

# Esercizio sui comandi Shell


## Parte 1

Mandando il comando TOP, è possibile controllare i processi attivi su kali Linux. Nella schermata che segue:

il **PID** ha la funzione di identificare univocamente il processo nel sistema. Non è modificabile e non varia per tutta la durata del processo di controllo.

L'**USER** fa riferimento all'utente che esegue il processo (il root, ad esempio, è il nome utente dell'amministratore di sistema)

Il **COMMAND** rappresenta molto banalmente il nome del comando lanciato. Ad esempio Xorg corrisponde più precisamente al comando per l'implementazione open source del gestore grafico X Window System. O, ancora, Polkitd (PolicyKit) è un componente del sistema operativo che controlla i sistemi di privilegi



1

2

3

4

5

PS> kali@kali: /home/kali

File Actions Edit View Help

```
top - 10:15:35 up 10 min, 1 user, load average: 0.09, 0.08, 0.07
Tasks: 165 total, 8 running, 155 sleeping, 0 stopped, 2 zombie
%Cpu(s): 0.8 us, 0.8 sy, 0.0 ni, 97.3 id, 0.6 wa, 0.0 hi, 0.5 si, 0.0 st
MiB Mem : 1981.2 total, 777.1 free, 725.8 used, 478.3 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 1100.5 avail Mem
PID to signal/kill [default pid = 397]
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
397	polkitd	20	0	309920	11956	7452	S	15.3	0.6	0:01.00	polkitd
3545	lightdm	20	0	668372	108412	78948	S	1.1	5.3	0:00.46	lightdm-gtk-gre
3608	root	20	0	0	0	0	Z	0.9	0.0	0:00.03	lightdm
949	kali	20	0	203984	31528	18260	S	0.6	1.6	0:02.66	panel-13-cpugra
645	root	20	0	358232	111376	57328	S	0.3	5.5	0:10.70	Xorg
852	kali	20	0	152916	2744	2268	S	0.3	0.1	0:02.11	VBoxClient
953	kali	20	0	350252	30156	20416	S	0.3	1.5	0:01.26	panel-15-genmon
3503	root	20	0	345668	79020	57080	D	0.3	3.9	0:00.26	Xorg
1	root	20	0	167548	12116	8980	S	0.0	0.6	0:00.83	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.02	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
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	R	0.0	0.0	0:00.05	ksoftirqd/0
15	root	20	0	0	0	0	R	0.0	0.0	0:00.39	rcu_preempt
16	root	rt	0	0	0	0	S	0.0	0.0	0:00.01	migration/0
17	root	20	0	0	0	0	I	0.0	0.0	0:00.01	kworker/0:1-mm_percpu_wq
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	0:00.15	migration/1
21	root	20	0	0	0	0	S	0.0	0.0	0:00.08	ksoftirqd/1

Con il comando **GREP**, è possibile filtrare i risultati in base a nomi di file di input. Nei due screen successivi i risultati sono stati filtrati prima impostando come user kali, poi root.

```
File Actions Edit View Help

(kali㉿kali)-[~]
$ top | grep kali
852 kali      20    0 152916   2744   2268 S   6.2   0.1   0:24.10 VBoxClient
949 kali      20    0 203984   32464  18988 S   1.0   1.6   0:28.28 panel-13-cpugra
852 kali      20    0 152916   2744   2268 S   0.7   0.1   0:24.12 VBoxClient
901 kali      20    0 931320  105896  77040 S   0.7   5.2   0:15.20 xfwm4
953 kali      20    0 350252   30256  20424 S   0.3   1.5   0:12.28 panel-15-genmon
25936 kali    20    0 468220  107524  87804 S   0.3   5.3   0:00.55 qterminal
25939 kali    20    0 3686372 101416  59552 S   0.3   5.0   0:00.70 pwsh
852 kali      20    0 152916   2744   2268 S   1.0   0.1   0:24.15 VBoxClient
949 kali      20    0 203984   32464  18988 S   0.3   1.6   0:28.29 panel-13-cpugra
954 kali      20    0 665824   45800  34628 S   0.3   2.3   0:03.05 panel-16-pulsea

(kali㉿kali)-[~]
$ top | grep root
645 root      20    0 374500  127772  57184 R  13.3   6.3   0:46.44 Xorg
1 root       20    0 167548  12116   8980 S   0.0   0.6   0:00.98 systemd
2 root       20    0      0      0      0 S   0.0   0.0   0:00.03 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
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   0:00.18 ksoftirqd/0
15 root      20    0      0      0      0 I   0.0   0.0   0:02.86 rcu_preempt
16 root      rt    0      0      0      0 S   0.0   0.0   0:00.15 migration/0
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   0:00.17 migration/1
21 root      20    0      0      0      0 S   0.0   0.0   0:00.31 ksoftirqd/1
23 root       0 -20      0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-events_highpri
```

Successivamente, dopo aver aperto il desktop, è stata creata la directory "Epicode\_Lab" con il comando **MKDIR**. Dopo aver verificato che ciò fosse avvenuto con successo, sfruttando il comando **LS** (nell'esecuzione ho lanciato per errore LS-L), è stato usato il comando **CD** per spostarsi sulla nuova directory creata e inserirvi il file "Esercizio.txt", tramite il comando **TOUCH**. Dopo aver verificato con **LS** che il file fosse stato creato con successo, si è utilizzato l'editor di testo da riga di comando **NANO** per modificare il file e, digitando dapprima CTRL+X, poi Y, le modifiche sono state salvate. Il tutto è documentato nel prossimo screenshot.

```
File Actions Edit View Help

(kali㉿kali)-[~]
$ open desktop
sofsoft Corporation.

(kali㉿kali)-[~]
$ desktop
to get help.

(kali㉿kali)-[~/desktop]
$ ls -l
total 0

(kali㉿kali)-[~/desktop]
$ mkdir Epicode_Lab

(kali㉿kali)-[~/desktop]
$ ls -l
total 4
drwxr-xr-x 2 kali kali 4096 Jan 31 12:45 Epicode_Lab
```

```

(kali㉿kali)-[~/desktop]
$ cd Epicode_Lab

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ touch Esercizio.txt

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ ls
Esercizio.txt

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ nano Esercizio.txt

```

## Parte 2

Per dimostrare che il file "Esercizio.txt" sia stato modificato, viene usato il comando CAT

```

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ nano Esercizio.txt

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ cat Esercizio.txt
Esercizio.txt modificato

```

Dopo aver controllato i permessi del file con il comando LS-LA, si può procedere a modificare gli stessi in due modi, parimenti utilizzando il comando CHMOD. Qualora si voglia procedere file per file, si usi CHMOD U+X "NOME FILE" -per aggiungere un privilegio- e CHMOD U-X "NOME FILE" -per rimuovere un privilegio, dove u= utente e x=privilegio. Alternativamente, se ci si ricorda della seguente tabella, si può procedere più agilmente usando i numeri.

7 corrisponde a **rwX**  
6 corrisponde a **rw**  
5 corrisponde a **rx**  
4 corrisponde a **r**  
3 corrisponde a **wX**  
2 corrisponde a **w**  
1 corrisponde a **x**  
0 negato ogni accesso

Dunque, si procederà a modificare i privilegi in modo tale che l'utente corrente abbia i privilegi r w x, il gruppo r w, gli altri utenti solo r. Infine con il comando LS -LA si può verificare che le modifiche siano state salvate.

```

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Jan 31 13:15 .
drwxr-xr-x 3 kali kali 4096 Jan 31 12:45 ..
-rw-r--r-- 1 kali kali 25 Jan 31 13:15 Esercizio.txt

```

```

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ chmod 764 Esercizio.txt

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Jan 31 13:15 .
drwxr-xr-x 3 kali kali 4096 Jan 31 12:45 ..
-rwxrw-r-- 1 kali kali 25 Jan 31 13:15 Esercizio.txt

```

Lo step successivo è quello di creare un nuovo utente, servendosi del comando USERADD e PASSWD, per assegnarli una password

```

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ sudo useradd Michele

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ sudo passwd Michele
New password:
Retype new password:
passwd: password updated successfully

```

Con il nuovo utente, si può procedere a utilizzare CHMOD per alterare i privilegi del file.txt in modo che gli altri utenti non siano abilitati alla lettura. Il comando CHMOD manualmente si usa nel seguente modo:

CHMOD U(utente)/G(gruppo)/O(other - altri utenti) +/- "nome file". Dunque si procederà così:

```

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

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Jan 31 13:15 .
drwxr-xr-x 3 kali kali 4096 Jan 31 12:45 ..
-rwxrw--- 1 kali kali 25 Jan 31 13:15 Esercizio.txt

```

Si procede con lo spostamento del file nella directory di root. Più precisamente: si sposta usando NANO e poi il comando MV seguito dalla sorgente e dalla destinazione (il root si indica con /). Con CD (e indicando la destinazione) si cambia directory e ci si sposta sul root, per controllare che il file "Esercizio.txt" stia nello stesso.

```

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ sudo mv Esercizio.txt /
[sudo] password for kali:

(kali㉿kali)-[~/desktop/Epicode_Lab]
$ cd /

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

```

Dopo aver usato il comando SU seguito da un nome utente, per cambiare lo stesso, si aprirà in lettura il file.txt creato in precedenza, riscontrando l'errore di permesso negato. Quello che ci aspettavamo, visto che ciò non fornisce altro che una riprova del fatto che lo spostamento sulla directory root sia andato a buon fine. Nel secondo screen, segue l'errore ricevuto provando ad aprire il file

```
(kali㉿kali)-[/]  
$ su Michele  
Password:  
$ cat Esercizio.txt  
cat: Esercizio.txt: Permission denied
```

```
$ nano cat Esercizio.txt  
Unable to create directory /home/Michele/.local/share/nano/: No such file or directory  
It is required for saving/loading search history or cursor positions.
```

```
[ Error reading Esercizio.txt: Permission denied ] ...
```

```
^T Execute ^C Location M-U Undo
```

Pertanto, tornati (sempre usando SU) sul vecchio utente, i permessi dei file devono essere modificati nuovamente, facendo questa volta in modo che il nuovo utente possa leggere l'input.

```
$ su kali  
Password:  
(kali㉿kali)-[/]  
$ chmod o+r Esercizio.txt  
  
(kali㉿kali)-[/]  
$ su Michele  
Password:  
$ cat Esercizio.txt  
Esercizio.txt modificato  
$
```

In conclusione, bisognerà riportare lo scenario allo stato iniziale, rimuovendo il file, la cartella e l'utente creato, utilizzando i comandi SUDO rispettivamente con RM, RM-R e USERDEL. In alternativa è possibile mandare il comando SUDO REBOOT e assicurarsi che sia tutto sparito.

```
(kali㉿kali)-[/home/kali]  
PS> sudo userdel Michele  
[sudo] password for kali:  
  
(kali㉿kali)-[/home/kali]  
PS> su Michele  
su: user Michele does not exist or the user entry does not contain all the required fields
```

```
(kali㉿kali)-[/home/kali/Desktop]  
PS> ls  
  
(kali㉿kali)-[/home/kali/Desktop]  
PS>
```