

In questa immagine, abbiamo aperto il shell di Kali Linux sulla nostra virtual machine. Una volta aperta la terminale, possiamo usare il comando <top> per vedere tutti i processi in esecuzione sul sistema, molto simile a il *task manager* di windows.

Questa interfaccia ci da tanta informazione su ogni processo, ma in evidenza ci sono 3

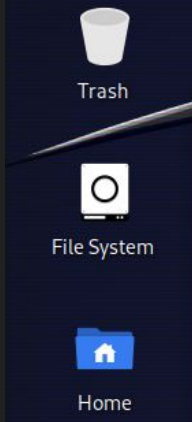
- **PID:** è semplicemente il numero di identificazione del processo.
- **USER:** è il nome del usuario che fa il processo.
- **COMMAND:** Ci indica i comandi che sta ordinando ogni processo, di solito senza interazione diretta dell utente.

kali@kali: ~

File Actions Edit View Help

top - 06:02:32 up 27 min, 2 users, load average: 0.06, 0.03, 0.06
Tasks: 187 total, 1 running, 186 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.6 us, 0.6 sy, 0.0 ni, 98.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3914.5 total, 2864.4 free, 832.8 used, 435.4 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 3081.7 avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
740	root	20	0	388292	122224	53948	S	2.3	3.0	0:07.61	Xorg
1173	kali	20	0	488092	62636	36200	S	1.0	1.6	0:01.62	xfdesktop
7515	kali	20	0	446048	102564	83744	S	1.0	2.6	0:00.89	qterminal
1053	kali	20	0	217968	3072	2816	S	0.7	0.1	0:03.01	VBoxClient
1044	kali	20	0	217452	2944	2688	S	0.3	0.1	0:00.78	VBoxClient
1117	kali	20	0	1461164	110568	77476	S	0.3	2.8	0:03.52	xfwm4
1181	kali	20	0	286812	37880	19072	S	0.3	0.9	0:02.77	panel-13-cpugra
13521	root	20	0	11704	5248	3200	R	0.3	0.1	0:00.12	top
1	root	20	0	20768	12388	9316	S	0.0	0.3	0:01.75	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
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	0:01.54	kworker/u10:0-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	0:00.49	rcu_preempt



Qua siamo ancora in l'interfaccia del processo top, ma aggiungendo << | grep root>> abbiamo filtrato per solo vedere i processi fatti dal user root.

```
kali@kali: ~
File Actions Edit View Help
top - 07:15:00 up 1:39, 1 user, load average: 0.01, 0.04, 0.00
740 root 20 0 399288 133200 53948 S 0.3 3.3 0:25.06 Xorg
336 root 20 0 49852 15664 14640 S 0.3 0.4 0:00.58 systemd+
740 root 20 0 399288 133200 53948 S 0.3 3.3 0:25.07 Xorg
657 root 20 0 358516 3204 2944 S 0.3 0.1 0:00.89 VBoxSer+
740 root 20 0 399288 133200 53948 S 0.3 3.3 0:25.08 Xorg
740 root 20 0 399288 133200 53948 S 0.3 3.3 0:25.09 Xorg
740 root 20 0 399288 133200 53948 S 0.7 3.3 0:25.11 Xorg
740 root 20 0 399288 133200 53948 S 3.3 3.3 0:25.21 Xorg
1 root 20 0 20908 12388 9316 S 0.0 0.3 0:01.98 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
8 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker+
10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_perc+
$ top | grep root
740 root 20 0 399288 133200 53948 S 6.2 3.3 0:24.69 Xorg
1448 root 20 0 470924 17756 11452 S 6.2 0.4 0:00.19 udisksd
1 root 20 0 20908 12388 9316 S 0.0 0.3 0:01.98 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
8 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 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 0:00.05 ksoftir+
```



Trash



File System



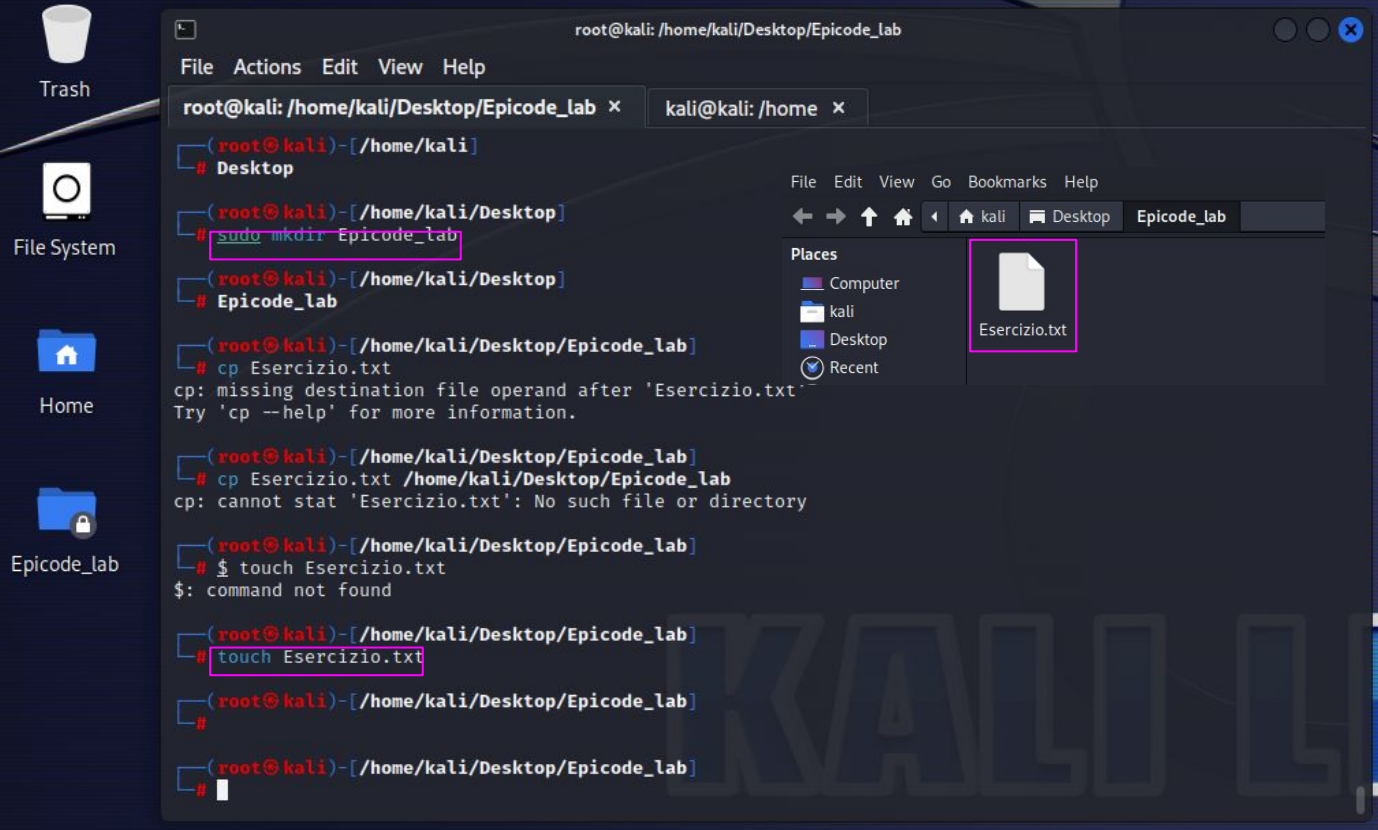
Home

Qua abbiamo fatto lo stesso processo della slide scorsa, ma invece scrivere *root*, abbiamo scritto *kali*, per vedere i processi che fa *kali*,

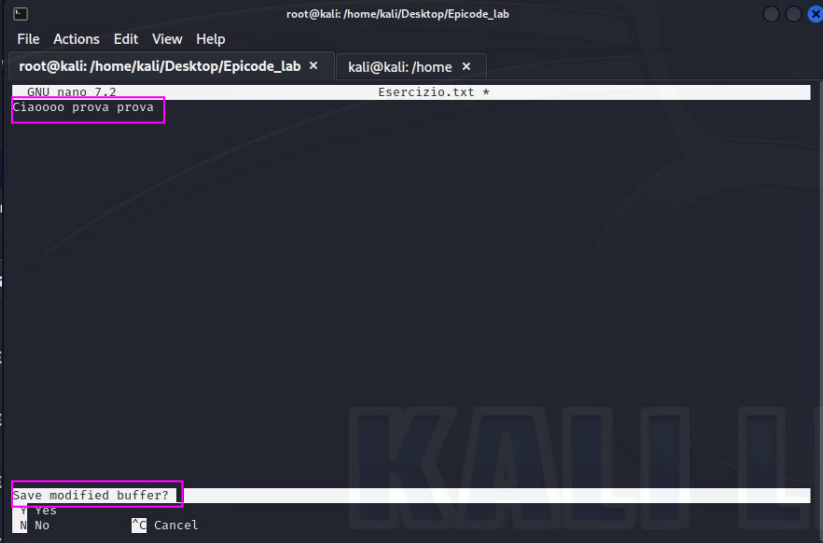
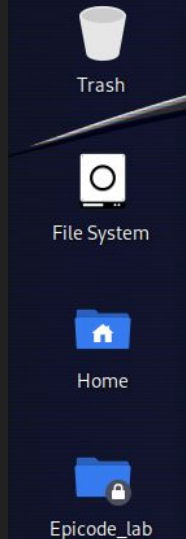
kali@kali: ~											
File	Actions	Edit	View	Help							
1053	kali	20	0	217968	3072	2816	S	0.3	0.1	0:11.67	VBoxCli+
51942	kali	20	0	11688	5248	3200	R	0.3	0.1	0:00.16	top
1117	kali	20	0	1461164	110568	77476	S	0.3	2.8	0:11.95	xfwm4
1181	kali	20	0	286812	38264	19072	S	0.3	1.0	0:10.44	panel-1+
1183	kali	20	0	423676	28060	20820	S	0.3	0.7	0:12.25	panel-1+
7515	kali	20	0	446180	102564	83616	S	0.3	2.6	0:12.31	qtermin+
1053	kali	20	0	217968	3072	2816	S	0.3	0.1	0:11.68	VBoxCli+
1117	kali	20	0	1461164	110568	77476	S	0.3	2.8	0:11.96	xfwm4
1181	kali	20	0	286812	38264	19072	S	0.3	1.0	0:10.45	panel-1+
51942	kali	20	0	11688	5248	3200	R	0.3	0.1	0:00.17	top
1044	kali	20	0	217452	2944	2688	S	0.3	0.1	0:03.12	VBoxCli+
1053	kali	20	0	217968	3072	2816	S	0.3	0.1	0:11.69	VBoxCli+
1152	kali	20	0	305084	29628	19924	S	0.3	0.7	0:01.04	xfsetti+
1183	kali	20	0	423676	28060	20820	S	0.3	0.7	0:12.26	panel-1+
51942	kali	20	0	11688	5248	3200	R	0.7	0.1	0:00.19	top
1117	kali	20	0	1461164	110568	77476	S	0.3	2.8	0:11.97	xfwm4
1183	kali	20	0	423676	28060	20820	S	0.3	0.7	0:12.27	panel-1+
7515	kali	20	0	446180	102564	83616	S	0.3	2.6	0:12.32	qtermin+
1053	kali	20	0	217968	3072	2816	S	0.3	0.1	0:11.70	VBoxCli+
1117	kali	20	0	1461164	110568	77476	S	0.3	2.8	0:11.98	xfwm4
1181	kali	20	0	286812	38264	19072	S	0.3	1.0	0:10.46	panel-1+
1183	kali	20	0	423676	28060	20820	S	0.3	0.7	0:12.28	panel-1+
51942	kali	20	0	11688	5248	3200	R	0.3	0.1	0:00.20	top
1053	kali	20	0	217968	3072	2816	S	0.3	0.1	0:11.71	VBoxCli+
1117	kali	20	0	1461164	110568	77476	S	0.3	2.8	0:11.99	xfwm4
1183	kali	20	0	423676	28060	20820	S	0.7	0.7	0:12.30	panel-1+
1053	kali	20	0	217968	3072	2816	S	0.3	0.1	0:11.72	VBoxCli+
1117	kali	20	0	1461164	110568	77476	S	0.3	2.8	0:12.00	xfwm4
1181	kali	20	0	286812	38264	19072	S	0.3	1.0	0:10.47	panel-1+
7515	kali	20	0	446180	102564	83616	S	0.3	2.6	0:12.33	qtermin+
51942	kali	20	0	11688	5248	3200	R	0.3	0.1	0:00.21	top

Qua abbiamo fatto 2 cose nei comandi segnalati. Prima abbiamo creato un directory chiamato *Epicode_lab* nel directory di Desktop, usando il comando *mkdir*, infatti si può vedere questo directory nel UI del desktop di linux.

Poi abbiamo creato dentro la cartella di *Epicode_lab* il file *Esercizio.txt* usando il comando *touch*.



Sapendo che il file è lì, possiamo usare il comando *nano* per editare i suoi contenuti, in questo caso ho scritto un messaggio molto simpatico. Una volta scritto il messaggio, facciamo «ctrl+x» e successivamente «y».



Abbiamo fatto molte in questa screenshot. Prima abbiamo usato il comando `cat` prima di inserire il nome del file/directory per vedere i contenuti, in questo caso mio messaggio molto simpatico.

Poi abbiamo usato il comando `ls -la` per vedere i privilegi dell'utente attuale, i gruppi e altri utenti, rappresentati come u/g/o. Vediamo che per nostro obiettivo all'utente attuale manca il permesso di esecuzione (x), e al gruppo manda il permesso di scrivere (w).

Con il comando `chmod` eseguito della lettera rappresentate del usuario, possiamo aggiungere (o in un'altro caso rimuovere) dei permessi.

Qui abbiamo scritto `u+x` per dare al usuario attuale (u) il permesso di eseguire.

Finalmente facciamo un comando `ls -la` ancora per controllare in nuovi permessi

```
root@kali: /home/kali/Desktop/Epicode_lab

File Actions Edit View Help

root@kali: /home/kali/Desktop/Epicode_lab x  kali@kali: /home x

(root@kali)-[/home/kali/Desktop/Epicode_lab]
# sudo nano Esercizio.txt

(root@kali)-[/home/kali/Desktop/Epicode_lab]
# cat Esercizio.txt
Ciaooooo prova prova

(root@kali)-[/home/kali/Desktop/Epicode_lab]
# ls -la
total 12
drwxr-xr-x 2 root root 4096 Nov 28 08:07 .
drwxr-xr-x 3 kali kali 4096 Nov 28 07:48 ..
-rw-r--r-- 1 root root  21 Nov 28 08:07 Esercizio.txt

(root@kali)-[/home/kali/Desktop/Epicode_lab]
# ls -la Esercizio.txt
-rw-r--r-- 1 root root 21 Nov 28 08:07 Esercizio.txt

(root@kali)-[/home/kali/Desktop/Epicode_lab]
# chmod u+x Esercizio.txt

(root@kali)-[/home/kali/Desktop/Epicode_lab]
# chmod g+w Esercizio.txt

(root@kali)-[/home/kali/Desktop/Epicode_lab]
# ls -la Esercizio.txt
-rwxrw-r-- 1 root root 21 Nov 28 08:07 Esercizio.txt

(root@kali)-[/home/kali/Desktop/Epicode_lab]
#
```

Ora vogliamo aggiungere un utente nuovo e una password nuova, quindi scriviamo ***sudo useradd*** e dopo il nome del nostro nuovo utente.

Ora dobbiamo dargli sua password. Penso si poteva fare insieme a la creazione dell'utente, ma non sono riuscito. Non é molto problema perché scrivendo ancora ***sudo***, abbiamo i poteri di amministratore, e con questi possiamo scrivere il comando ***passwd*** per poter modificare la password.

```
(kali㉿kali)-[~]  
$ sudo useradd epicgamer123  
[sudo] password for kali:
```

```
(kali㉿kali)-[~]  
$ sudo passwd epicgamer123  
New password:  
Retype new password:  
passwd: password updated successfully
```



Trash



File System



Home



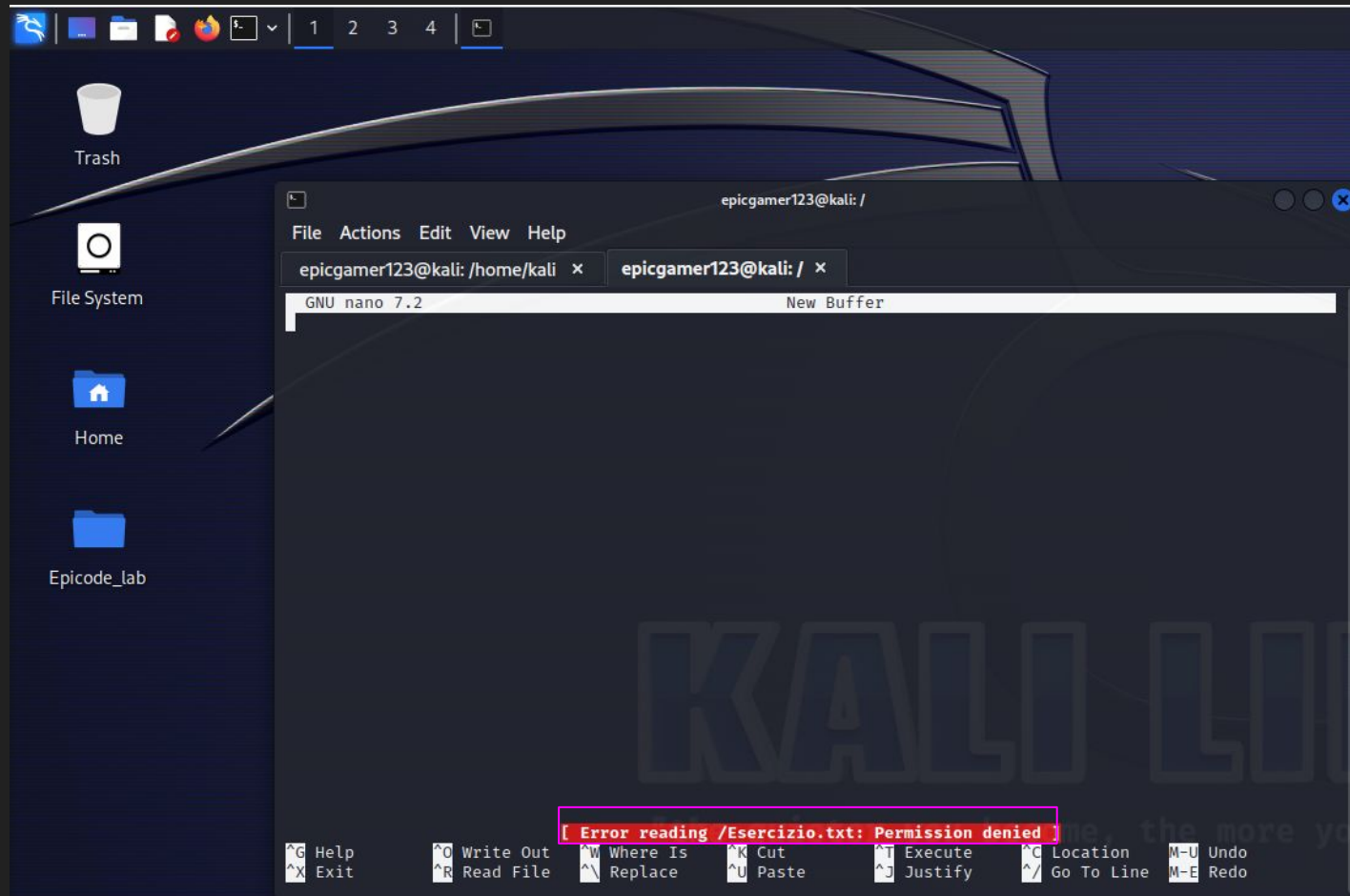
Epicode_lab

Ora vogliamo vedere cosa succede se rimuoviamo il permesso di leggere a questo nuovo utente. Vediamo le conseguenze nella seguente slide.

Dopo vogliamo spostare il file `Esercizio.txt` sul directory root (/) usando il comando `mv`

```
kali@kali: ~/Desktop/Epicode_lab
File Actions Edit View Help
epicgamer123@kali: /home/kali x kali@kali: ~/Desktop/Epicode_lab x
(kali@kali)-[~]
$ Desktop
(kali@kali)-[~/Desktop]
$ Epicode_lab
(kali@kali)-[~/Desktop/Epicode_lab]
$ sudo chmod o-r Esercizio.txt
[sudo] password for kali:
(kali@kali)-[~/Desktop/Epicode_lab]
$ sudo mv /home/kali/Desktop/Epicode_lab/Esercizio.txt /
(kali@kali)-[~/Desktop/Epicode_lab]
$
```

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



Ora non possiamo
leggere i contenuti
del file Esercizio.txt

Ma é un pó cattivo
lasciare a
epicgamer123 senza il
permesso di leggere,
quindi si lo diamo di
nuovo. E infatti, ora
lo possiamo leggere

```
kali@kali: /  
File Actions Edit View Help  
epicgamer123@kali: /home/kali x epicgamer123@kali: / x kali@kali: / x  
(kali@kali)-[~]  
$ cd /  
(kali@kali)-[/]  
$ sudo chmod o+r Esercizio.txt  
[sudo] password for kali:  
(kali@kali)-[/]  
$
```

```
epicgamer123@kali: /  
File Actions Edit View Help  
epicgamer123@kali: /home/kali x epicgamer123@kali: / x kali@kali: / x  
GNU nano 7.2 /Esercizio.txt  
Ciaoooo prova prova
```

Non mi piace più niente di questa nuova roba, quindi cancelliamo tutto.

Con il comando `rm` eseguito da il nome di un file, riusciamo a eliminarlo.

Con il comando `rmdir` possiamo eliminare un directory

E con il comando `deluser` possiamo dire ciao a epicgamer123 :(

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[/]
$ rm Esercizio.txt
rm: remove write-protected regular file 'Esercizio.txt'?
(kali@kali)-[/]
$ cd /home/kali/Desktop
cd: no such file or directory: /home/kali/Desktop
(kali@kali)-[/]
$ cd /home/kali/Desktop
(kali@kali)-[~/Desktop]
$ ls
Epicode_lab
(kali@kali)-[~/Desktop]
$ rmdir Epicode_lab
(kali@kali)-[~/Desktop]
$ sudo deluser epicgamer123
info: Removing crontab ...
info: Removing user 'epicgamer123' ...
userdel: user epicgamer123 is currently used by process 3821
fatal: '/usr/sbin/userdel epicgamer123' returned error code 8. Exiting.
(kali@kali)-[~/Desktop]
$ sudo deluser epicgamer123
info: Removing crontab ...
info: Removing user 'epicgamer123' ...
(kali@kali)-[~/Desktop]
```

Thanks
for
watching!