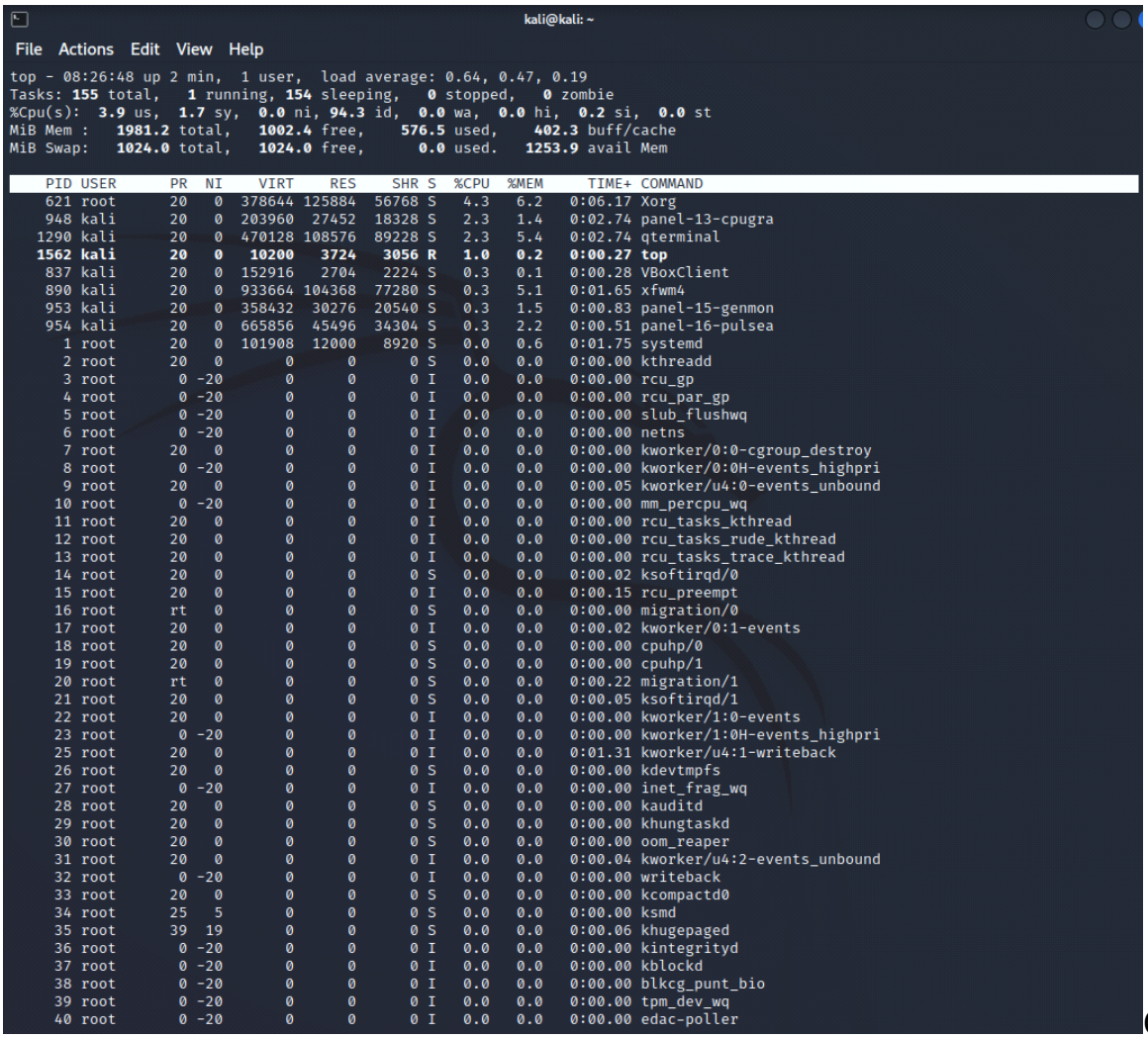
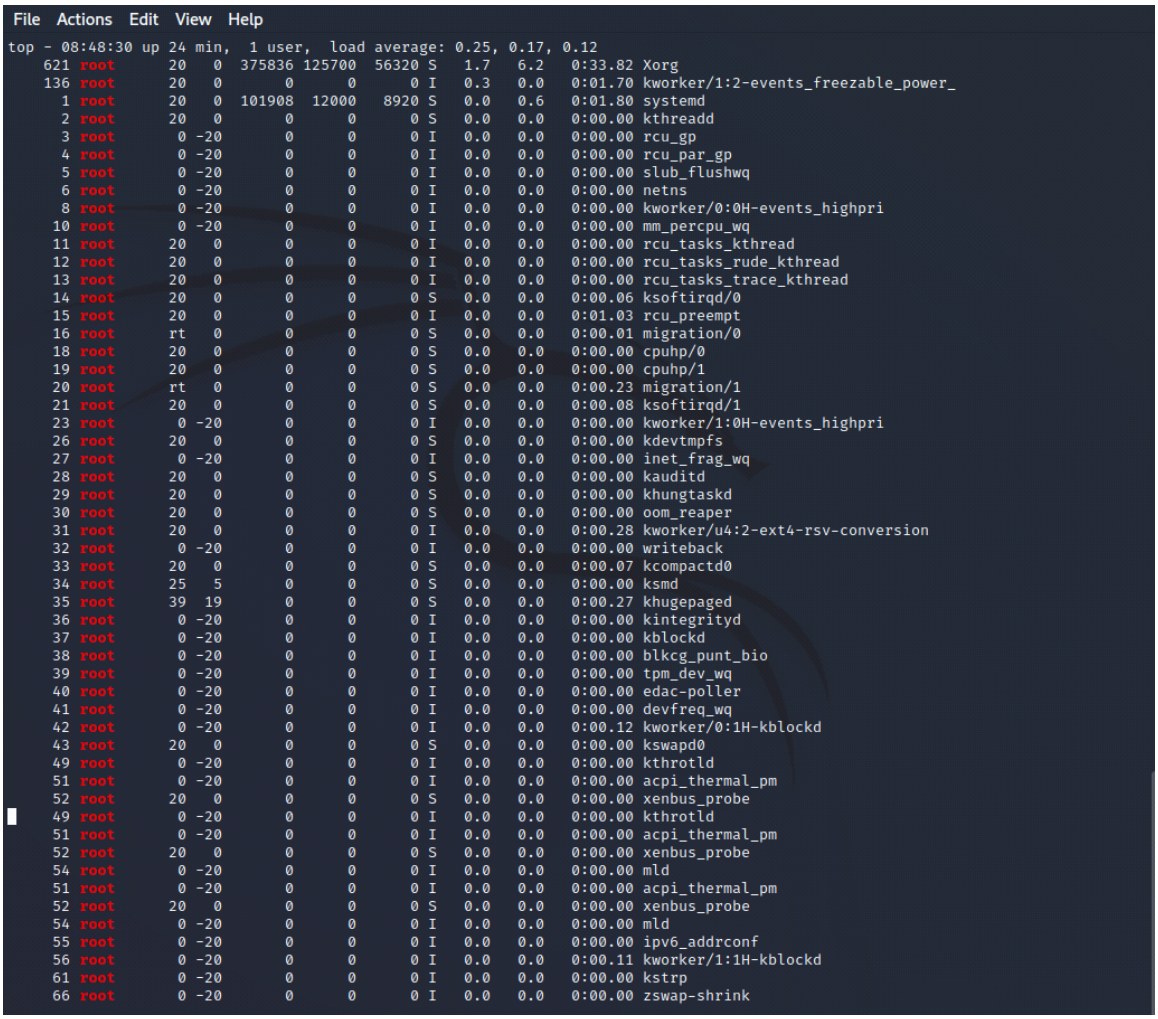
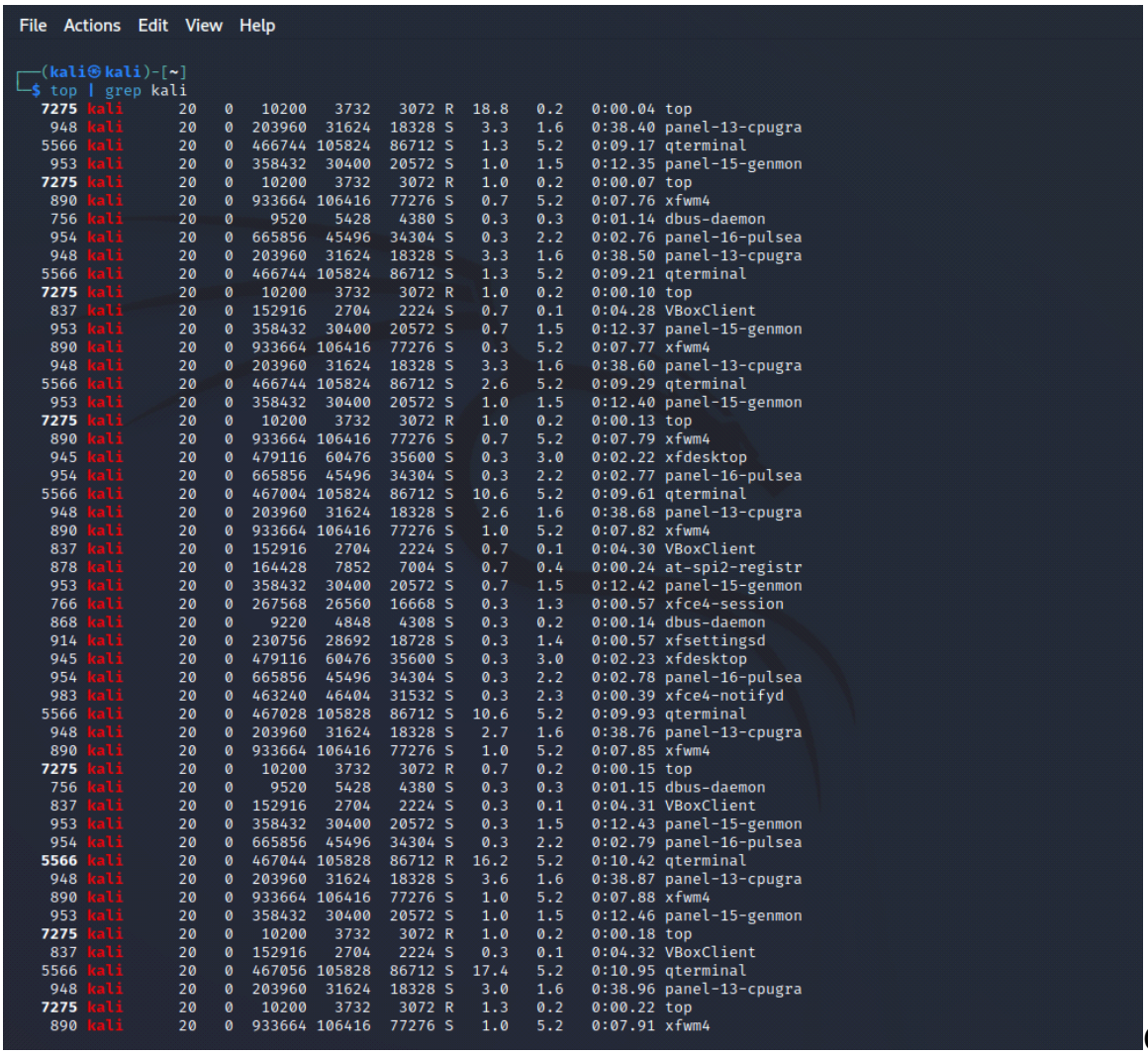
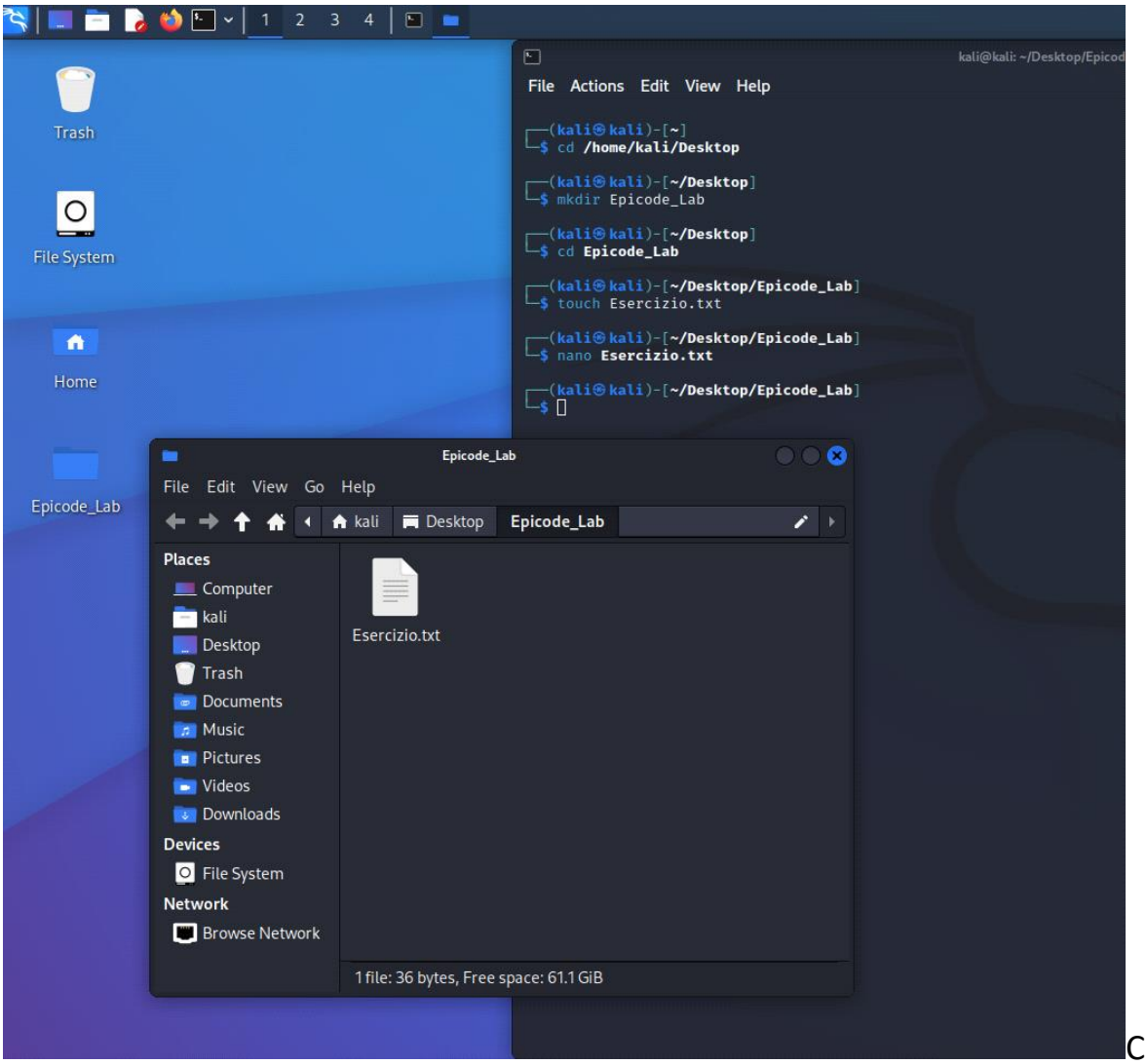


Con il comando "top" possiamo vedere tutti i processi attivi sulla macchina, e per ognuno di loro vengono fornite varie informazioni come il PID, che sta per process identifier ed è un numero univoco che rappresenta un determinato processo, nella colonna user invece troviamo il nome dell' utente che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

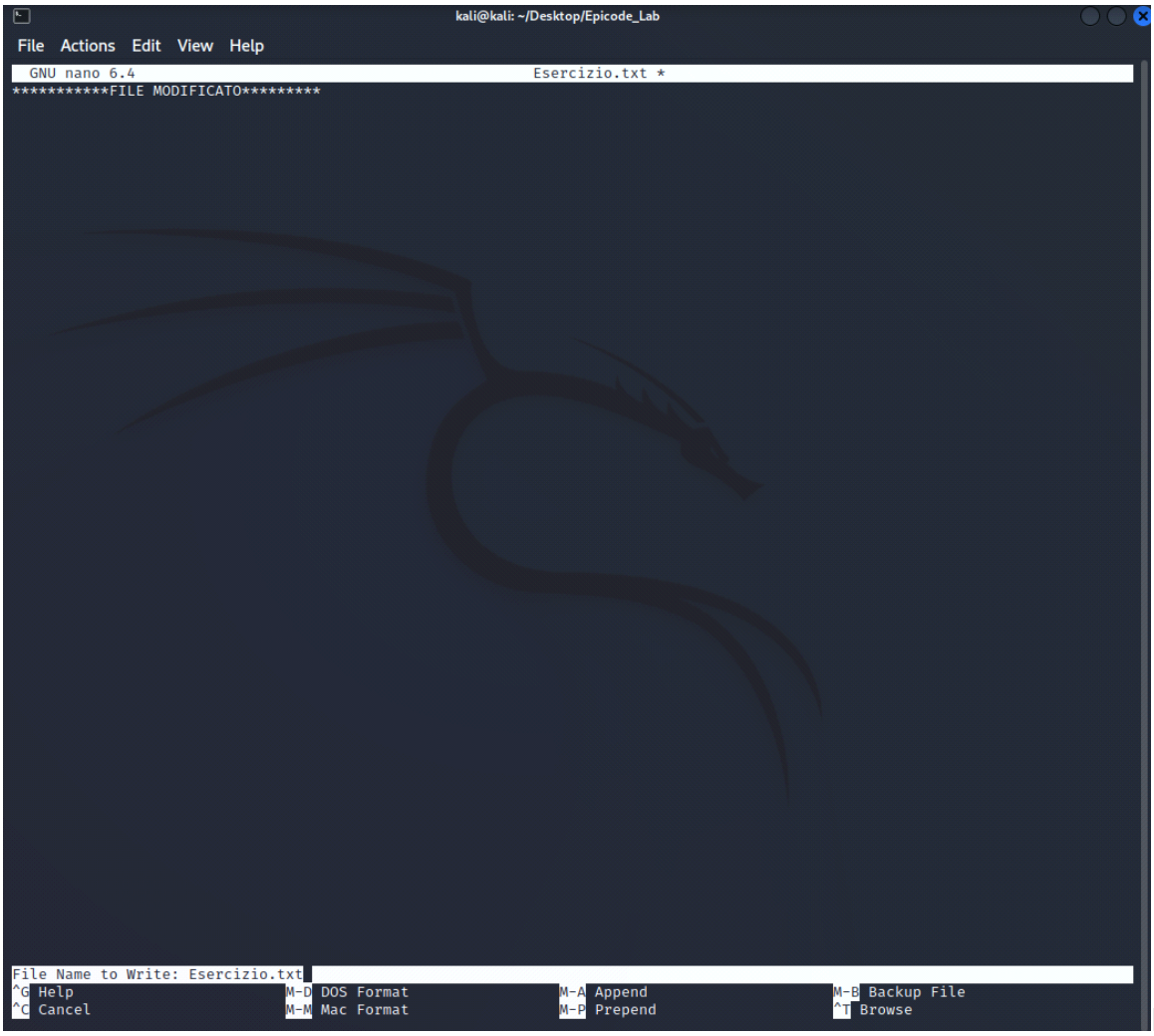

File Actions Edit View Help
top - 08:48:30 up 24 min, 1 user, load average: 0.25, 0.17, 0.12
621 root 20 0 375836 125700 56320 S 1.7 6.2 0:33.82 Xorg
136 root 20 0 0 0 0 I 0.3 0.0 0:01.70 kworker/1:2-events_freezable_power_
1 root 20 0 101908 12000 8920 S 0.0 0.6 0:01.80 systemd
2 root 20 0 0 0 0 S 0.0 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 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 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



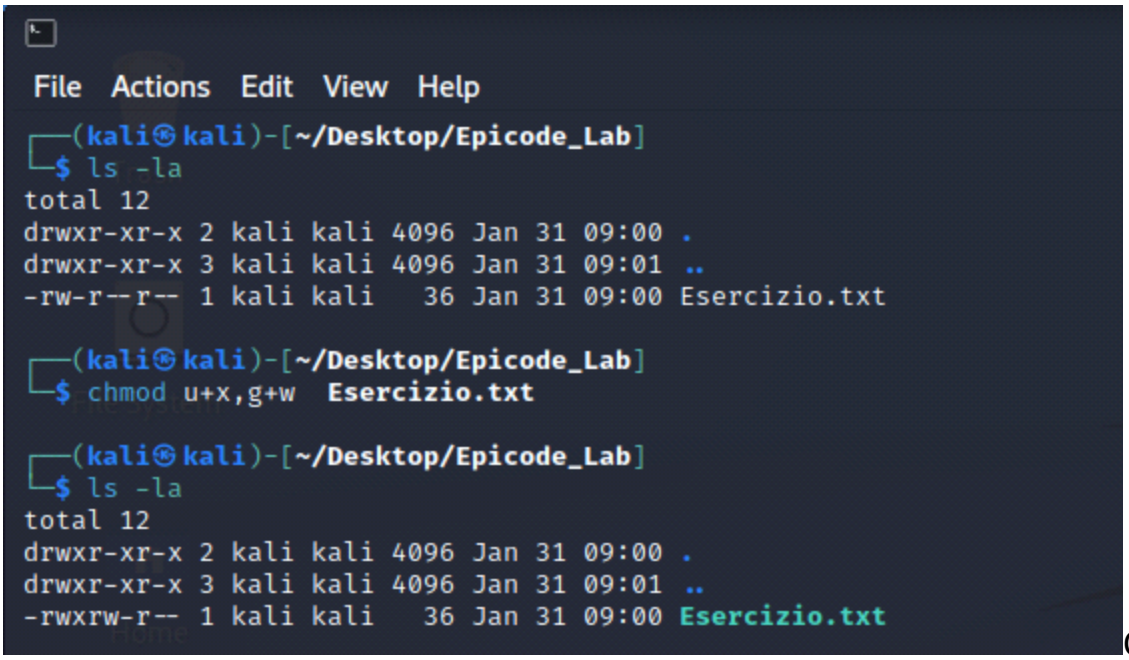
Con l'operatore pipe "|" possiamo concatenare due comandi, in questo caso top e grep, usando il secondo come filtro nell' operazione da fare, nel primo esempio è stato impostato come filtro il nome utente root, nel secondo kali. Questo tipo di filtro ci permette di organizzare in maniera più efficente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



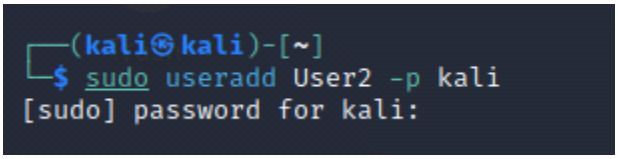
Creazione cartella e file.txt



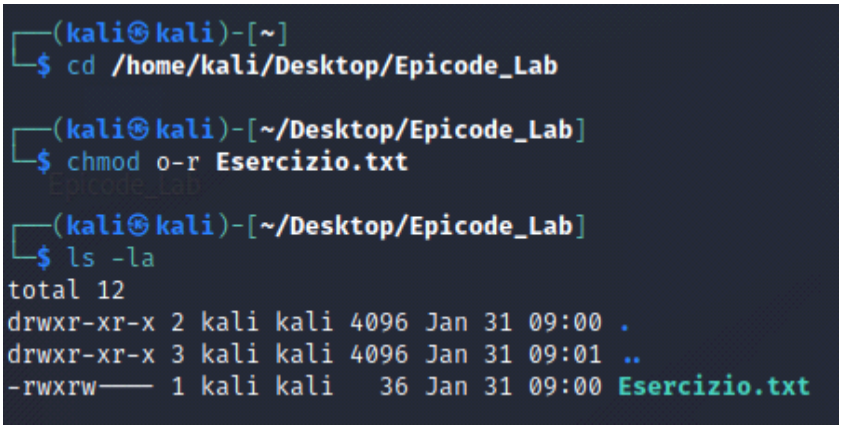
Interf
accia nano



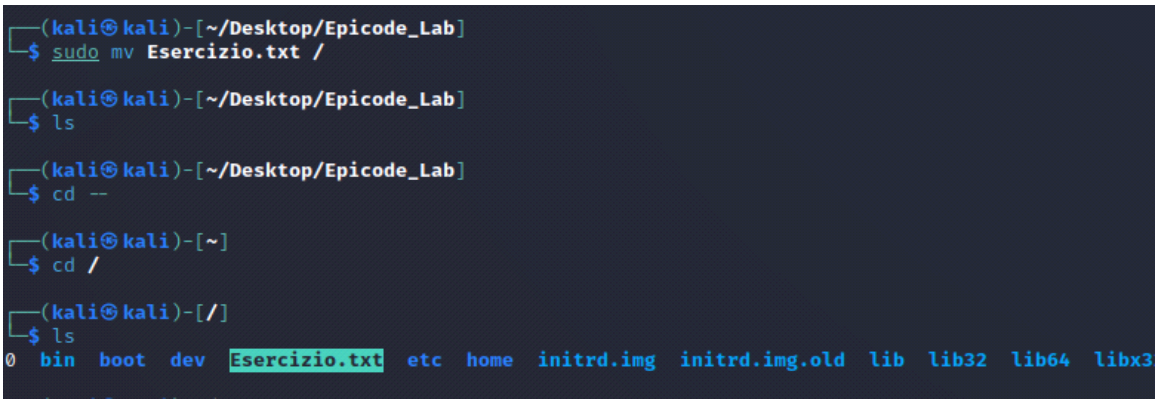
Cambio permessi per scrittura ed esecuzione del file



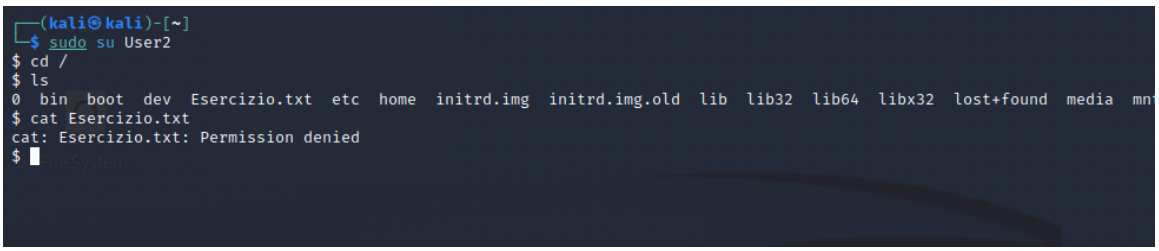
Creo nuovo utente



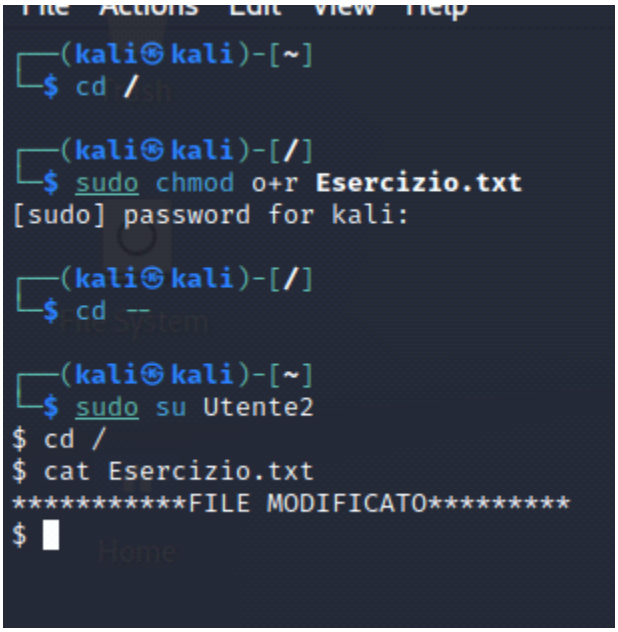
Modifico i permessi per non far leggere il file a utenti esterni



Trasporto in root

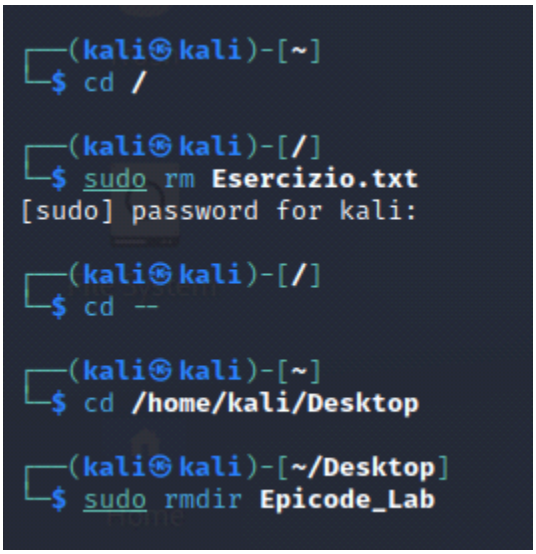


Tentando di accedere al file tramite utente esterno veniamo bloccati a causa dei permessi precendentemente impostati.



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

leggere il suo contenuto.



Elimino il file e la cartella