | grep root`, si controllano i processi attivi, filtrati tramite `|`, dell'utente *root*.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
—(kali@kali)~  
$ top | grep kali  
42055 kali 20 0 10392 3680 3140 R 12,5 0,2 0:00.02  
887 kali 20 0 327912 49416 34376 S 2,3 2,4 0:01.04  
888 kali 20 0 353888 40976 22520 S 2,0 2,0 2:37.58  
41601 kali 20 0 432512 104476 83984 S 1,3 5,1 0:00.68  
890 kali 20 0 359848 30888 20960 S 1,0 1,5 1:07.09  
884 kali 20 0 475468 54920 36668 S 0,7 2,7 0:03.99  
713 kali 20 0 269776 28340 18376 S 0,3 1,4 0:02.08  
842 kali 20 0 932744 104220 77440 S 0,3 5,1 0:29.40  
867 kali 20 0 232220 29780 19496 S 0,3 1,5 0:02.05  
879 kali 20 0 413216 55148 39832 S 0,3 2,7 0:02.97  
889 kali 20 0 342048 27612 18208 S 0,3 1,4 0:01.56  
893 kali 20 0 668300 47008 35436 S 0,3 2,3 0:13.61  
894 kali 20 0 335052 43608 32652 S 0,3 2,1 0:01.85  
895 kali 20 0 392464 46012 32968 S 0,3 2,3 0:01.81  
896 kali 20 0 400496 43532 32652 S 0,3 2,1 0:01.70  
919 kali 20 0 262744 20016 15724 S 0,3 1,0 0:01.33  
946 kali 20 0 188944 22656 16184 S 0,3 1,1 0:01.50  
956 kali 20 0 376564 55592 32676 S 0,3 2,7 0:02.28  
983 kali 20 0 560188 51912 38212 S 0,3 2,6 0:01.74  
  
—(kali@kali)~  
$
```


Processi attivi su macchina Linux filtrati per utente *kali*

Attraverso il comando: `top | grep kali`, si controllano i processi attivi, filtrati tramite `|`, dell'utente *kali*.



The screenshot shows a Kali Linux terminal window with a dark theme. The title bar at the top reads "kali@kali: ~". Below the title bar is a menu bar with the options "File", "Azioni", "Modifica", "Visualizza", and "Aiuto". The terminal content shows the prompt "(kali@kali)-[~]" followed by the command "\$ mkdir /home/kali/Scrivania/Epicode_Lab". The command has been executed, and the prompt is now "\$" on a new line.


```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ mkdir /home/kali/Scrivania/Epicode_Lab  
  
(kali@kali)-[~]  
$
```



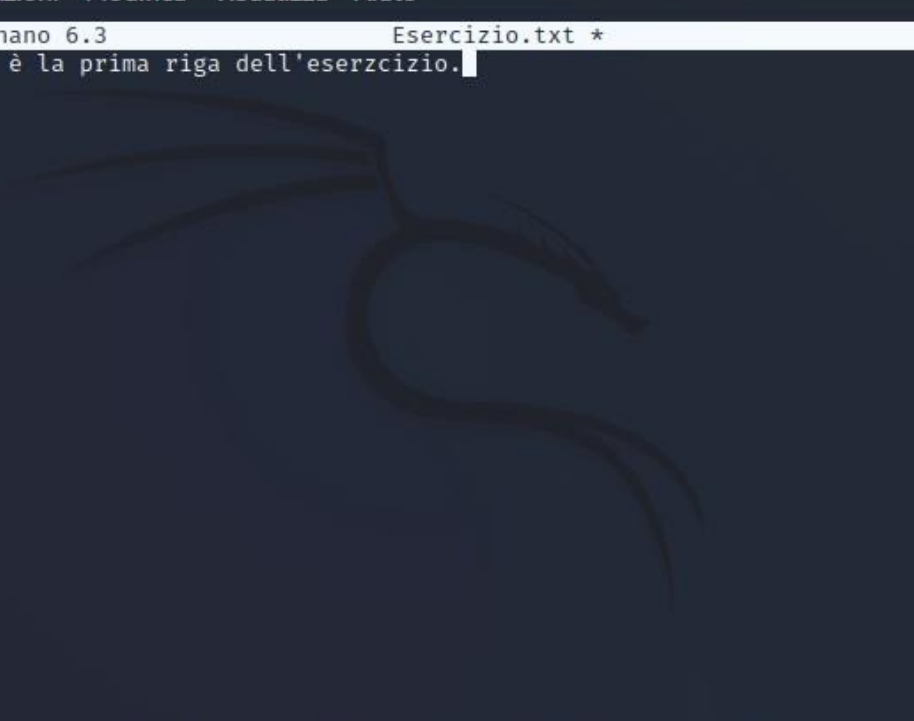
The screenshot shows a Kali Linux terminal window. The title bar at the top reads "kali@kali: ~/Scrivania/Epicode_Lab". Below the title bar is a menu bar with the options "File", "Azioni", "Modifica", "Visualizza", and "Aiuto". The terminal content shows the following sequence of commands and prompts:

```
(kali㉿kali)-[~]  
$ cd /home/kali/Scrivania/Epicode_Lab  
  
(kali㉿kali)-[~/Scrivania/Epicode_Lab]  
$
```

The prompt changes from "(kali㉿kali)-[~]" to "(kali㉿kali)-[~/Scrivania/Epicode_Lab]" after the "cd" command is executed. The cursor is positioned at the end of the second prompt line.



```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~/Scrivania/Epicode_Lab]
$ nano Esercizio.txt
(kali@kali)-[~/Scrivania/Epicode_Lab]
$
```



```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto
GNU nano 6.3 Esercizio.txt *
Questa è la prima riga dell'esercizio.
^G Help      ^O Salva     ^W Cerca     ^K Cut       ^T Execute
^X Esci      ^R Inserisci ^\ Sostituisci ^U Paste     ^J Giustifica
```



```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto

(kali@kali)-[~/Scrivania/Epicode_Lab]
$ cat Esercizio.txt
Questa è la prima riga dell'esercizio.

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

```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto

(kali@kali)-[~/Scrivania/Epicode_Lab]
$ ls -la Esercizio.txt
-rw-r--r-- 1 kali kali 41  2 nov 16.38 Esercizio.txt

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

```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto

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

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

(kali@kali)-[~/Scrivania/Epicode_Lab]
$ ls -la Esercizio.txt
-rwxrw-r-- 1 kali kali 41  2 nov 16.38 Esercizio.txt

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

Comandi per visualizzare *Esercizio.txt* e modificare privilegi

Attraverso il comando *cat Esercizio.txt*, come mostrato nell'immagine in alto, si legge a schermo il file *Esercizio.txt*.

Attraverso il comando: *ls -la Esercizio.txt*, come mostrato nell'immagine a destra, si verificano i permessi del file *Esercizio.txt*, dove si nota che l'utente corrente ha privilegi di lettura e scrittura, il gruppo ed altri utenti, solo di lettura.

Attraverso i comandi: *chmod u+x Esercizio.txt* e, successivamente, *chmod g+w Esercizio.txt*, come mostrato nell'immagine a sinistra, si aggiunge al file *Esercizio.txt*, nella directory *Epicode_Lab*, il privilegio di esecuzione all'utente *kali* e di scrittura al gruppo.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ useradd ilak  
useradd: Permission denied.  
useradd: cannot lock /etc/passwd; try again later.  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ sudo useradd ilak  
(kali@kali)-[~]  
$ sudo passwd ilak  
Nuova password:  
Reimmettere la nuova password:  
passwd: password aggiornata correttamente  
(kali@kali)-[~]  
$
```

```
kali@kali: ~/Scrivania/Epicode_Lab  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~/Scrivania/Epicode_Lab]  
$ chmod o-r Esercizio.txt  
(kali@kali)-[~/Scrivania/Epicode_Lab]  
$ ls -la Esercizio.txt  
-rwxrwx--- 1 kali kali 41  2 nov 16.38 Esercizio.txt  
(kali@kali)-[~/Scrivania/Epicode_Lab]  
$
```

Creazione nuovo utente e modifica privilegi *Esercizio.txt*

Attraverso il comando *useradd ilak*, come mostrato nell'immagine in alto a sinistra, non si ha il permesso di creare un nuovo utente, essendo un comando che necessita di permessi di amministratore.

Attraverso il comando: *sudo useradd ilak*, come mostrato nell'immagine in alto a destra, si crea l'utente *ilak*, tramite i permessi di amministratore e, attraverso il comando: *sudo passwd ilak*, si imposta una password per l'utente appena creato.

Attraverso il comando: *chmod o-r Esercizio.txt*, come mostrato nell'immagine in basso, si rimuove al file *Esercizio.txt*, nella directory *Epicode_Lab*, il privilegio di lettura a gli altri utenti.

```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto

(kali@kali)-[~/Scrivania/Epicode_Lab]
$ mv Esercizio.txt /
mv: impossibile creare il file regolare '/Esercizio.txt': Permesso negato

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

```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto

(kali@kali)-[~/Scrivania/Epicode_Lab]
$ sudo mv Esercizio.txt /
[sudo] password di kali:

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

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

Spostamento di *Esercizio.txt* nella directory root (/)

Attraverso il comando: *mv Esercizio.txt /*, come mostrato nell'immagine a sinistra, non si ha il permesso di spostare *Esercizio.txt*, essendo un comando che necessita di permessi di amministratore, vista l'importanza di /, cartella principale del sistema.

Attraverso il comando: *sudo mv Esercizio.txt /*, come mostrato nell'immagine a destra, si può spostare *Esercizio.txt*, tramite i permessi di amministratore, nella directory / e, tramite il comando: *ls /*, si verifica la presenza di *Esercizio.txt* nella directory /.


```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto

(kali@kali)-[~/Scrivania/Epicode_Lab]
$ su ilak
Password:
$ nano /Esercizio.txt
```

```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto

GNU nano 6.3 Nuovo buffer

[ Errore durante la lettura di /Esercizio.txt: Permesso negato ] ...
^G Help      ^O Salva     ^W Cerca    ^K Cut       ^T Execute
^X Esci      ^R Inserisci ^\ Sostituisci ^U Paste     ^J Giustifica
```

Cambio utente e apertura *Esercizio.txt*

Attraverso il comando: *su ilak*, si cambia utente e, successivamente, con il comando *nano /Esercizio.txt*, si prova ad aprire *Esercizio.txt* nella directory / ma, il permesso è negato.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ chmod o+r /Esercizio.txt  
(kali@kali)-[~]  
$ ls -la /Esercizio.txt  
-rwxrw-r-- 1 kali kali 41  2 nov 16.38 /Esercizio.txt  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ su ilak  
Password:  
$ nano /Esercizio.txt
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
GNU nano 6.3 /Esercizio.txt  
Questa è la prima riga dell'esercizio.  
  
[ Il file "/Esercizio.txt" non è scrivibile ]...  
^G Help      ^O Salva     ^W Cerca    ^K Cut       ^T Execute  
^X Esci      ^R Inserisci ^\ Sostituisci ^U Paste     ^J Giustifica
```

Modifica privilegi *Esercizio.txt* e riapertura da nuovo utente

Attraverso il comando: `chmod o+r`, come mostrato nell'immagine in alto, si aggiunge il privilegio di lettura a gli altri utenti e, successivamente, con il comando `ls -la /Esercizio.txt`, si verificano i privilegi di *Esercizio.txt* nella directory `/`.

Attraverso il comando: `su ilak`, si cambia utente e, successivamente, con il comando `nano /Esercizio.txt`, si prova ad aprire *Esercizio.txt* nella directory `/` ma, risulta non scrivibile.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo rm /Esercizio.txt  
[sudo] password di kali:  
  
(kali@kali)-[~]  
$ ls /  
0      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  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ rmdir /home/kali/Scrivania/Epicode_Lab  
  
(kali@kali)-[~]  
$ ls /home/kali/Scrivania  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo userdel ilak  
[sudo] password di kali:  
  
(kali@kali)-[~]  
$ su ilak  
su: user ilak does not exist or the user entry does not contain all the requi  
red fields  
  
(kali@kali)-[~]  
$
```

Cancellazione *Esercizio.txt*, directory e utente

Attraverso il comando: `sudo rm /Esercizio.txt`, come mostrato nell'immagine in alto a sinistra, si elimina *Esercizio.txt*, con permessi di *root*, visto che si trova nella cartella `/` e, con il comando `ls /`, si può verificare la sua assenza.

Attraverso il comando: `rmdir /home/kali/Scrivania/Epicode_Lab`, come mostrato nell'immagine a in alto a destra, si elimina *Epicode_Lab* e, con il comando: `ls /home/kali/Scrivania`, si può verificare l'assenza della directory.

Attraverso il comando: `sudo userdel ilak`, come mostrato nell'immagine in basso, si elimina l'utente *ilak*, tramite i permessi di amministratore e, con il comando: `su ilak`, si può verificare come l'utente non esista.