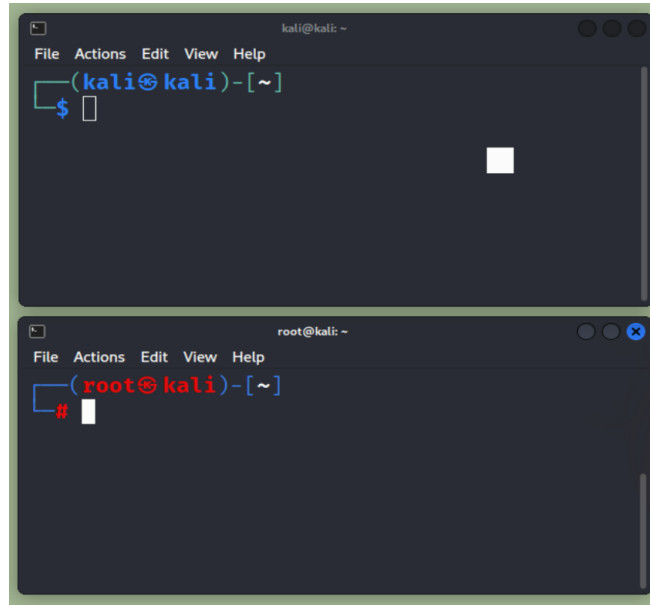


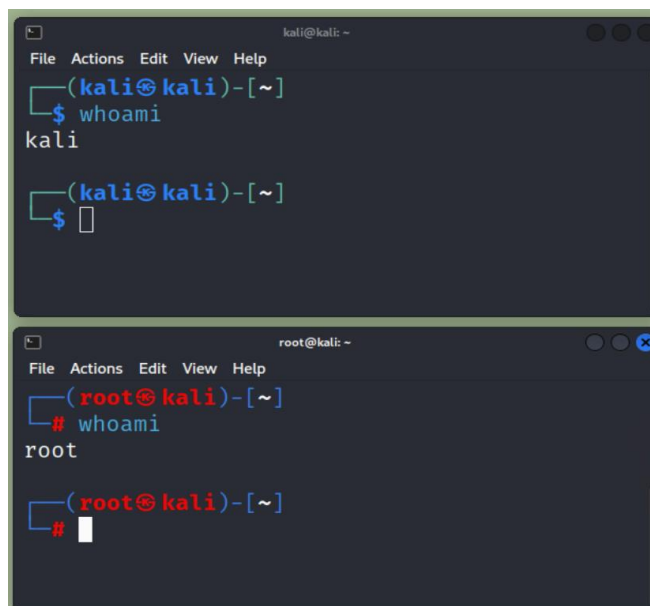
Ejercicio de Clase 1

ACTIVIDAD 1:

Vamos a probar los IDs asociados a un usuario. Para reproducir las acciones de este ejercicio vamos a entrar a nuestro sistema Linux en 2 terminales. En una terminal se requiere que estés logueado como usuario root y en la otra terminal que estés logueado como usuario “no-root”.



En ocasiones el nombre de usuario (o username) no se muestra en el prompt de la terminal, entonces ¿Cómo saber qué usuario soy? Una manera de comprobarlo consiste en ejecutar el comando “whoami” en ambas terminales.



Vamos a probar un comando que requiere privilegios de root. Un ejemplo es el comando fdisk.

¿Qué hace este comando?

Se le considera una utilidad basada en texto que permite visualizar y administrar particiones de disco duro dentro de sistemas basados en Unix.

Investiga la opción -l (guión y la letra ele) del comando fdisk

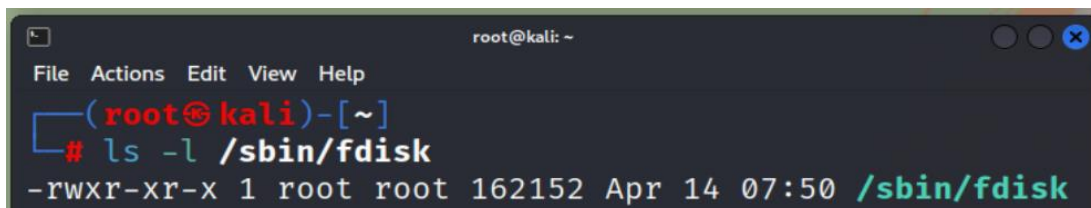
Con esta opción seguida del comando será posible mostrar el listado de particiones del disco duro actual.

Ejecuta el comando fdisk -l con el usuario “no-root” para que te muestre el mensaje de error “Permiso denegado”. IMPORTANTE: Dependiendo de la distribución de Linux, puede mostrarse un mensaje de error o no.



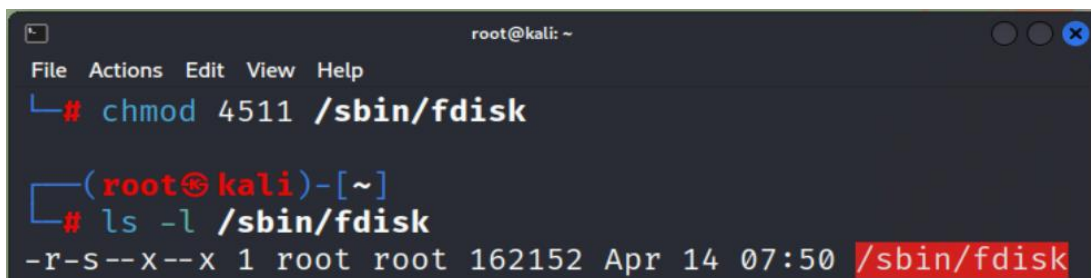
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ fdisk -l  
fdisk: cannot open /dev/sda: Permission denied
```

Ahora nos cambiamos a la terminal del usuario root y revisamos los permisos actuales del comando fdisk.



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# ls -l /sbin/fdisk  
-rwxr-xr-x 1 root root 162152 Apr 14 07:50 /sbin/fdisk
```

Ahora modificamos los permisos del comando fdisk modificando el bit “setuid”. Y corroboramos que se cambiaron los permisos.



```
root@kali: ~  
File Actions Edit View Help  
# chmod 4511 /sbin/fdisk  
  
(root@kali)-[~]  
# ls -l /sbin/fdisk  
-r-s--x--x 1 root root 162152 Apr 14 07:50 /sbin/fdisk
```

Regresamos a la terminal del usuario “no-root” y ejecutamos nuevamente el comando que hace un momento nos indicó “Permiso denegado”.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ fdisk -l  
Disk /dev/sda: 100 GiB, 107374182400 bytes, 209715200 sectors  
Disk model: VMware Virtual S  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x72bd05d3  
  
Device      Boot      Start         End      Sectors  Size Id Type  
/dev/sda1   *          2048    165771263    165769216   79G 83 Linux  
/dev/sda2             165773310    167770111     1996802   975M  5 Extended  
/dev/sda5             165773312    167770111     1996800   975M 82 Linux swap / So
```

Ahora regresamos los permisos originales al fdisk.

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# chmod 755 /sbin/fdisk  
  
(root@kali)-[~]  
# ls -l /sbin/fdisk  
-rwxr-xr-x 1 root root 162152 Apr 14 07:50 /sbin/fdisk
```

Actividad 2:

Ahora escribe el programa 2 llamado ids.c

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 6.3 ids.c  
#include <stdio.h>  
#include <unistd.h>  
#include <stdlib.h>  
  
int main(void)  
{  
    printf("Real user ID: %d\n", getuid());  
    printf("Effective user ID: %d\n", geteuid());  
    printf("Real group ID: %d\n", getgid());  
    printf("Effective group ID: %d\n", getegid());  
    return 0;  
}  
[ Wrote 12 lines ]  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Si lo compilas y ejecutas obtendrás que el usuario real y el usuario efectivo dan el mismo valor. ¿Porqué? Porque lo estás ejecutando con el mismo usuario que es el dueño del ejecutable.

Ejemplo de ejecución con el usuario root

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ gcc ids.c -o ids  
  
(kali@kali)-[~]  
$ ./ids  
Real user ID: 1000  
Effective user ID: 1000  
Real group ID: 1000  
Effective group ID: 1000
```

```
root@kali: /home/kali  
File Actions Edit View Help  
(root@kali)-[/home/kali]  
# ls -l ids  
-rwxr-xr-x 1 kali kali 16304 Aug 30 22:20 ids  
  
(root@kali)-[/home/kali]  
# chmod 4511 ids  
  
(root@kali)-[/home/kali]  
# ls -l ids  
-r-s--x--x 1 kali kali 16304 Aug 30 22:20 ids  
  
(root@kali)-[/home/kali]  
# ./ids  
Real user ID: 0  
Effective user ID: 1000  
Real group ID: 0  
Effective group ID: 0
```

Ejemplo de ejecución con el usuario kali

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# ls -l ids2
-rwxr-xr-x 1 root root 16304 Aug 30 22:32 ids2

(root@kali)-[/home/kali]
# chmod 4511 ids

(root@kali)-[/home/kali]
# ls -l ids2
-rwxr-xr-x 1 root root 16304 Aug 30 22:32 ids2

(root@kali)-[/home/kali]
# chmod 4511 ids2

(root@kali)-[/home/kali]
# ls -l ids2
-r-s--x--x 1 root root 16304 Aug 30 22:32 ids2
```

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ ./ids2
Real user ID: 1000
Effective user ID: 1000
Real group ID: 1000
Effective group ID: 1000

(kali@kali)-[~]
$ ./ids2
Real user ID: 1000
Effective user ID: 0
Real group ID: 1000
Effective group ID: 1000
```