

Esercizio 09/05 week 2

Per controllare i processi attivi sulla nostra macchina (in questo caso linux), sul nostro terminale eseguendo il comando `sudo top` davanti a noi si mostrerà un output di dati dove tra le categorie troveremo:

- 1) PID (process identifier): è l'identificativo di un processo attivo a cui viene attribuito un numero
- 2) USER: è l'identificativo dell'utente che sta compiendo il processo
- 3) COMMAND: specifica l'azione che avviene dentro al terminale

```
(kali@kali)-[~]
$ sudo top
top - 08:19:06 up 11 min, 4 users, load average: 0.04, 0.14, 0.09
Tasks: 160 total, 1 running, 151 sleeping, 8 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1972.4 total, 921.2 free, 787.2 used, 419.7 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 1185.2 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
    1 root        20   0 102224 12028 8964 S   0.0   0.6   0:00.52 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
   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   0:00.03 ksoftirqd/0
   15 root        20   0      0      0      0 I   0.0   0.0   0:00.11 rcu_preempt
   16 root        rt    0      0      0      0 S   0.0   0.0   0:00.00 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   0:00.13 migration/1
   21 root        20   0      0      0      0 S   0.0   0.0   0:00.02 ksoftirqd/1
   23 root         0  -20      0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-events_highpri
   25 root        20   0      0      0      0 I   0.0   0.0   0:00.57 kworker/u4:1-events_unbound
   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
   28 root        20   0      0      0      0 S   0.0   0.0   0:00.00 kauditd
   29 root        20   0      0      0      0 S   0.0   0.0   0:00.00 khungtaskd
   30 root        20   0      0      0      0 S   0.0   0.0   0:00.00 oom_reaper
```

successivamente abbiamo filtrato col comando `grep`:

`top|grep kali` (immagine 1)

`top|grep root` (immagine 2)

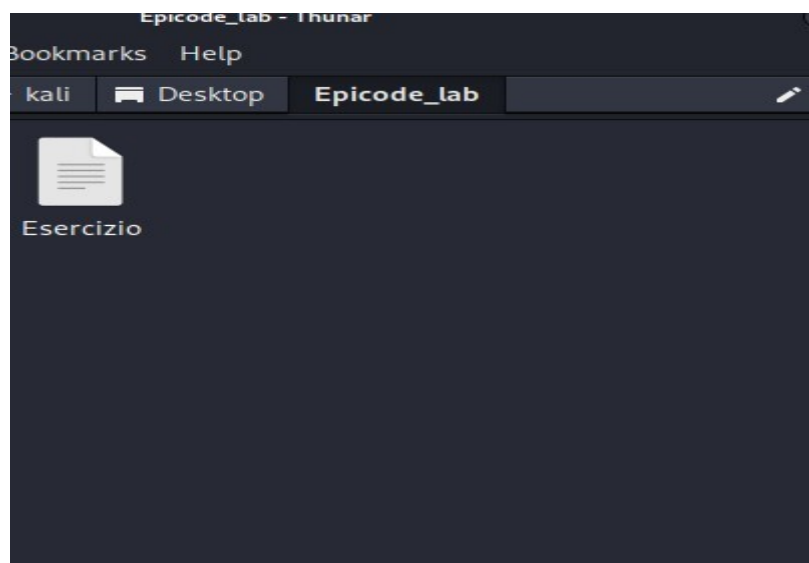
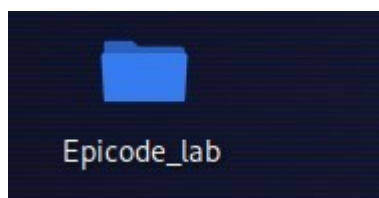
```
(kali@kali)-[~]
$ top|grep kali
65439 kali        20   0 446028 109396 89824 S   4.5   5.4   0:00.59 qtermin+
65439 kali        20   0 446028 109396 89824 S   0.3   5.4   0:00.60 qtermin+
1003 kali        20   0 350340 28768 20820 S   0.5   1.4   0:11.26 panel-1+
1004 kali        20   0 666636 45348 34052 S   0.5   2.2   0:03.33 panel-1+
1001 kali        20   0 352528 40484 22168 S   0.3   2.0   0:11.09 panel-1+
66944 kali        20   0 11580 5004 3104 R   0.3   0.2   0:00.01 top
```

```

(kali㉿kali)-[~]
$ top|grep root
  1 root      20   0 102224 12156  9020 S   0.0   0.6 0:00.63 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
 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 0:00.19 ksoftir+
 15 root      20   0      0      0      0 I   0.0   0.0 0:01.28 rcu_pre+
 16 root      rt   0      0      0      0 S   0.0   0.0 0:00.01 migrati+
 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 migrati+

```

successivamente abbiamo creato una nuova cartella chiamata epicode lab dove al suo interno abbiamo creato il file esercizio:



sul terminale siamo entrati nella directory con l'editor di testo nano per modificarne il contenuto

```
File Actions Edit View Help
(kali@kali)-[~/Desktop/Epicode_lab]
$ nano -h
```

```
File Actions Edit View Help
GNU nano 7.2
hello world
```

sempre nella directory abbiamo inserito il comando cat che ci permette di leggere il contenuto del file da terminale:

```
(kali@kali)-[~/Desktop/Epicode_lab]
$ cat esercizio
hello world
```

mentre col comando `ls -la` abbiamo visto quali permessi erano disponibili per l'utente kali, il gruppo e gli altri utenti:

```
(kali@kali)-[~/Desktop/Epicode_lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 May  9 09:28 .
drwxr-xr-x 3 kali kali 4096 May  9 08:08 ..
-rw-r--r-- 1 kali kali  13 May  9 09:28 esercizio
```

col comando `chmod` siamo andati a modificare i permessi per il nostro file dove:

kali ha il permesso di leggerlo,modificarlo ed eseguirlo

il gruppo può leggerlo e modificarlo

mentre gli altri utenti possono solo leggerlo

```
(kali@kali)-[~]  
$ chmod u=rwx,g=rw,o=r esercizio
```

siamo andati così a creare un altro utente chiamandolo kali 2, successivamente abbiamo spostato il nostro file sulla directory "/",eseguendone un cattura e modificando i permessi di lettura per gli utenti del gruppo:

```
(kali@kali)-[~/Desktop/Epicode_lab]  
$ su kali2  
Password:  
$ whoami  
kali2  
$
```

```
(kali@kali)-[~/Desktop/Epicode_lab]  
$ sudo mv esercizio /  
  
(kali@kali)-[~/Desktop/Epicode_lab]  
$ cd /  
  
(kali@kali)-[/]  
$ cat esercizio  
hello world
```

```
(kali@kali)-[/]  
$ su kali2  
Password:  
$ cat esercizio  
cat: esercizio: Permission denied  
$
```

la risposta alla cattura dell'utente kali 2 ci ha risposto che non può leggerlo perchè col comando **chmod g-r** abbiamo tolto il permesso di lettura agli utenti del solito gruppo di kali.

Infine nel abbiamo riassegnato i permessi all'utente kali 2 e come si vede dall'immagine abbiamo eseguito una cattura dove riesce a leggere il contenuto del nostro file

```
(kali㉿kali)-[/  
$ su kali2  
Password:  
$ cat esercizio  
hello world  
$ █
```