

A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. They are set against a dark blue background with faint, lighter blue diagonal stripes.

consegna S2/L2

per prima cosa andiamo ad usare il comando “top” per controllare quale sia il PID(process identification) lo user (ovvero kali in questo caso) che sta usando suddetto processo ed il comando usato “top” nel nostro caso.

lo eseguiamo sia per root che kali

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1227	kali	20	0	14656	3948	1536	S	0.0	0.2	0:00.02	xcap
1235	kali	20	0	307700	10384	5760	S	0.0	0.5	0:00.00	gvfs-mtp+
1249	kali	20	0	633732	48900	37832	S	0.0	2.4	0:00.07	nm-applet
1262	kali	20	0	459924	10608	7552	S	0.0	0.5	0:00.00	gvfsd-tr+
1273	kali	20	0	234192	8088	5504	S	0.0	0.4	0:00.00	gvfsd-me+
1274	kali	20	0	309692	8704	7296	S	0.0	0.4	0:00.02	xiccd
1279	kali	20	0	230212	5376	4992	S	0.0	0.3	0:00.00	dconf-se+
1280	kali	20	0	381968	8192	5632	S	0.0	0.4	0:00.00	agent
1303	colord	20	0	316872	15212	9688	S	0.0	0.8	0:00.07	colord
1390	kali	20	0	48888	7936	7296	S	0.0	0.4	0:00.00	obexd
4102	root	20	0	0	0	0	I	0.0	0.0	0:00.00	kworker/+
6330	kali	20	0	307460	8184	5632	S	0.0	0.4	0:00.00	xfconfd
6400	root	20	0	0	0	0	I	0.0	0.0	0:00.00	kworker/+
6990	kali	20	0	445888	102168	83340	S	0.0	5.1	0:00.72	qterminal
6993	kali	20	0	10488	5996	3968	S	0.0	0.3	0:00.04	zsh
7068	kali	20	0	12124	5248	3200	R	0.0	0.3	0:01.08	top

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ top | grep root  
d 1 root 20 0 20788 12624 9424 S 0.0 0.6 0:00.55 system  
dd 2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthrea  
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_pa  
top - 15:44:48 up 7 min, 1 user, load average: 0.00, 0.11, 0.08  
587 root 20 0 447976 124108 62184 S 0.8 6.2 0:03.82 Xorg  
1 root 20 0 20788 12624 9424 S 0.0 0.6 0:00.55 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+  
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 0:00.04 kworker+  
9 root 20 0 0 0 0 I 0.0 0.0 0:00.40 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 0:00.15 ksoftir+  
15 root 20 0 0 0 0 I 0.0 0.0 0:00.12 rcu_pre+  
16 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migrati+  
19 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/0
```

ora creiamo una directory col comando “mkdir” chiamata Epicode_Lab dove poi ci spostiamo dentro con “cd” per poi inserire un file di nome Esercizio.txt nel quale andiamo a scrivere qualcosa e lo salviamo

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ mkdir /home/kali/Desktop/Epicode_Lab
```

```
kali@kali: ~/Desktop/Epicode_Lab
File Actions Edit View Help
GNU nano 7.2 New Buffer *
Hello world
```

KALI

Welcome to nano. For basic help, type Ctrl+G.

Help	Write Out	Where Is	Cut	Execute
Exit	Read File	Replace	Paste	Justify

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

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

```
kali@kali: ~/Desktop/Epicode_Lab
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ mkdir /home/kali/Desktop/Epicode_Lab

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

(kali@kali)-[~/Desktop/Epicode_Lab]
$ sudo nano Esercitazione.txt
```

utilizziamo il comando “cat” per vedere cosa c’è scritto dentro al file. poi controlliamo i privilegi tramite “ls -la” cambiamo poi i privilegi per tutti gli utenti. Creiamo un nuovo utente con password

```
(kali㉿kali)-[~/Desktop]
$ sudo useradd Army

(kali㉿kali)-[~/Desktop]
$ sudo passwd Army
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~/Desktop]
$
```

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ cat Esercizio.txt
Hello world
```

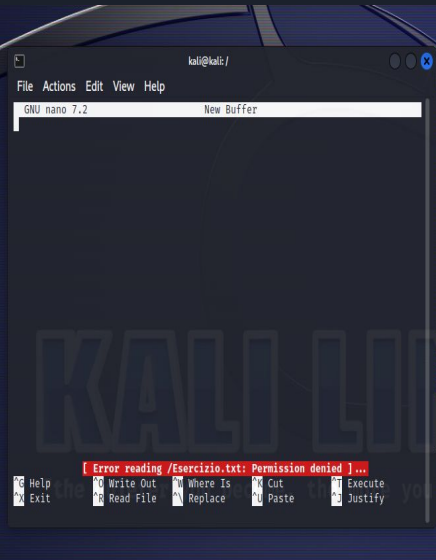
```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ sudo chmod u+x Esercizio.txt

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 15:47 .
drwxr-xr-x 3 kali kali 4096 Nov 28 15:40 ..
-rwxrwr-- 1 root root  12 Nov 28 15:47 Esercizio.txt

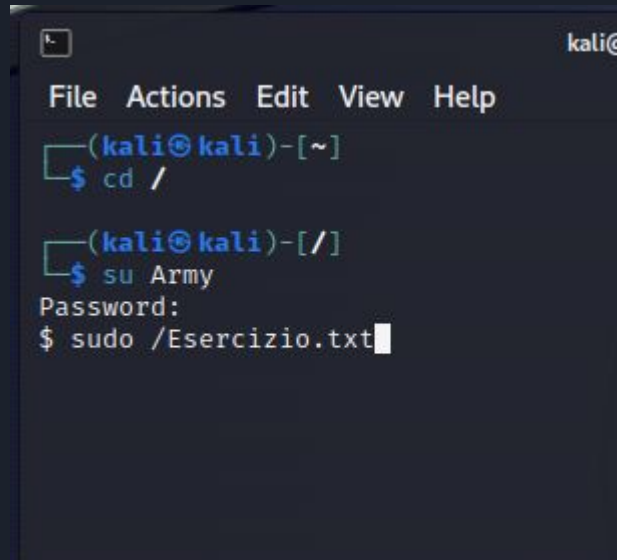
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$
```

spostiamo il file nella cartella root e cambiamo poi user ed apriamo il file per leggerlo, noteremo che ci apparirà un errore in quanto non abbiamo i privilegi



```
kali@kali: /
File Actions Edit View Help
GNU nano 7.2 New Buffer

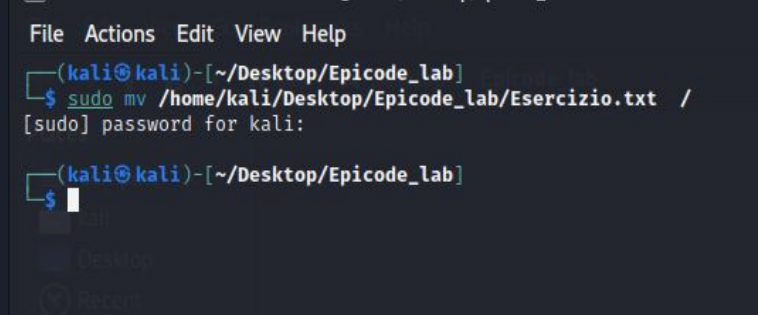
[Error reading /Esercizio.txt: Permission denied]...
Help Write Out Where Is Cut Execute
Exit Read File Replace Paste Justify
```



```
kali@
File Actions Edit View Help

(kali@kali)-[~]
$ cd /

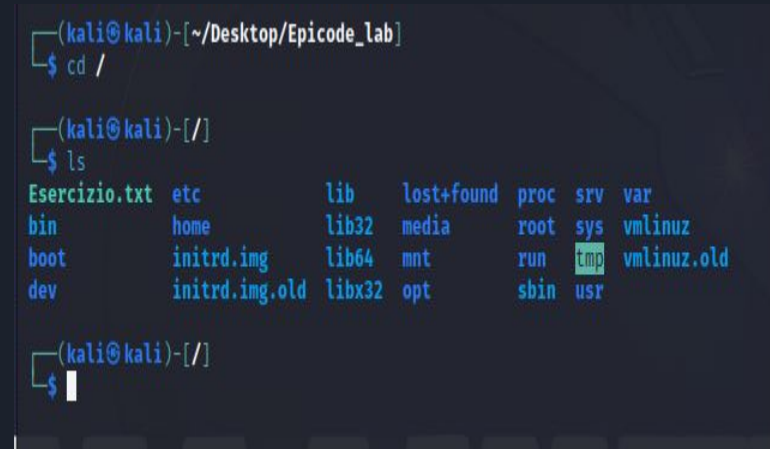
(kali@kali)-[/]
$ su Army
Password:
$ sudo /Esercizio.txt
```



```
File Actions Edit View Help

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

(kali@kali)-[~/Desktop/Epicode_lab]
$
```



```
(kali@kali)-[~/Desktop/Epicode_lab]
$ cd /

(kali@kali)-[/]
$ ls
Esercizio.txt  etc          lib          lost+found  proc  srv  var
bin            home         lib32        media       root  sys  vmlinuz
boot          initrd.img   lib64        mnt         run   tmp  vmlinuz.old
dev          initrd.img.old  libx32       opt         sbin  usr
```

diamo al nuovo utente solo il privilegio di leggere
apriamo poi il file sul nuovo utente e vediamo che ora
possiamo solo leggere il file senza poter fare altro.
Infine eliminiamo il file col comando “rm” la directory con
“rmdir” e per finire il nuovo user con “userdel”

```
(kali@kali)-[/]  
$ sudo chmod o+r /Esercizio.txt  
[sudo] password for kali:
```

```
(kali@kali)-[/]  
$ ls -la  
total 84  
drwxr-xr-x 19 root root 4096 Nov 28 16:26 .  
drwxr-xr-x 19 root root 4096 Nov 28 16:26 ..  
drwx----- 2 root root 4096 Nov 28 15:31 .cache  
-rwxrwxr-- 1 root root 12 Nov 28 15:47 Esercizio.txt  
1 rwxrwxrwx 1 root root 7 Nov 28 15:33 file - user/kali
```

```
(kali@kali)-[/Desktop]  
$ sudo deluser Army  
[sudo] password for kali:  
info: Removing crontab ...  
info: Removing user `Army' ...  
  
(kali@kali)-[/Desktop]  
$
```

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

```
(kali@kali)-[/]  
$ cd /home/kali/Desktop
```

```
(kali@kali)-[/Desktop]  
$ sudo rmdir Epicode_lab
```

