

```
kali@kali: ~  
File Actions Edit View Help  
top - 08:26:48 up 2 min, 1 user, load average: 0.64, 0.47, 0.19  
Tasks: 155 total, 1 running, 154 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 3.9 us, 1.7 sy, 0.0 ni, 94.3 id, 0.0 wa, 0.0 hi, 0.2 si, 0.0 st  
MiB Mem : 1981.2 total, 1002.4 free, 576.5 used, 402.3 buff/cache  
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used, 1253.9 avail Mem  
  
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND  
621 root 20 0 378644 125884 56768 S 4.3 6.2 0:06.17 Xorg  
948 kali 20 0 203960 27452 18328 S 2.3 1.4 0:02.74 panel-13-cpugra  
1290 kali 20 0 470128 108576 89228 S 2.3 5.4 0:02.74 qterminal  
1562 kali 20 0 10200 3724 3056 R 1.0 0.2 0:00.27 top  
837 kali 20 0 152916 2704 2224 S 0.3 0.1 0:00.28 VBoxClient  
890 kali 20 0 933664 104368 77280 S 0.3 5.1 0:01.65 xfw4  
953 kali 20 0 358432 30276 20540 S 0.3 1.5 0:00.83 panel-15-genmon  
954 kali 20 0 665856 45496 34304 S 0.3 2.2 0:00.51 panel-16-pulsea  
1 root 20 0 101908 12000 8920 S 0.0 0.6 0:01.75 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 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 0:00.00 kworker/0:0-cgroup_destroy  
8 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/0:0H-events_highpri  
9 root 20 0 0 0 0 I 0.0 0.0 0:00.05 kworker/u4:0-events_unbound  
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 0:00.02 ksoftirqd/0  
15 root 20 0 0 0 0 I 0.0 0.0 0:00.15 rcu_preempt  
16 root rt 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 0:00.02 kworker/0:1-events  
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 S 0.0 0.0 0:00.22 migration/1  
21 root 20 0 0 0 0 S 0.0 0.0 0:00.05 ksoftirqd/1  
22 root 20 0 0 0 0 I 0.0 0.0 0:00.00 kworker/1:0-events  
23 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/1:0H-events_highpri  
25 root 20 0 0 0 0 I 0.0 0.0 0:01.31 kworker/u4:1-writeback  
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 0:00.00 khungtaskd  
30 root 20 0 0 0 0 S 0.0 0.0 0:00.00 oom_reaper  
31 root 20 0 0 0 0 I 0.0 0.0 0:00.04 kworker/u4:2-events_unbound  
32 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 writeback  
33 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kcompactd0  
34 root 25 5 0 0 0 S 0.0 0.0 0:00.00 ksmd  
35 root 39 19 0 0 0 S 0.0 0.0 0:00.06 khugepaged  
36 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kintegrityd  
37 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kblockd  
38 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 blkcg_punt_bio  
39 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 tpm_dev_wq  
40 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 edac-poller
```

Con il

comando "top" possiamo vedere tutti i processi attivi sulla macchina, e per ognuno di loro vengono fornite varie informazioni come il PID, che sta per process identifier ed è un numero univoco che rappresenta un determinato processo, nella colonna user invece troviamo il nome dell' utente che ha avviato il processo, infine la colonna command ci mostra il nome a basso livello che identifica il processo.

```

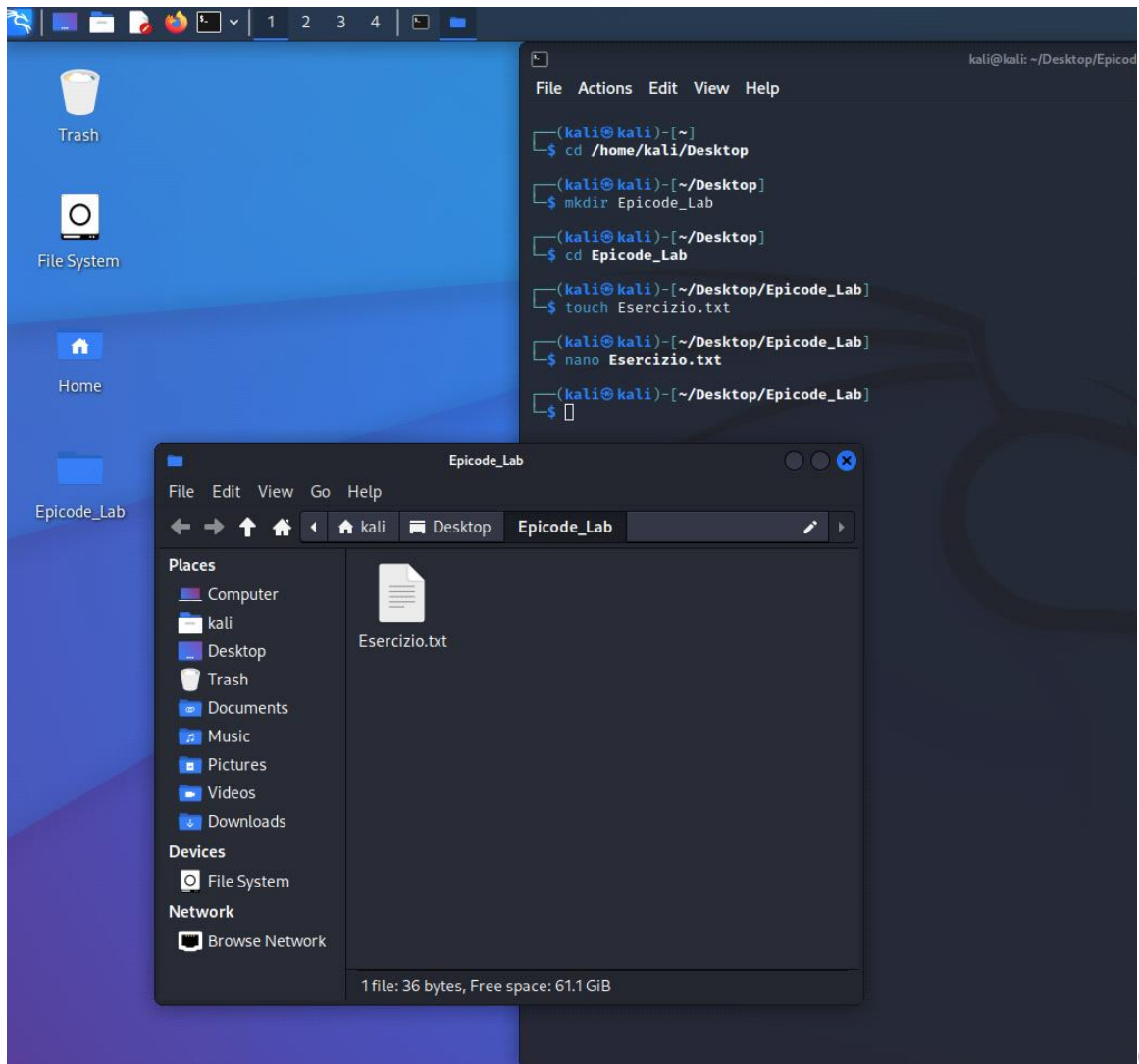
File  Actions  Edit  View  Help
top - 08:48:30 up 24 min, 1 user, load average: 0.25, 0.17, 0.12
621 root    20  0  375836 125700 56320 S  1.7  6.2  0:33.82 Xorg
136 root    20  0  0  0  0 I  0.3  0.0  0:01.70 kworker/1:2-events_freezable_power_
1 root     20  0  101908 12000 8920 S  0.0  0.6  0:01.80 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 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  0:00.06 ksoftirqd/0
15 root    20  0  0  0  0 I  0.0  0.0  0:01.03 rcu_preempt
16 root    rt  0  0  0  0  0 S  0.0  0.0  0:00.01 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  0 S  0.0  0.0  0:00.23 migration/1
21 root    20  0  0  0  0 S  0.0  0.0  0:00.08 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  0:00.00 khungtaskd
30 root    20  0  0  0  0 S  0.0  0.0  0:00.00 oom_reaper
31 root    20  0  0  0  0 I  0.0  0.0  0:00.28 kworker/u4:2-ext4-rsv-conversion
32 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 writeback
33 root    20  0  0  0  0 S  0.0  0.0  0:00.07 kcompactd0
34 root    25  5  0  0  0 S  0.0  0.0  0:00.00 ksmd
35 root    39 19  0  0  0 S  0.0  0.0  0:00.27 khugepaged
36 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 kintegrityd
37 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 kblockd
38 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 blkcg_punt_bio
39 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 tpm_dev_wq
40 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 edac-poller
41 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 devfreq_wq
42 root    0 -20  0  0  0 I  0.0  0.0  0:00.12 kworker/0:1H-kblockd
43 root    20  0  0  0  0 S  0.0  0.0  0:00.00 kswapd0
49 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 kthrotld
51 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 acpi_thermal_pm
52 root    20  0  0  0  0 S  0.0  0.0  0:00.00 xenbus_probe
49 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 kthrotld
51 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 acpi_thermal_pm
52 root    20  0  0  0  0 S  0.0  0.0  0:00.00 xenbus_probe
54 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 mld
51 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 acpi_thermal_pm
52 root    20  0  0  0  0 S  0.0  0.0  0:00.00 xenbus_probe
54 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 mld
55 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 ipv6_addrconf
56 root    0 -20  0  0  0 I  0.0  0.0  0:00.11 kworker/1:1H-kblockd
61 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 kstrp
66 root    0 -20  0  0  0 I  0.0  0.0  0:00.00 zswap-shrink

```

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ top | grep kali
7275 kali 20 0 10200 3732 3072 R 18.8 0.2 0:00.04 top
948 kali 20 0 203960 31624 18328 S 3.3 1.6 0:38.40 panel-13-cpugra
5566 kali 20 0 466744 105824 86712 S 1.3 5.2 0:09.17 qterminal
953 kali 20 0 358432 30400 20572 S 1.0 1.5 0:12.35 panel-15-genmon
7275 kali 20 0 10200 3732 3072 R 1.0 0.2 0:00.07 top
890 kali 20 0 933664 106416 77276 S 0.7 5.2 0:07.76 xfwm4
756 kali 20 0 9520 5428 4380 S 0.3 0.3 0:01.14 dbus-daemon
954 kali 20 0 665856 45496 34304 S 0.3 2.2 0:02.76 panel-16-pulsea
948 kali 20 0 203960 31624 18328 S 3.3 1.6 0:38.50 panel-13-cpugra
5566 kali 20 0 466744 105824 86712 S 1.3 5.2 0:09.21 qterminal
7275 kali 20 0 10200 3732 3072 R 1.0 0.2 0:00.10 top
837 kali 20 0 152916 2704 2224 S 0.7 0.1 0:04.28 VBoxClient
953 kali 20 0 358432 30400 20572 S 0.7 1.5 0:12.37 panel-15-genmon
890 kali 20 0 933664 106416 77276 S 0.3 5.2 0:07.77 xfwm4
948 kali 20 0 203960 31624 18328 S 3.3 1.6 0:38.60 panel-13-cpugra
5566 kali 20 0 466744 105824 86712 S 2.6 5.2 0:09.29 qterminal
953 kali 20 0 358432 30400 20572 S 1.0 1.5 0:12.40 panel-15-genmon
7275 kali 20 0 10200 3732 3072 R 1.0 0.2 0:00.13 top
890 kali 20 0 933664 106416 77276 S 0.7 5.2 0:07.79 xfwm4
945 kali 20 0 479116 60476 35600 S 0.3 3.0 0:02.22 xfdesktop
954 kali 20 0 665856 45496 34304 S 0.3 2.2 0:02.77 panel-16-pulsea
5566 kali 20 0 467004 105824 86712 S 10.6 5.2 0:09.61 qterminal
948 kali 20 0 203960 31624 18328 S 2.6 1.6 0:38.68 panel-13-cpugra
890 kali 20 0 933664 106416 77276 S 1.0 5.2 0:07.82 xfwm4
837 kali 20 0 152916 2704 2224 S 0.7 0.1 0:04.30 VBoxClient
878 kali 20 0 164428 7852 7004 S 0.7 0.4 0:00.24 at-spi2-registr
953 kali 20 0 358432 30400 20572 S 0.7 1.5 0:12.42 panel-15-genmon
766 kali 20 0 267568 26560 16668 S 0.3 1.3 0:00.57 xfce4-session
868 kali 20 0 9220 4848 4308 S 0.3 0.2 0:00.14 dbus-daemon
914 kali 20 0 230756 28692 18728 S 0.3 1.4 0:00.57 xfsettingsd
945 kali 20 0 479116 60476 35600 S 0.3 3.0 0:02.23 xfdesktop
954 kali 20 0 665856 45496 34304 S 0.3 2.2 0:02.78 panel-16-pulsea
983 kali 20 0 463240 46404 31532 S 0.3 2.3 0:00.39 xfce4-notifyd
5566 kali 20 0 467028 105828 86712 S 10.6 5.2 0:09.93 qterminal
948 kali 20 0 203960 31624 18328 S 2.7 1.6 0:38.76 panel-13-cpugra
890 kali 20 0 933664 106416 77276 S 1.0 5.2 0:07.85 xfwm4
7275 kali 20 0 10200 3732 3072 R 0.7 0.2 0:00.15 top
756 kali 20 0 9520 5428 4380 S 0.3 0.3 0:01.15 dbus-daemon
837 kali 20 0 152916 2704 2224 S 0.3 0.1 0:04.31 VBoxClient
953 kali 20 0 358432 30400 20572 S 0.3 1.5 0:12.43 panel-15-genmon
954 kali 20 0 665856 45496 34304 S 0.3 2.2 0:02.79 panel-16-pulsea
5566 kali 20 0 467044 105828 86712 R 16.2 5.2 0:10.42 qterminal
948 kali 20 0 203960 31624 18328 S 3.6 1.6 0:38.87 panel-13-cpugra
890 kali 20 0 933664 106416 77276 S 1.0 5.2 0:07.88 xfwm4
953 kali 20 0 358432 30400 20572 S 1.0 1.5 0:12.46 panel-15-genmon
7275 kali 20 0 10200 3732 3072 R 1.0 0.2 0:00.18 top
837 kali 20 0 152916 2704 2224 S 0.3 0.1 0:04.32 VBoxClient
5566 kali 20 0 467056 105828 86712 S 17.4 5.2 0:10.95 qterminal
948 kali 20 0 203960 31624 18328 S 3.0 1.6 0:38.96 panel-13-cpugra
7275 kali 20 0 10200 3732 3072 R 1.3 0.2 0:00.22 top
890 kali 20 0 933664 106416 77276 S 1.0 5.2 0:07.91 xfwm4
```

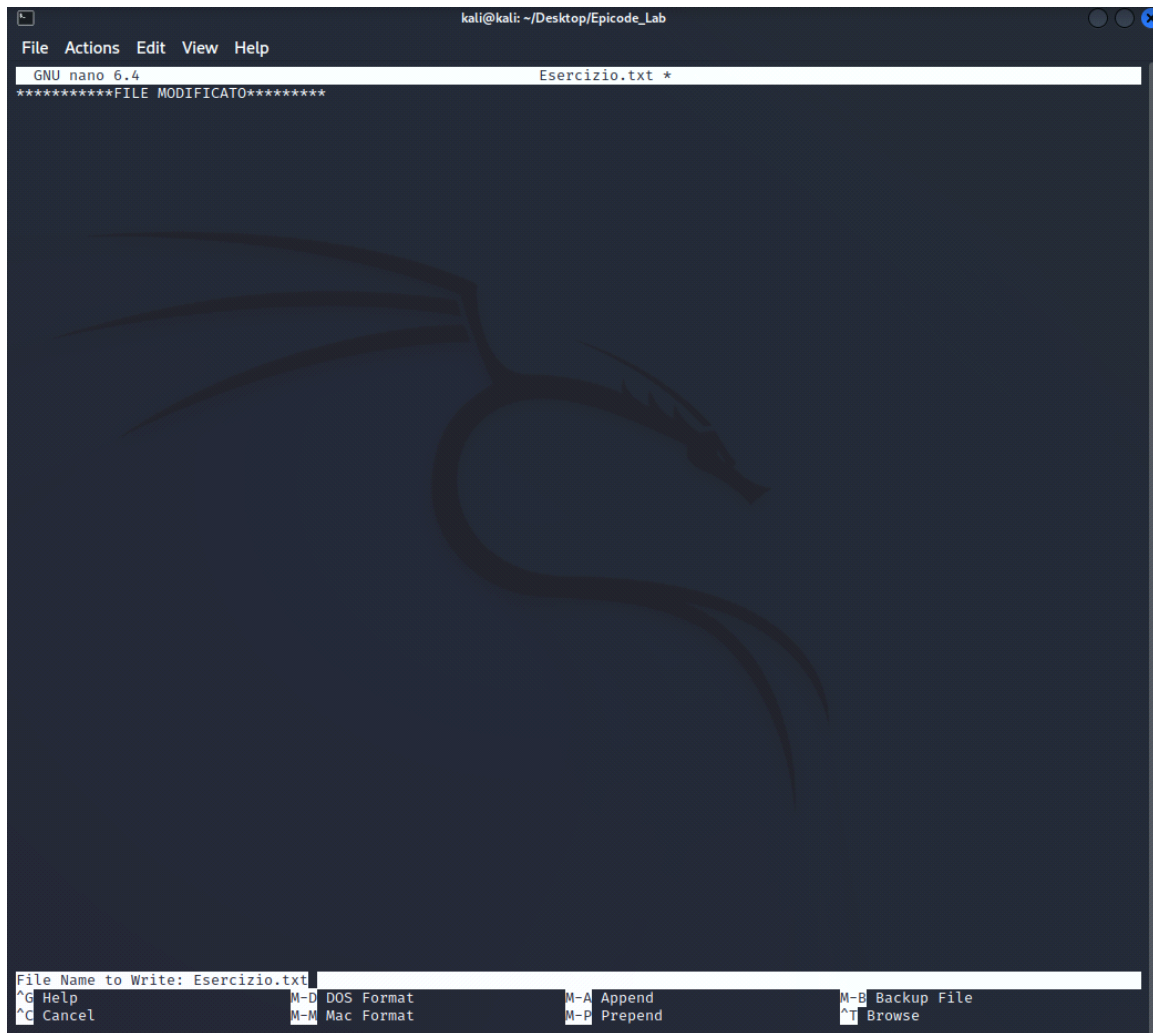
Con

l'operatore pipe "|" possiamo concatenare due comandi, in questo caso top e grep, usando il secondo come filtro nell' operazione da fare, nel primo esempio è stato impostato come filtro il nome utente root, nel secondo kali. Questo tipo di filtro ci permette di organizzare in maniera più efficiente ed ordinata le nostre scansioni.



Creazi

one cartella e file.txt



Interf

accia nano

```
File Actions Edit View Help
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Jan 31 09:00 .
drwxr-xr-x 3 kali kali 4096 Jan 31 09:01 ..
-rw-r--r-- 1 kali kali  36 Jan 31 09:00 Esercizio.txt

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ chmod u+x,g+w Esercizio.txt

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Jan 31 09:00 .
drwxr-xr-x 3 kali kali 4096 Jan 31 09:01 ..
-rwxrw-r-- 1 kali kali  36 Jan 31 09:00 Esercizio.txt
```

Cambio

permessi per scrittura ed esecuzione del file

```
(kali㉿kali)-[~]
$ sudo useradd User2 -p kali
[sudo] password for kali:
```

Creo nuovo utente

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

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Jan 31 09:00 .
drwxr-xr-x 3 kali kali 4096 Jan 31 09:01 ..
-rwxrw--- 1 kali kali  36 Jan 31 09:00 Esercizio.txt
```

Modifico i permessi per non far leggere il file a utenti esterni

```

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ sudo mv Esercizio.txt /
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ cd --
(kali㉿kali)-[~]
$ cd /
(kali㉿kali)-[/]
$ ls
0 bin boot dev Esercizio.txt etc home initrd.img initrd.img.old lib lib32 lib64 libx3

```

Trasporto in root

```

(kali㉿kali)-[~]
$ sudo su User2
$ cd /
$ ls
0 bin boot dev Esercizio.txt etc home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found media mn
$ cat Esercizio.txt
cat: Esercizio.txt: Permission denied
$ █

```

Tentando di accedere al file tramite utente esterno veniamo bloccati a causa dei permessi precedentemente impostati.

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /
(kali㉿kali)-[/]
$ sudo chmod o+r Esercizio.txt
[sudo] password for kali:
(kali㉿kali)-[/]
$ cd --
(kali㉿kali)-[~]
$ sudo su Utente2
$ cd /
$ cat Esercizio.txt
*****FILE MODIFICATO*****
$ █

```

Modificando nuovamente i permessi possiamo eseguire il comando cat sul file e

leggere il suo contenuto.

```
(kali㉿kali)-[~]  
$ cd /  
  
(kali㉿kali)-[/]  
$ sudo rm Esercizio.txt  
[sudo] password for kali:  
  
(kali㉿kali)-[/]  
$ cd --  
  
(kali㉿kali)-[~]  
$ cd /home/kali/Desktop  
  
(kali㉿kali)-[~/Desktop]  
$ sudo rmdir Epicode_Lab
```

Elimino il file e la cartella

