

Familiarizzazione con la schell Linux

Fase 1

Nella prima fase siamo andati a controllare i processi attivi sulla macchina, trovando le colonne PID, USER, COMMAND che ci mostrano l'utilizzo del utente da parte dei processi in corso della macchina.

Poi abbiamo filtrato attraverso il comando TOP, prima i programmi in esecuzione per l'utente root e poi per l'utente Kali, come vediamo nell'immagine seguenti.

```
top - 09:27:33 up 6 min, 1 user, load average: 0.11, 0.23, 0.14
Tasks: 150 total, 1 running, 149 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.9 us, 1.6 sy, 0.0 ni, 97.6 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1981.3 total, 885.8 free, 631.6 used, 463.8 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 1196.7 avail Mem

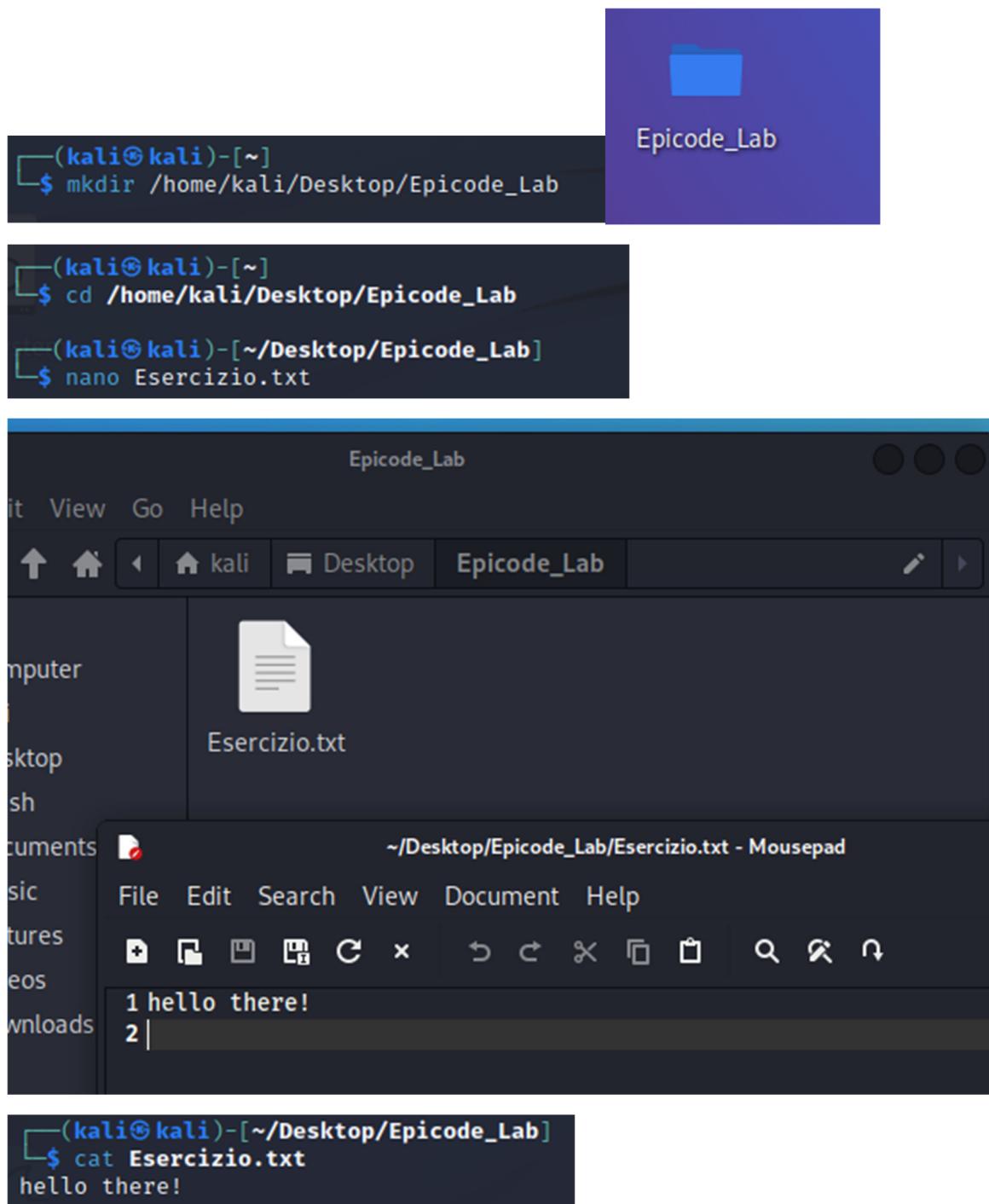
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 633 root 20 0 387156 107392 56936 S 2.0 5.3 0:12.46 Xorg
 877 kali 20 0 867500 106508 76880 S 1.0 5.2 0:03.29 xfwm4
 929 kali 20 0 602088 48168 34756 S 0.7 2.4 0:00.75 panel-16-pulsea
 2470 kali 20 0 434108 104200 85352 S 0.7 5.1 0:00.33 qterminal
 15 root 20 0 0 0 0 I 0.3 0.0 0:00.35 rcu_preempt
 195 root 20 0 0 0 0 I 0.3 0.0 0:00.78 kworker/1:2-events
 828 kali 20 0 153000 2696 2216 S 0.3 0.1 0:01.30 VBoxClient
 924 kali 20 0 204992 27944 18800 S 0.3 1.4 0:02.23 panel-13-cpugra
 928 kali 20 0 350972 30312 20636 S 0.3 1.5 0:01.32 panel-15-genmon
 980 kali 20 0 266812 25704 16644 S 0.3 1.3 0:00.45 light-locker
 2503 root 20 0 0 0 0 I 0.3 0.0 0:00.01 kworker/0:0-events
```

```
File Actions Edit View Help
top - 09:58:55 up 37 min, 1 user, load average: 0.05, 0.03, 0.02
 633 root 20 0 387156 107392 56936 S 0.7 5.3 0:29.34
 15 root 20 0 0 0 0 I 0.3 0.0 0:01.38
 151 root -51 0 0 0 0 S 0.3 0.0 0:00.88
 3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 7 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 9 root 0 -20 0 0 0 I 0.0 0.0 0:00.81
 10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 11 root 20 0 0 0 0 I 0.0 0.0 0:00.00
 3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 7 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 9 root 0 -20 0 0 0 I 0.0 0.0 0:00.81
 10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00
 11 root 20 0 0 0 0 I 0.0 0.0 0:00.00
 12 root 20 0 0 0 0 I 0.0 0.0 0:00.00
```

```
(kali㉿kali)-[~]
$ top | grep kali
 877 kali 20 0 867500 106508 76880 S 0.7 5.2 0:09.47 xfwm4
 828 kali 20 0 153000 2696 2216 S 0.3 0.1 0:08.48 VBoxClient
 924 kali 20 0 204992 32176 18800 S 0.3 1.6 0:11.97 panel-13-cpugra
 929 kali 20 0 602088 48320 34756 S 0.3 2.4 0:02.34 panel-16-pulsea
 10917 kali 20 0 10412 3836 3276 R 0.3 0.2 0:00.01 top
 924 kali 20 0 204992 32176 18800 S 0.7 1.6 0:11.99 panel-13-cpugra
 828 kali 20 0 153000 2696 2216 S 0.3 0.1 0:08.49 Vboxclient
 877 kali 20 0 867500 106508 76880 S 0.3 5.2 0:09.48 xfwm4
 928 kali 20 0 350972 30412 20644 S 0.3 1.5 0:06.43 panel-15-genmon
 929 kali 20 0 602088 48320 34756 S 0.3 2.4 0:02.35 panel-16-pulsea
 9958 kali 20 0 433972 106220 85448 S 0.3 5.2 0:00.81 qterminal
 828 kali 20 0 153000 2696 2216 S 0.3 0.1 0:08.50 VBoxClient
 877 kali 20 0 867500 106508 76880 S 0.3 5.2 0:09.49 xfwm4
```

Fase 2

Nella fase successiva abbiamo creato una Directory chiamata EPCODE_Lab attraverso il comando mkdir e al suo interno un documento di testo Esercizio.txt utilizzando il comando nano, inserendo il testo al suo interno: Hello There, inoltre attraverso il comando cat abbiamo aperto da comandi il file testo con la relativa scritto come vediamo nelle immagini seguenti.



Fase 3

In questa fase siamo andati a controllare i vari permessi che aveva il file per la lettura, scrittura ed esecuzione (W, R, X) per utente, gruppo e altri utenti, dopo avere controllato i permessi con i comandi ls-la, entrando nella nostra cartella con il comando cd , ho modificato i permessi attraverso il comando chmod e utilizzando i numeri 764(metodo numerico) che sono il metodo più veloce così

da permettere all'utente la possibilità di leggere, scrivere e eseguire il file, al gruppo la possibilità di leggere e scrivere e infine agli altri utenti la sola lettura, come vediamo nella verifica successiva nelle immagini seguenti.

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls-la
ls-la: command not found

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov  2 10:36 .
drwxr-xr-x 3 kali kali 4096 Nov  2 10:33 ..
-rw-r--r-- 1 kali kali    13 Nov  2 10:36 Esercizio.txt
```

```
(kali㉿kali)-[~]
$ cd /home/kali/Desktop/Epicode_Lab
stem
(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ chmod 764 Esercizio.txt

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov  2 10:36 .
drwxr-xr-x 3 kali kali 4096 Nov  2 10:33 ..
-rwxrwxr-- 1 kali kali    13 Nov  2 10:36 Esercizio.txt
```

Fase 4

In questa fase abbiamo creato un altro utente che ho chiamato jak, poi abbiamo cambiato i permessi sul nostro file di testo non permettendo agli altri utenti nessun permesso, ho modificato sempre con chmod il numero 760, lo zero finale toglie proprio tutti i permessi agli altri utenti. Possiamo verificare infatti che attraverso il comando su e passando all'utente jak non riusciamo a leggere il file di testo, ricevendo errore. Inoltre abbiamo poi spostato il file Esercizio.txt nella directory root/ come vediamo nelle immagini seguenti. Per tutta questa fase abbiamo usato il comando sudo altrimenti non avremmo potuto fare le modifiche.

```
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ sudo useradd jak
[sudo] password for kali:
└──(kali㉿kali)-[~]
$ sudo passwd jak
New password:
Retype new password:
passwd: password updated successfully
└──(kali㉿kali)-[~]
$ █

File Actions Edit View Help
└──(kali㉿kali)-[~]
$ cd /home/kali/Desktop/Epicode_Lab
└──(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ chmod 760 Esercizio.txt
└──(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov  2 10:36 .
drwxr-xr-x 3 kali kali 4096 Nov  2 10:33 ..
-rw-rw-r-- 1 kali kali   13 Nov  2 10:36 Esercizio.txt

File Actions Edit View Help
└──(kali㉿kali)-[~]
$ su jak
Password:
$ cat Esercizio.txt
cat: Esercizio.txt: No such file or directory
$ █

File Actions Edit View Help
└──(kali㉿kali)-[~]
$ cd /home/kali/Desktop/Epicode_Lab
└──(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ sudo mv Esercizio.txt /
[sudo] password for kali:
└──(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ █
```

Fase 5

Nell'ultima fase, tornando sul nostro user principale che è kali abbiamo rimodificato i permessi ma questa volta permettendo la lettura agli altri utenti e quindi inserendo il numero 764, siamo riusciti così ad aprire il file testo con il nostro user jak. Infine abbiamo cancellato tutti procedimenti creati con il comando rm e rmdir, anche in questo caso utilizzando il comando sudo per le stesse ragioni di permessi di modifica; come possiamo vedere nelle immagini seguenti.

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ su jak
Password:
$ cat Esercizio.txt
Hello there!
$
```

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo userdel jak
[sudo] password for kali:

(kali㉿kali)-[~]
$ su jak
su: user jak does not exist or the user entry does not contain all the required fields

(kali㉿kali)-[~]
$
```

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

(kali㉿kali)-[~/Desktop/Epicode_Lab]
$ rm Esercizio.txt

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

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