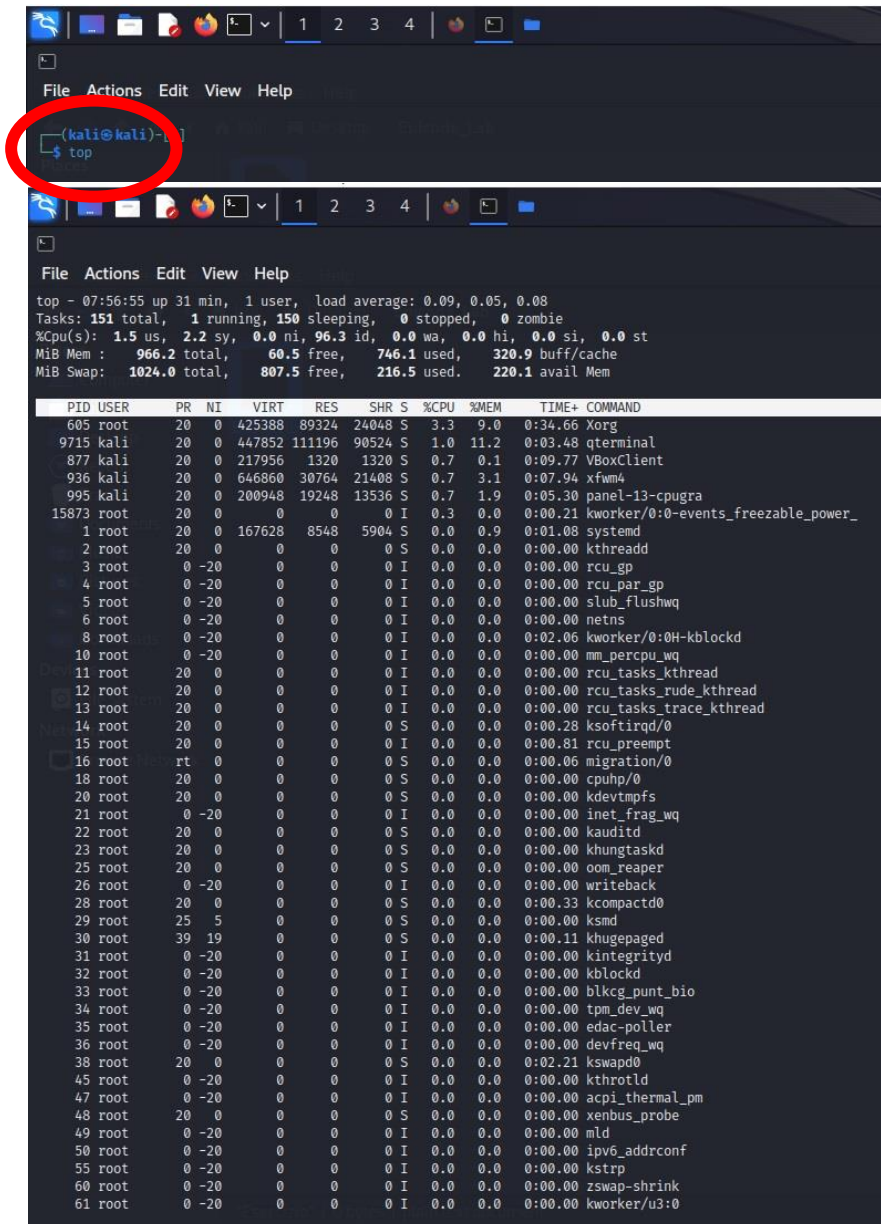


ESERCIZIO 09/05/2023

- 1) Utilizzando il comando TOP ho controllato i processi attivi sulla macchina Linux, notando che ad ogni processo corrisponde un PID (identificativo del processo attivo, identificato da un numero), un user, identificativo dell'utente che sta svolgendo il processo, nel mio caso ci sono root e kali) e un command (che specifica l'azione che avviene nel terminale).



```
(kali@kali)-  
$ top  
  
top - 07:56:55 up 31 min, 1 user, load average: 0.09, 0.05, 0.08  
Tasks: 151 total, 1 running, 150 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 1.5 us, 2.2 sy, 0.0 ni, 96.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
MiB Mem : 966.2 total, 60.5 free, 746.1 used, 320.9 buff/cache  
MiB Swap: 1024.0 total, 807.5 free, 216.5 used, 220.1 avail Mem  
  
  PID USER   PR    NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND  
  605 root    20     0 425388 89324 24048 S   3.3   9.0   0:34.66 Xorg  
 9715 kali    20     0 447852 111196 90524 S   1.0  11.2   0:03.48 qterminal  
   877 kali    20     0 217956  1320  1320 S   0.7   0.1   0:09.77 VBoxClient  
   936 kali    20     0 646860 30764 21408 S   0.7   3.1   0:07.94 xfwm4  
   995 kali    20     0 200948 19248 13536 S   0.7   1.9   0:05.30 panel-13-cpugra  
15873 root    20     0      0      0      0 I   0.3   0.0   0:00.21 kworker/0:0-events_freezable_power_  
     1 root    20     0 167628  8548  5904 S   0.0   0.9   0:01.08 systemd  
     2 root    20     0      0      0      0 S   0.0   0.0   0:00.00 kthreadd  
     3 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 rcu_gp  
     4 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp  
     5 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 slub_flushwq  
     6 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 netns  
     8 root     0 -20     0      0      0      0 I   0.0   0.0   0:02.06 kworker/0:0H-kblockd  
    10 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq  
    11 root    20     0      0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread  
    12 root    20     0      0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread  
    13 root    20     0      0      0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread  
    14 root    20     0      0      0      0      0 S   0.0   0.0   0:00.28 ksoftirqd/0  
    15 root    20     0      0      0      0      0 I   0.0   0.0   0:00.81 rcu_preempt  
    16 root    rt     0      0      0      0      0 S   0.0   0.0   0:00.06 migration/0  
    18 root    20     0      0      0      0      0 S   0.0   0.0   0:00.00 cpuhp/0  
    20 root    20     0      0      0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs  
    21 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq  
    22 root    20     0      0      0      0      0 S   0.0   0.0   0:00.00 kauditd  
    23 root    20     0      0      0      0      0 S   0.0   0.0   0:00.00 khungtaskd  
    25 root    20     0      0      0      0      0 S   0.0   0.0   0:00.00 oom_reaper  
    26 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 writeback  
    28 root    20     0      0      0      0      0 S   0.0   0.0   0:00.33 kcompactd0  
    29 root    25     5      0      0      0      0 S   0.0   0.0   0:00.00 ksm  
    30 root    39    19      0      0      0      0 S   0.0   0.0   0:00.11 khugepaged  
    31 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 kintegrityd  
    32 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 kblockd  
    33 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 blkcg_punt_bio  
    34 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 tpm_dev_wq  
    35 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 edac-poller  
    36 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 devfreq_wq  
    38 root    20     0      0      0      0      0 S   0.0   0.0   0:02.21 kswapd0  
    45 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 kthrotld  
    47 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 acpi_thermal_pm  
    48 root    20     0      0      0      0      0 S   0.0   0.0   0:00.00 xenbus_probe  
    49 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 mld  
    50 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 ipv6_addrconf  
    55 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 kstrp  
    60 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 zswap-shrink  
    61 root     0 -20     0      0      0      0 I   0.0   0.0   0:00.00 kworker/u3:0
```

2) Mediante il comando `top|grep root` ho isolato tutti i processi attivi che lo user root sta svolgendo.

```
(kali@kali)-[~]
$ top|grep root
605 root      0 0 425388 89324 24048 S 6.7 9.0 0:35.08 Xorg
      root      0 0 167628 8548 5904 S 0.0 0.9 0:01.08 systemd
      root      0 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
      root      0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
      root      0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par+
      root      0 -20 0 0 0 I 0.0 0.0 0:00.00 slub_fl+
      root      0 -20 0 0 0 I 0.0 0.0 0:00.00 netns
      root      0 -20 0 0 0 I 0.0 0.0 0:02.06 kworker+
      root      0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_perc+
      root      0 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tas+
      root      0 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tas+
      root      0 0 0 0 0 I 0.0 0.0 0:00.00 rcu_tas+
      root      0 0 0 0 0 S 0.0 0.0 0:00.29 ksoftir+
      root      0 0 0 0 0 I 0.0 0.0 0:00.82 rcu_pre+
      root      0 0 0 0 0 S 0.0 0.0 0:00.06 migrati+
      root      0 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/0
```

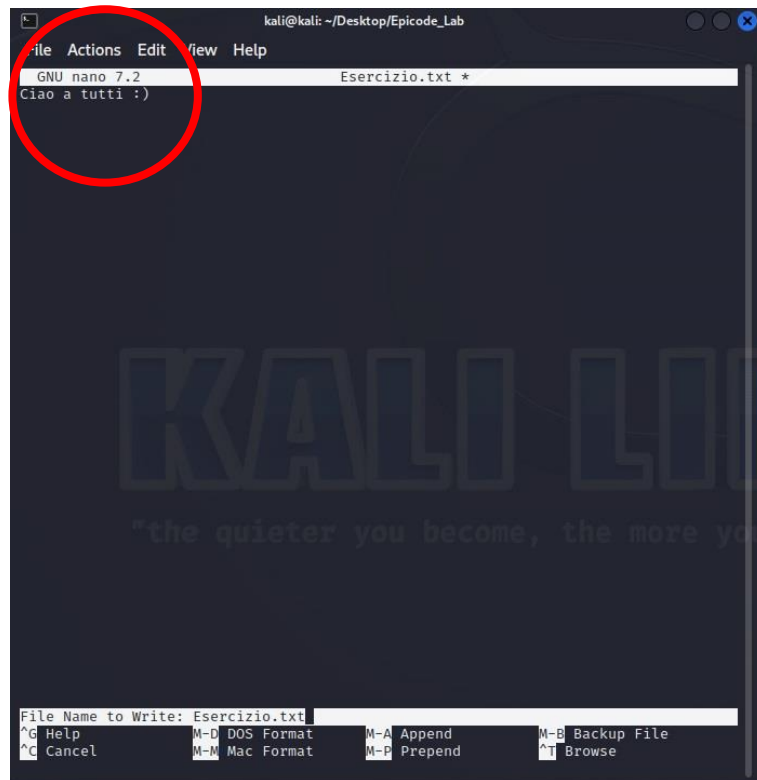
2) Mediante il comando `top|grep kali` ho isolato tutti i processi attivi che lo user kali sta svolgendo.

```
(kali@kali)-[~]
$ top|grep kali
977 kali      0 0 479480 46824 21792 S 6.2 4.7 0:02.12 xfdeskt+
17831 kali    20 0 11580 4984 3084 R 6.2 0.5 0:00.01 top
877 kali      0 0 217956 1320 1320 S 0.7 0.1 0:10.31 VBoxCli+
786 kali      0 0 9744 4524 3556 S 0.3 0.5 0:00.61 dbus-da+
936 kali      0 0 646860 30764 21408 S 0.3 3.1 0:08.24 xfwm4
1000 kali     20 0 424052 17508 14508 S 0.3 1.8 0:03.61 panel-1+
995 kali      0 0 200948 19248 13536 S 0.7 1.9 0:05.58 panel-1+
870 kali      0 0 217440 1280 1264 S 0.3 0.1 0:01.50 VBoxCli+
877 kali      0 0 217956 1320 1320 S 0.3 0.1 0:10.32 VBoxCli+
897 kali      0 0 217544 2116 2112 S 0.3 0.2 0:00.73 VBoxCli+
977 kali      0 0 479480 46824 21792 S 0.3 4.7 0:02.13 xfdeskt+
1111 kali     20 0 2742472 164936 73608 S 0.3 16.7 0:05.83 firefox+
9715 kali     20 0 447852 111196 90524 S 0.3 11.2 0:03.81 qtermin+
877 kali      0 0 217956 1320 1320 S 0.7 0.1 0:10.34 VBoxCli+
936 kali      0 0 646860 30764 21408 S 0.3 3.1 0:08.25 xfwm4
972 kali      0 0 495372 44720 29804 S 0.3 4.5 0:04.82 Thunar
9715 kali     20 0 447856 111196 90524 S 0.3 11.2 0:03.82 qtermin+
9715 kali     20 0 447856 111196 90524 S 0.7 11.2 0:03.84 qtermin+
877 kali      0 0 217956 1320 1320 S 0.3 0.1 0:10.35 VBoxCli+
936 kali      0 0 646860 30764 21408 S 0.3 3.1 0:08.26 xfwm4
995 kali      0 0 200948 19248 13536 S 0.3 1.9 0:05.59 panel-1+
1000 kali     20 0 424052 17508 14508 S 0.3 1.8 0:03.62 panel-1+
17831 kali    20 0 11580 4984 3084 R 0.3 0.5 0:00.02 top
877 kali      0 0 217956 1320 1320 S 0.7 0.1 0:10.37 VBoxCli+
1006 kali     20 0 601064 17264 14280 S 0.7 1.7 0:01.28 panel-1+
936 kali      0 0 646860 30764 21408 S 0.3 3.1 0:08.27 xfwm4
1000 kali     20 0 424052 17508 14508 S 0.3 1.8 0:03.63 panel-1+
9715 kali     20 0 447856 111196 90524 S 0.3 11.2 0:03.85 qtermin+
877 kali      0 0 217956 1320 1320 S 0.3 0.1 0:10.38 VBoxCli+
936 kali      0 0 646860 30764 21408 S 0.3 3.1 0:08.28 xfwm4
995 kali      0 0 200948 19248 13536 S 0.3 1.9 0:05.60 panel-1+
1020 kali     20 0 312392 7420 5092 S 0.3 0.7 0:00.30 gvfs-af+
9715 kali     20 0 447856 111196 90524 S 0.3 11.2 0:03.86 qtermin+
```

4) Con il comando `cd Desktop` ho raggiunto l'omonima cartella dove con il comando `mkdir Epcode_Lab` ho creato l'omonima cartella. Subito dopo ho usato il comando `nano Esercizio.txt` che per creare per l'appunto il file Esercizio.txt.

```
kali@kali: ~/Desktop/Epcode_Lab
File Actions Edit View Help
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ mkdir Epcode_Lab
(kali@kali)-[~/Desktop]
$ cd Epcode_Lab
(kali@kali)-[~/Desktop/Epcode_Lab]
$ nano Esercizio.txt
```

Ho modificato il file scrivendo “Ciao a tutti 😊” al suo interno e ho provveduto a salvarlo mediante i comandi CTRL + O, INVIO e CTRL + Y

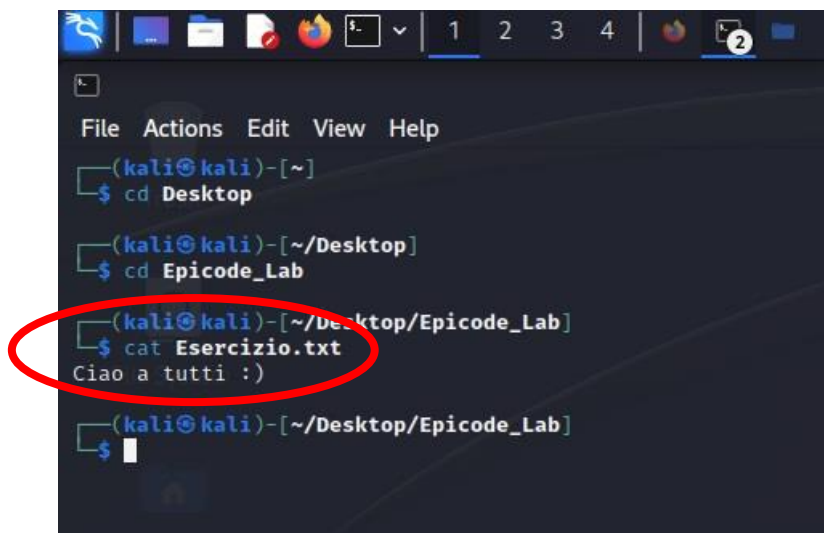


```
kali@kali: ~/Desktop/Epicode_Lab
File Actions Edit View Help
GNU nano 7.2 Esercizio.txt *
Ciao a tutti :)

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

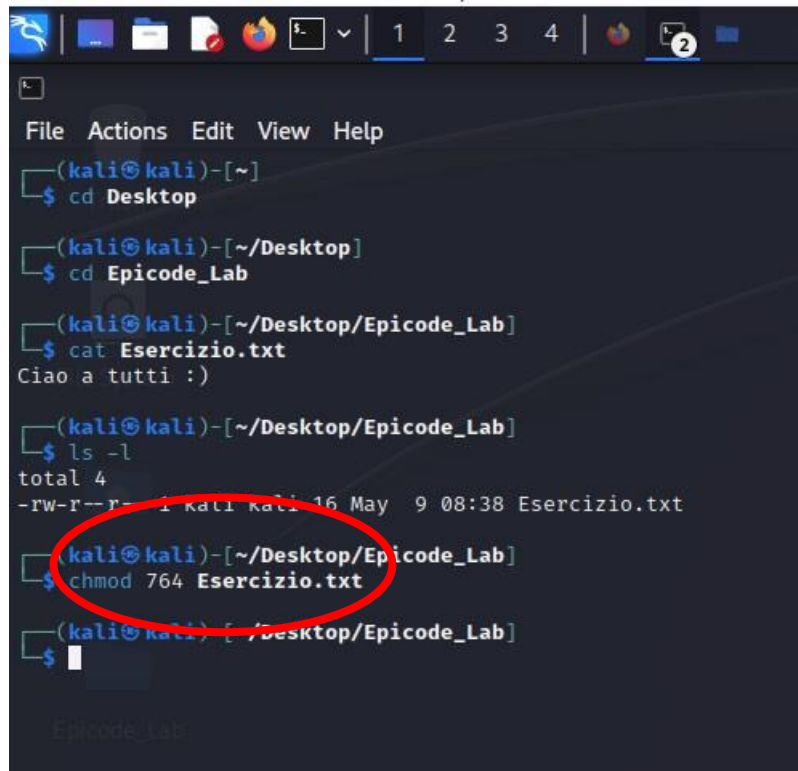
File Name to Write: Esercizio.txt
^G Help      M-D DOS Format  M-A Append     M-B Backup File
^C Cancel    M-M Mac Format  M-P Prepend    ^T Browse
```

Mediante il comando “cat Esercizio.txt” ho letto regolarmente il file Esercizio.txt



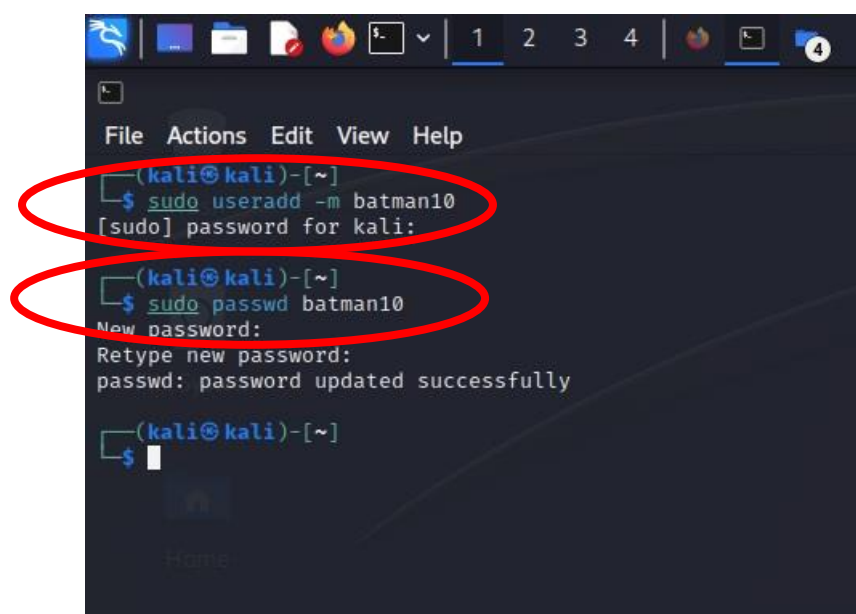
```
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ cd Epicode_Lab
(kali@kali)-[~/Desktop/Epicode_Lab]
$ cat Esercizio.txt
Ciao a tutti :)
(kali@kali)-[~/Desktop/Epicode_Lab]
$
```

Sempre all'interno della cartella Epicode_Lab, in cui era presente solo il mio file, ho controllato i permessi del file Esercizio.txt. Successivamente ho cambiato i permessi come da traccia con il comando "chmod 764 Esercizio.txt", assegnando al mio utente tutti i privilegi (r,w,x), al gruppo i privilegi r,w, e agli altri utenti solo i permessi di lettura (r).

A terminal window with a dark background and light blue text. The terminal shows a series of commands and their outputs. The first command is 'cd Desktop', followed by 'cd Epicode_Lab'. Then, 'cat Esercizio.txt' is executed, showing the output 'Ciao a tutti :)'. Next, 'ls -l' is run, displaying file details for 'Esercizio.txt'. Finally, 'chmod 764 Esercizio.txt' is executed, and the prompt returns. The 'chmod' command and its output are circled in red. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The top bar shows icons for various applications and a tab labeled '2'.

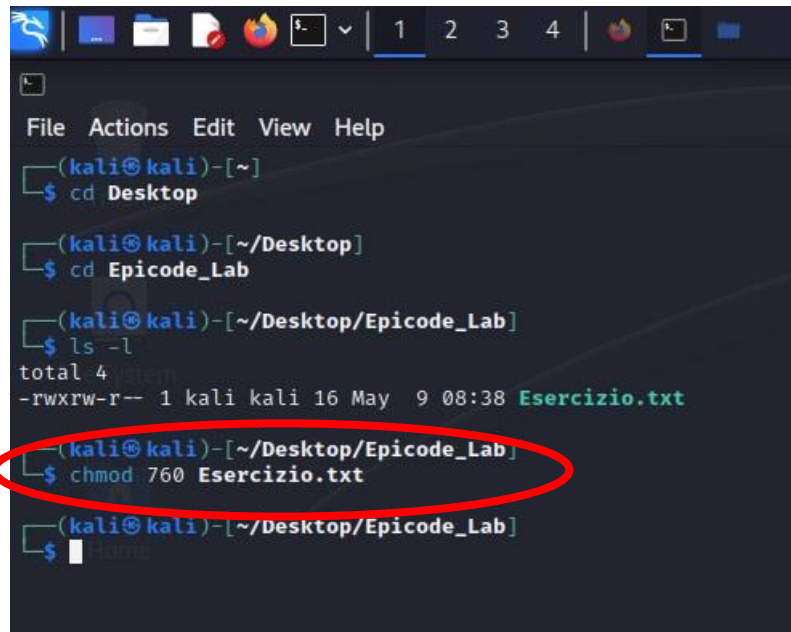
```
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ cd Epicode_Lab
(kali@kali)-[~/Desktop/Epicode_Lab]
$ cat Esercizio.txt
Ciao a tutti :)
(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -l
total 4
-rw-r--r-- 1 kali kali 16 May  9 08:38 Esercizio.txt
(kali@kali)-[~/Desktop/Epicode_Lab]
$ chmod 764 Esercizio.txt
(kali@kali)-[~/Desktop/Epicode_Lab]
$
```

In seguito tramite comando "sudo useradd -m batman10" ho creato un nuovo utente, inserendo relativa password con il comando "sudo passwd".

A terminal window with a dark background and light blue text. The terminal shows two commands being executed. The first is 'sudo useradd -m batman10', which prompts for a password for the user 'kali'. The second is 'sudo passwd batman10', which prompts for a new password and then confirms it. Both commands and their prompts are circled in red. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The top bar shows icons for various applications and a tab labeled '4'.

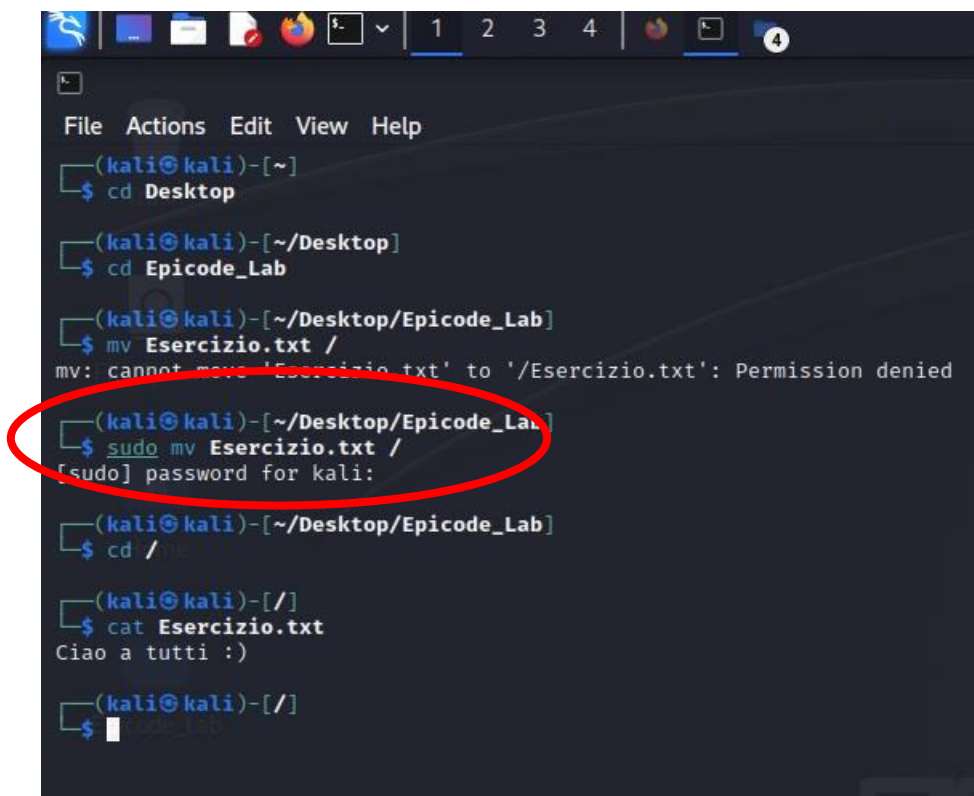
```
(kali@kali)-[~]
$ sudo useradd -m batman10
[sudo] password for kali:
(kali@kali)-[~]
$ sudo passwd batman10
New password:
Retype new password:
passwd: password updated successfully
(kali@kali)-[~]
$
```


Come da traccia ho cambiato nuovamente i privilegi degli altri utenti con il comando “chmod 760) per non dar il privilegio di lettura del mio file ad altri utenti.

A terminal window with a dark background and light blue text. The prompt is (kali@kali)-[~]. The user navigates to the Desktop directory, then to the Epicode_Lab directory. They run 'ls -l' and see a file named 'Esercizio.txt' with permissions '-rwxrw-r--'. The command 'chmod 760 Esercizio.txt' is entered and highlighted with a red oval. The prompt then changes to (kali@kali)-[~/Desktop/Epicode_Lab].

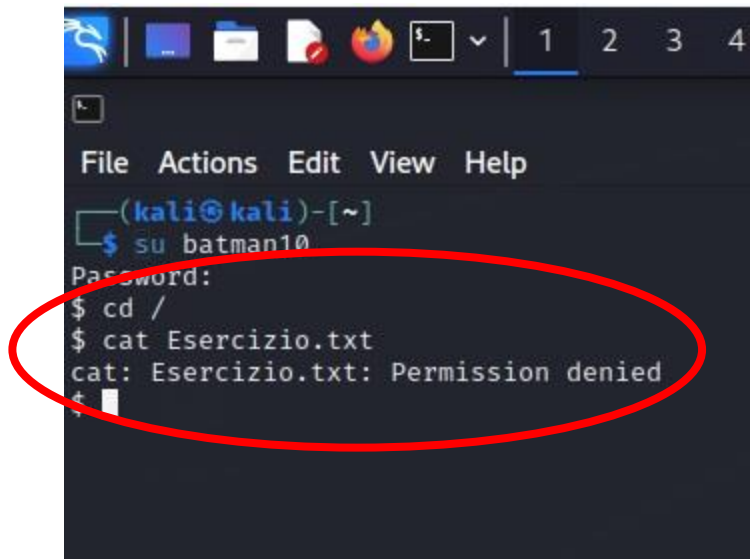
```
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ cd Epicode_Lab
(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -l
total 4
-rwxrw-r-- 1 kali kali 16 May  9 08:38 Esercizio.txt
(kali@kali)-[~/Desktop/Epicode_Lab]
$ chmod 760 Esercizio.txt
(kali@kali)-[~/Desktop/Epicode_Lab]
$
```

Con il comando “sudo mv Esercizio.txt /” ho spostato il mio file nella cartella di root.

A terminal window with a dark background and light blue text. The user navigates to the Desktop directory, then to the Epicode_Lab directory. They run 'mv Esercizio.txt /' and receive the error 'mv: cannot move 'Esercizio.txt' to '/Esercizio.txt': Permission denied'. The command 'sudo mv Esercizio.txt /' is entered and highlighted with a red oval. The prompt then changes to (kali@kali)-[~/Desktop/Epicode_Lab]. The user runs 'cd /' and the prompt changes to (kali@kali)-[/]. They then run 'cat Esercizio.txt' and see the output 'Ciao a tutti :)'.

```
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ cd Epicode_Lab
(kali@kali)-[~/Desktop/Epicode_Lab]
$ mv Esercizio.txt /
mv: cannot move 'Esercizio.txt' to '/Esercizio.txt': Permission denied
(kali@kali)-[~/Desktop/Epicode_Lab]
$ sudo mv Esercizio.txt /
[sudo] password for kali:
(kali@kali)-[~/Desktop/Epicode_Lab]
$ cd /
(kali@kali)-[ / ]
$ cat Esercizio.txt
Ciao a tutti :)
(kali@kali)-[ / ]
$
```

Mediante comando “su batman10” ho cambiato utente, mediante comando “cd /” sono entrato nella cartella in cui è presente il file Esercizio.txt, il quale non può essere letto a causa del problema “permission denied”, in quanto da utente principale ho impostato il parametro “0” che non permette ad altri utenti di svolgere nessuna azione sul file in questione.

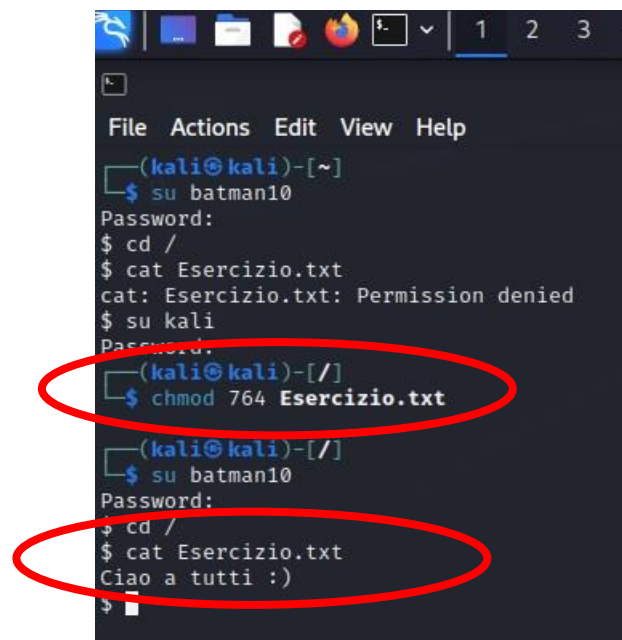
A terminal window with a dark background and light text. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the following commands and output:

```
(kali@kali)-[~]  
$ su batman10  
Password:  
$ cd /  
$ cat Esercizio.txt  
cat: Esercizio.txt: Permission denied  
$
```

 A red oval highlights the last three lines of the terminal output, from '\$ cd /' to '\$'.

```
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ su batman10  
Password:  
$ cd /  
$ cat Esercizio.txt  
cat: Esercizio.txt: Permission denied  
$
```

Sono tornato sull'utente principale dove con il comando “chmod 764 Esercizio.txt” ho dato il privilegio di lettura ad altri utenti, e ritornando nell'utente batman10 ho avuto la possibilità di leggere il contenuto del file Esercizio.txt

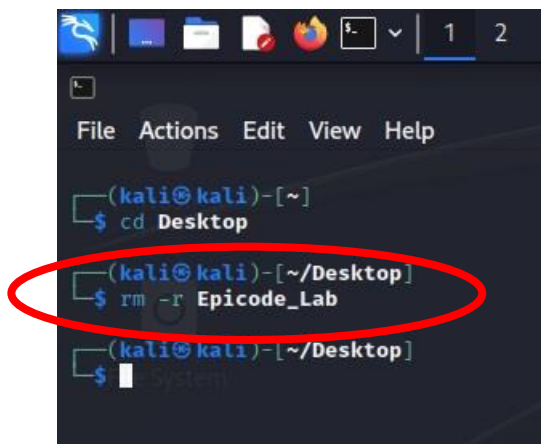
A terminal window with a dark background and light text. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the following commands and output:

```
(kali@kali)-[~]  
$ su batman10  
Password:  
$ cd /  
$ cat Esercizio.txt  
cat: Esercizio.txt: Permission denied  
$ su kali  
Password:  
(kali@kali)-[/]  
$ chmod 764 Esercizio.txt  
  
(kali@kali)-[/]  
$ su batman10  
Password:  
$ cd /  
$ cat Esercizio.txt  
Ciao a tutti :)  
$
```

 Two red ovals highlight specific parts of the terminal output. The first oval highlights the command '\$ chmod 764 Esercizio.txt' and the second oval highlights the output '\$ cat Esercizio.txt' and 'Ciao a tutti :)'.

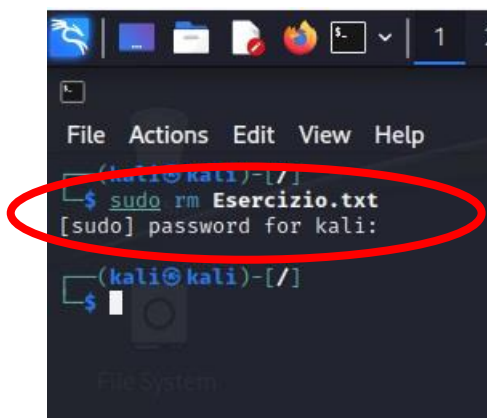
```
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ su batman10  
Password:  
$ cd /  
$ cat Esercizio.txt  
cat: Esercizio.txt: Permission denied  
$ su kali  
Password:  
(kali@kali)-[/]  
$ chmod 764 Esercizio.txt  
  
(kali@kali)-[/]  
$ su batman10  
Password:  
$ cd /  
$ cat Esercizio.txt  
Ciao a tutti :)  
$
```

- Infine mediante comando “rm -r Epicode_Lab” ho rimosso la directory;



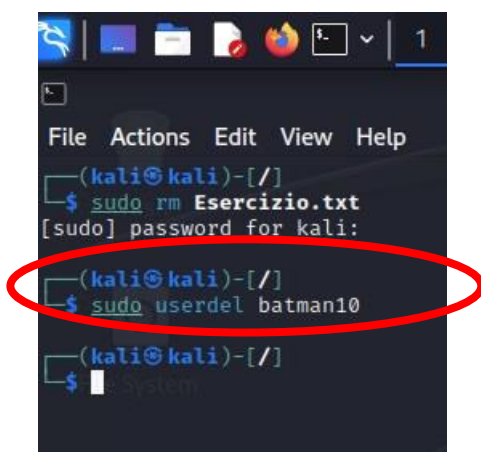
```
(kali㉿kali)-[~]  
$ cd Desktop  
$ rm -r Epicode_Lab  
$
```

- Mediante il comando sudo rm Esercizio.txt ho rimosso il file Esercizio.txt



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

- Mediante il comando “sudo userdel batman10” ho rimosso l’utente, portando tutto allo stato originario.



```
(kali㉿kali)-[~]  
$ sudo rm Esercizio.txt  
[sudo] password for kali:  
$ sudo userdel batman10  
(kali㉿kali)-[~]  
$
```