




# Consegna S2/L2 CyberSecurity

Riccardo Agostino Monti



Come richiesto dall'esercizio analizziamo i processi attivi ed in pausa, controllando anche i campi PID, Utente e Command:

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
741	root	20	0	462604	138432	63408	S	2.0	3.5	0:03.23	Xorg
1489	kali	20	0	448956	104968	85692	S	1.3	2.6	0:01.31	qterminal
993	kali	20	0	218320	3072	2688	S	0.3	0.1	0:00.14	VBoxClient
<b>1633</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>12172</b>	<b>5248</b>	<b>3072</b>	<b>R</b>	<b>0.3</b>	<b>0.1</b>	<b>0:00.09</b>	<b>top</b>
1	root	20	0	20940	12616	9288	S	0.0	0.3	0:00.77	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd

Il PID indica l'identificativo del processo, nel nostro caso 1633;

User è colui che sta eseguendo il processo

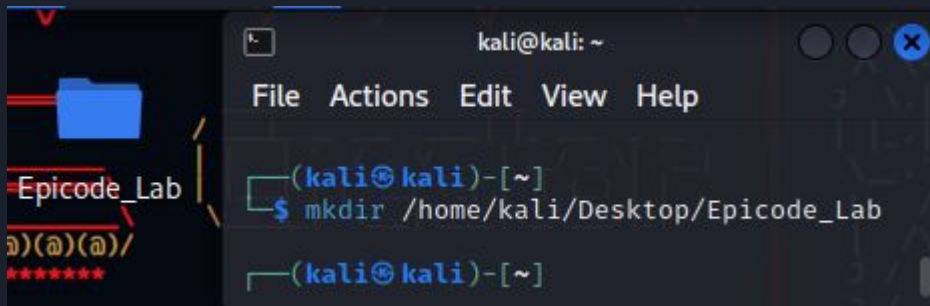
Command è il comando eseguito dal processo

Fatto ciò possiamo filtrare i processi prima con l'user root e poi kali

```
(kali㉿kali)-[~]  
$ top | grep root  
1 root      20   0   20940  12616   9288 S   0.0   0.3   0:00.77 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  
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   0:00.04 ksoftir+  
15 root     20   0       0      0      0 I   0.0   0.0   0:00.07 rcu_pre+
```

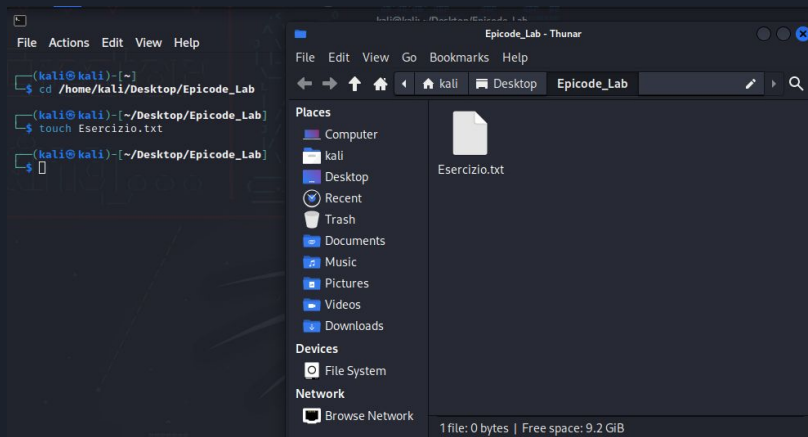
```
kali@kali: ~  
File Actions Edit View Help  
(kali㉿kali)-[~]  
$ top | grep kali  
4870 kali    20   0  449108 105232 86120 S   1.0   2.6   0:00.25 qtermin+  
1047 kali    20   0 1020216 105504 77360 S   0.5   2.6   0:01.44 xfwm4  
1107 kali    20   0  568208 80700  43928 S   0.2   2.0   0:01.61 xfdesk+  
4870 kali    20   0  449108 105232 86120 S   2.4   2.6   0:00.28 qtermin+  
4870 kali    20   0  449108 105232 86120 S   1.2   2.6   0:00.32 qtermin+  
993 kali     20   0  218320   3072   2688 S   0.3   0.1   0:00.59 VBoxCli+  
1115 kali    20   0  278000  27264  18816 S   0.3   0.7   0:00.72 panel-1+  
1117 kali    20   0  432292  30060  20776 S   0.3   0.7   0:00.72 panel-1+  
5074 kali    20   0   12116   5120   3072 R   0.3   0.1   0:00.01 top  
5163 kali    20   0  539948  43748  35296 S   5.6   1.1   0:00.17 xfce4-t+  
1047 kali    20   0 1020216 105504 77360 S   1.3   2.6   0:01.48 xfwm4  
1096 kali    20   0  541796  48012  35408 S   0.7   1.2   0:00.56 xfce4-p+  
985 kali     20   0  217804   3072   2688 S   0.3   0.1   0:00.19 VBoxCli+  
1077 kali    20   0  305508  29728  19980 S   0.3   0.7   0:00.22 xfsetti+  
4870 kali    20   0  449108 105232 86120 S   0.3   2.6   0:00.33 qtermin+  
1047 kali    20   0 1020216 105504 77360 S   0.7   2.6   0:01.50 xfwm4  
4870 kali    20   0  449108 105232 86120 S   0.7   2.6   0:00.35 qtermin+  
1117 kali    20   0  432292  30060  20776 S   0.3   0.7   0:00.73 panel-1+  
1119 kali    20   0  472944  42600  32356 S   0.3   1.1   0:00.18 panel-1+  
993 kali     20   0  218320   3072   2688 S   0.3   0.1   0:00.60 VBoxCli+  
1115 kali    20   0  278000  27264  18816 S   0.3   0.7   0:00.73 panel-1+
```

Dopodiché andiamo a creare la cartella e spostiamoci al suo interno:

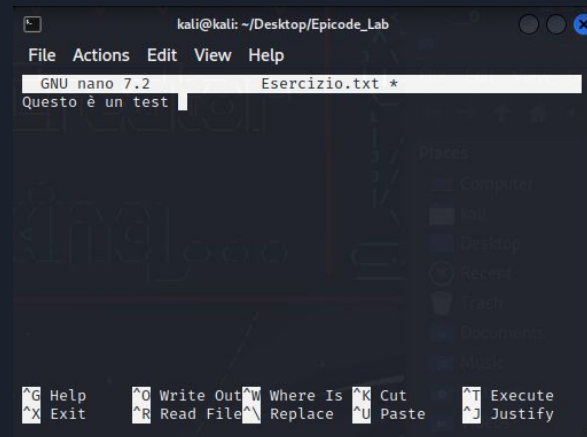


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ mkdir /home/kali/Desktop/Epicode_Lab  
(kali@kali)-[~]
```

Adesso creiamo il file Esercizio.txt e modifichiamolo nel seguente modo:



```
(kali@kali)-[~]  
$ cd /home/kali/Desktop/Epicode_Lab  
(kali@kali)-[~/Desktop/Epicode_Lab]  
$ touch Esercizio.txt  
(kali@kali)-[~/Desktop/Epicode_Lab]  
$
```



```
kali@kali: ~/Desktop/Epicode_Lab  
File Actions Edit View Help  
GNU nano 7.2 Esercizio.txt *  
Questo è un test
```

A questo punto utilizziamo il comando cat per visualizzare il messaggio:

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ cat Esercizio.txt
Questo è un test

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

Adesso controlliamo i permessi e modifichiamoli come richiesto da consegna

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 12:13 .
drwxr-xr-x 3 kali kali 4096 Nov 28 12:08 ..
-rw-r--r-- 1 kali kali  19 Nov 28 12:13 Esercizio.txt

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ sudo chmod 764 Esercizio.txt
[sudo] password for kali:

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 12:13 .
drwxr-xr-x 3 kali kali 4096 Nov 28 12:08 ..
-rwxrw-r-- 1 kali kali  19 Nov 28 12:13 Esercizio.txt

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

Adesso creiamo un nuovo utente e impostiamo la password:

```
(kali㉿kali)-[~/Scrivania/Epicode_Lab]
$ sudo useradd kali2

(kali㉿kali)-[~/Scrivania/Epicode_Lab]
$ sudo passwd kali2
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
```

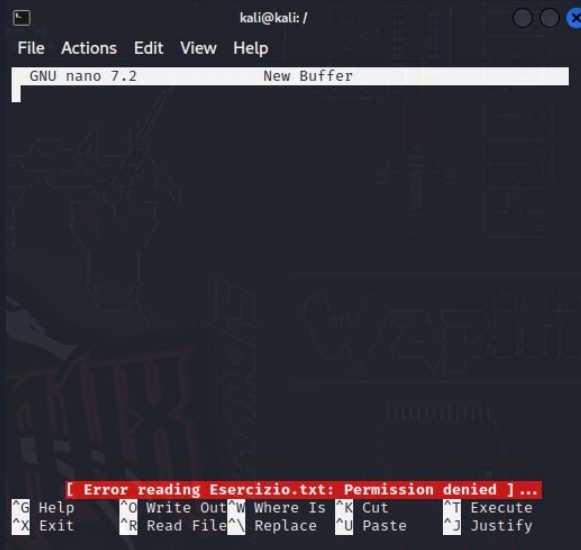
Modifichiamo nuovamente i privilegi in modo da togliere i permessi di lettura agli utenti “others”:

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 28 12:13 .
drwxr-xr-x 3 kali kali 4096 Nov 28 12:08 ..
-rwxrwx--- 1 kali kali 19 Nov 28 12:13 Esercizio.txt
```

E cambiamo l'utente.

```
(kali㉿kali)-[/]
$ su kali2
Password:
```

Adesso ci spostiamo con “ cd / ” nella cartella root e proviamo ad aprire il file:



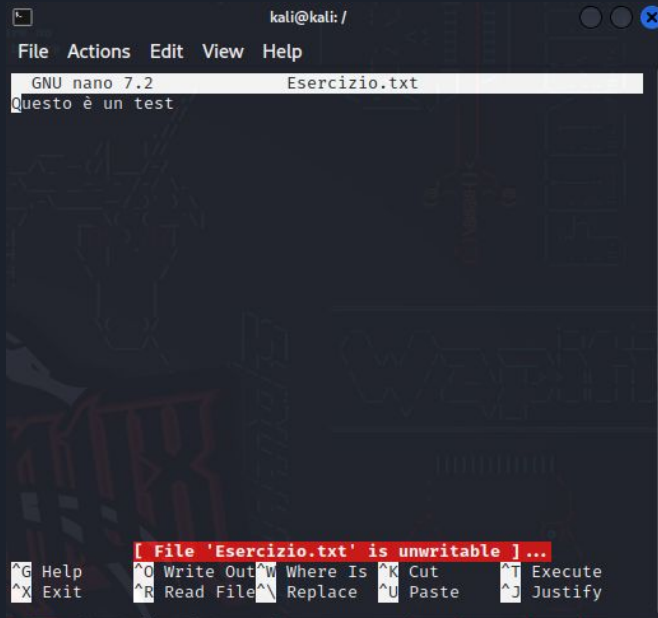
The screenshot shows a terminal window titled 'kali@kali: /'. The window contains the nano text editor interface. At the top, there is a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, a status bar indicates 'GNU nano 7.2' and 'New Buffer'. The main area of the terminal is dark with some faint, stylized text. At the bottom, a red error message is displayed: '[ Error reading Esercizio.txt: Permission denied ] ...'. Below the error message, there is a list of keyboard shortcuts: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^X Exit, ^R Read File, ^\ Replace, ^U Paste, and ^J Justify.

Come notiamo ci viene negato il permesso di leggere il file.

A questo punto cambiamo nuovamente i permessi in modo tale che gli utenti "others" riescano a leggere il file


```
(kali㉿kali)-[/]  
$ ls -la /Esercizio.txt  
-rwxrw-r-- 1 kali kali 19 Nov 28 12:13 /Esercizio.txt
```

E adesso proviamo nuovamente ad aprire il file, questo è il risultato:



```
kali@kali: /  
File Actions Edit View Help  
GNU nano 7.2 Esercizio.txt  
Questo è un test  
  
[ File 'Esercizio.txt' is unwritable ] ...  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute  
^X Exit ^R Read File ^_ Replace ^U Paste ^J Justify
```





A questo punto concludiamo eliminando il file, la directory e l'utente creato.

```
(kali㉿kali)-[/]  
$ sudo rm /Esercizio.txt  
  
(kali㉿kali)-[/]  
$ sudo rm -r /home/kali/Desktop/Epicode_Lab  
  
(kali㉿kali)-[/]  
$ sudo userdel -r kali2
```