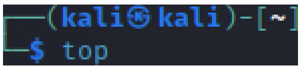
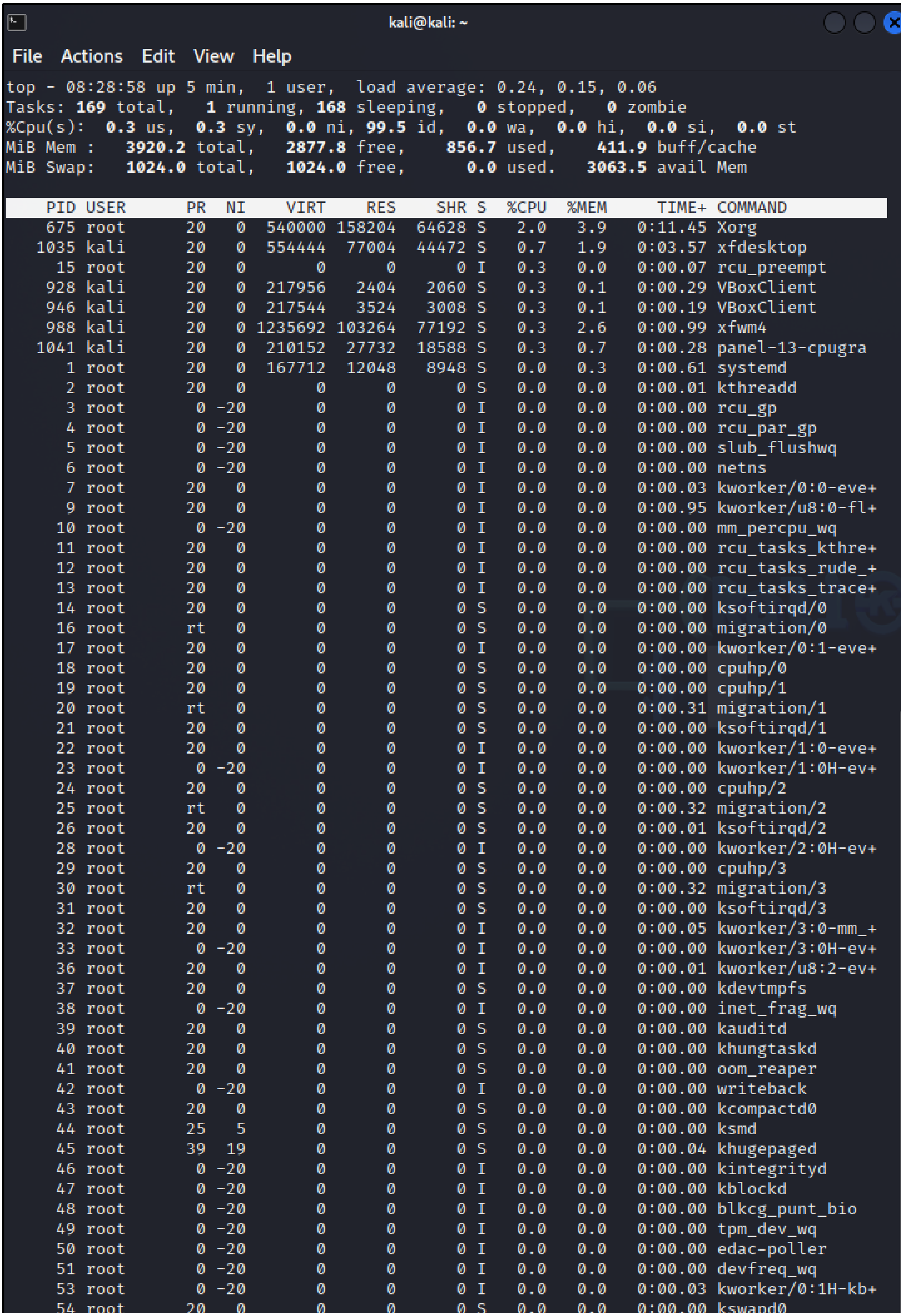
U1W2L2



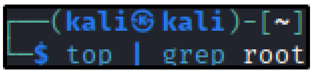
```
┌──(kali㉿kali)-[~]
└─$ top
```



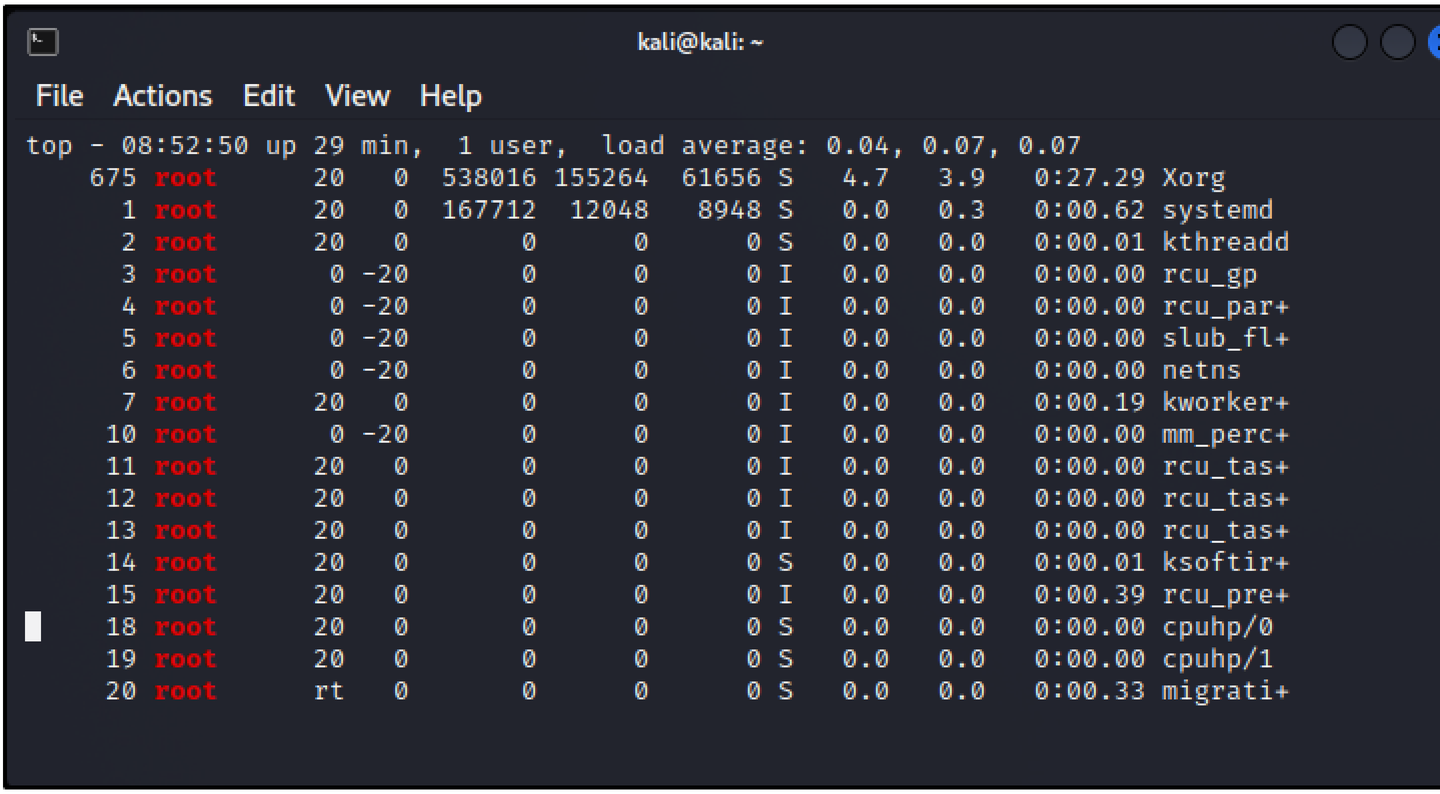
```
top - 08:28:58 up 5 min,  1 user,  load average: 0.24, 0.15, 0.06
Tasks: 169 total,   1 running, 168 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.3 us,  0.3 sy,  0.0 ni, 99.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  3920.2 total,  2877.8 free,   856.7 used,   411.9 buff/cache
MiB Swap:  1024.0 total,  1024.0 free,     0.0 used.  3063.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    675 root      20   0  540000 158204  64628 S   2.0   3.9   0:11.45 Xorg
   1035 kali      20   0  554444  77004  44472 S   0.7   1.9   0:03.57 xfdesktop
     15 root      20   0       0      0      0 I   0.3   0.0   0:00.07 rcu_preempt
    928 kali      20   0  217956   2404   2060 S   0.3   0.1   0:00.29 VBoxClient
    946 kali      20   0  217544   3524   3008 S   0.3   0.1   0:00.19 VBoxClient
    988 kali      20   0 1235692 103264  77192 S   0.3   2.6   0:00.99 xfwm4
   1041 kali      20   0  210152  27732  18588 S   0.3   0.7   0:00.28 panel-13-cpugra
      1 root      20   0  167712  12048   8948 S   0.0   0.3   0:00.61 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 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
      7 root      20   0       0      0      0 I   0.0   0.0   0:00.03 kworker/0:0-eve+
      9 root      20   0       0      0      0 I   0.0   0.0   0:00.95 kworker/u8:0-fl+
     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_kthre+
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_+
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace+
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 ksoftirqd/0
     16 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     17 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/0:1-eve+
     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   0:00.31 migration/1
     21 root      20   0       0      0      0 S   0.0   0.0   0:00.00 ksoftirqd/1
     22 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0-eve+
     23 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-ev+
     24 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/2
     25 root      rt   0       0      0      0 S   0.0   0.0   0:00.32 migration/2
     26 root      20   0       0      0      0 S   0.0   0.0   0:00.01 ksoftirqd/2
     28 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/2:0H-ev+
     29 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/3
     30 root      rt   0       0      0      0 S   0.0   0.0   0:00.32 migration/3
     31 root      20   0       0      0      0 S   0.0   0.0   0:00.00 ksoftirqd/3
     32 root      20   0       0      0      0 I   0.0   0.0   0:00.05 kworker/3:0-mm_+
     33 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/3:0H-ev+
     36 root      20   0       0      0      0 I   0.0   0.0   0:00.01 kworker/u8:2-ev+
     37 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     38 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
     39 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
     40 root      20   0       0      0      0 S   0.0   0.0   0:00.00 khungtaskd
     41 root      20   0       0      0      0 S   0.0   0.0   0:00.00 oom_reaper
     42 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 writeback
     43 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kcompactd0
     44 root      25   5       0      0      0 S   0.0   0.0   0:00.00 ksmd
     45 root      39  19       0      0      0 S   0.0   0.0   0:00.04 khugepaged
     46 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kintegrityd
     47 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kblockd
     48 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 blkcg_punt_bio
     49 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 tpm_dev_wq
     50 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 edac-poller
     51 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 devfreq_wq
     53 root       0 -20       0      0      0 I   0.0   0.0   0:00.03 kworker/0:1H-kb+
     54 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kswapd0
```

Eseguo il comando **top** (table of process) dal terminale per mostrare i processi attivi in tempo reale ed i task del kernel.

Il **PID** (process identifier) identifica il numero del processo, l'**USER**mostra il nome dell'utente mentre **COMMAND** è il programma o utility che è eseguito nella command line.

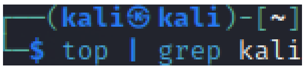


```
┌──(kali㉿kali)-[~]
└─$ top | grep root
```

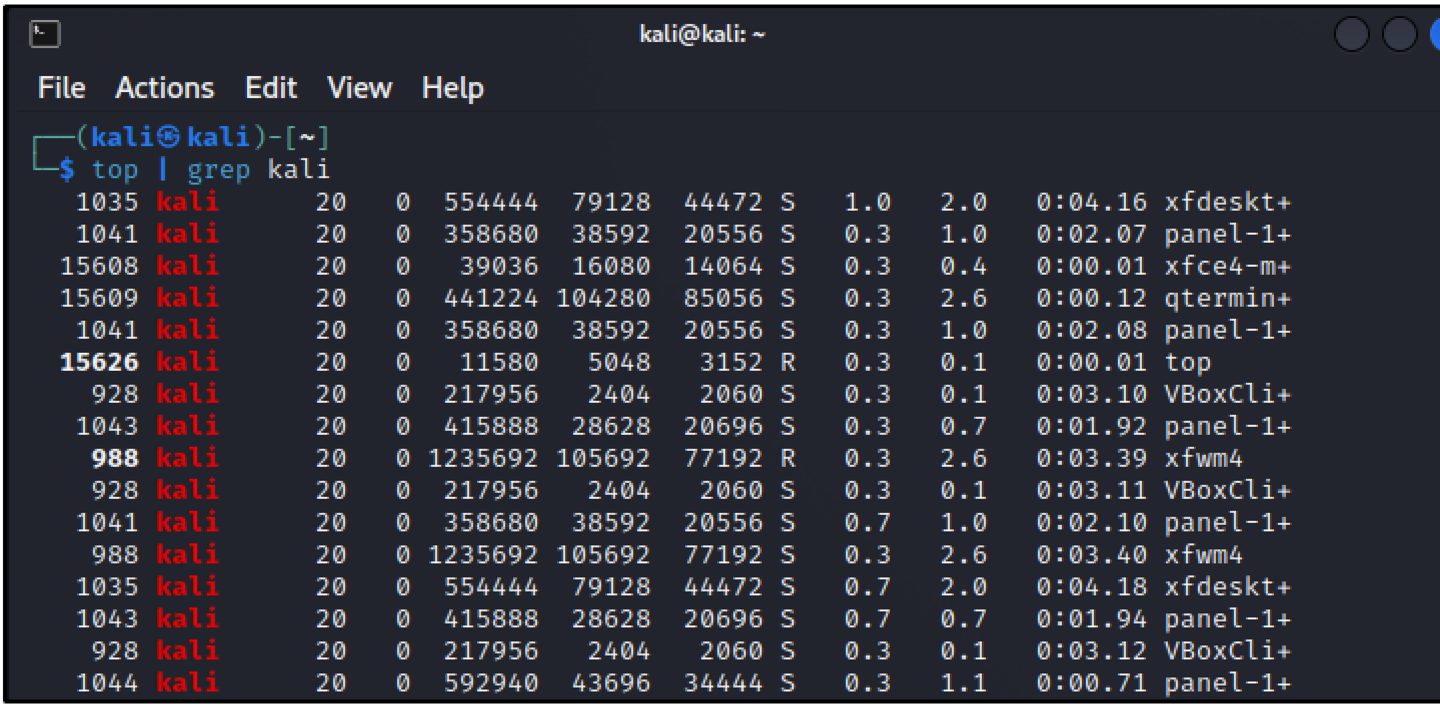


```
top - 08:52:50 up 29 min,  1 user,  load average: 0.04, 0.07, 0.07
    675 root      20   0  538016 155264  61656 S   4.7   3.9   0:27.29 Xorg
      1 root      20   0  167712  12048   8948 S   0.0   0.3   0:00.62 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      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
      7 root      20   0       0      0      0 I   0.0   0.0   0:00.19 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   0:00.01 ksoftir+
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.39 rcu_pre+
     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   0:00.33 migrati+
```

Filtro i risultati per root

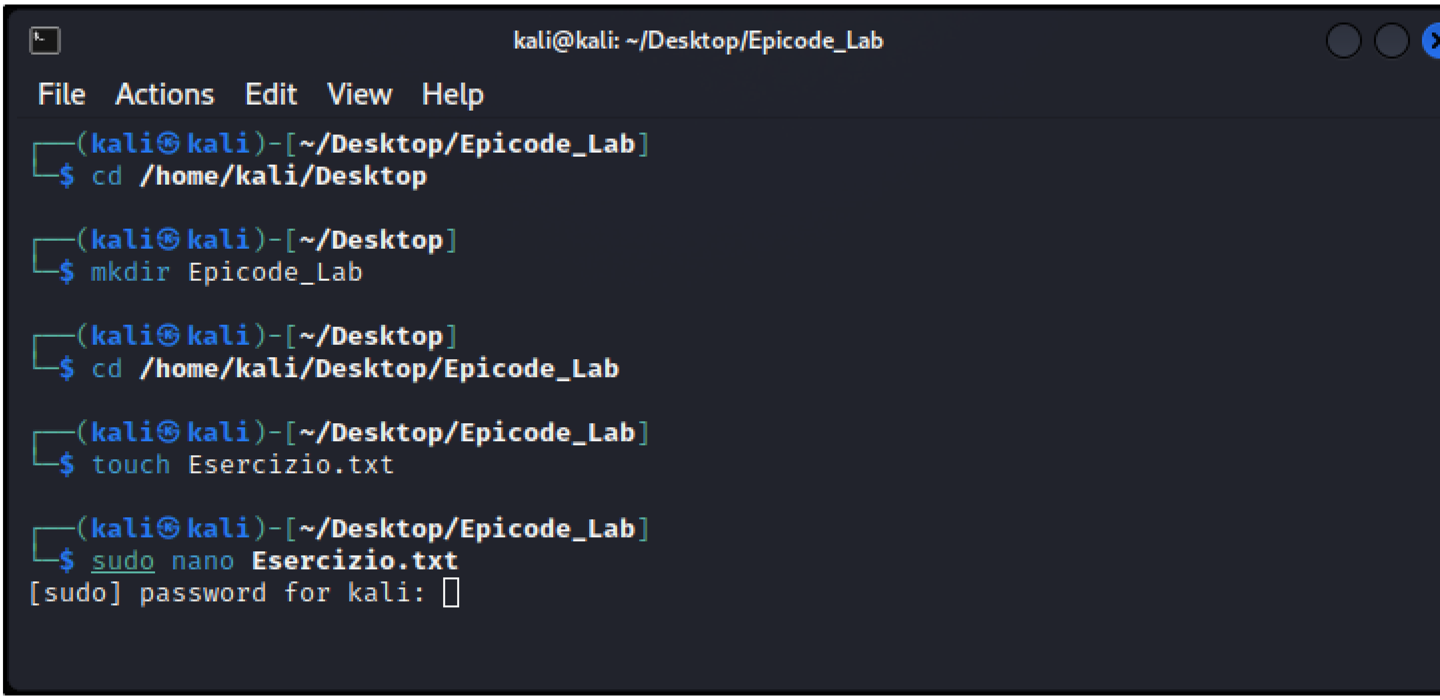


```
┌──(kali㉿kali)-[~]
└─$ top | grep kali
```



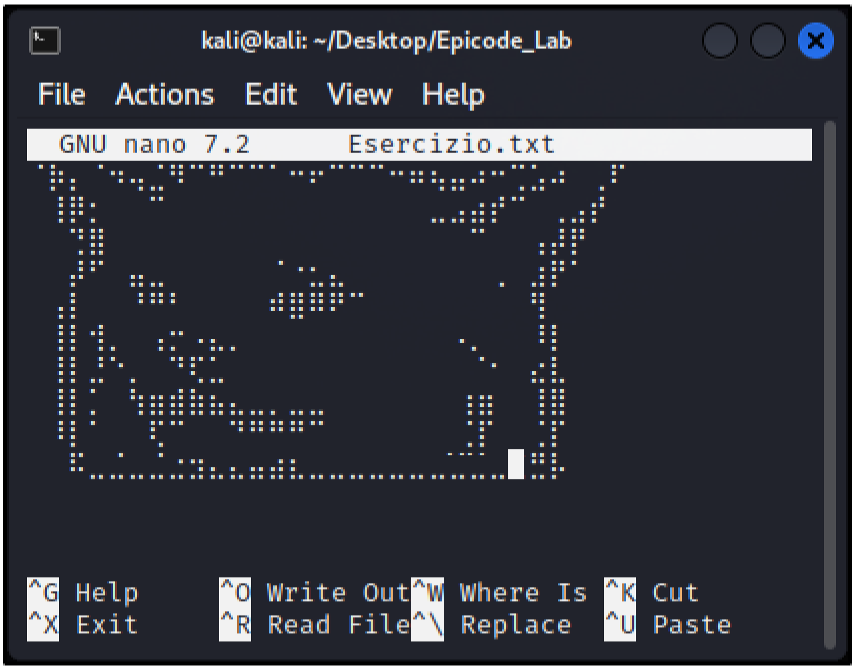
```
┌──(kali㉿kali)-[~]
└─$ top | grep kali
   1035 kali      20   0  554444  79128  44472 S   1.0   2.0   0:04.16 xfdeskt+
   1041 kali      20   0  358680  38592  20556 S   0.3   1.0   0:02.07 panel-1+
  15608 kali      20   0   39036  16080  14064 S   0.3   0.4   0:00.01 xfce4-m+
  15609 kali      20   0  441224 104280  85056 S   0.3   2.6   0:00.12 qtermin+
   1041 kali      20   0  358680  38592  20556 S   0.3   1.0   0:02.08 panel-1+
  15626 kali      20   0   11580   5048   3152 R   0.3   0.1   0:00.01 top
    928 kali      20   0  217956   2404   2060 S   0.3   0.1   0:03.10 VBoxCli+
   1043 kali      20   0  415888  28628  20696 S   0.3   0.7   0:01.92 panel-1+
    988 kali      20   0 1235692 105692  77192 R   0.3   2.6   0:03.39 xfwm4
    928 kali      20   0  217956   2404   2060 S   0.3   0.1   0:03.11 VBoxCli+
   1041 kali      20   0  358680  38592  20556 S   0.7   1.0   0:02.10 panel-1+
    988 kali      20   0 1235692 105692  77192 S   0.3   2.6   0:03.40 xfwm4
   1035 kali      20   0  554444  79128  44472 S   0.7   2.0   0:04.18 xfdeskt+
   1043 kali      20   0  415888  28628  20696 S   0.7   0.7   0:01.94 panel-1+
    928 kali      20   0  217956   2404   2060 S   0.3   0.1   0:03.12 VBoxCli+
   1044 kali      20   0  592940  43696  34444 S   0.3   1.1   0:00.71 panel-1+
```

Filtro i risultati per kali



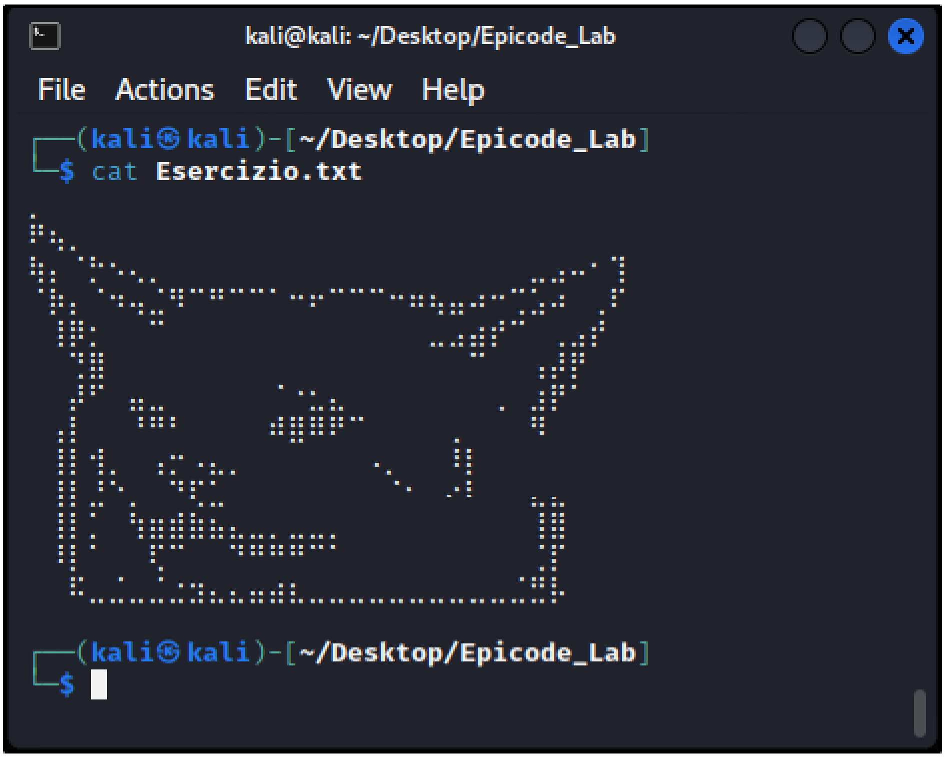
```
┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ cd /home/kali/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir Epicode_Lab

┌──(kali㉿kali)-[~/Desktop]
└─$ cd /home/kali/Desktop/Epicode_Lab

┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ touch Esercizio.txt

┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ sudo nano Esercizio.txt
[sudo] password for kali: 
```

Mi muovo nelle directory e creo il file Esercizio.txt



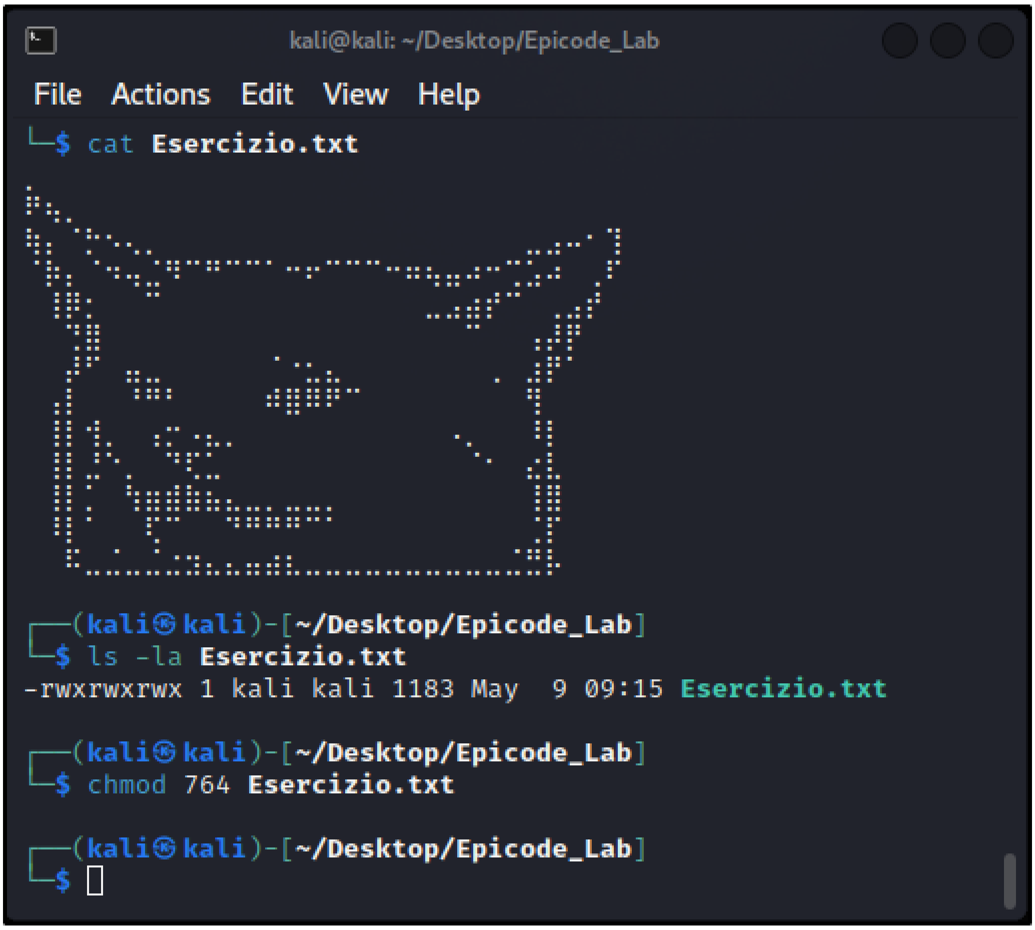
```
  GNU nano 7.2         Esercizio.txt

^G Help      ^O Write Out^W Where Is  ^K Cut
^X Exit      ^R Read File^\ Replace   ^U Paste
```

Modifico con l'editor di testo



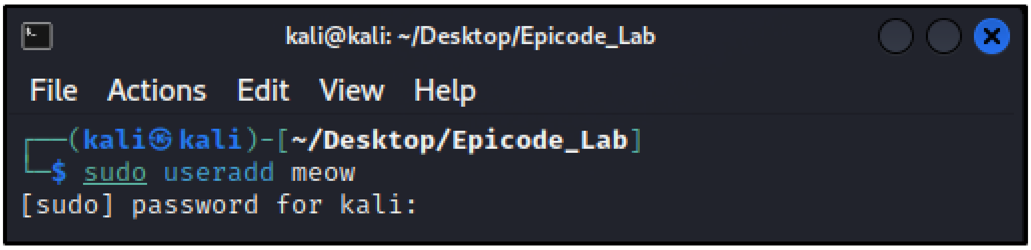
```
┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ cat Esercizio.txt

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

Leggo il file con il comando **cat**



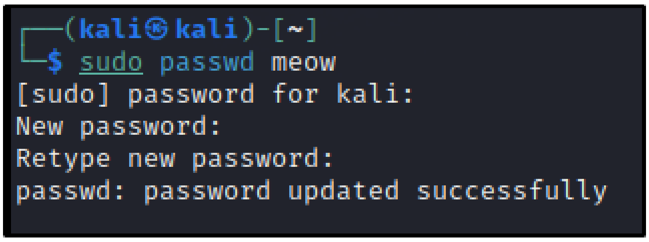
```
└─$ cat Esercizio.txt

┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ ls -la Esercizio.txt
-rwxrwxrwx 1 kali kali 1183 May  9 09:15 Esercizio.txt

┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ chmod 764 Esercizio.txt

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

Controllo i permessi con ls -la e poi li cambio, 7rwx 6rw e 4r per il file creato



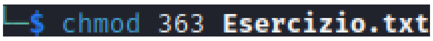
```
┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ sudo useradd meow
[sudo] password for kali:
```

Aggiungo l'user meow



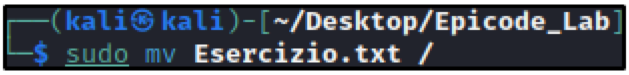
```
┌──(kali㉿kali)-[~]
└─$ sudo passwd meow
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully
```

Imposto la password



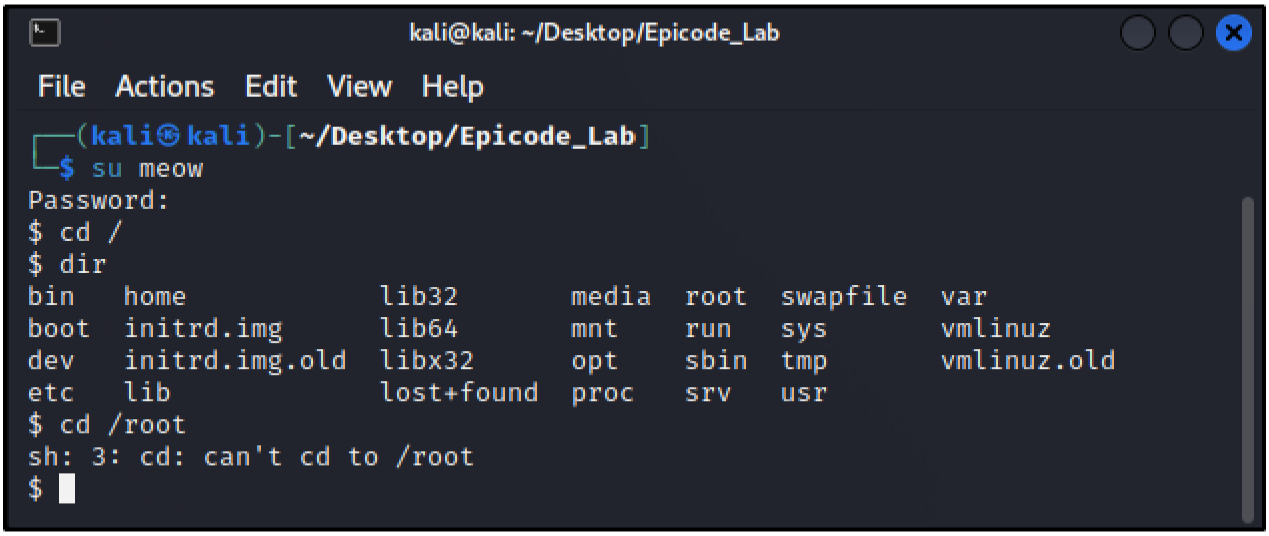
```
└─$ chmod 363 Esercizio.txt
```

Cambio i permessi 3r 6rw e 3r



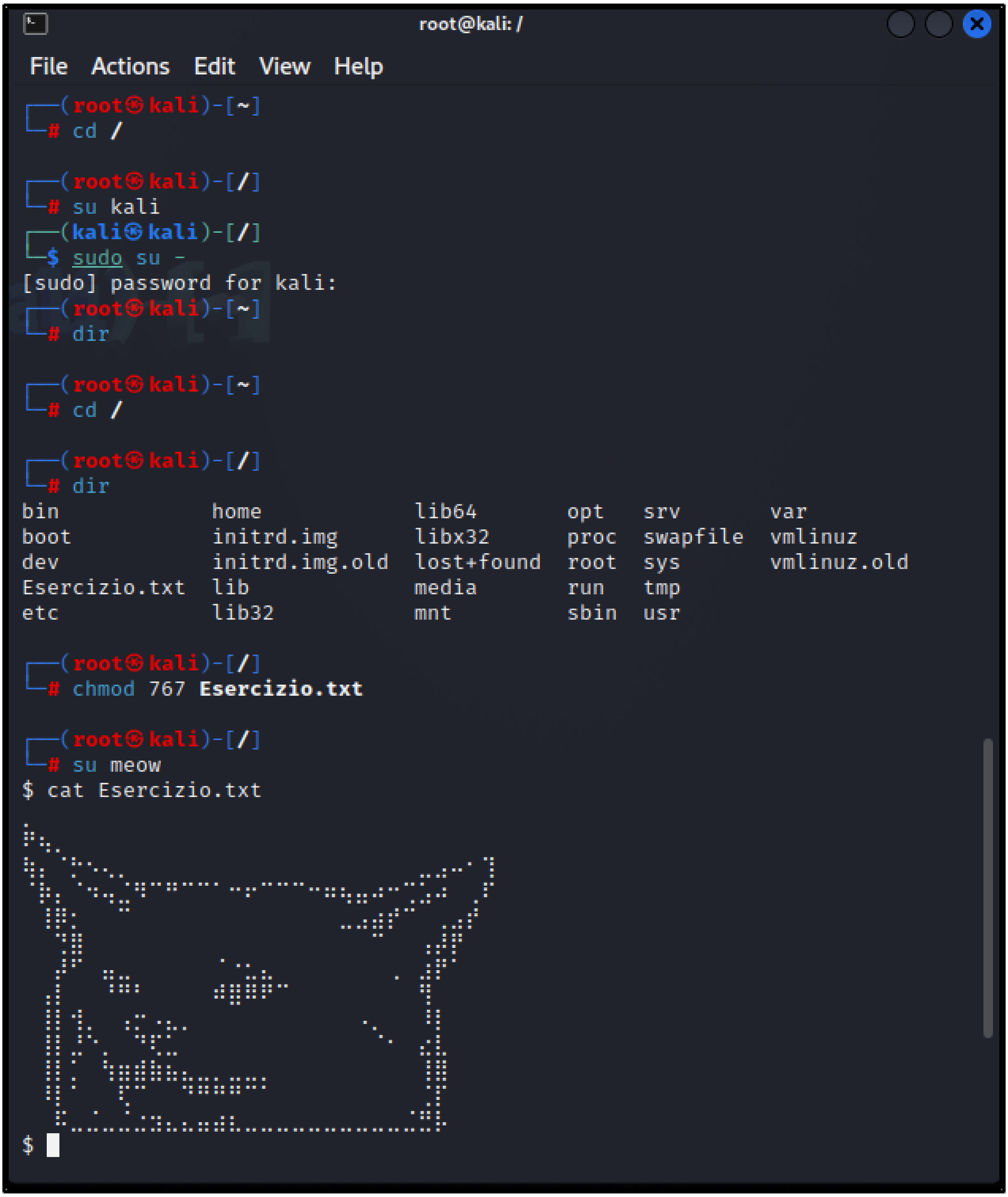
```
┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ sudo mv Esercizio.txt /
```

Sposto il file nella cartella root



```
┌──(kali㉿kali)-[~/Desktop/Epicode_Lab]
└─$ su meow
Password:
$ cd /
$ dir
bin   home            lib32       media  root  swapfile  var
boot  initrd.img      lib64       mnt    run   sys       vmlinuz
dev   initrd.img.old  libx32      opt    sbin  tmp       vmlinuz.old
etc   lib             lost+found  proc   srv   usr
$ cd /root
sh: 3: cd: can't cd to /root
$ 
```

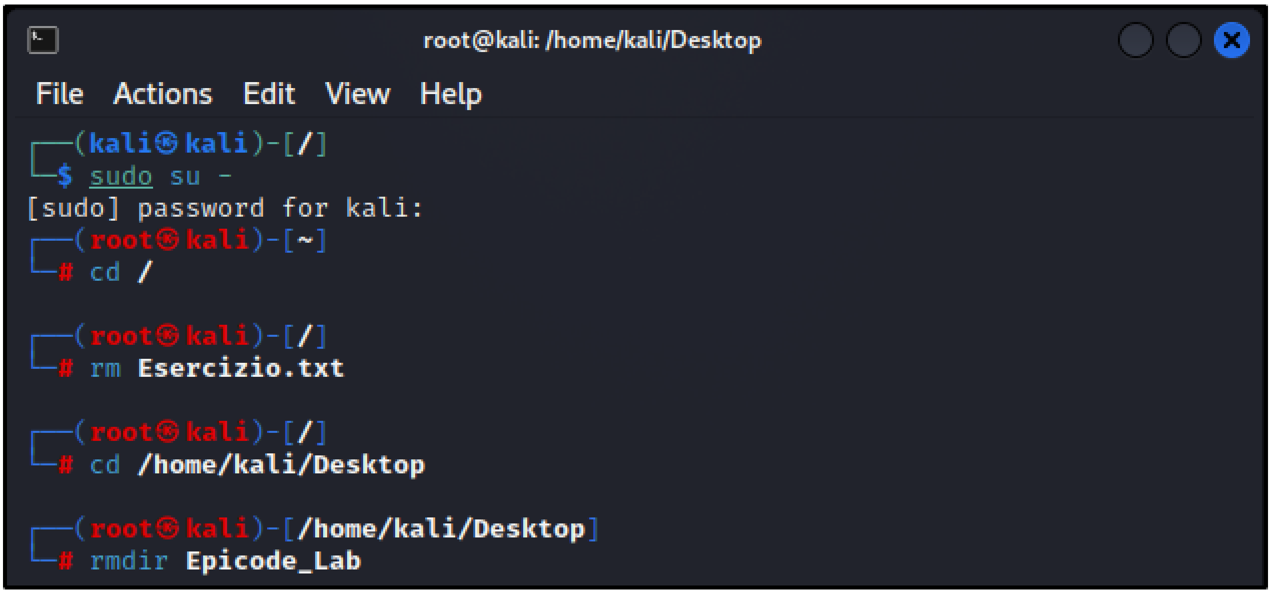
L'errore sh3 riflette l'user creato che non ha i permessi per muoversi in root



```
┌──(root㉿kali)-[~]
└─# cd /

┌──(root㉿kali)-[/]
└─# su kali
┌──(kali㉿kali)-[/]
└─$ sudo su -
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# dir

┌──(root㉿kali)-[~]
└─# cd /

┌──(root㉿kali)-[/]
└─# dir
bin            home           lib64        opt   srv       var
boot           initrd.img     libx32       proc  swapfile  vmlinuz
dev            initrd.img.old lost+found   root  sys       vmlinuz.old
Esercizio.txt  lib            media        run   tmp
etc            lib32          mnt          sbin  usr

┌──(root㉿kali)-[/]
└─# chmod 767 Esercizio.txt

┌──(root㉿kali)-[/]
└─# su meow
$ cat Esercizio.txt
```

```
$
```

sudo su -e modifico i permessi per il file, torno sull'user creato e apro il file



```
┌──(kali㉿kali)-[/]
└─$ sudo su -
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# cd /

┌──(root㉿kali)-[/]
└─# rm Esercizio.txt

┌──(root㉿kali)-[/]
└─# cd /home/kali/Desktop

┌──(root㉿kali)-[/home/kali/Desktop]
└─# rmdir Epicode_Lab
```

Alla fine elimino sia il file che la cartella