

## FAMILIARIZZAZIONE CON LA SHELL LINUX

La traccia dell'esercizio di oggi è la seguente:

Nell'esercizio di oggi familiarizzeremo con i comandi da shell Linux. Pertanto, si richiede allo studente di:

- ☐ Controllare i processi attivi sulla macchina Linux con il comando «top» e descrivere il significato delle colonne: l) PID, USER, COMMAND;
- ☐ Filtrare i risultati del comando top inviando l'output al comando grep (utilizzare la pipe «|» per mostrare solo i programmi in esecuzione per l'utente «root»)
- ☐ Ripetere il punto 2, filtrando i risultati per mostrare solamente i processi in esecuzione dall'utente kali
- ☐ Creare una nuova directory chiamata «Epicode\_Lab» nella seguente directory /home/kali/Desktop
- ☐ Spostarsi nella directory appena creata e creare il file «Esercizio.txt»
- ☐ Modificare il file con l'editor di testo «nano», e salvarlo. Per salvare il file utilizzate la sequenza «ctrl+x» e successivamente «y», come mostrato in figura sotto.
- ☐ Utilizzare il comando «cat» per leggere a schermo il file.txt appena modificato
- ☐ Controllare i permessi del file con il comando ls -la
- ☐ Modificare i privilegi del file in modo tale che l'utente corrente abbia tutti i privilegi (r,w,x), il gruppo (r,w), gli altri utenti solo lettura (r)
- ☐ Creare un nuovo utente, chiamatelo pure come volete. Utilizzate il comando «useradd» per creare un utente e «passwd» seguita dal nome dell'utente per assegnare una password.
- ☐ Con l'utente attuale cambiate i privilegi del file .txt creato in precedenza in modo tale che «altri utenti» non siano abilitati alla lettura
- ☐ Spostate il file nella directory di root (/)
- ☐ Cambiate utente con il comando «su» seguito dal nome dell'utente che volete utilizzare
- ☐ Provate ad aprire in lettura il file.txt creato in precedenza con il comando nano, che errore ricevete?
- ☐ Modificate i permessi del file per far in modo che il vostro nuovo utente possa leggerlo e ripetete gli ultimi 2 step.
- ☐ Rimuovete il file, la cartelle e l'utente che avete creato, riportando lo scenario allo stato iniziale.

Dopo aver aperto il terminale, il primo comando che ho lanciato è stato “top”, come descritto nella traccia e ho ottenuto ciò:

PID	USER	PR	NI	VRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
661	root	20	0	489868	120752	63464	S	3.3	1.6	0:42.86	Xorg
13048	kali	20	0	434244	104600	85764	S	2.0	1.4	0:05.59	qterminal
954	kali	20	0	353176	37248	21432	S	1.3	0.5	0:27.84	panel-13-cpugra
955	kali	20	0	341160	26904	17636	S	0.7	0.3	0:01.44	panel-14-sysira
956	kali	20	0	359168	30208	20404	S	0.7	0.4	0:12.74	panel-15-genmon
990	kali	20	0	262048	19612	15376	S	0.7	0.3	0:01.41	xfce4-notifyd
784	kali	20	0	269048	27732	17776	S	0.3	0.4	0:02.09	xfce4-session
908	kali	20	0	932732	106092	76836	S	0.3	1.4	0:10.37	xfwm4
933	kali	20	0	231588	29412	18904	S	0.3	0.4	0:02.23	xfsettingsd
953	kali	20	0	541124	99168	43328	S	0.3	1.3	0:06.41	xfdesktop
960	kali	20	0	391660	42968	32120	S	0.3	0.6	0:01.58	panel-17-notifi
962	kali	20	0	326044	44776	31952	S	0.3	0.6	0:01.62	panel-22-action
1015	kali	20	0	193768	26620	17136	S	0.3	0.3	0:01.68	xfce4-power-man
1067	kali	20	0	375996	55500	31920	S	0.3	0.7	0:02.45	blueman-applet
1088	kali	20	0	187284	17712	13720	S	0.3	0.2	0:01.26	polkit-gnome-au
16137	root	20	0	0	0	0	I	0.3	0.0	0:00.25	kworker/1:0-events
1	root	20	0	168008	11880	8856	S	0.0	0.2	0:01.50	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	netns
7	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H-events_highpri
9	root	0	-20	0	0	0	I	0.0	0.0	0:00.12	kworker/0:1H-kblockd
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	0:00.12	ksoftirqd/0
15	root	20	0	0	0	0	I	0.0	0.0	0:01.21	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

Nella colonna PID (freccia gialla) possiamo vedere i numeri che identificano in maniera univoca i processi attivi.

La colonna USER (freccia rossa) ci indica invece quale utente sta svolgendo quei determinati processi.

Infine nella colonna COMMAND (freccia verde) abbiamo il nome del comando che ha dato l'avvio al processo.

Per filtrare i risultati del comando “top” per l’utente root ho dato il comando “top | grep root” che mi ha restituito questa schermata:

```
kali@kali: ~/Desktop
File Actions Edit View Help
top - 10:23:26 up 1:08, 1 user, load average: 0.20, 0.19, 0.18
661 root      20   0 409860 120752 63464 S   1.0   1.6   0:44.39 Xorg
1 root      20   0 168008 11880 8856 S   0.0   0.2   0:01.50 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 netns
7 root      0 -20 0 0 0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
9 root      0 -20 0 0 0 I   0.0   0.0   0:00.12 kworker/0:1H-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   0:00.13 ksoftirqd/0
15 root     20  0 0 0 0 I   0.0   0.0   0:01.25 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   0:00.41 migration/1
21 root     20  0 0 0 0 S   0.0   0.0   0:00.07 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 com_reaper
31 root     0 -20 0 0 0 I   0.0   0.0   0:00.00 writeback
32 root     20  0 0 0 0 S   0.0   0.0   0:00.11 kcompactd0
33 root     25  5 0 0 0 S   0.0   0.0   0:00.00 ksmd
```

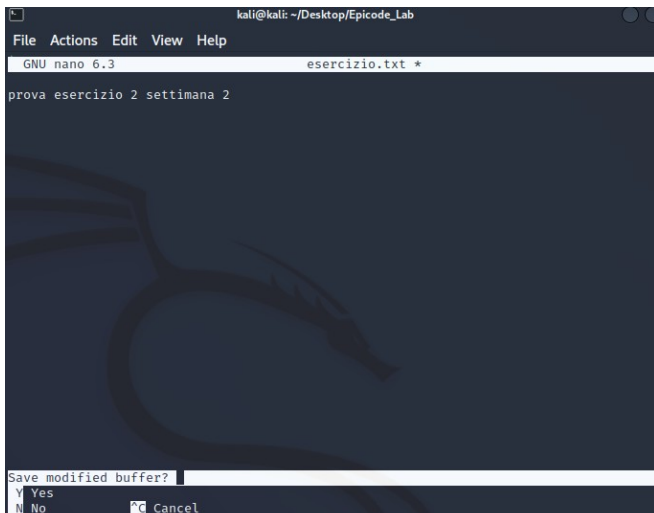
Lanciando invece lo stesso comando ma per l’utente kali ho ricevuto quest’altra schermata:

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ top | grep kali
13048 kali      20   0 434240 104628 85780 R   3.3   1.4   0:06.97 qterminal
954 kali      20   0 353176 37248 21432 S   1.0   0.5   0:29.19 panel-13-cpugra
947 kali      20   0 413308 55040 38972 S   0.7   0.7   0:02.35 Thunar
953 kali      20   0 541124 99168 43328 S   0.7   1.3   0:06.48 xfdesktop
956 kali      20   0 359168 30208 20404 S   0.7   0.4   0:13.35 panel-15-genmon
990 kali      20   0 262048 19612 15376 S   0.7   0.3   0:01.47 xfce4-notifyd
1015 kali     20   0 193768 26620 17136 S   0.7   0.3   0:01.75 xfce4-power-man
1042 kali     20   0 498176 29692 20116 S   0.7   0.4   0:01.81 light-locker
784 kali      20   0 269048 27732 17776 S   0.3   0.4   0:02.17 xfce4-session
908 kali      20   0 932732 106092 76836 S   0.3   1.4   0:10.77 xfwm4
933 kali      20   0 231588 29412 18904 S   0.3   0.4   0:02.31 xfsettingsd
955 kali      20   0 341160 26904 17636 S   0.3   0.3   0:01.49 panel-14-systra
958 kali      20   0 667660 46080 34656 S   0.3   0.6   0:04.15 panel-16-pulsea
960 kali      20   0 391660 42968 32120 S   0.3   0.6   0:01.64 panel-17-notifi
961 kali      20   0 391732 45412 32352 S   0.3   0.6   0:01.86 panel-18-power-
1067 kali     20   0 375996 55500 31920 S   0.3   0.7   0:02.53 blueman-applet
1088 kali     20   0 187284 17712 13720 S   0.3   0.2   0:01.32 polkit-gnome-au
1099 kali     20   0 551176 50692 37116 S   0.3   0.7   0:01.83 nm-applet
13048 kali     20   0 434240 104628 85780 S   4.7   1.4   0:07.11 qterminal
954 kali      20   0 353176 37248 21432 S   1.7   0.5   0:29.24 panel-13-cpugra
956 kali      20   0 359168 30208 20404 S   0.7   0.4   0:13.35 panel-15-genmon
```

Proseguendo nell’esercizio sono passato quindi alla creazione della directory Epicode\_Lab nel percorso indicato nella traccia andando anche a creare il file esercizio.txt al suo interno:

```
kali@kali: ~/Desktop/Epicode_Lab
File Actions Edit View Help
$ cd /home/kali/Desktop
(kali@kali)-[~/Desktop]
$ mkdir Epicode_Lab
(kali@kali)-[~/Desktop]
$ cd /home/kali/Desktop/Epicode_Lab
(kali@kali)-[~/Desktop/Epicode_Lab]
$ nano esercizio.txt
(kali@kali)-[~/Desktop/Epicode_Lab]
$ ls
esercizio.txt
(kali@kali)-[~/Desktop/Epicode_Lab]
$ nano esercizio.txt
```

Il passo successivo è stato la modifica di esercizio.txt tramite l’editor “nano” e salvare le modifiche apportate:



Dopo ciò sono andato prima a confermare che le modifiche fossero state salvate. Avuta conferma ho quindi controllato i permessi del file:

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov  2 10:31 .
drwxr-xr-x 3 kali kali 4096 Nov  2 10:27 ..
-rw-r--r-- 1 kali kali  30 Nov  2 10:28 esercizio.txt
```

Possiamo vedere sottolineati in rosso proprio i permessi del file esercizio.txt

Sono quindi passato alla modifica di questi permessi come indicato nella traccia:

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ chmod u+x esercizio.txt
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ chmod g+w esercizio.txt
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov  2 10:31 .
drwxr-xr-x 3 kali kali 4096 Nov  2 10:27 ..
-rwxrw-r-- 1 kali kali  30 Nov  2 10:28 esercizio.txt
```

La fase successiva è stata quella di creare un nuovo utente, che ho chiamato prova:

```
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ useradd adminprova
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$
```

Come si può vedere nell'immagine qui a sinistra, senza l'utilizzo del comando sudo non è stato possibile creare un nuovo utente.



Invece utilizzando il comando `sudo` `useradd` prova non ci sono stati problemi, come dimostra l'immagine qui a destra

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ passwd prova
passwd: You may not view or modify password information for prova.

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

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

Continuando a seguire le istruzioni della traccia sono andato a modificare i permessi del nostro file `esercizio.txt` privando gli utenti esterni anche della sola possibilità di lettura e l'ho spostato nella cartella `root`. Una volta cambiato utente tramite il comando `su` `prova`, ho provato ad aprire il file per leggerlo ma mi ha ridato questa schermata:

```
[ Error reading esercizio.txt: Permission denied ] ...
^O Write Out ^W Where Is ^K Cut ^T Execute ^C Lo
```

Dopo aver nuovamente cambiato i permessi per permettere ad utenti esterni di leggere il file ma non di poterlo modificare ho invece avuto questo avviso sul fondo della schermata:

```
[ File 'esercizio.txt' is unwritable ] ...
Out ^W Where Is ^K Cut ^T Execute
```

Infine, dopo essere tornato sull'utente `kali` ho proceduto all'eliminazione del file `esercizio.txt` (dovendo usare il comando `sudo`) e della directory `Epicode_Lab`:

```
(kali㉿kali)-[/]
$ rm esercizio.txt
rm: cannot remove 'esercizio.txt': Permission denied

(kali㉿kali)-[/]
$ sudo rm esercizio.txt
```

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

(kali㉿kali)-[~/Desktop]
$
```