

Consegna S2/L1

Controlliamo i processi attivi e analizziamo i processi PID, User e Command

```
kali@kali: ~  
File Actions Edit View Help  
  
top - 08:06:37 up 10 min, 1 user, load average: 0.03, 0.04, 0.02  
Tasks: 152 total, 1 running, 151 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 0.3 us, 0.5 sy, 0.0 ni, 98.7 id, 0.5 wa, 0.0 hi, 0.0 si, 0.0 st  
MiB Mem : 1967.1 total, 1001.7 free, 704.4 used, 409.4 buff/cache  
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 1262.6 avail Mem  
  
  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND  
  680 root        20   0 385672 120132 54812 S   0.7   6.0   0:05.85 Xorg  
  924 kali        20   0 217968   3200  2816 S   0.7   0.2   0:01.35 VBoxClient  
 1046 kali        20   0 277584 33264 19456 S   0.7   1.7   0:01.19 panel-13-cpugra  
  916 kali        20   0 217452   3200  2816 S   0.3   0.2   0:00.30 VBoxClient  
 1027 kali        20   0 548364 45472 34976 S   0.3   2.3   0:00.48 xfce4-panel  
 1048 kali        20   0 497408 28344 21028 S   0.3   1.4   0:01.16 panel-15-genmon  
 6087 kali        20   0 11716   5248  3200 R   0.3   0.3   0:00.01 top  
    1 root        20   0 20784  12396  9324 S   0.0   0.6   0:00.85 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
```

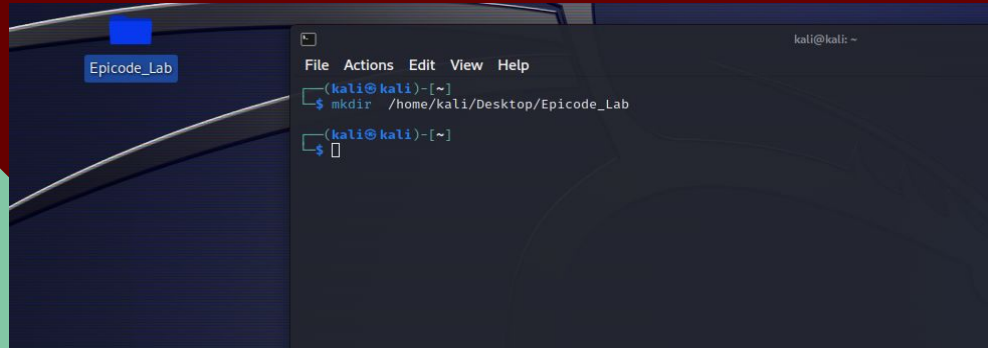
Il PID indica l'identificativo del processo, l'User chi lo sta eseguendo e Command è il comando eseguito.

Filtriamo i processi con root e kali

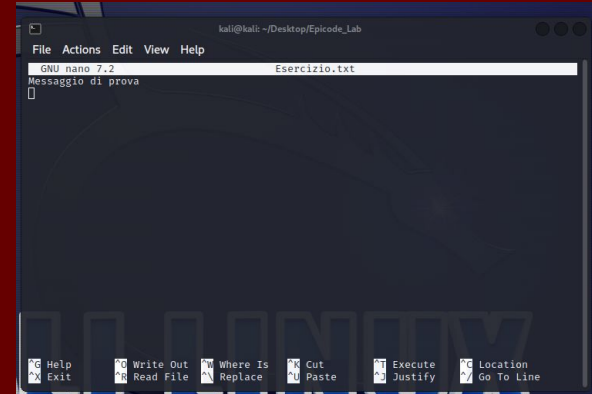
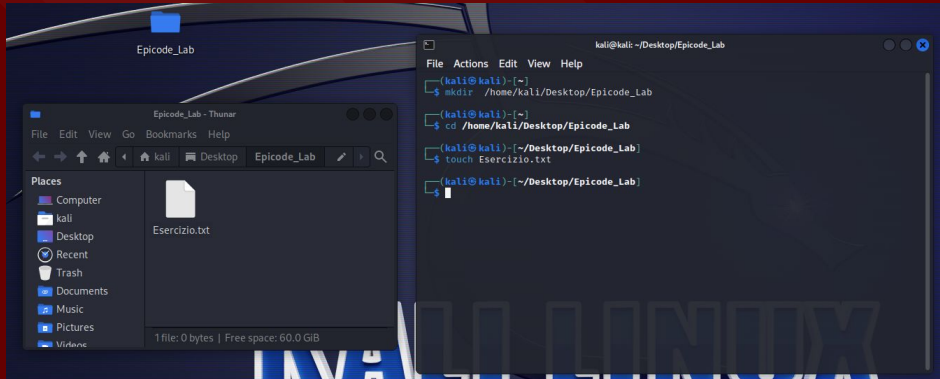
```
(kali㉿kali)-[~]  
$ top | grep root  
680 root      20    0   385672 120132  54812 S    6.2   6.0   0:06.79 Xorg  
1 root       20    0   20784   12396   9324 S    0.0   0.6   0:00.86 systemd  
2 root       20    0      0      0      0 S    0.0   0.0   0:00.00 kthreadd  
3 root       0 -20    0      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  
9 root       20    0      0      0      0 I    0.0   0.0   0:00.02 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   0:00.06 ksoftir+  
15 root       20    0      0      0      0 I    0.0   0.0   0:00.21 rcu_pre+  
16 root       rt    0      0      0      0 S    0.0   0.0   0:00.00 migrati+  
17 root      -51    0      0      0      0 S    0.0   0.0   0:00.00 idle_in+
```

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali㉿kali)-[~]  
$ top | grep kali  
7810 kali      20    0   11688   5376   3328 R    0.4   0.3   0:00.01 top  
978 kali       20    0   955012 106332  77604 S    0.8   5.3   0:02.50 xfwm4  
6051 kali      20    0   447236 104248  85260 S    0.8   5.2   0:00.80 qtermi+  
7810 kali      20    0   11688   5376   3328 R 100.0  0.3   0:00.02 top  
924 kali       20    0   217968 3200    2816 S    2.6   0.2   0:01.84 VBoxCli+  
7810 kali      20    0   11688   5376   3328 R    2.6   0.3   0:00.03 top  
924 kali       20    0   217968 3200    2816 S    3.1   0.2   0:01.85 VBoxCli+  
1046 kali      20    0   277584 33264   19456 S    3.1   1.7   0:01.58 panel-1+  
7810 kali      20    0   11688   5376   3328 R    2.1   0.3   0:00.04 top  
7810 kali      20    0   11688   5376   3328 R 100.0  0.3   0:00.05 top  
6051 kali      20    0   447236 104248  85260 S    1.1   5.2   0:00.81 qtermi+
```

Creiamo la cartella Epcode_Lab



In seguito creiamo il file .txt e lo modifichiamo



Utilizziamo il comando Cat per visualizzare il messaggio

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

Poi modifichiamo i permessi

```
(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 08:23 .
drwxr-xr-x 3 kali kali 4096 Nov 28 08:15 ..
-rw-r--r-- 1 kali kali 19 Nov 28 08:22 Esercizio.txt

(kali@kali)-[~/Desktop/Epicode_Lab]
$ sudo chmod 764 Esercizio.txt
[sudo] password for kali:

(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 08:23 .
drwxr-xr-x 3 kali kali 4096 Nov 28 08:15 ..
-rwxrw-r-- 1 kali kali 19 Nov 28 08:22 Esercizio.txt
```

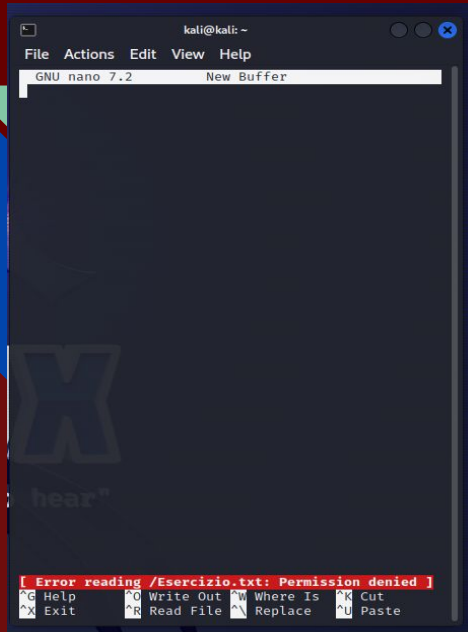
Ora creiamo un nuovo utente e
modifichiamo i privilegi

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

```
(kali@kali)-[~/Desktop/Epicode_Lab]  
$ sudo passwd gabri  
New password:  
Retype new password:  
passwd: password updated successfully
```

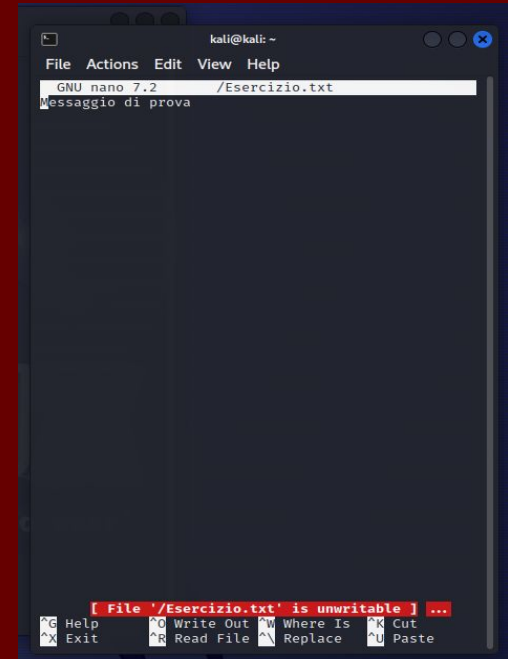
```
(kali@kali)-[~/Desktop/Epicode_Lab] ly used by process  
$ ls -la  
total 12  
drwxr-xr-x 2 kali kali 4096 Nov 28 09:10 .  
drwxr-xr-x 3 kali kali 4096 Nov 28 09:10 .. used by process  
-rwxrw---- 1 kali kali 19 Nov 28 08:22 Esercizio.txt
```

Ci spostiamo nel nuovo utente e proviamo a leggere il file.txt



A terminal window titled 'kali@kali: ~' showing the GNU nano 7.2 editor. The file being edited is '/Esercizio.txt'. The content of the file is 'Messaggio di prova'. At the bottom, a red error message reads: '[Error reading '/Esercizio.txt': Permission denied]'. Below the error message is a standard nano editor help menu with shortcuts for Help, Exit, Write Out, Read File, Where Is, Replace, Cut, and Paste.

Dopodichè cambiamo nuovamente i permessi e il risultato è il seguente



A terminal window titled 'kali@kali: ~' showing the GNU nano 7.2 editor. The file being edited is '/Esercizio.txt'. The content of the file is 'Messaggio di prova'. At the bottom, a red error message reads: '[File '/Esercizio.txt' is unwritable] ...'. Below the error message is a standard nano editor help menu with shortcuts for Help, Exit, Write Out, Read File, Where Is, Replace, Cut, and Paste.

A questo punto eliminiamo tutto tornando al punto di partenza

```
(kali㉿kali)-[/]  
$ sudo rm /Esercizio.txt  
  
(kali㉿kali)-[/]  
$ sudo rm -r /home/kali/Desktop/Epicode_Lab  
  
(kali㉿kali)-[/]  
$ sudo userdel -r gabri
```