

Relazione esercitazione del 03/10/2023

```
top - 08:02:45 up 3 min, 1 user, load average: 1.80, 1.48, 0.63
Tasks: 167 total, 1 running, 166 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1.7 us, 2.1 sy, 0.0 ni, 95.5 id, 0.0 wa, 0.0 hi, 0.7 si, 0.0 st
MiB Mem : 1972.2 total, 968.5 free, 746.2 used, 409.5 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 1226.1 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
794	root	20	0	384216	124196	57424	S	9.6	6.1	0:21.00	Xorg
1076	kali	20	0	1022768	107852	77456	S	1.3	5.3	0:04.43	xfwm4
1014	kali	20	0	217956	2464	2116	S	1.0	0.1	0:00.57	VBoxClient
1737	kali	20	0	445800	108700	88980	S	1.0	5.4	0:03.16	qterminal
27	root	20	0	0	0	0	I	0.3	0.0	0:01.90	kworker/2:0-ata_sff
188	root	20	0	0	0	0	I	0.3	0.0	0:00.62	kworker/0:3-events
222	root	20	0	0	0	0	I	0.3	0.0	0:00.86	kworker/1:2-events
576	root	20	0	0	0	0	I	0.3	0.0	0:00.33	kworker/2:4-events
1009	kali	20	0	217440	2400	2052	S	0.3	0.1	0:00.46	VBoxClient
1108	kali	20	0	231152	29096	19220	S	0.3	1.4	0:01.11	xfsettingsd
1125	kali	20	0	413596	58024	35392	S	0.3	2.9	0:03.56	xfdesktop
1131	kali	20	0	207096	27744	18520	S	0.3	1.4	0:01.86	panel-13-cpugra
1133	kali	20	0	358524	30576	20704	S	0.3	1.5	0:01.25	panel-15-genmon
2030	kali	20	0	11772	5316	3168	R	0.3	0.3	0:00.14	top
1	root	20	0	167896	12248	8948	S	0.0	0.6	0:04.97	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.01	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
7	root	20	0	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0-events
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	0:00.00	kworker/u6:0-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	0:00.62	ksoftirqd/0
15	root	20	0	0	0	0	I	0.0	0.0	0:00.89	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	0:00.94	kworker/0:1-cgroup_destroy
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	0:00.26	migration/1
21	root	20	0	0	0	0	S	0.0	0.0	0:00.09	ksoftirqd/1
22	root	20	0	0	0	0	I	0.0	0.0	0:00.39	kworker/1:0-events
23	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/1:0H-events_highpri
24	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/2
25	root	rt	0	0	0	0	S	0.0	0.0	0:00.28	migration/2
26	root	20	0	0	0	0	S	0.0	0.0	0:00.29	ksoftirqd/2
28	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/2:0H-kblockd
30	root	20	0	0	0	0	I	0.0	0.0	0:00.02	kworker/u6:1-flush-8:0
31	root	20	0	0	0	0	I	0.0	0.0	0:06.60	kworker/u6:2-flush-8:0
32	root	20	0	0	0	0	S	0.0	0.0	0:00.11	kdevtmpfs
33	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	inet_frag_wq

ui abbiamo
utilizzato il
comando top per
visualizzare tutti i
processi in corso sul
nostro terminale. In
Linux, ogni processo
è identificato da un
numero il PID.
User sta per l'user
che sta utilizzando
quel determinato
processo e infine
abbiamo

COMMAND che è il
nome del comando

```
(kali㉿kali)-[//]
```

```
$ top | grep root
```

794	root	20	0	416024	144684	63000	S	55.0	7.2	7:14.37	Xorg
1	root	20	0	167896	12248	8948	S	0.0	0.6	0:05.34	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+
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	0:02.21	ksoftir+
15	root	20	0	0	0	0	I	0.0	0.0	0:13.23	rcu_pre+

```
(kali㉿kali)-[//]
```

```
$ top | grep kali
```

1076	kali	20	0	1022768	112084	77456	S	5.0	5.5	1:42.96	xfwm4
1133	kali	20	0	358524	30680	20704	S	5.0	1.5	0:46.50	panel-1+
48944	kali	20	0	11580	4972	3068	R	5.0	0.2	0:00.01	top
923	kali	20	0	9684	5432	4236	S	1.3	0.3	0:06.58	dbus-da+
1014	kali	20	0	217956	2464	2116	S	0.7	0.1	0:38.04	VBoxCli+
1076	kali	20	0	1022768	112084	77456	S	0.7	5.5	1:42.98	xfwm4
1131	kali	20	0	355624	38844	20800	S	0.7	1.9	0:54.46	panel-1+
1737	kali	20	0	445996	109664	89560	S	0.7	5.4	0:50.61	qtermin+
1009	kali	20	0	217440	2400	2052	S	0.3	0.1	0:25.71	VBoxCli+
1116	kali	20	0	403044	48860	34744	S	0.3	2.4	0:04.99	xfce4-p+
1133	kali	20	0	358524	30680	20704	S	0.3	1.5	0:46.51	panel-1+
1134	kali	20	0	601108	45712	34416	S	0.3	2.3	0:19.34	panel-1+
48944	kali	20	0	11580	4972	3068	R	0.3	0.2	0:00.02	top
1076	kali	20	0	1022768	112084	77456	S	4.5	5.5	1:43.12	xfwm4
1131	kali	20	0	355624	38844	20800	S	1.0	1.9	0:54.49	panel-1+
1133	kali	20	0	358524	30680	20704	S	1.0	1.5	0:46.54	panel-1+
1737	kali	20	0	445996	109664	89560	S	1.0	5.4	0:50.64	qtermin+
1014	kali	20	0	217956	2464	2116	S	0.6	0.1	0:38.06	VBoxCli+
1009	kali	20	0	217440	2400	2052	S	0.3	0.1	0:25.72	VBoxCli+
48944	kali	20	0	11580	4972	3068	R	0.3	0.2	0:00.03	top

Qui abbiamo applicato dei
filtri al nostro comando
TOP, con pipe | GREP
e abbiamo nel primo screen
tutti i processi di root e nel
secondo tutti i processi
di kali

```
(kali㉿kali)-[~]  
$ cd /home/kali/Desktop  
  
(kali㉿kali)-[~/Desktop]  
$ cd /home/kali/Desktop  
  
(kali㉿kali)-[~/Desktop]  
$ mkdir Epicode_Lab  
  
(kali㉿kali)-[~/Desktop]  
$ cd /home/kali/Desktop/Epicode_Lab  
  
(kali㉿kali)-[~/Desktop/Epicode_Lab]  
$ touch Esercizio.txt  
  
(kali㉿kali)-[~/Desktop/Epicode_Lab]  
$
```



ui ci siamo spostati sul desktop, comando CD, abbiamo creato una cartella chiamata Epicode_Lab, comando MKDIR, al cui interno abbiamo creato un file di testo comando TOUCH (Esercizio.txt)
E lo abbiamo modificato col comando NANO, successivamente salvato con ctrl+x e y

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ cat Esercizio.txt
Questo e` il file di testo creato per l'esercizio di oggi

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Oct  3 08:38 .
drwxr-xr-x 3 kali kali 4096 Oct  3 08:32 ..
-rw-r--r-- 1 kali kali   59 Oct  3 08:38 Esercizio.txt

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

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Oct  3 08:38 .
drwxr-xr-x 3 kali kali 4096 Oct  3 08:32 ..
-rw-rw-r-- 1 kali kali   59 Oct  3 08:38 Esercizio.txt

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Oct  3 08:38 .
drwxr-xr-x 3 kali kali 4096 Oct  3 08:32 ..
-rwxrw-r-- 1 kali kali   59 Oct  3 08:38 Esercizio.txt

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

KALI LINUX

"the quieter you become, the more you are able to hear"

Qui abbiamo visualizzato il contenuto del documento con il comando CAT, visualizzato i privilegi col comando LS -LA e in seguito a modificarli


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

(kali㉿kali)-[/]
$ passwd pippo
passwd: You may not view or modify password information for pippo.

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

```
$ ls
bin boot dev Esercizio.txt etc 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)-[/]
$ su pippo
Password:
$ cat Esercizio.txt
cat: Esercizio.txt: Permission denied
$
```

```
-rwxrwx-r-- 1 kali kali 59 Oct 3 08:38 Esercizio.txt
drwxr-xr-x 176 root root 12288 Oct 3 09:01 etc
drwxr-xr-x 3 root root 4096 Mar 10 2023 home
lrwxrwxrwx 1 root root 33 Mar 10 2023 initrd.img → boot/initrd.img-6.1.0-kali5-amd64
lrwxrwxrwx 1 root root 33 Mar 10 2023 initrd.img.old → boot/initrd.img-6.1.0-kali5-amd64
lrwxrwxrwx 1 root root 7 Mar 10 2023 lib → usr/lib
lrwxrwxrwx 1 root root 9 Mar 10 2023 lib32 → usr/lib32
lrwxrwxrwx 1 root root 9 Mar 10 2023 lib64 → usr/lib64
lrwxrwxrwx 1 root root 10 Mar 10 2023 libx32 → usr/libx32
drwx----- 2 root root 16384 Mar 10 2023 lost+found
drwxr-xr-x 2 root root 4096 Mar 10 2023 media
drwxr-xr-x 2 root root 4096 Mar 10 2023 mnt
drwxr-xr-x 3 root root 4096 Mar 10 2023 opt
dr-xr-xr-x 228 root root 0 Oct 3 07:59 proc
drwx----- 6 root root 4096 Oct 3 08:25 root
drwxr-xr-x 31 root root 780 Oct 3 08:01 run
lrwxrwxrwx 1 root root 8 Mar 10 2023 sbin → usr/sbin
drwxr-xr-x 3 root root 4096 Mar 10 2023 srv
-rw----- 1 root root 1073741824 Mar 10 2023 swapfile
dr-xr-xr-x 13 root root 0 Oct 3 07:59 sys
drwxrwxrwt 12 root root 4096 Oct 3 09:09 tmp
drwxr-xr-x 16 root root 4096 Mar 10 2023 usr
drwxr-xr-x 12 root root 4096 Mar 10 2023 var
lrwxrwxrwx 1 root root 30 Mar 10 2023 vmlinuz → boot/vmlinuz-6.1.0-kali5-amd64
lrwxrwxrwx 1 root root 30 Mar 10 2023 vmlinuz.old → boot/vmlinuz-6.1.0-kali5-amd64
```

```
(kali㉿kali)-[/]
$ su pippo
Password:
$ cat Esercizio.txt
Questo e' il file di testo creato per l'esercizio di oggi

$
```

Qui abbiamo creato un nuovo utente, che come possiamo vedere non ha i privilegi per leggerlo e quindi successivamente gli abbiamo dato i privilegi per leggerlo.