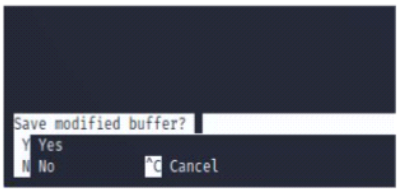
Andrea Cuore

02/11/2022

UTILIZZO SHELL KALI LINUX

TASK:

- Controllare i processi attivi sulla macchina Linux con il comando «top» e descrivere il significato delle colonne: I) 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 salvatelo. Per salvare il file utilizzate la sequenza «ctrl+x» e successivamente «y», come mostrato in figura sotto.



3

EPICODE — **Esercizio** — Comandi shell Linux

Traccia:

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

- 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.

Parte 1:

Per il controllo dei processi attivi su macchina Linux ci siamo avvalsi del comando <<top>>, che riporterà la schermata di tutti i processi attivi , per filtrare i processi con usr root, abbiamo utilizzato lo stesso comando con l'aggiunta dell'argomento -u (che sta per user) Root

```
top - 06:39:10 up 41 min,  2 users,  load average: 0.25, 0.08, 0.02
Tasks: 146 total,   1 running, 145 sleeping,   0 stopped,   0 zombie
%Cpu(s): 13.0 us,  6.8 sy,  0.0 ni, 79.9 id,  0.3 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3929.8 total,   2813.5 free,    578.5 used,    537.8 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   3135.0 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    656 root      20   0  370644 120872  54212 S   9.3   3.0   0:08.90 Xorg
  11394 kali      20   0  431764 102064  83544 S   3.0   2.5   0:00.43 qterminal
    977 kali      20   0  413056  62272  35456 S   2.3   1.5   0:01.16 xfdesktop
    923 kali      20   0  164588   9932   7028 S   0.7   0.2   0:00.04 at-spi2-registr
    978 kali      20   0  201136  29732  18380 S   0.7   0.7   0:07.16 panel-13-cpugra
    982 kali      20   0  398692  44716  32032 S   0.7   1.1   0:00.26 panel-17-notifi
    986 kali      20   0  390636  44584  31808 S   0.7   1.1   0:00.28 panel-22-action
    793 kali      20   0  267784  26640  16732 S   0.3   0.7   0:00.36 xfce4-session
    887 kali      20   0  153056   2860   2388 S   0.3   0.1   0:03.24 VBoxClient
    935 kali      20   0  636056  97180  76620 S   0.3   2.4   0:03.02 xfwm4
    957 kali      20   0  230676  28920  18484 S   0.3   0.7   0:00.36 xfsettingsd
    971 kali      20   0  341252  24076  16812 S   0.3   0.6   0:00.23 Thunar
    980 kali      20   0  292768  30012  20300 S   0.3   0.7   0:03.81 panel-15-genmon
    981 kali      20   0  600080  47908  34768 S   0.3   1.2   0:01.06 panel-16-pulsea
    985 kali      20   0  398820  46864  32032 S   0.3   1.2   0:00.29 panel-18-power-
   1054 kali      20   0  431952  29844  20324 S   0.3   0.7   0:00.26 light-locker
   1068 kali      20   0  374148  52852  31772 S   0.3   1.3   0:00.58 blueman-applet
   1071 kali      20   0  187384  19856  15344 S   0.3   0.5   0:00.18 xfce4-power-man
   1098 kali      20   0  558516  50696  37204 S   0.3   1.3   0:00.25 nm-applet
      1 root      20   0  101960  11996   8884 S   0.0   0.3   0:00.68 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
```

```
top - 06:47:29 up 49 min,  2 users,  load average: 0.38, 0.12, 0.03
Tasks: 147 total,   1 running, 146 sleeping,   0 stopped,   0 zombie
%Cpu(s):  5.2 us,  4.5 sy,  0.0 ni, 90.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3929.8 total,   2810.3 free,    580.1 used,    539.5 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   3133.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    656 root      20   0  370644 120872  54212 S   4.3   3.0   0:12.22 Xorg
   7717 root      20   0       0      0      0 I   0.3   0.0   0:00.56 kworker/0:0-events
      1 root      20   0  101960  11996   8884 S   0.0   0.3   0:00.68 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_hi+
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.10 kworker/0:1H-events_hi+
     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   0:00.11 ksoftirqd/0
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.49 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
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     21 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
     22 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
     23 root      20   0       0      0      0 S   0.0   0.0   0:00.00 khungtaskd
     25 root      20   0       0      0      0 S   0.0   0.0   0:00.00 oom_reaper
     26 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 writeback
     28 root      20   0       0      0      0 S   0.0   0.0   0:00.12 kcompactd0
```

Di seguito riportato il significato per ogni nomenclatura superiore:

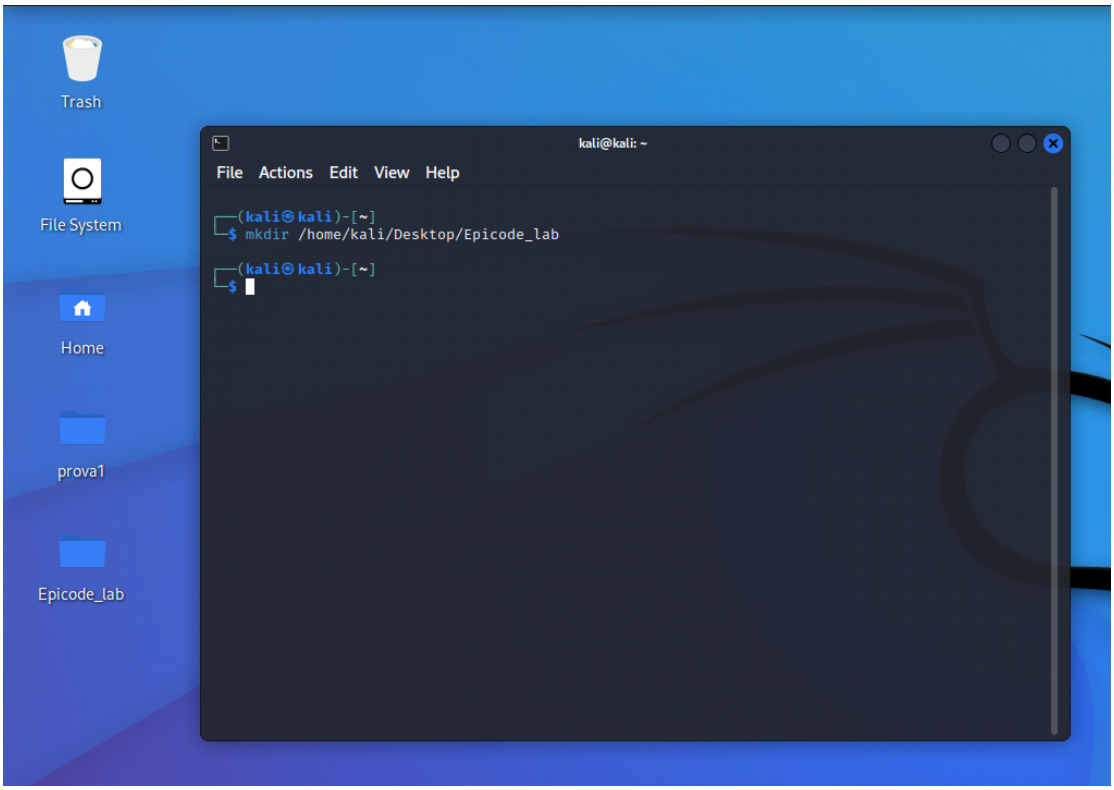
- PID : Il numero identificativo del processo
- USER: Il nome dell'User sulla quale è attivo il processo
- PR: La priorità di scheduling del processo

- NI: Un numero che se negativo assegna una priorità maggiore
- VIRT: Memoria virtuale assegnata al processo
- RES: Memoria fisica utilizzata dal processo
- SHR: Memoria condivisa con il processo
- S: Stato del processo che si suddivide -R (Running) -S (Sleeping)
- %CPU : % della CPU in utilizzo
- %MEM: % della memoria in utilizzo
- Command: nome con la quale avviare il processo

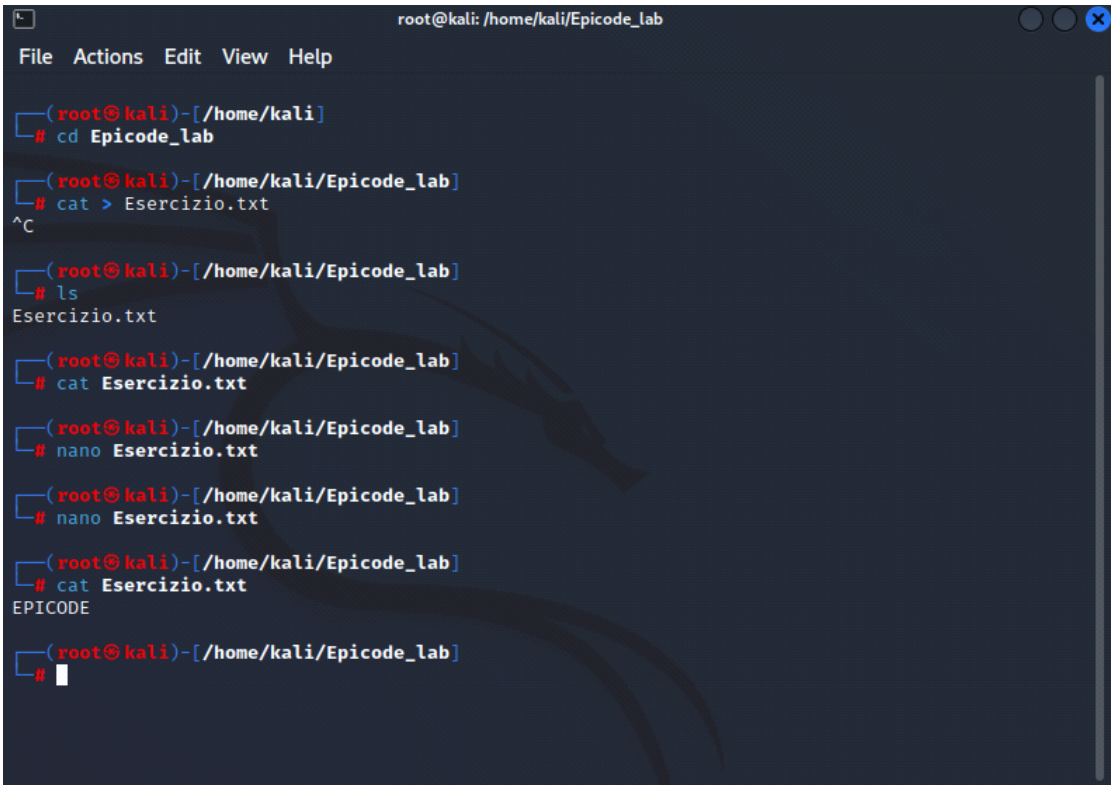
Dopo l'analisi dei processi , si è proseguito con la creazione di una directory e creazione di un file .txt.

Per la creazione della directory abbiamo utilizzato il comando MKDIR, seguendo il path richiesto dalla traccia dunque : mkdir /home/kali/Desktop/Epicode_lab, successivamente con il comando << cd Epicode_lab>> siamo entrati nella directory richiesta e con il comando <<cat > Esercizio.txt>> abbiamo creato il file txt richiesto, per la modifica è stato utilizzato il comando nano.

MKDIR:



Creazione e modifica file txt:



FASE 2:

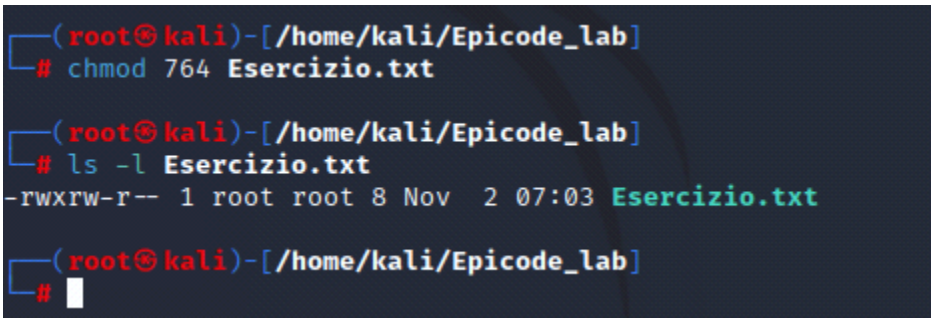
Ci è stato chiesto di visualizzare i permessi del file appena creato, questa operazione è possibile effettuarla con il comando ls -la (nome file), mentre per la modifica dei permessi del file abbiamo utilizzato il comando chmod , assegnando rispettivamente:

User --> rwx

Group --> rw

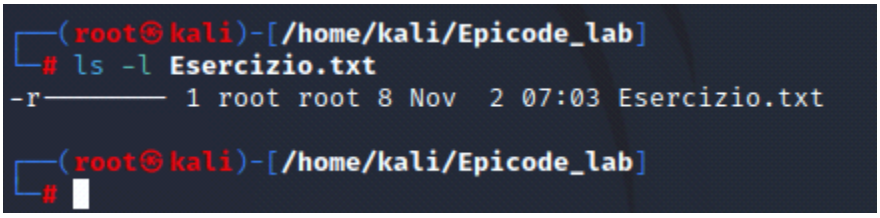
Other --> r

dunque abbiamo potuto utilizzare chmod 764.

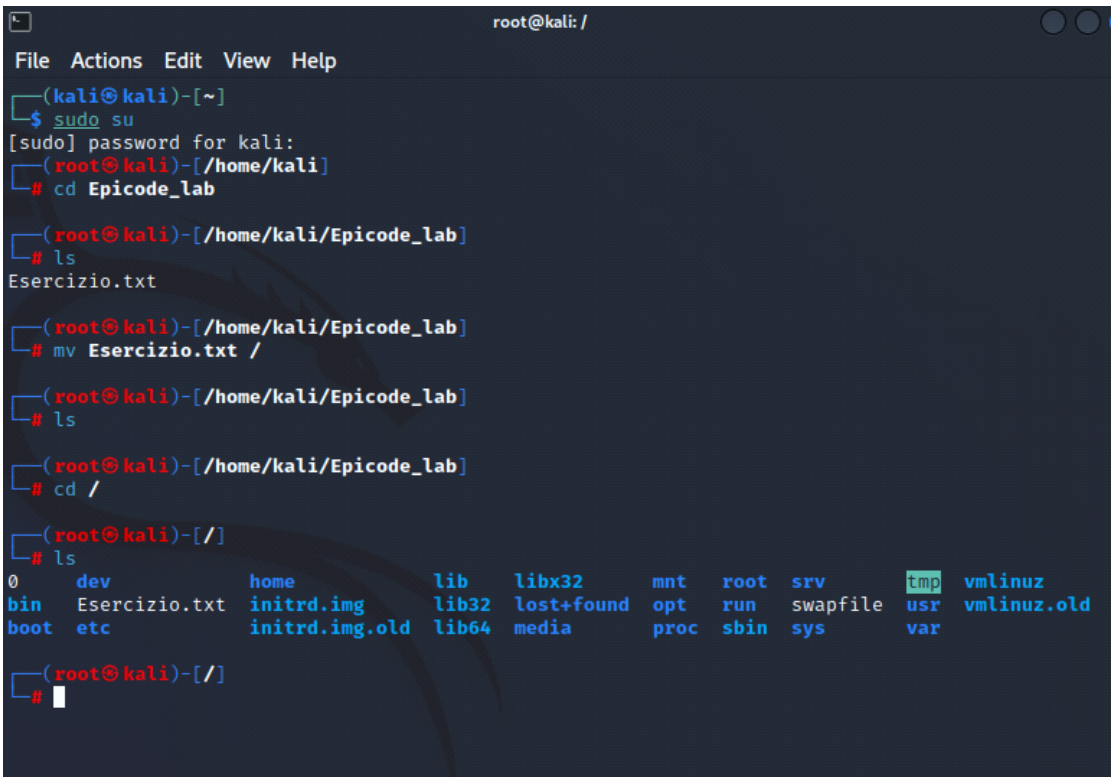


Per la creazione di un nuovo utente utiliziamo il comando Useradd e passwd per aggiungere un nuovo utente con password, successivamente ricambiamo i valori dei permessi in modo tale da avere solo l'utente principale con i permessi di lettura e gli altri senza.

Ripetiamo dunque il procedimento entrando nella directory di Epicode_lab e facendo questa volta un chmod 400 , in modo tale da abilitare la lettura solo sul nostro user.



Fatto ciò spostiamo il file Esercizio.txt nella directory di root << / >> con il comando <<mv Esercizio.txt />>



ed accediamo tramite il comando su all'User Andrea, recandoci nella directory di root e lanciando il comando << cat Esercizio.txt>> ci comparirà l'errore "Permission Denied".

```
┌──(root㉿kali)-[/]
└─# su Andrea
$ ls
0     dev            home            lib    libx32      mnt   root  srv       tmp  vmlinuz
bin   Esercizio.txt  initrd.img      lib32  lost+found  opt   run   swapfile  usr  vmlinuz.old
boot  etc            initrd.img.old  lib64  media       proc  sbin  sys       var
$ cat Esercizio.txt
cat: Esercizio.txt: Permission denied
$
```

Per abilitare la lettura al nuovo Usr ho ripetuto il procedimento iniziale impostando come chmod 764.

```
┌──(root㉿kali)-[/]
└─# su Andrea
$ ls
0     dev            home            lib    libx32      mnt   root  srv       tmp  vmlinuz
bin   Esercizio.txt  initrd.img      lib32  lost+found  opt   run   swapfile  usr  vmlinuz.old
boot  etc            initrd.img.old  lib64  media       proc  sbin  sys       var
$ cat Esercizio.txt
EPICODE
$
```

Infine ho riportato tutto allo stato iniziale cancellando il file.txt e il nuovo user.

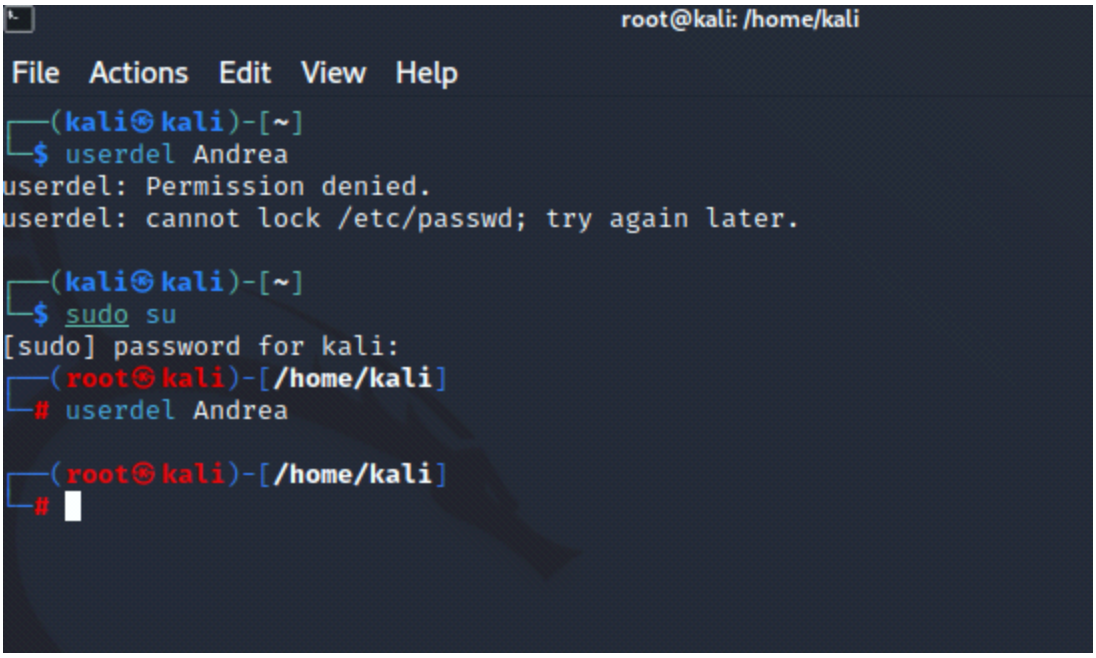
Per cancellare il file.txt ho utilizzato il comando <<rm Esercizio.txt>>

```
┌──(kali㉿kali)-[/]
└─$ sudo su
[sudo] password for kali:
rSorry, try again.
[sudo] password for kali:
┌──(root㉿kali)-[/]
└─# rm Esercizio.txt

┌──(root㉿kali)-[/]
└─# ls
0     dev   initrd.img      lib32   lost+found  opt   run   swapfile  usr      vmlinuz.old
bin   etc   initrd.img.old  lib64   media       proc  sbin  sys       var
boot  home  lib             libx32  mnt         root  srv   tmp       vmlinuz

┌──(root㉿kali)-[/]
└─#
```

Mentre per la rimozione dell'user ho utilizzato il comando <<Userdel Andrea>>


root@kali: /home/kali
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ userdel Andrea
userdel: Permission denied.
userdel: cannot lock /etc/passwd; try again later.
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# userdel Andrea
┌──(root㉿kali)-[/home/kali]
└─#