

Report familiarizzazione con shell Linux

Per prima cosa controlliamo i processi attivi sulla macchina con il comando <<TOP>>

```
File Actions Edit View Help
top - 09:29:53 up 5:03, 1 user, load average: 0.05, 0.10, 0.14
Tasks: 157 total, 1 running, 156 sleeping, 0 stopped, 0 zombie
%Cpu(s): 2.3 us, 1.0 sy, 0.0 ni, 96.4 id, 0.0 wa, 0.0 hi, 0.3 si, 0.0 st
MiB Mem : 1981.3 total, 293.5 free, 1051.6 used, 636.1 buff/cache
MiB Swap: 1024.0 total, 934.6 free, 89.4 used. 752.6 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
 583 root        20   0 623128 302208 80816 S   1.6   14.9   2:57.97 Xorg
67500 kali       20   0 437920 108100 89068 S   1.3    5.3   0:01.66 qterminal
 872 kali       20   0 353152 34948 21856 S   1.0    1.7   3:48.36 panel-13-cpugra
 878 kali       20   0 359140 25236 20124 S   0.7    1.2   1:40.73 panel-15-genmon
75815 kali       20   0 10408  3876  3192 R   0.7    0.2   0:00.14 top
 778 kali       20   0 153000 3208  3052 S   0.3    0.2   0:51.95 VBoxClient
 828 kali       20   0 948544 101148 74388 S   0.3    5.0   1:24.30 xfwm4
 879 kali       20   0 667628 38956 31864 S   0.3    1.9   0:25.41 panel-16-pulsea
73667 root        20   0      0      0      0 I   0.3    0.0   0:00.34 kworker/0:1-events
   1 root        20   0 102412 12080  9012 S   0.0    0.6   0:01.67 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 netns
   7 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 kworker/0:0H-events_highpri
   9 root        0 -20      0      0      0 I   0.0    0.0   0:00.79 kworker/0:1H-kblockd
  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   0:01.64 ksoftirqd/0
  15 root        20   0      0      0      0 I   0.0    0.0   0:10.94 rcu_preempt
  16 root        rt   0      0      0      0 S   0.0    0.0   0:00.11 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   0:00.46 migration/1
  21 root        20   0      0      0      0 S   0.0    0.0   0:00.62 ksoftirqd/1
  23 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 kworker/1:0H-events_highpri
  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   0:00.02 khungtaskd
  30 root        20   0      0      0      0 S   0.0    0.0   0:00.00 oom_reaper
  31 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 writeback
  32 root        20   0      0      0      0 S   0.0    0.0   0:01.64 kcompactd0
  33 root        25   5      0      0      0 S   0.0    0.0   0:00.00 ksmd
  34 root        39  19      0      0      0 S   0.0    0.0   0:01.56 khugepaged
  35 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 kintegrityd
  36 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 kblockd
  37 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 blkcg_punt_bio
  38 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 tpm_dev_wq
  39 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 edac-poller
  40 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 devfreq_wq
  42 root        20   0      0      0      0 S   0.0    0.0   0:00.56 kswapd0
  49 root        0 -20      0      0      0 I   0.0    0.0   0:00.00 kthrotld
```

Qui possiamo vedere le colonne:PID che identifica il processo in esecuzione. USER: che identifica l'utente utilizzatore del processo. TIME e COMMAND che ci dà informazioni sul periodo di tempo in cui un determinato comando è in run.

Dopodichè filtriamo i risultati sia per root ed in secondo step con kali

```
File Actions Edit View Help
top - 09:54:54 up 5:28, 1 user, load average: 0.24, 0.12, 0.10
Task 583 root 20 0 629688 306348 84956 R 0.2 15.1 3:20.90
%CPU 15 root 3 us, 20 5 0 0.0 0.3 9.0 10.0 I 0.3 0.0 0:11.94 0.0 st
MiB Me1 root 1981 20 0 102412 12080 9012 S 0.0 0.6 0:01.69 cache
MiB Sw2 root 1024 20 0 930.6 0 0 0 S 0.0 0.0 0:00.01 Mem
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
14 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 COMMAND
585 root 0 -20 614.0 299.0 83.0 I 0.0 0.0 0:00.00 Xorg
67507 root 0 -20 427.0 105.0 87.0 I 0.0 0.0 0:00.00 qterminal
809 root 0 -20 344.0 34.0 21.0 I 0.0 0.0 0:00.84 panel-13-cpugra
11 root 20 0 149.0 3.0 3.0 I 0.0 0.0 0:00.00 VBoxClient
81712 root 20 0 427.0 105.0 87.0 I 0.0 0.0 0:00.00 qterminal
813 root 20 0 350.0 24.0 19.0 I 0.0 0.0 0:00.00 panel-15-genmon
19114 root 20 0 2911.0 325.0 148.0 S 0.0 0.0 0:01.76 firefox-esr
19212 root 20 0 2351.0 95.0 73.0 I 0.0 0.0 0:00.00 WebExtensions
75816 root rt 0 11.90 4.0 3.0 S 0.0 0.0 0:00.12 top
18 root 20 0 100.00 11.0 8.0 S 0.0 0.0 0:00.00 systemd
12 root 20 0 0.00 0.0 0.0 I 0.0 0.0 0:00.00 kthreadd
13 root 20 0 0.00 0.0 0.0 I 0.0 0.0 0:00.00 rcu_gp
14 root 20 0 0.00 0.0 0.0 S 0.0 0.0 0:01.75 rcu_par_gp
15 root 20 0 0.00 0.0 0.0 I 0.0 0.0 0:11.90 netns
16 root rt 0 0.00 0.0 0.0 S 0.0 0.0 0:00.12 kworker/0:0H-events_highpri
18 root 20 0 0.00 0.0 0.0 S 0.0 0.0 0:00.00 kworker/0:1H-events_highpri
19 root 20 0 0.00 0.0 0.0 S 0.0 0.0 0:00.00 mm_percpu_wq
20 root rt 0 0.00 0.0 0.0 S 0.0 0.0 0:00.48 rcu_tasks_kthread
21 root 20 0 0.00 0.0 0.0 S 0.0 0.0 0:00.68 rcu_tasks_rude_kthread
13 root 20 0 0.0m 0.0m 0.0m I 0.0 0.0 0:00.00 rcu_tasks_trace_kthread
14 root 20 0 0.0m 0.0m 0.0m S 0.0 0.0 0:01.76 ksoftirqd/0
15 root 20 0 0.0m 0.0m 0.0m I 0.0 0.0 0:11.93 rcu_preempt
16 root rt 0 0.0m 0.0m 0.0m S 0.0 0.0 0:00.12 migration/0
18 root 20 0 0.0m 0.0m 0.0m S 0.0 0.0 0:00.00 cpuhp/0
19 root 20 0 0.0m 0.0m 0.0m S 0.0 0.0 0:00.00 cpuhp/1
```

| File | Actions | Edit | View | Help |
|------------|---------|------|---------|---|
| 19261 kali | 20 | 0 | 2408316 | 98168 75284 S 0.3 4.8 0:13.64 WebExtensions |
| 872 kali | 20 | 0 | 353152 | 34948 21856 S 1.3 1.7 4:05.93 panel-13-cpugra |
| 67500 kali | 20 | 0 | 437920 | 108392 89192 S 1.0 5.3 0:20.11 qterminal |
| 82374 kali | 20 | 0 | 437788 | 107856 89008 S 1.0 5.3 0:00.45 qterminal |
| 878 kali | 20 | 0 | 359140 | 25236 20124 S 0.7 1.2 1:49.48 panel-15-genmon |
| 828 kali | 20 | 0 | 948544 | 101152 74388 S 0.3 5.0 1:31.38 xfwm4 |
| 879 kali | 20 | 0 | 667628 | 39196 31924 S 0.3 1.9 0:27.44 panel-16-pulsea |
| 19147 kali | 20 | 0 | 2981788 | 334216 152360 S 0.3 16.5 1:19.71 firefox-esr |
| 75815 kali | 20 | 0 | 12172 | 4784 3940 S 0.3 0.2 0:05.94 top |
| 82470 kali | 20 | 0 | 10408 | 3920 3236 R 0.3 0.2 0:00.11 top |
| 67500 kali | 20 | 0 | 437920 | 108392 89192 S 1.3 5.3 0:20.15 qterminal |
| 872 kali | 20 | 0 | 353152 | 34948 21856 S 1.0 1.7 4:05.96 panel-13-cpugra |
| 75815 kali | 20 | 0 | 12172 | 4784 3940 S 0.6 0.2 0:05.96 top |
| 82374 kali | 20 | 0 | 437788 | 107856 89008 S 0.6 5.3 0:00.47 qterminal |
| 778 kali | 20 | 0 | 153000 | 3208 3052 S 0.3 0.2 0:55.63 VBoxClient |
| 828 kali | 20 | 0 | 948544 | 101152 74388 S 0.3 5.0 1:31.39 xfwm4 |
| 878 kali | 20 | 0 | 359140 | 25236 20124 S 0.3 1.2 1:49.49 panel-15-genmon |
| 82470 kali | 20 | 0 | 10408 | 3920 3236 R 0.3 0.2 0:00.12 top |
| 872 kali | 20 | 0 | 353152 | 34948 21856 S 1.7 1.7 4:06.01 panel-13-cpugra |
| 67500 kali | 20 | 0 | 437920 | 108392 89192 S 1.0 5.3 0:20.18 qterminal |
| 878 kali | 20 | 0 | 359140 | 25236 20124 S 0.7 1.2 1:49.51 panel-15-genmon |
| 82374 kali | 20 | 0 | 437788 | 107856 89008 S 0.7 5.3 0:00.49 qterminal |
| 82470 kali | 20 | 0 | 10408 | 3920 3236 R 0.7 0.2 0:00.14 top |
| 696 kali | 20 | 0 | 10356 | 5276 4164 S 0.3 0.3 0:08.05 dbus-daemon |
| 828 kali | 20 | 0 | 948544 | 101152 74388 S 0.3 5.0 1:31.40 xfwm4 |
| 75815 kali | 20 | 0 | 12172 | 4784 3940 S 0.3 0.2 0:05.97 top |
| 82374 kali | 20 | 0 | 437788 | 107856 89008 S 1.6 5.3 0:00.54 qterminal |
| 872 kali | 20 | 0 | 353152 | 34948 21856 S 1.0 1.7 4:06.04 panel-13-cpugra |
| 67500 kali | 20 | 0 | 437920 | 108392 89192 S 1.0 5.3 0:20.21 qterminal |
| 879 kali | 20 | 0 | 667628 | 39196 31924 S 0.7 1.9 0:27.46 panel-16-pulsea |
| 778 kali | 20 | 0 | 153000 | 3208 3052 S 0.3 0.2 0:55.64 VBoxClient |
| 828 kali | 20 | 0 | 948544 | 101152 74388 S 0.3 5.0 1:31.41 xfwm4 |
| 870 kali | 20 | 0 | 585944 | 104420 40124 S 0.3 5.1 0:03.33 xfdesktop |
| 878 kali | 20 | 0 | 359140 | 25236 20124 S 0.3 1.2 1:49.52 panel-15-genmon |
| 19147 kali | 20 | 0 | 2981788 | 333924 152360 S 0.3 16.5 1:19.72 firefox-esr |
| 82470 kali | 20 | 0 | 10408 | 3920 3236 R 0.3 0.2 0:00.15 top |
| 82374 kali | 20 | 0 | 437788 | 108200 89132 S 1.3 5.3 0:00.58 qterminal |
| 828 kali | 20 | 0 | 948544 | 101152 74388 S 1.0 5.0 1:31.44 xfwm4 |
| 872 kali | 20 | 0 | 353152 | 34948 21856 S 1.0 1.7 4:06.07 panel-13-cpugra |
| 67500 kali | 20 | 0 | 437920 | 108392 89192 S 1.0 5.3 0:20.24 qterminal |
| 878 kali | 20 | 0 | 359140 | 25236 20124 S 0.6 1.2 1:49.54 panel-15-genmon |
| 75815 kali | 20 | 0 | 12172 | 4784 3940 S 0.6 0.2 0:05.99 top |
| 778 kali | 20 | 0 | 153000 | 3208 3052 S 0.3 0.2 0:55.65 VBoxClient |
| 82470 kali | 20 | 0 | 10408 | 3920 3236 R 0.3 0.2 0:00.16 top |
| 82374 kali | 20 | 0 | 437788 | 108200 89132 S 1.6 5.3 0:00.63 qterminal |
| 872 kali | 20 | 0 | 353152 | 34948 21856 S 1.3 1.7 4:06.11 panel-13-cpugra |
| 67500 kali | 20 | 0 | 437920 | 108392 89192 S 1.0 5.3 0:20.27 qterminal |
| 828 kali | 20 | 0 | 948544 | 101152 74388 S 0.7 5.0 1:31.46 xfwm4 |
| 778 kali | 20 | 0 | 153000 | 3208 3052 S 0.3 0.2 0:55.66 VBoxClient |
| 878 kali | 20 | 0 | 359140 | 25236 20124 S 0.3 1.2 1:49.55 panel-15-genmon |
| 82470 kali | 20 | 0 | 10408 | 3920 3236 R 0.3 0.2 0:00.17 top |

Adesso creiamo una nuova directory denominandola <<epicode_lab>> utilizzando il comando <<mkdir /home/kali/Desktop/epicode_lab

Quindi ci possiamo spostare nella directory appena creata e creiamo il file <<esercizio.txt>>, modificando il file con editor di

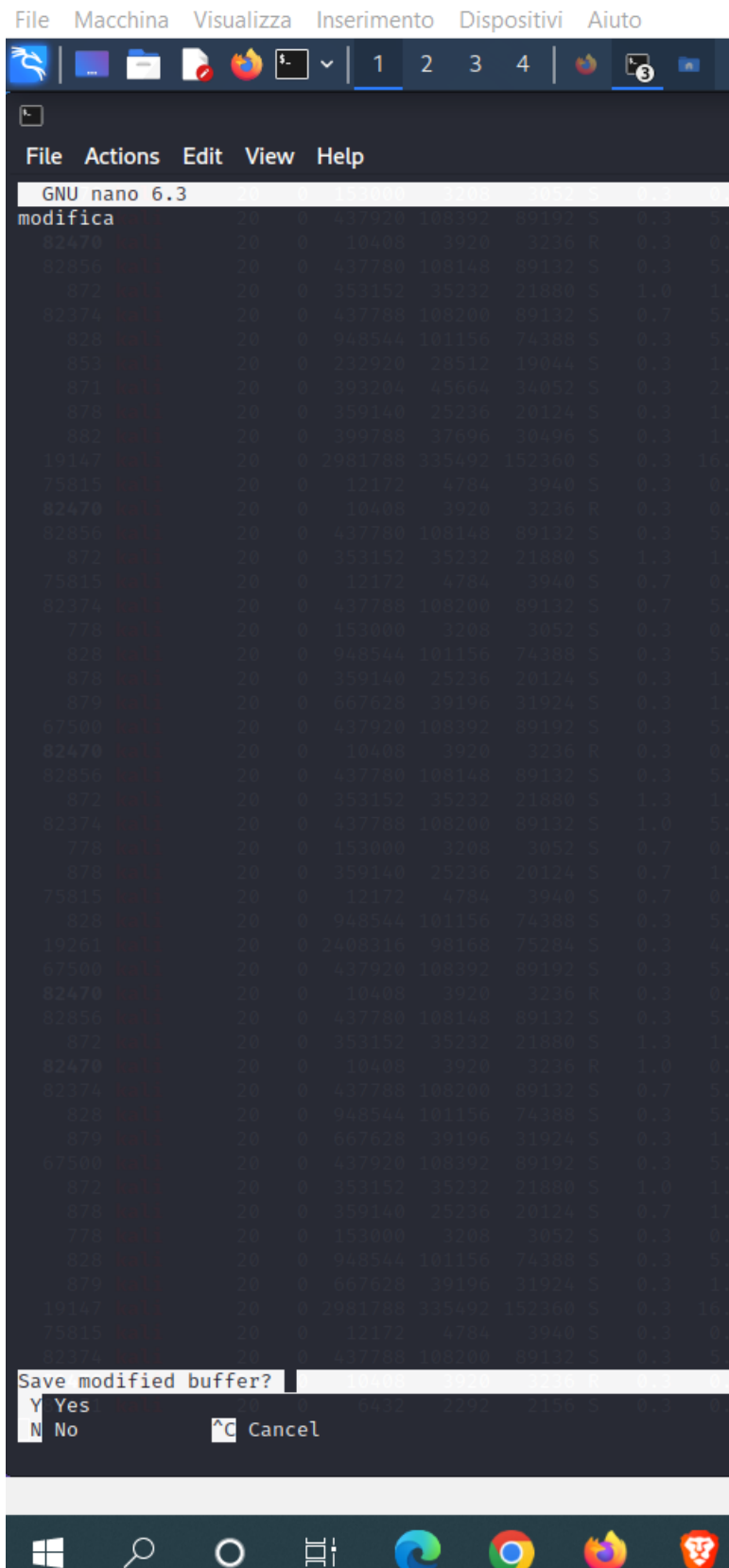
testo <<nano>> “modifica”

```
(kali㉿kali)-[~] Desktop/epicode_lab/esercizio.txt
$ cd epicode_lab Desktop/epicode_lab/esercizio.txt: No such file or directory

(kali㉿kali)-[~/epicode_lab]
$ nano esercizio.txt
cat: esercizio.txt: No such file or directory

(kali㉿kali)-[~/epicode_lab]
$ cat esercizio.txt
modifica file.txt
cat: file.txt: No such file or directory

(kali㉿kali)-[~/epicode_lab]
$
```



Come da immagine ho modificato il file scrivendo “modifica” (salvando la modifica).

A questo punto controlliamo i permessi del file.

```

cat: file.txt: No such file or directory
(kali㉿kali)-[~/epicode_lab]
$ ls -la
total 12
drwxr-xr-x  2 kali kali 4096 Nov  2 10:37 .
drwxr-xr-x 18 kali kali 4096 Nov  2 10:22 ..
-rw-r--r--  1 kali kali  10 Nov  2 10:37 esercizio.txt

(kali㉿kali)-[~/epicode_lab]
$

```

Ora cambiamo i permessi come richiesto da esercizio

```

(kali㉿kali)-[~/epicode_lab]
$ chmod u=rwx esercizio.txt

(kali㉿kali)-[~/epicode_lab]
$

passwd: password updated successfully
(kali㉿kali)-[~/epicode_lab]
$ chmod o-r esercizio.txt

(kali㉿kali)-[~/epicode_lab]
$

```

Creiamo quindi un nuovo utente, cambiando privilegi del file in modo che altri utenti non possano leggerlo

```

(kali㉿kali)-[~/epicode_lab]
$ sudo useradd violet
[sudo] password for kali:

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

(kali㉿kali)-[~/epicode_lab]
$ sudo passwd violet
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~/epicode_lab]
$

```

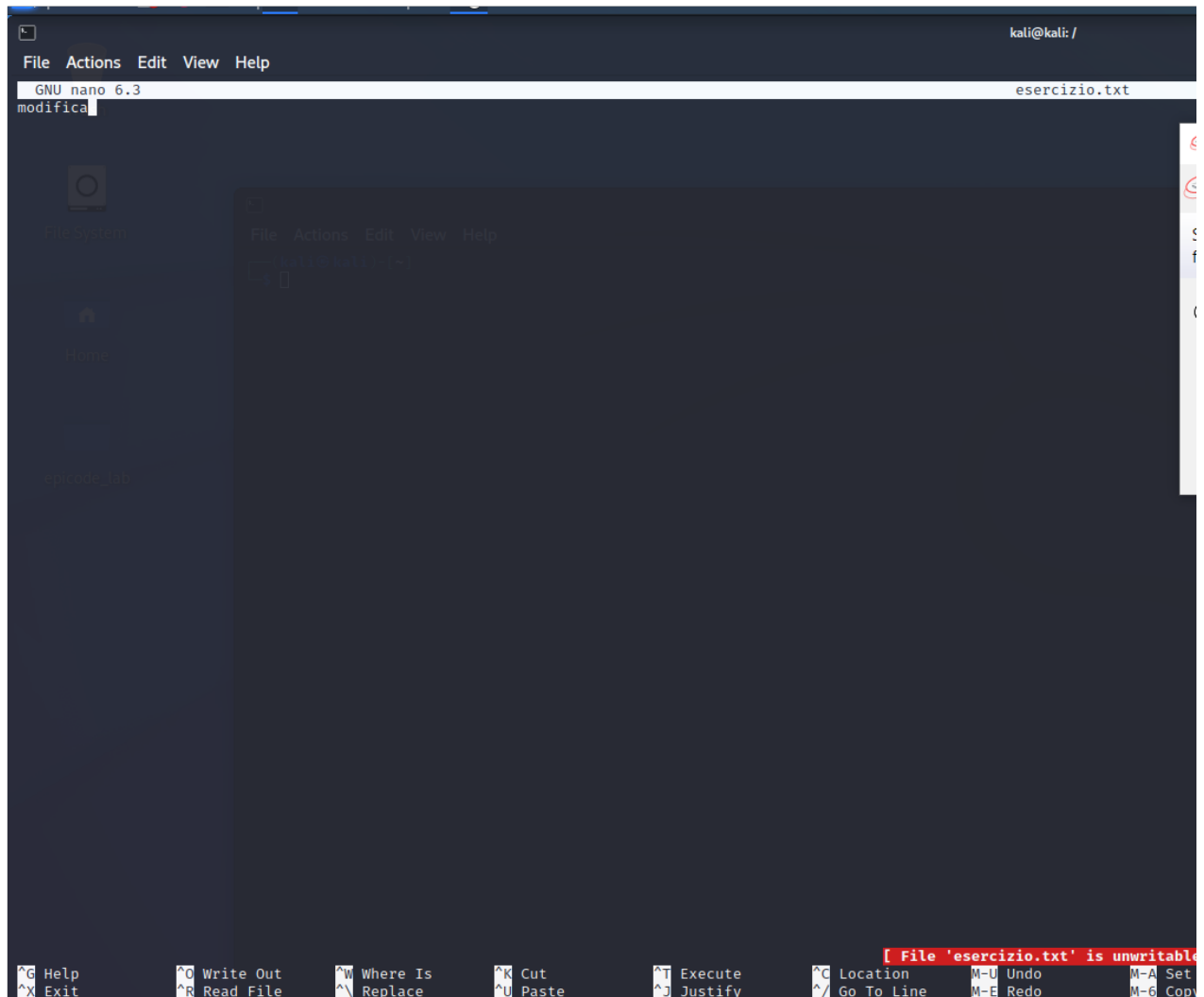
E spostiamo il file in directory/root con il comando <<sudo mv esercizio.txt (inserendo pass Kali), cambiando utente tramite comando <<su>> quindi in questo caso << su violet>>

```

(kali㉿kali)-[~/epicode_lab]
$ su violet
Password:
$

```

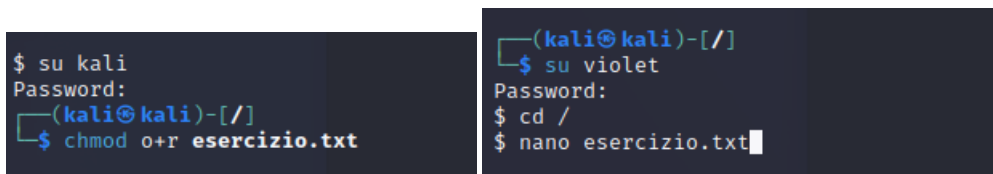
Provando a leggere il file, riceveremo un errore del genere:



```
kali@kali: /
File Actions Edit View Help
GNU nano 6.3 esercizio.txt
modifica

[ File 'esercizio.txt' is unwritable ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo     M-6 Copy
```

Adesso, come richiesto cambiamo permessi al nuovo utente



```
$ su kali
Password:
(kali@kali)-[/]
$ chmod o+r esercizio.txt

(kali@kali)-[/]
$ su violet
Password:
$ cd /
$ nano esercizio.txt
```

Una volta reso possibile ogni privilegio all'utente, procediamo alla

```
password:
(kali㉿kali)-[/]
$ sudo rm esercizio.txt
[sudo] password for kali:

(kali㉿kali)-[/]
$ cd /home/kali/Desktop

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

cancellazione di directory e file

dell'utente con il comando <<sudo userdel violet>>

ed infine