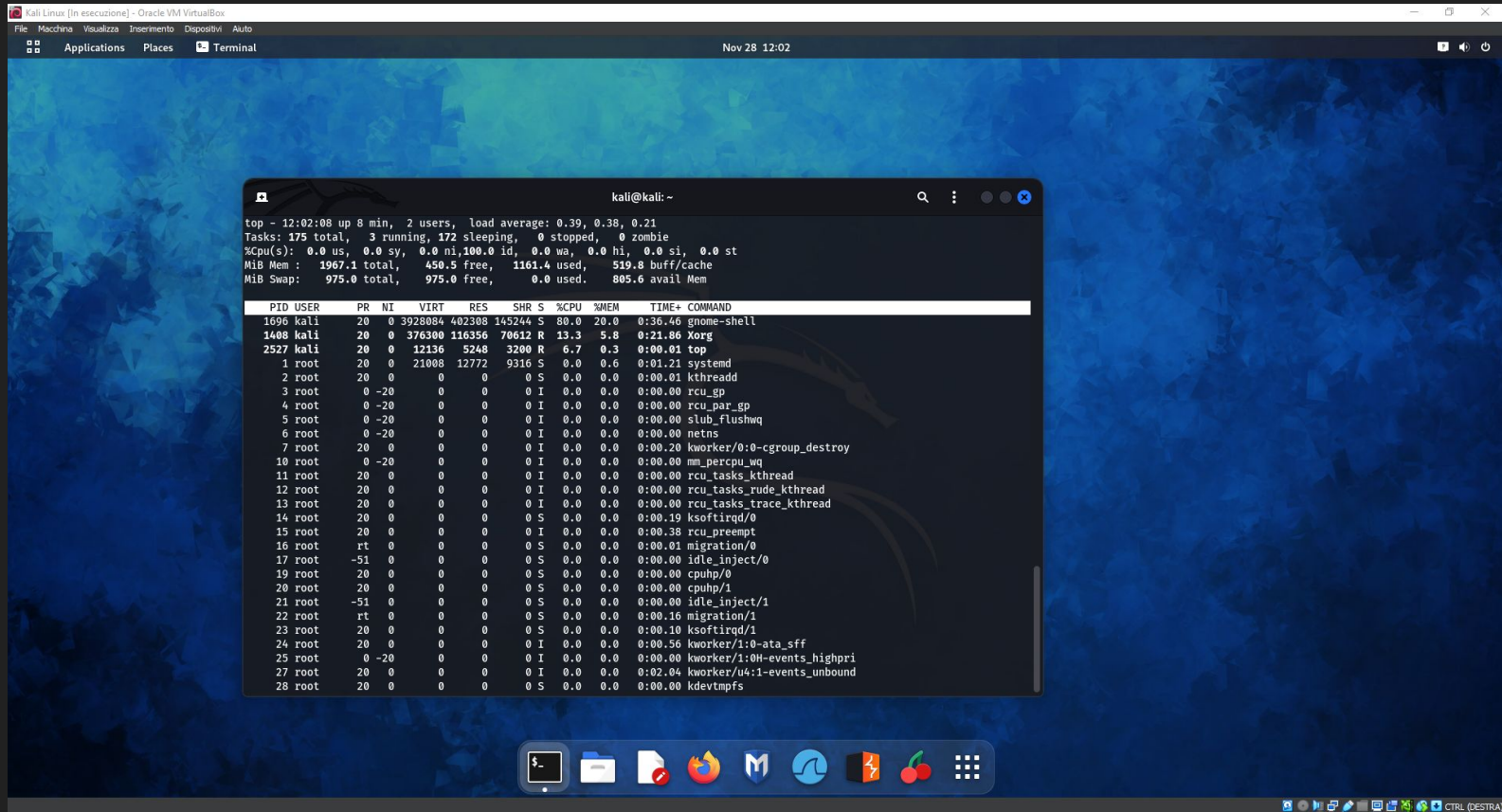


Come da consegna ho digitato il comando “top” all’interno del terminale linux, ottenendo la lista completa dei processi in esecuzione all’interno della macchina.



```
top - 12:02:08 up 8 min, 2 users, load average: 0.30, 0.38, 0.21
Tasks: 175 total, 3 running, 172 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1967.1 total, 450.5 free, 1161.4 used, 519.8 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used, 805.6 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 1696 kali        20   0 3928084 402308 145244 S   80.0  20.0   0:36.46 gnome-shell
 1408 kali        20   0 376300 116356 70612 R   13.3   5.8   0:21.86 Xorg
 2527 kali        20   0 12136  5248  3200 R    6.7   0.3   0:00.01 top
    1 root         20   0 21008 12772  9316 S    0.0   0.6   0:01.21 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 slab_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   0:00.20 kworker/0:0-cgroup_destroy
   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   0:00.19 ksoftirqd/0
   15 root         20   0    0    0    0 I    0.0   0.0   0:00.38 rcu_preempt
   16 root        rt    0    0    0    0 S    0.0   0.0   0:00.01 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   0:00.00 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   0:00.15 migration/1
   23 root         20   0    0    0    0 S    0.0   0.0   0:00.10 ksoftirqd/1
   24 root         20   0    0    0    0 I    0.0   0.0   0:00.56 kworker/1:0-ata_sff
   25 root         0 -20    0    0    0 I    0.0   0.0   0:00.00 kworker/1:0H-events_highpri
   27 root         20   0    0    0    0 I    0.0   0.0   0:02.04 kworker/u4:1-events_unbound
   28 root         20   0    0    0    0 S    0.0   0.0   0:00.00 kdevtmpfs
```

- PID: Process ID, numero identificativo e univoco del processo in esecuzione
- USER: Quale utente ha avviato il processo
- COMMAND:

Kali Linux (in esecuzione) - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Auto

Applications Places Terminal

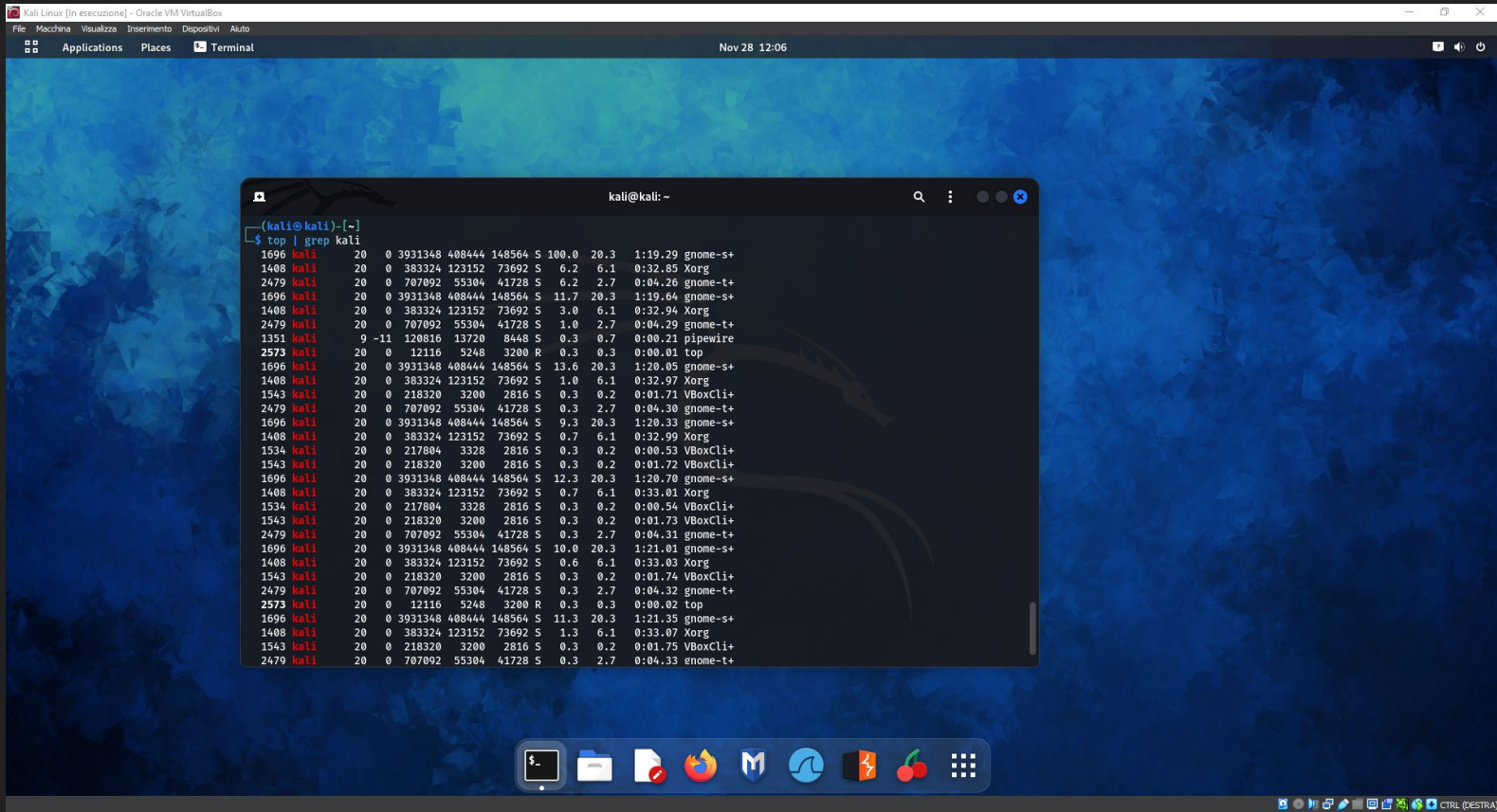
Nov 28 12:04

```
kali@kali: ~  
top - 12:04:01 up 10 min, 2 users, load average: 0.33, 0.34, 0.21  
1 root 20 0 21008 12772 9316 S 0.0 0.6 0:01.21 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 0:00.20 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 0:00.19 ksoftir+  
15 root 20 0 0 0 0 I 0.0 0.0 0:00.40 rcu_pre+  
16 root rt 0 0 0 S 0.0 0.0 0:00.01 migrati+  
25 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/1:0H-events_highpri  
27 root 20 0 0 0 0 I 0.0 0.0 0:02.04 kworker/u4:1-events_unbound  
  
(kali@kali)-[~]  
$ top | grep root  
1 root 20 0 21008 12772 9316 S 0.0 0.6 0:01.21 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 0:00.20 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 0:00.19 ksoftir+  
15 root 20 0 0 0 0 I 0.0 0.0 0:00.39 rcu_pre+  
16 root rt 0 0 0 S 0.0 0.0 0:00.01 migrati+
```

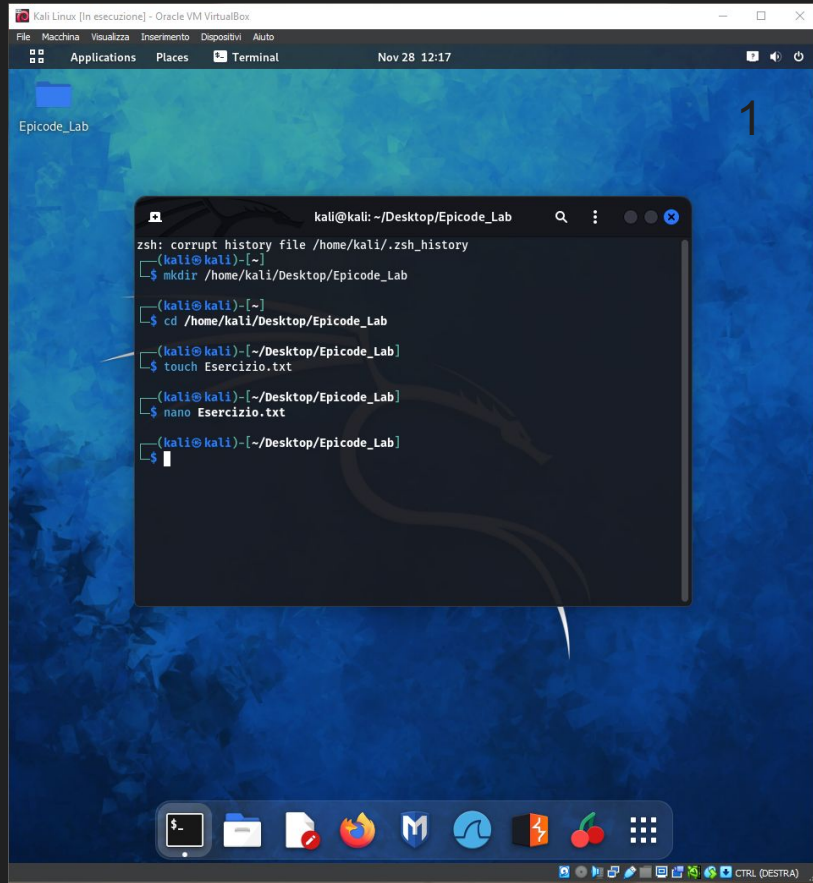
metasploit framework

CTRL (DESTRA)

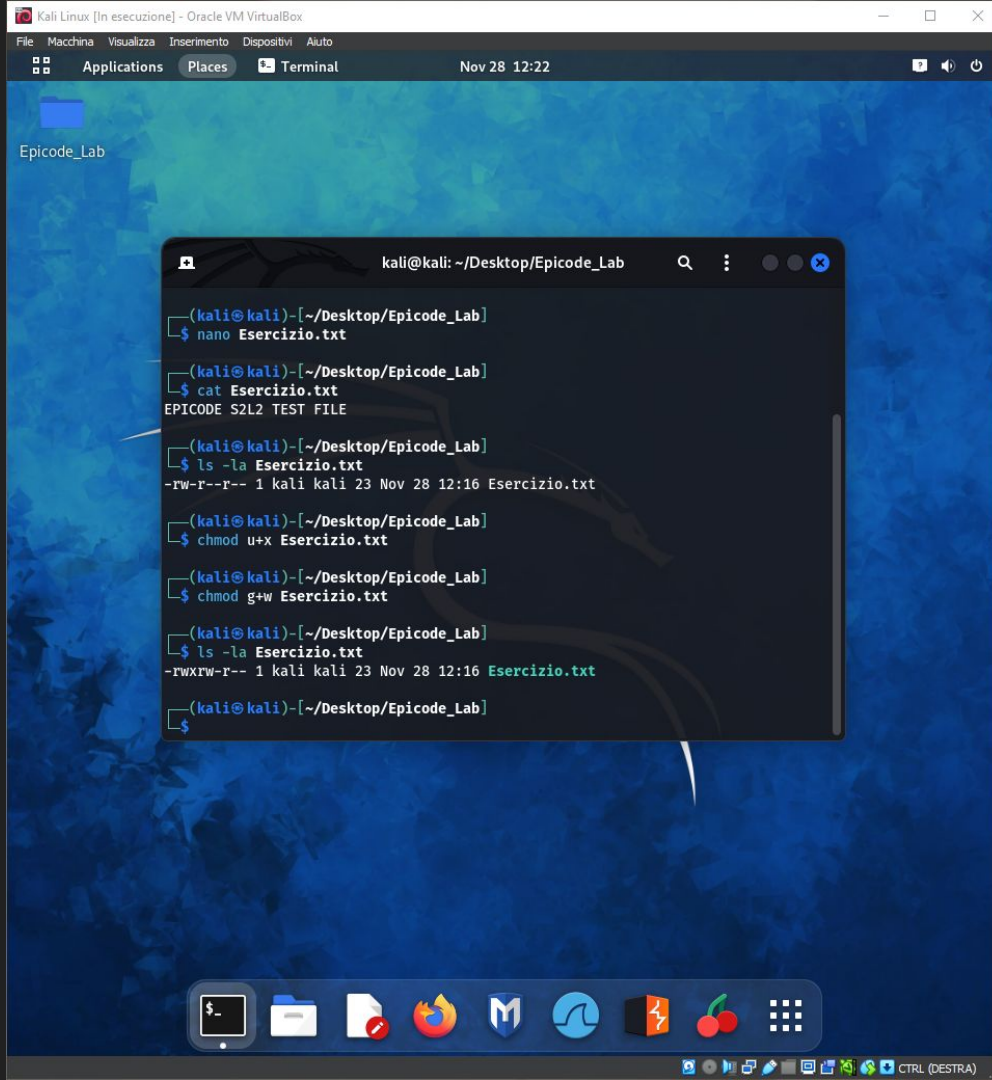
Ho proseguito utilizzando la pipe con il comando `grep (top | grep root)` per filtrare i processi, mostrando solamente quelli creati dall'utente root.



Con la stessa
procedura della
slide precedente
ho filtrato solo i
processi
dell'user kali



Procedo creando la directory `Epicode_Lab` all'interno del desktop, entro nella directory appena aggiunta e creo il file `"Esercizio.txt"` al suo interno. Eseguo il comando `"nano Esercizio.txt"` per aprire il file di testo e modificarlo, come mostrato nella foto 2.



Salvando il file con la combinazione Ctrl+x e in seguito y torno al terminale e eseguendo il comando cat mostro il contenuto del file di testo, che è stato correttamente modificato.

Continuo controllando i permessi del file con il comando “ls -la Esercizio.txt” e procedo a modificarli come chiesto dalla consegna, dando permessi completi all’utente attuale, permessi di scrittura al gruppo e mantenendo sola lettura agli altri utenti

```
kali@kali: ~  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ sudo useradd kali2  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$ sudo passwd kali2  
New password:  
Retype new password:  
passwd: password updated successfully
```

Andiamo a creare un secondo user "kali2" e gli assegnamo una password con i comandi in figura.

```
kali@kali: ~/Desktop/Epicode_Lab
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ /home/kali/Desktop/Epicode_Lab

(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -la Esercizio.txt
-rwxrw-r-- 1 kali kali 23 Nov 28 12:16 Esercizio.txt

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

(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls -la Esercizio.txt
-rwxrw---- 1 kali kali 23 Nov 28 12:16 Esercizio.txt

(kali@kali)-[~/Desktop/Epicode_Lab]
$ sudo mv /home/kali/Desktop/Epicode_Lab/Esercizio.txt /
[sudo] password for kali:

(kali@kali)-[~/Desktop/Epicode_Lab]
$ su kali2
Password:
$ cd /
$ nano Esercizio.txt
```

```
kali@kali: ~/Desktop/Epicode_Lab
GNU nano 7.2 New Buffer

[ Error reading Esercizio.txt: Permission denied ]...

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste       ^J Justify     ^_ Go To Line
```

Seguendo lo stesso procedimento della slide 3 rimuoviamo i permessi di lettura a gli altri utenti, accediamo al user kali2 e proviamo ad accedere al file: come potevamo aspettarci il file non è accessibile da questo user.

Riattiviamo i permessi di lettura per gli altri utenti e testiamo nuovamente con kali2, questa volta il contenuto del file è accessibile ma come si può vedere dal testo evidenziato in rosso non è possibile scrivere all'interno del file.

```
kali@kali: /  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ cd /  
  
(kali@kali)-[/]  
$ chmod o+r Esercizio.txt  
  
(kali@kali)-[/]  
$ ls -la Esercizio.txt  
-rwxrw-r-- 1 kali kali 23 Nov 28 12:16 Esercizio.txt  
  
(kali@kali)-[/]  
$ su kali2  
Password:  
$ cd /  
$ nano Esercizio.txt
```

```
GNU nano 7.2 Esercizio.txt  
EPICODE S2L2 TEST FILE  
  
[ File 'Esercizio.txt' is unwritable ]...  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location  
^X Exit      ^R Read File  ^\ Replace    ^U Paste       ^J Justify    ^_ Go To Line
```




```
(kali@kali)-[~]  
$ sudo userdel -r kali2  
[sudo] password for kali:  
userdel: kali2 mail spool (/var/mail/kali2) not found  
userdel: kali2 home directory (/home/kali2) not found
```

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

```
(kali@kali)-[/]  
$ sudo rm Esercizio.txt
```

Concludiamo ristabilendo la macchina virtuale al suo stato predefinito, cancellando kali2, la directory Epicode_Lab e il file Esercizio.txt