

Esercizio S2L2

Controlliamo i processi attivi
su kali con il comando “top”

PID (Process IDentification):
Il PID è un numero intero univoco
assegnato a ciascun processo
in esecuzione nel sistema operativo.

USER:

Indica l'utente che ha avviato il processo. Ogni processo è associato a un utente che ne è il proprietario.

COMMAND:

Rappresenta il comando o il programma
eseguito dal processo.
Indica il nome dell'eseguibile o del comando che ha generato il processo.

```
File Actions Edit View Help
top - 05:59:05 up 10 min, 1 user, load average: 0.27, 0.90, 0.82
Tasks: 193 total, 2 running, 191 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.8 us, 0.3 sy, 0.0 ni, 98.8 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
MiB Mem : 5924.3 total, 4903.7 free, 813.7 used, 438.1 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 5110.6 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM    TIME+  COMMAND
  942 root        20   0 399720 132584 58992 S   4.0   2.2   0:08.77 Xorg
 1261 kali        20   0 217968   2944  2688 S   0.7   0.0   0:01.43 VBoxClient
 1316 kali        20   0 1610604 106016 77380 S   0.7   1.7   0:01.41 xfwm4
 1396 kali        20   0 469516  42720 34464 S   0.7   0.7   0:00.35 panel-16-pulsea
    15 root         20   0         0         0     0 R   0.3   0.0   0:01.49 rcu_preempt
 1374 kali        20   0 474632  44896 34632 S   0.3   0.7   0:00.63 xfce4-panel
 1421 kali        20   0 452368 108192 88912 S   0.3   1.8   0:02.10 qterminal
     1 root         20   0  20824  12004  9060 S   0.0   0.2   0:11.82 systemd
     2 root         20   0         0         0     0 S   0.0   0.0   0:00.61 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   0:00.35 ksoftirqd/0
    16 root          rt   0         0         0     0 S   0.0   0.0   0:00.21 migration/0
    17 root        -51   0         0         0     0 S   0.0   0.0   0:00.00 idle_inject/0
    19 root         20   0         0         0     0 S   0.0   0.0   0:00.01 cpuhp/0
    20 root         20   0         0         0     0 S   0.0   0.0   0:00.00 cpuhp/1
    21 root        -51   0         0         0     0 S   0.0   0.0   0:00.00 idle_inject/1
    22 root          rt   0         0         0     0 S   0.0   0.0   0:02.18 migration/1
    23 root         20   0         0         0     0 S   0.0   0.0   0:03.44 ksoftirqd/1
    24 root         20   0         0         0     0 I   0.0   0.0   0:01.05 kworker/1:0-events
    25 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   0:00.05 cpuhp/2
    27 root        -51   0         0         0     0 S   0.0   0.0   0:00.00 idle_inject/2
    28 root          rt   0         0         0     0 S   0.0   0.0   0:02.14 migration/2
    29 root         20   0         0         0     0 S   0.0   0.0   0:00.47 ksoftirqd/2
    30 root         20   0         0         0     0 I   0.0   0.0   0:01.21 kworker/2:0-events
    31 root          0 -20         0         0     0 I   0.0   0.0   0:00.00 kworker/2:0H-events_highpri
    32 root         20   0         0         0     0 S   0.0   0.0   0:00.04 cpuhp/3
    33 root        -51   0         0         0     0 S   0.0   0.0   0:00.00 idle_inject/3
    34 root          rt   0         0         0     0 S   0.0   0.0   0:02.21 migration/3
    35 root         20   0         0         0     0 S   0.0   0.0   0:00.51 ksoftirqd/3
    38 root         20   0         0         0     0 S   0.0   0.0   0:00.00 cpuhp/4
    39 root        -51   0         0         0     0 S   0.0   0.0   0:00.00 idle_inject/4
    40 root          rt   0         0         0     0 S   0.0   0.0   0:02.14 migration/4
    41 root         20   0         0         0     0 S   0.0   0.0   0:00.35 ksoftirqd/4
    43 root          0 -20         0         0     0 I   0.0   0.0   0:00.00 kworker/4:0H-events_highpri
    44 root         20   0         0         0     0 S   0.0   0.0   0:00.00 cpuhp/5
    45 root        -51   0         0         0     0 S   0.0   0.0   0:00.00 idle_inject/5
    46 root          rt   0         0         0     0 S   0.0   0.0   0:02.20 migration/5
    47 root         20   0         0         0     0 S   0.0   0.0   0:02.03 ksoftirqd/5
    49 root          0 -20         0         0     0 I   0.0   0.0   0:00.00 kworker/5:0H-events_highpri
    51 root         20   0         0         0     0 I   0.0   0.0   0:01.08 kworker/u12:1-flush-8:0
    52 root         20   0         0         0     0 I   0.0   0.0   0:01.17 kworker/u12:2-flush-8:0
    55 root         20   0         0         0     0 I   0.0   0.0   0:00.53 kworker/u12:5-writeback
    56 root         20   0         0         0     0 S   0.0   0.0   0:00.23 kdevtmpfs
    57 root          0 -20         0         0     0 I   0.0   0.0   0:00.00 inet_frag_wq
```



```
(kali@kali)-[~]
$ top | grep root
 1 root      20   0   20824   12004   9060 S   0.0   0.2   0:12.43 systemd
 2 root      20   0       0       0       0 S   0.0   0.0   0:00.62 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   0:00.62 ksoftir+
15 root      20   0       0       0       0 I   0.0   0.0   0:05.51 rcu_pre+
16 root      rt   0       0       0       0 S   0.0   0.0   0:00.37 migrati+
17 root      -51  0       0       0       0 S   0.0   0.0   0:00.00 idle_in+
19 root      20   0       0       0       0 S   0.0   0.0   0:00.01 cpuhp/0
```

```
(kali@kali)-[~]
$ top | grep kali
1253 kali      20   0   217452   3200   2688 S   0.3   0.1   0:03.72 VBoxCli+
1261 kali      20   0   283504   3072   2688 S   0.3   0.1   0:21.23 VBoxCli+
1363 kali      20   0   305088   29608   20068 S   0.3   0.5   0:01.03 xfsetti+
1393 kali      20   0   438404   42980   22400 S   0.3   0.7   0:11.14 panel-1+
22539 kali      20   0   11688    5248   3200 R  100.0   0.1   0:00.01 top
```

```
(kali@kali)-[~]
$
```

Possiamo filtrare i risultati del comando top usando il comando grep seguito da pipe « | »

Prima i programmi in esecuzione per l'utente «root» e poi per mostrare solamente i processi in esecuzione dall'utente kali.

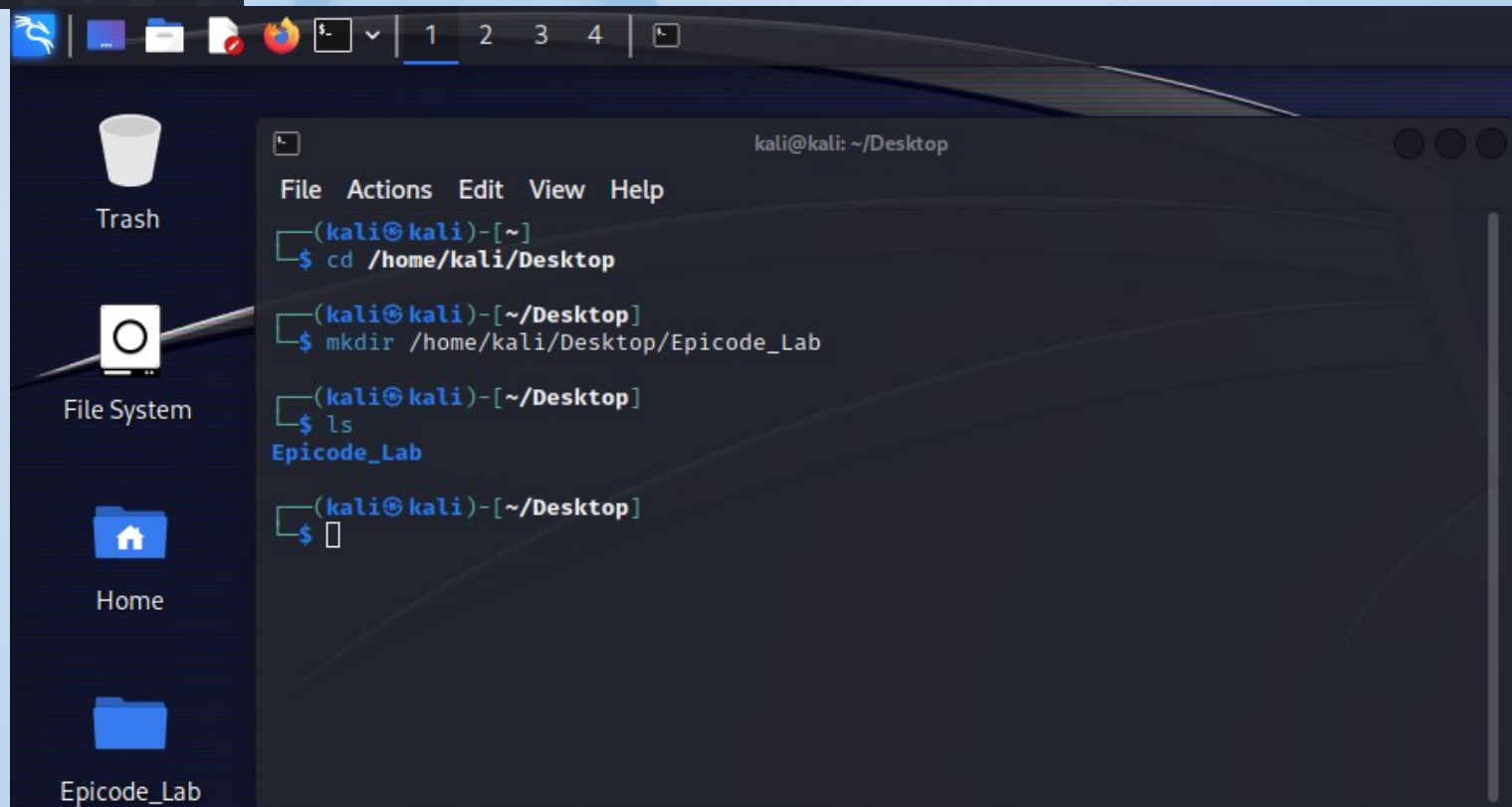
Ora possiamo creare una nuova directory chiamata

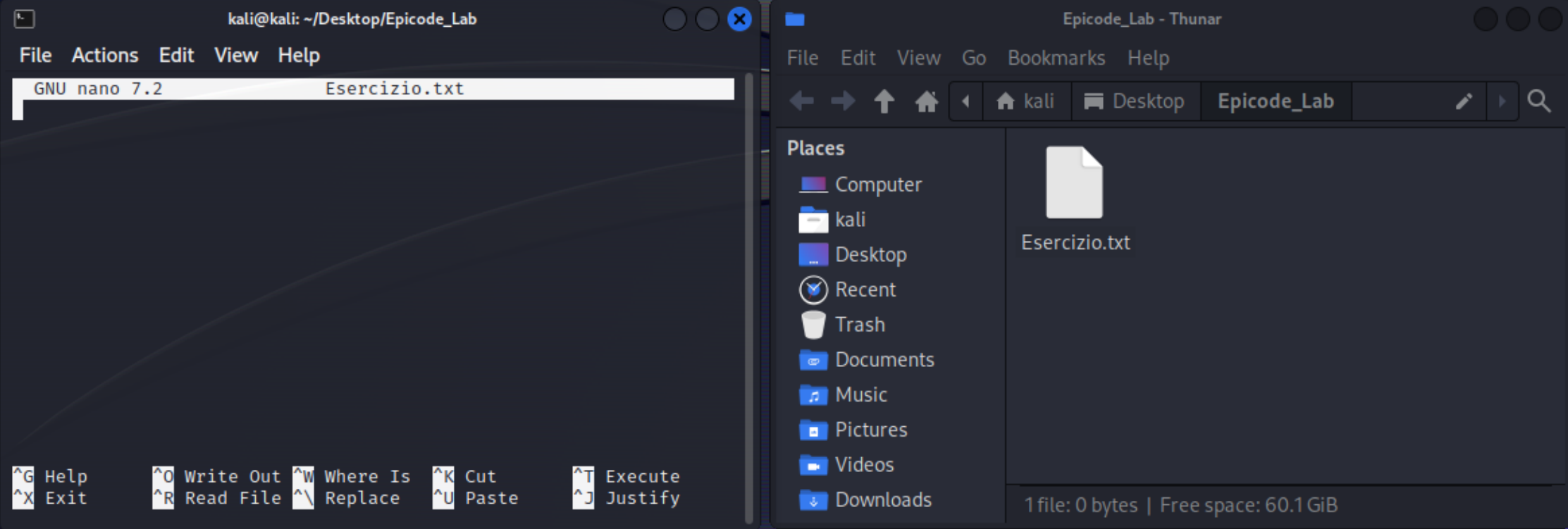
«Epicode_Lab»

nella seguente

directory /home/kali/Desktop

che appare su Desktop

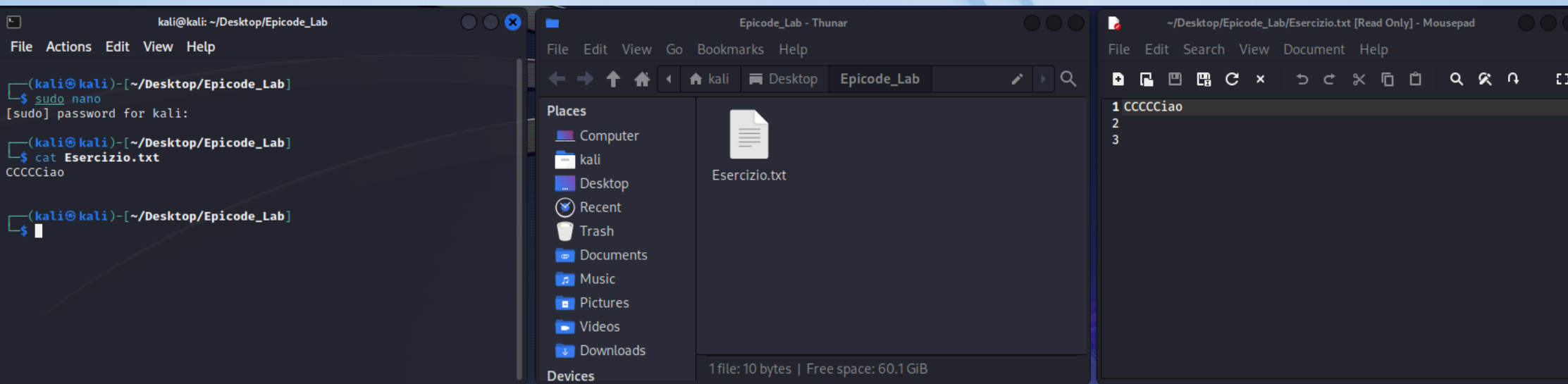




Qui ci spostiamo nella directory appena creata per creare il file «Esercizio.txt»

Modificare il file con l'editor di testo «nano», in seguito appare nella cartella.

Utilizziamo il comando «cat» per leggere a schermo il file.txt appena modificato




```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 09:21 .
drwxr-xr-x 3 kali kali 4096 Nov 28 07:54 ..
-rw-r--r-- 1 root root  10 Nov 28 08:50 Esercizio.txt
```

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

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

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 09:21 .
drwxr-xr-x 3 kali kali 4096 Nov 28 07:54 ..
-rwxrw-r-- 1 root root  10 Nov 28 08:50 Esercizio.txt
```

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

Utilizzando il comando `ls -la` controlliamo i permessi del file.

Ora dobbiamo modificare i privilegi del file in modo tale che l'utente corrente abbia tutti i privilegi (r,w,x) il gruppo (r,w) gli altri utenti solo lettura (r)

Dobbiamo creare un nuovo utente utilizzando il comando «`useradd`» lo chiamiamo Franco.

Utilizziamo invece il comando «`passwd`» seguita dal nome dell'utente per assegnare una password.

```
(kali㉿kali)-[~]
$ sudo useradd Franco
[sudo] password for kali:
```

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

```
(kali㉿kali)-[~]
$
```

Cambiamo di nuovo i privilegi
del file **Esercizio.txt**
creato in precedenza in modo
tale che «altri utenti»
non siano abilitati alla lettura

File Actions Edit View Help

```
(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 09:21 .
drwxr-xr-x 3 kali kali 4096 Nov 28 07:54 ..
-rwxrw-r-- 1 root root  10 Nov 28 08:50 Esercizio.txt

(kali@kali)-[~/Desktop/Epicode_Lab]
$ sudo chmod o-r Esercizio.txt

(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 09:21 .
drwxr-xr-x 3 kali kali 4096 Nov 28 07:54 ..
-rwxrw--- 1 root root  10 Nov 28 08:50 Esercizio.txt

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

```
kali@kali: ~/Desktop/Epicode_Lab
File Actions Edit View Help

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

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

Spostiamo il file nella directory di root (/)
Utilizzando il comando “mv”
e controlliamo con il comando “ls”
la presenza del file.


```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 Esercizio.txt

[ Path '.: Permission denied ] ...
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^_ Justify    ^_/ Go To Line
```

```
kali@kali: ~/Desktop/Epicode_Lab
File Actions Edit View Help

(kali@kali)-[~]
$ cd /home/kali/Desktop/Epicode_Lab

(kali@kali)-[~/Desktop/Epicode_Lab]
$ la -la
total 8
drwxr-xr-x 2 kali kali 4096 Nov 28 12:05 .
drwxr-xr-x 3 kali kali 4096 Nov 28 11:45 ..
-rw-r--r-- 1 root root   0 Nov 28 12:00 Esercizio.txt

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

```
kali@kali: ~
File Actions Edit View Help
$ cat Esercizio.txt
cat: Esercizio.txt: Permission denied
$

(kali@kali)-[/]
$ sudo chmod o+r Esercizio.txt

(kali@kali)-[/]
$ ls -la
total 1048660
drwxr-xr-x 18 root root      4096 Nov 28 10:05 .
drwxr-xr-x 18 root root      4096 Nov 28 10:05 ..
lrwxrwxrwx  1 root root         7 Aug 21 14:50 bin -> usr/bin
drwxr-xr-x  3 root root      4096 Aug 21 16:02 boot
drwxr-xr-x 17 root root     3380 Nov 28 07:24 dev
-rwxr--r--  1 root root      10 Nov 28 08:50 Esercizio.txt
```

Cambiamo utente con il comando «su» e proviamo ad aprire in lettura il file.txt creato in precedenza con il comando nano e comando cat. In entrambi i casi l'accesso alla lettura del file viene negata.

```
kali@kali: /
File Actions Edit View Help

(kali@kali)-[/]
$ su Franco
Password:
$ cat Esercizio.txt
CCCCCiao

$
```

Torniamo di nuovo per modificare i permessi del file per consentire la lettura al nuovo utente, Poi riproviamo ad aprire il file e leggiamo con successo il suo contenuto.

Per ultima cosa rimuoviamo prima il file txt

Poi procediamo ad eliminare
la cartella Epicode_Lab

Infine eliminiamo l'utente Franco
tornando allo stato iniziale.

The End

```
kali@kali: /  
File Actions Edit View Help  
  
(kali@kali)-[~/Desktop/Epicode_Lab]  
$ sudo rm /Esercizio.txt  
  
(kali@kali)-[~/Desktop/Epicode_Lab]  
$ cd /home/kali/Desktop  
  
(kali@kali)-[~/Desktop]  
  
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo rm -r /home/kali/Desktop/Epicode_Lab  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$  
  
kali@kali: ~/Desktop  
File Actions Edit View Help  
  
(kali@kali)-[~/Desktop]  
$ sudo deluser Franco  
info: Removing crontab ...  
info: Removing user `Franco' ...  
  
(kali@kali)-[~/Desktop]  
$ sudo deluser Franco  
fatal: The user `Franco' does not exist.  
  
(kali@kali)-[~/Desktop]  
$
```