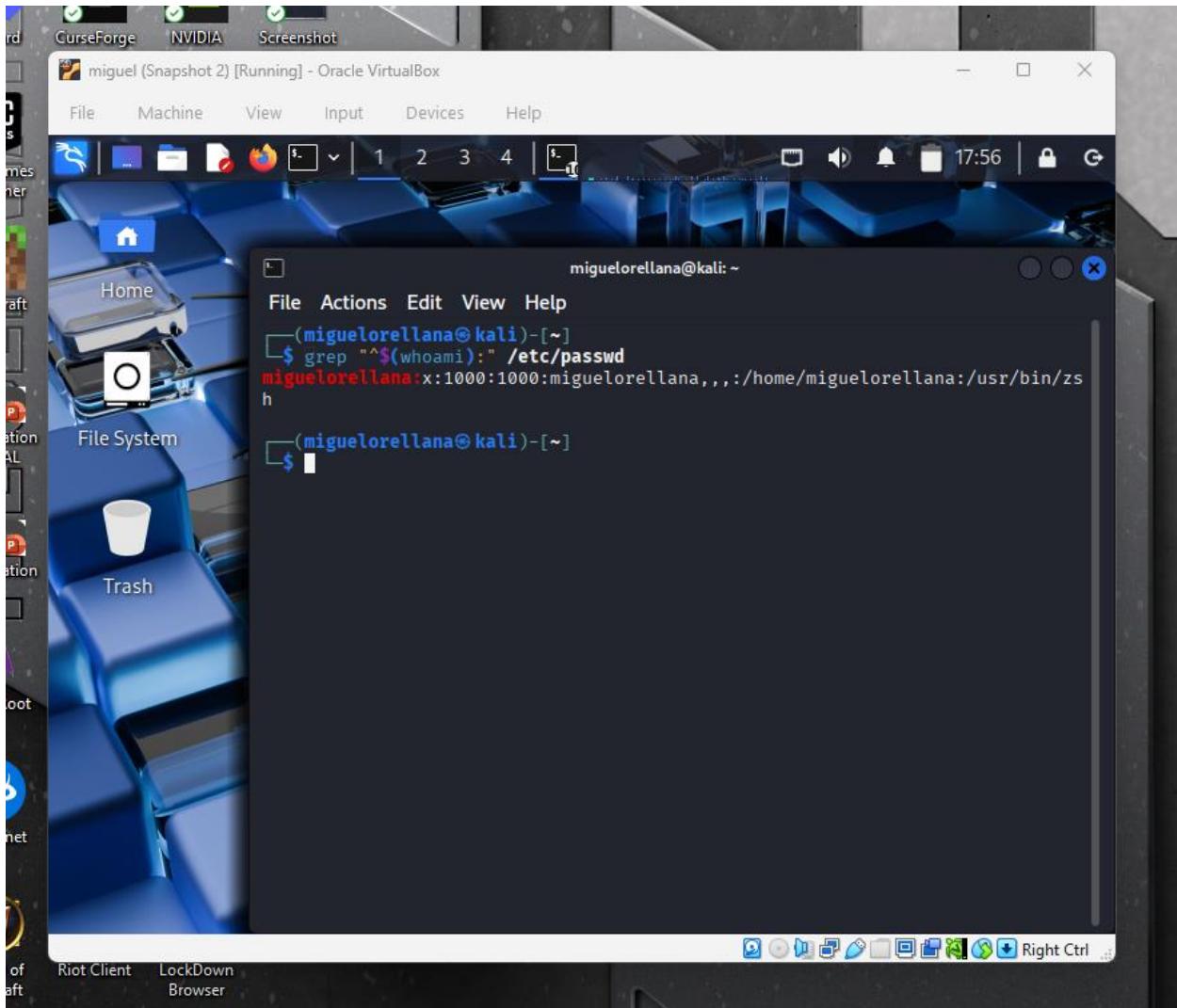


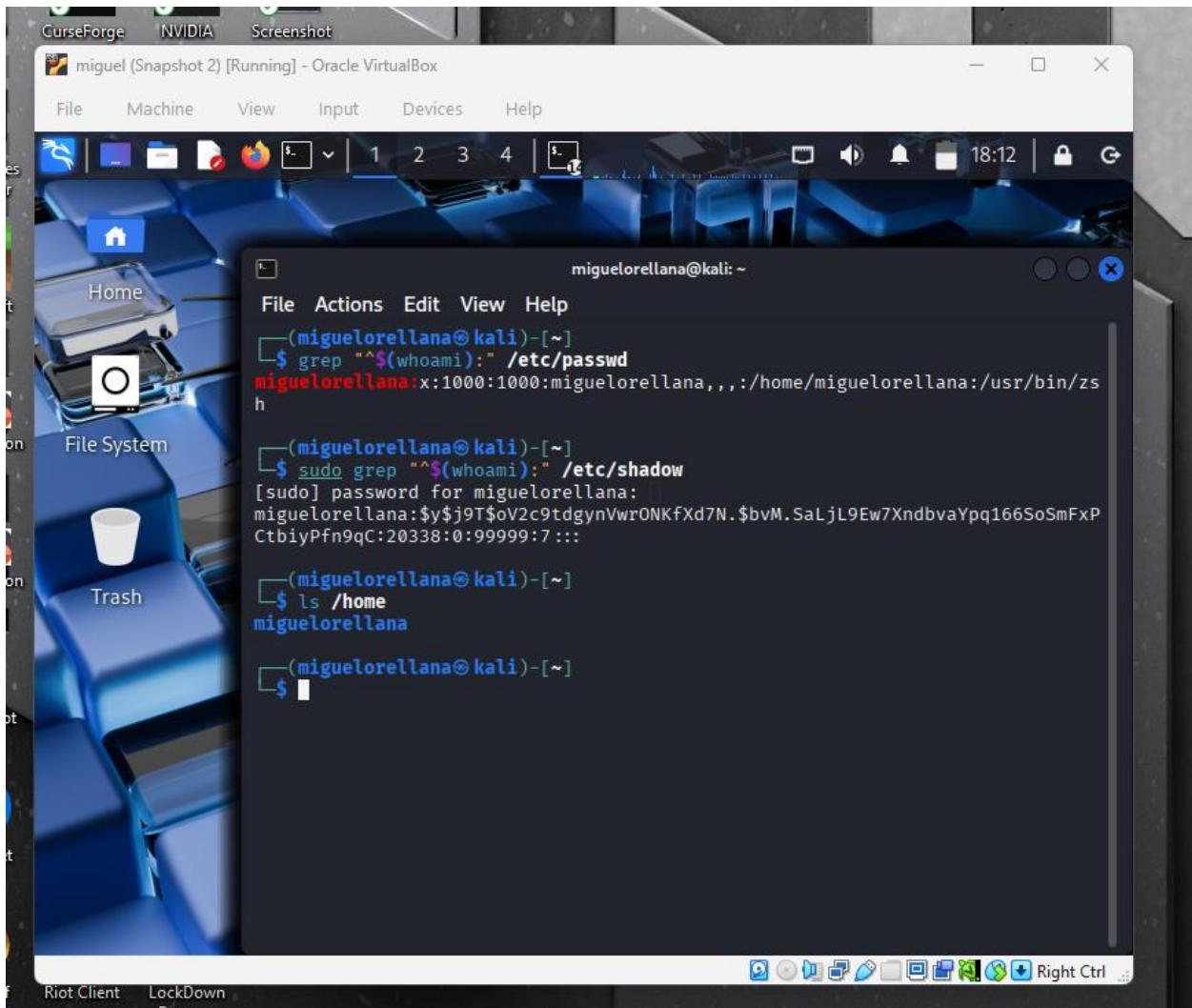
TASK A

1.



This searches /etc/passwd for the current username.

2.



The screenshot shows a Kali Linux desktop environment within Oracle VirtualBox. A terminal window is open, showing the following session:

```
miguelorellana@kali: ~
File Actions Edit View Help
(miguelorellana@kali)-[~]
$ grep '^$(whoami):' /etc/passwd
miguelorellana:x:1000:1000:miguelorellana,,,,:/home/miguelorellana:/usr/bin/zsh

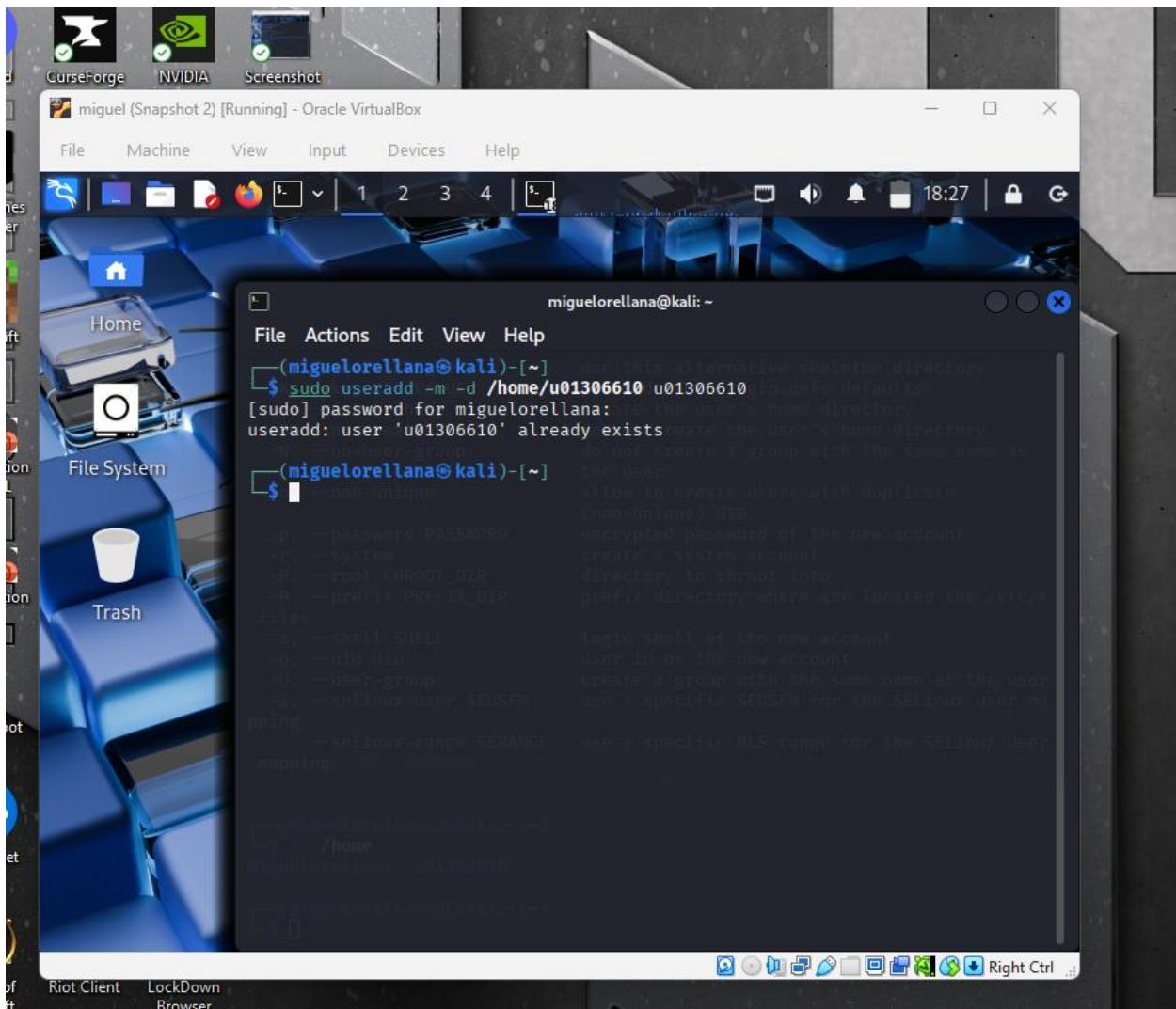
(miguelorellana@kali)-[~]
$ sudo grep '^$(whoami):' /etc/shadow
[sudo] password for miguelorellana:
miguelorellana:$y$j9T$ov2c9tdgynVwrONKFxd7N.$bvM.SaLjL9Ew7XndbvaYpq166SoSmFxCtbiyPfn9qC:20338:0:99999:7:::

(miguelorellana@kali)-[~]
$ ls /home
miguelorellana

(miguelorellana@kali)-[~]
$
```

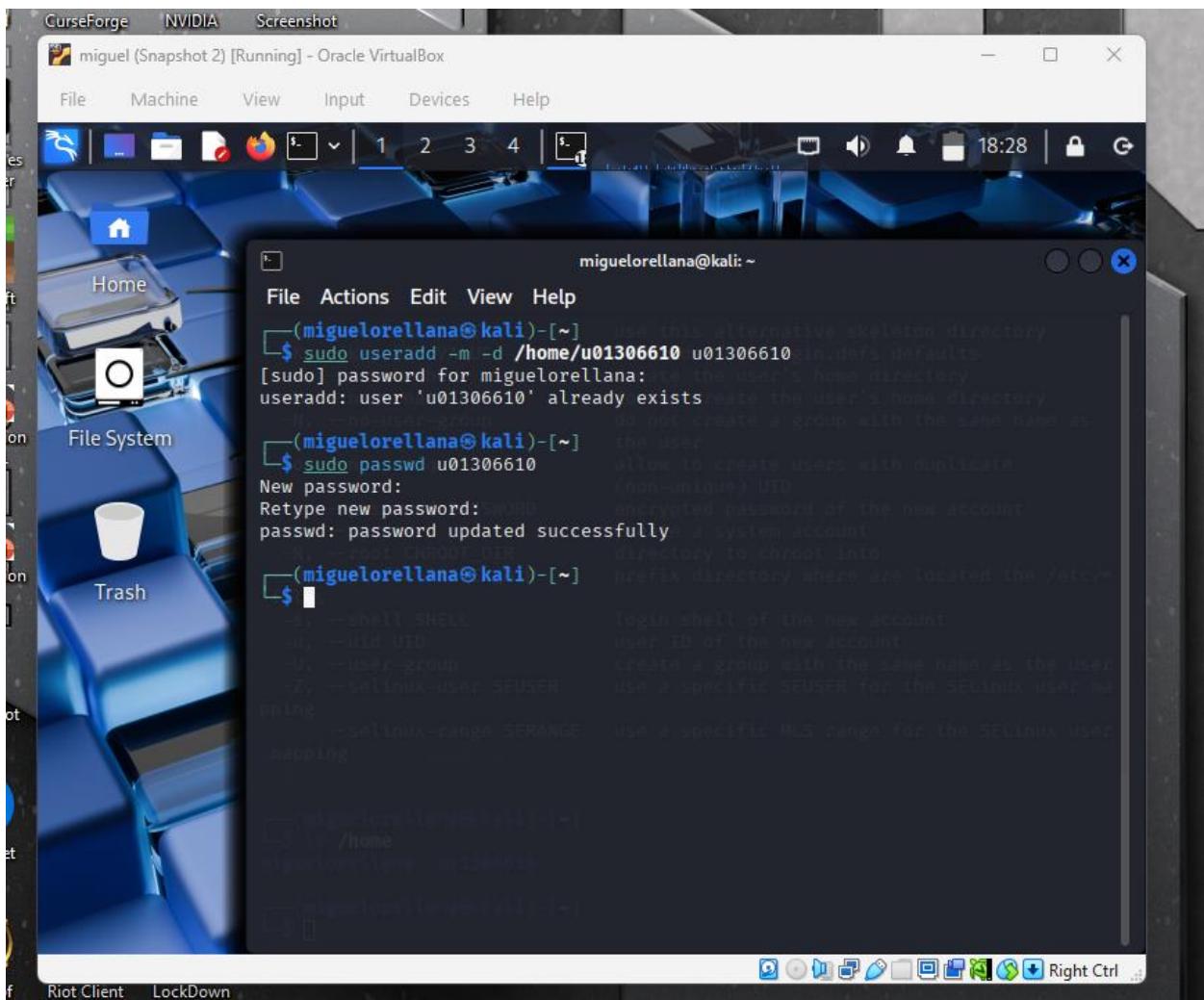
/etc/shadow contains encrypted passwords and aging info

3.



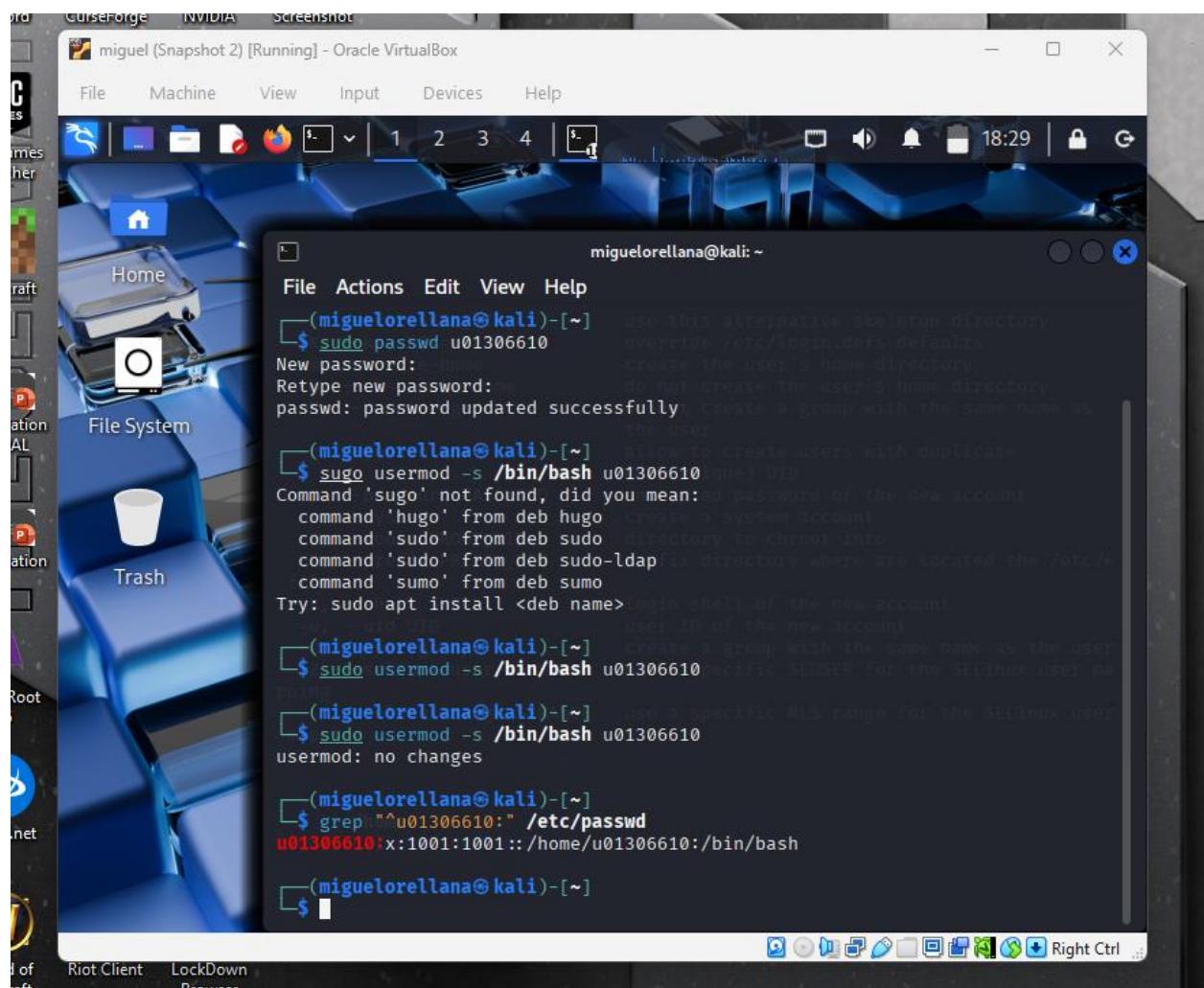
-m created the home directory, -d specifies its path

4.



The new user needs a password to log in

5.



```
miguelorellana@kali: ~
File Actions Edit View Help
(miguelorellana@kali)-[~]
$ sudo passwd u01306610
New password:
Retype new password:
passwd: password updated successfully

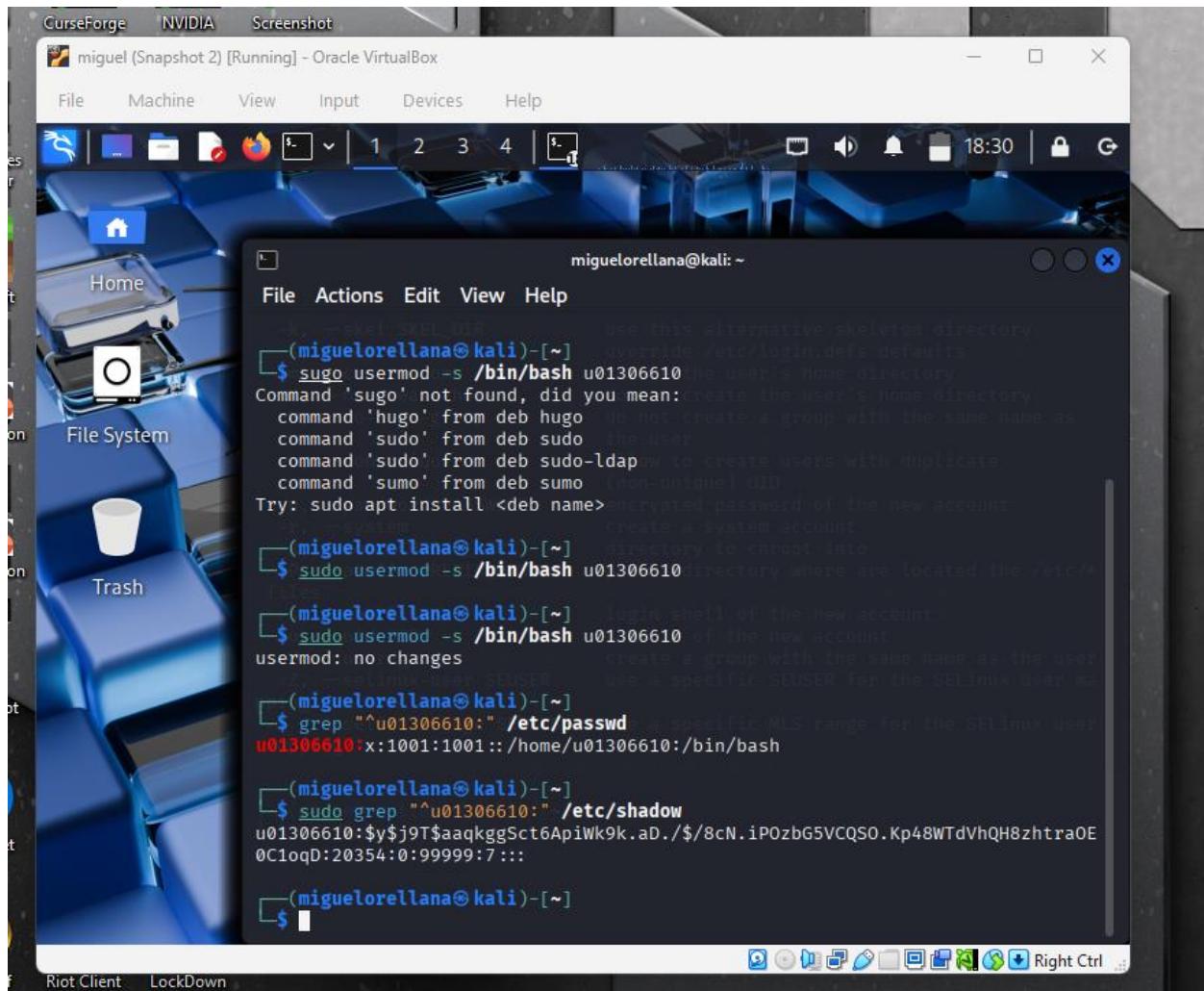
(miguelorellana@kali)-[~]
$ sudo usermod -s /bin/bash u01306610
Command 'sudo' not found, did you mean:
  command 'hugo' from deb hugo
  command 'sudo' from deb sudo
  command 'sudo' from deb sudo-ldap
  command 'sumo' from deb sumo
Try: sudo apt install <deb name>
usermod: no changes

(miguelorellana@kali)-[~]
$ grep "u01306610" /etc/passwd
u01306610:x:1001:1001::/home/u01306610:/bin/bash

(miguelorellana@kali)-[~]
$
```

Usermod -s sets the shell

6.



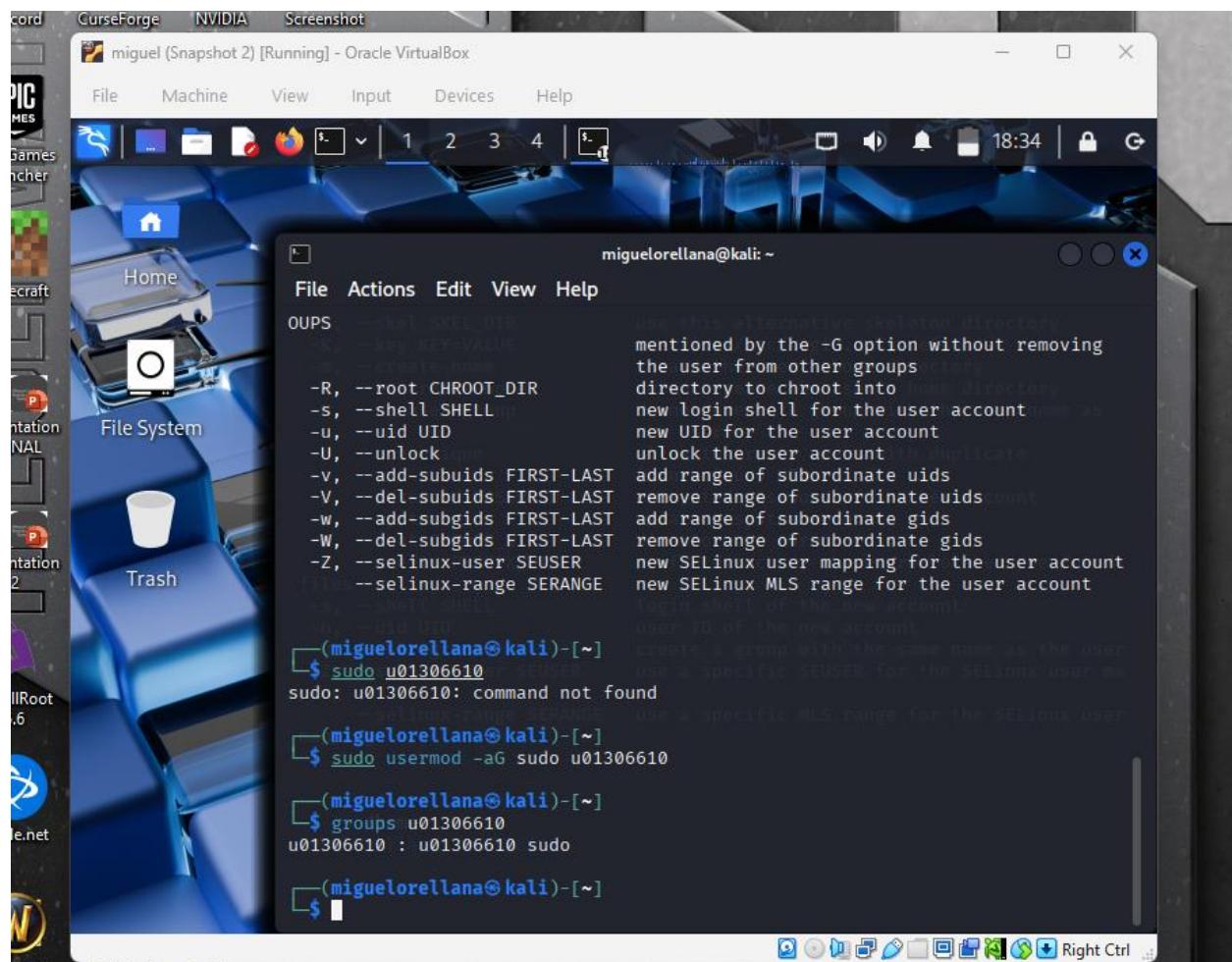
The screenshot shows a Kali Linux desktop environment within Oracle VirtualBox. The desktop background is a blue metallic keyboard. A terminal window is open in the foreground, showing the following command-line session:

```
miguelorellana@kali: ~
File Actions Edit View Help
[miguelorellana@kali] ~] override /etc/login.defs defaults
$ sudo usermod -s /bin/bash u01306610 he user's home directory
Command 'sugo' not found, did you mean:  create the user's home directory
  command 'hugo' from deb hugo  do not create a group with the same name as
  command 'sudo' from deb sudo  the user
  command 'sudo' from deb sudo-ldap  to create users with duplicate
  command 'sumo' from deb sumo  (non-unique) GID
Try: sudo apt install <deb name> encrypted password of the new account
$ sudo usermod -s /bin/bash u01306610 create a system account
$ sudo usermod -s /bin/bash u01306610 directory where are located the /etc/
files
$ sudo usermod -s /bin/bash u01306610 login shell of the new account
$ sudo usermod -s /bin/bash u01306610 of the new account
usermod: no changes
$ grep "u01306610:" /etc/passwd
u01306610:x:1001:1001::/home/u01306610:/bin/bash
$ sudo grep "u01306610:" /etc/shadow
u01306610:$y$j9T$aaqkgg5ct6ApiWk9k.aD./$8cN.iPOzbG5VCQSO.Kp48WTdVhQH8zhtraOE
0C1oqD:20354:0:99999:7:::
$
```

Displays password info for new user

Miguel orellana

7.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "miguelorellana@kali: ~". The terminal content includes SELinux documentation for the "usermod" command and several terminal commands:

```
miguelorellana@kali: ~
File Actions Edit View Help
OUPS
      KEYVALUE
-R, --root CHROOT_DIR
-s, --shell SHELL
-u, --uid UID
-U, --unlock
-v, --add-subuids FIRST-LAST
-V, --del-subuids FIRST-LAST
-w, --add-subgids FIRST-LAST
-W, --del-subgids FIRST-LAST
-Z, --selinux-user SEUSER
--selinux-range SERANGE

(miguelorellana@kali)-[~]
$ sudo u01306610
sudo: u01306610: command not found

(miguelorellana@kali)-[~]
$ sudo usermod -aG sudo u01306610

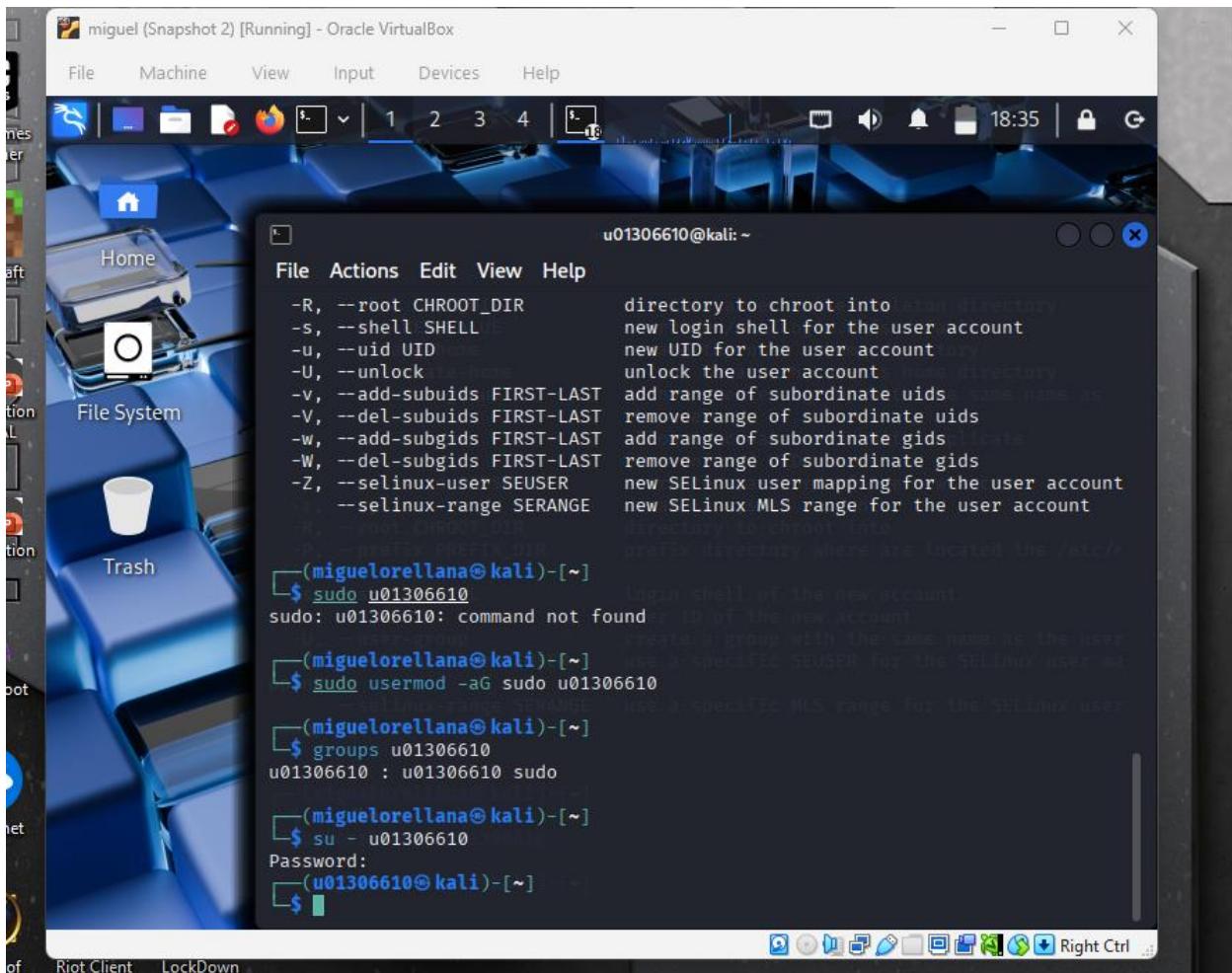
(miguelorellana@kali)-[~]
$ groups u01306610
u01306610 : u01306610 sudo

(miguelorellana@kali)-[~]
$
```

-aG appends to groups

8.

8.

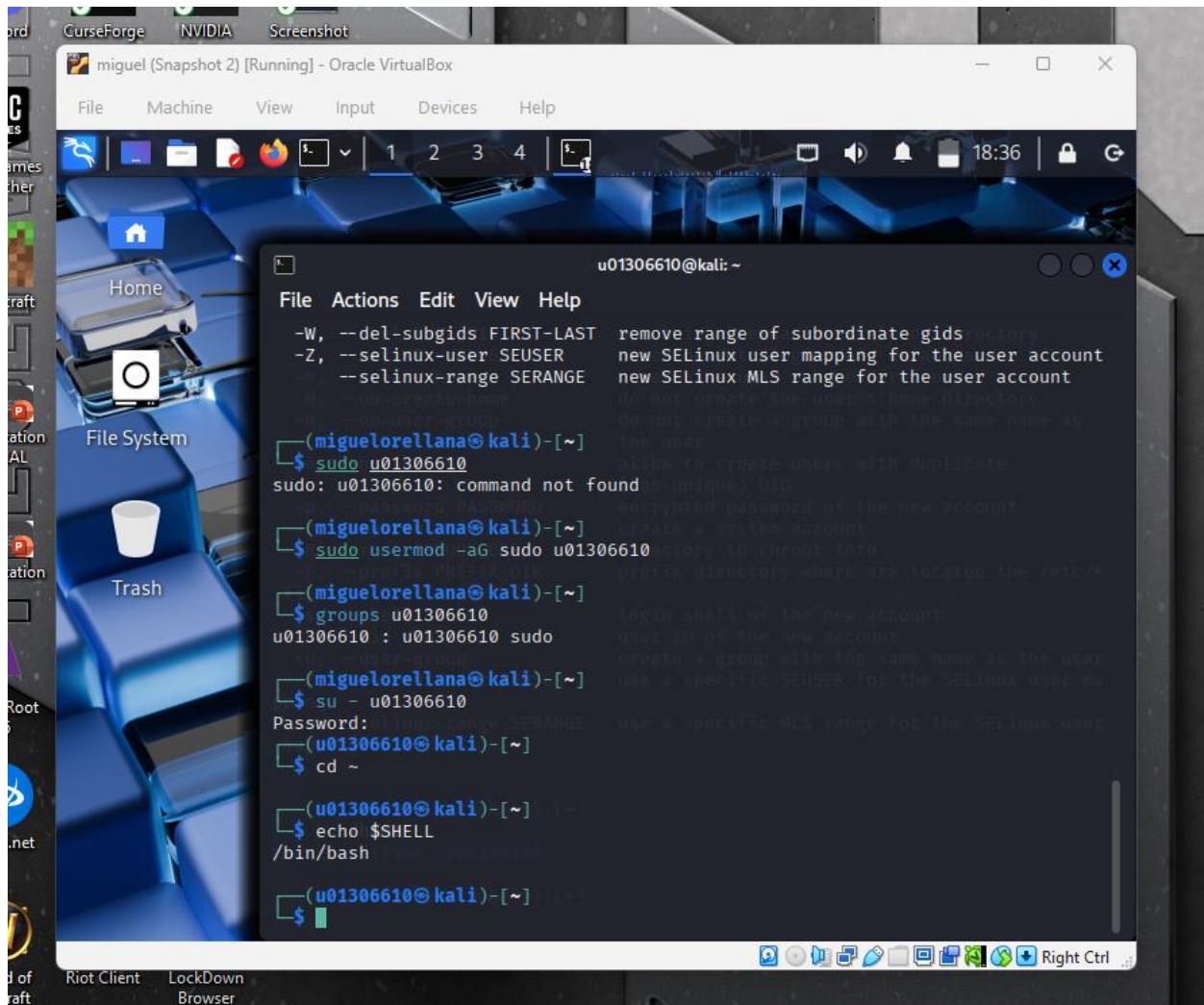


Tests that the account works and logs in properly

TASK B

Miguel orellana

1.



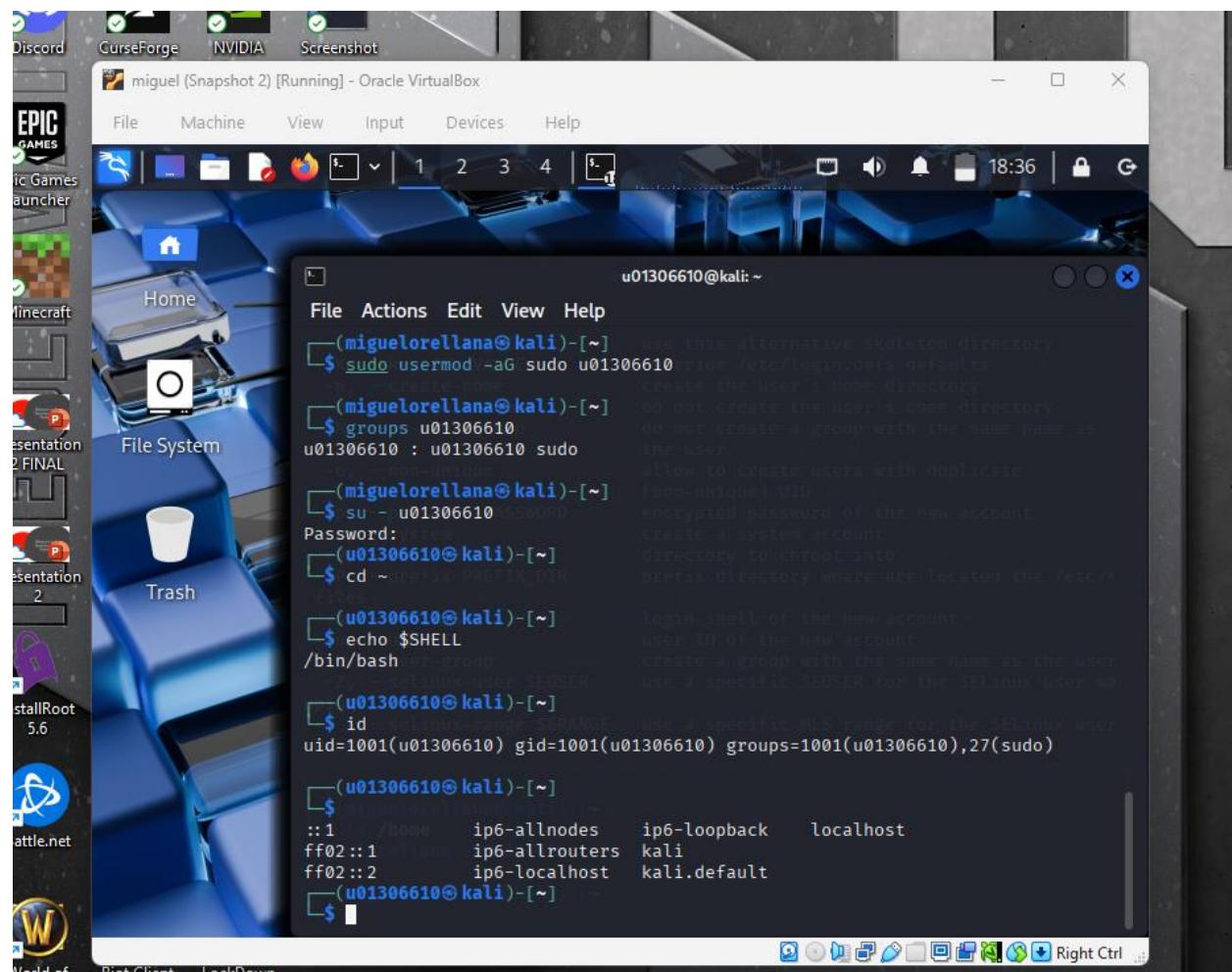
The screenshot shows a Kali Linux desktop environment within an Oracle VM VirtualBox window. The terminal window is titled 'miguel (Snapshot 2) [Running] - Oracle VirtualBox'. The terminal session is as follows:

```
u01306610@kali: ~
File Actions Edit View Help
-W, --del-subgids FIRST-LAST remove range of subordinate gids
-Z, --selinux-user SEUSER new SELinux user mapping for the user account
--selinux-range SERANGE new SELinux MLS range for the user account
do not create a group with the same name as the user
allow to create users with duplicate
File System
(miguelorellana@kali)-[~]
$ sudo u01306610
sudo: u01306610: command not found
(miguelorellana@kali)-[~]
$ sudo usermod -aG sudo u01306610
create a system account
factory to chroot into
prefix directory where are located the /etc/
login shell of the new account
user ID of the new account
create a group with the same name as the user
use a specific SEUSER for the SELinux user ma
use a specific MLS range for the SELinux user
$ groups u01306610
u01306610 : u01306610 sudo
(miguelorellana@kali)-[~]
$ su - u01306610
Password:
(miguelorellana@kali)-[~]
$ cd ~
(miguelorellana@kali)-[~]
$ echo $SHELL
/bin/bash
(miguelorellana@kali)-[~]
$
```

Confirms current shell environment

Miguel orellana

2.



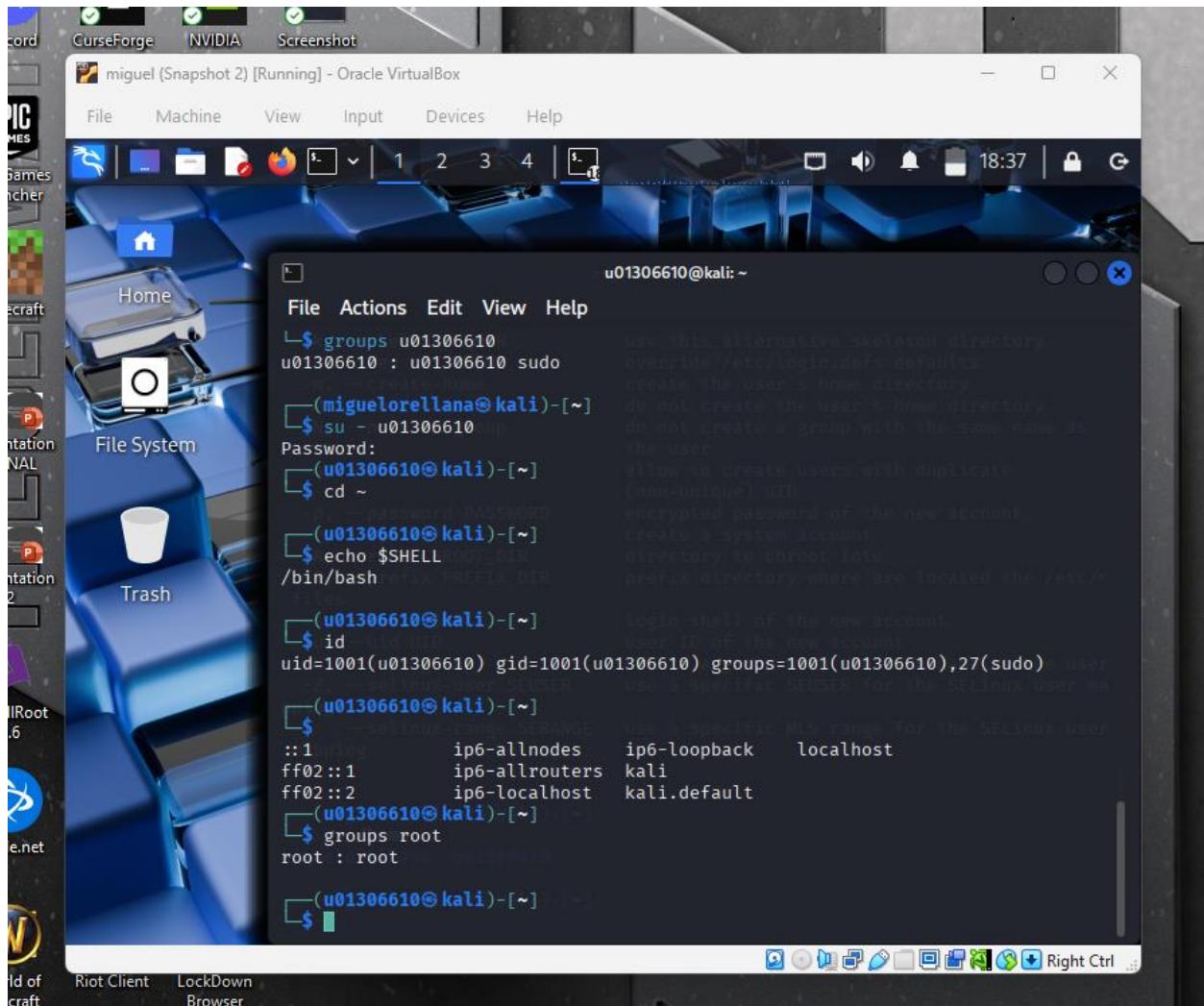
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "miguel (Snapshot 2) [Running] - Oracle VirtualBox". The terminal content shows a user privilege escalation exploit:

```
File Actions Edit View Help
(miguelorellana㉿kali)-[~] $ sudo usermod -A sudo u01306610
(miguelorellana㉿kali)-[~] $ groups u01306610
u01306610 : u01306610 sudo
(miguelorellana㉿kali)-[~] $ su - u01306610
Password:
(u01306610㉿kali)-[~] $ cd ~
(u01306610㉿kali)-[~] $ echo $SHELL
/bin/bash
(u01306610㉿kali)-[~] $ id
uid=1001(u01306610) gid=1001(u01306610) groups=1001(u01306610),27(sudo)
(u01306610㉿kali)-[~] $ ::1    /home      ip6-allnodes    ip6-loopback      localhost
ff02 :: 1      ip6-allrouters  kali
ff02 :: 2      ip6-localhost  kali.default
(u01306610㉿kali)-[~] $
```

Shows UID,GID, and group memberships

Miguel orellana

3.

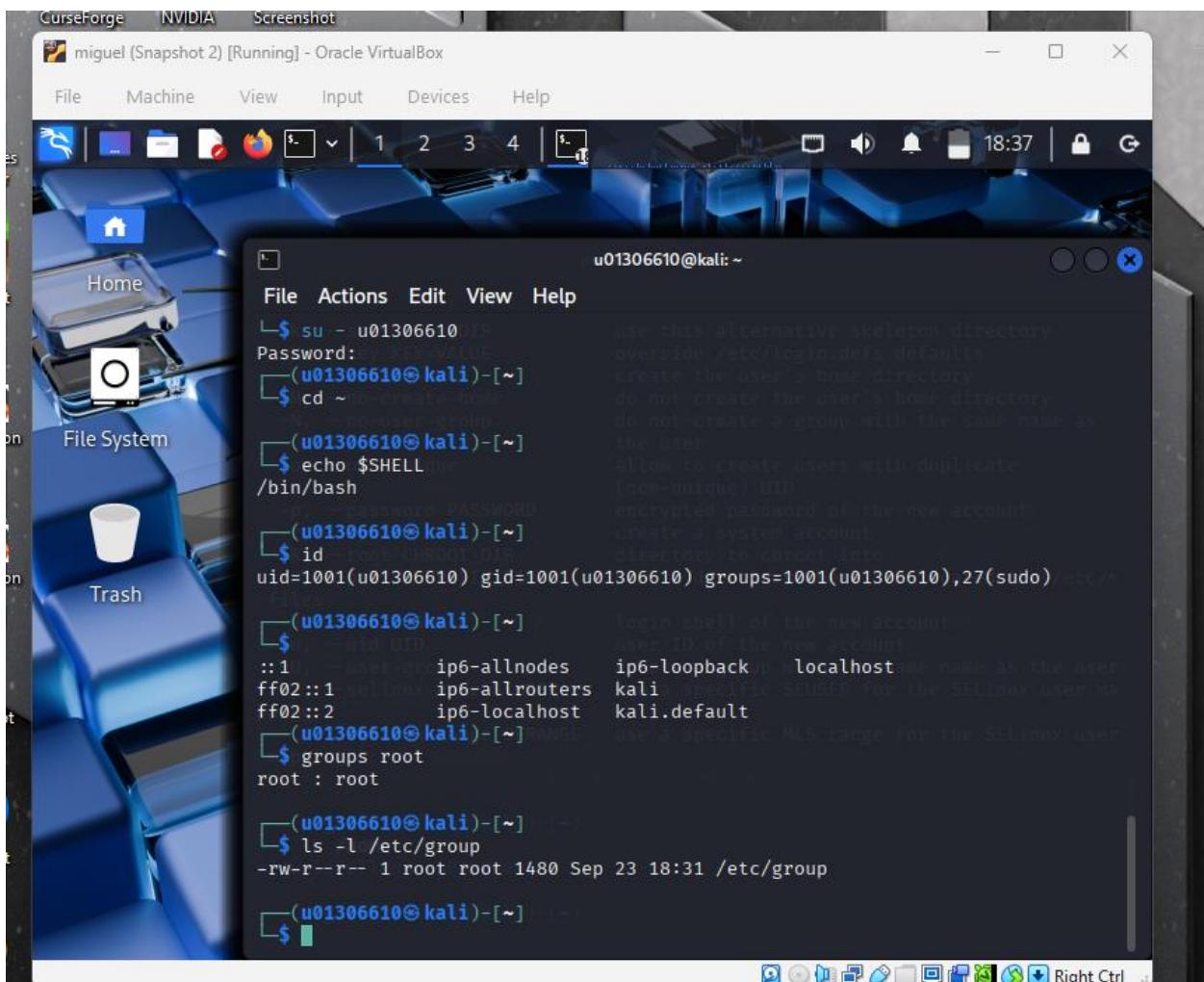


The screenshot shows a Kali Linux desktop environment within Oracle VirtualBox. The desktop background is a blue metallic keyboard. A terminal window is open in the foreground, showing the following session:

```
u01306610@miguel: ~
File Actions Edit View Help
└$ groups u01306610
u01306610 : u01306610 sudo
└(miguelorellana㉿kali)-[~]
└$ su - u01306610
Password:
└(u01306610㉿kali)-[~]
└$ cd ~
└$ echo $SHELL
/bin/bash
└(u01306610㉿kali)-[~]
└$ id
uid=1001(u01306610) gid=1001(u01306610) groups=1001(u01306610),27(sudo)
└(u01306610㉿kali)-[~]
└$ ip6 -a
::1      ip6-allnodes  ip6-loopback  localhost
ff02 ::1 ip6-allrouters  kali
ff02 ::2 ip6-localhost  kali.default
└(u01306610㉿kali)-[~]
└$ groups root
root : root
└(u01306610㉿kali)-[~]
```

Verifies root's group associations

4.

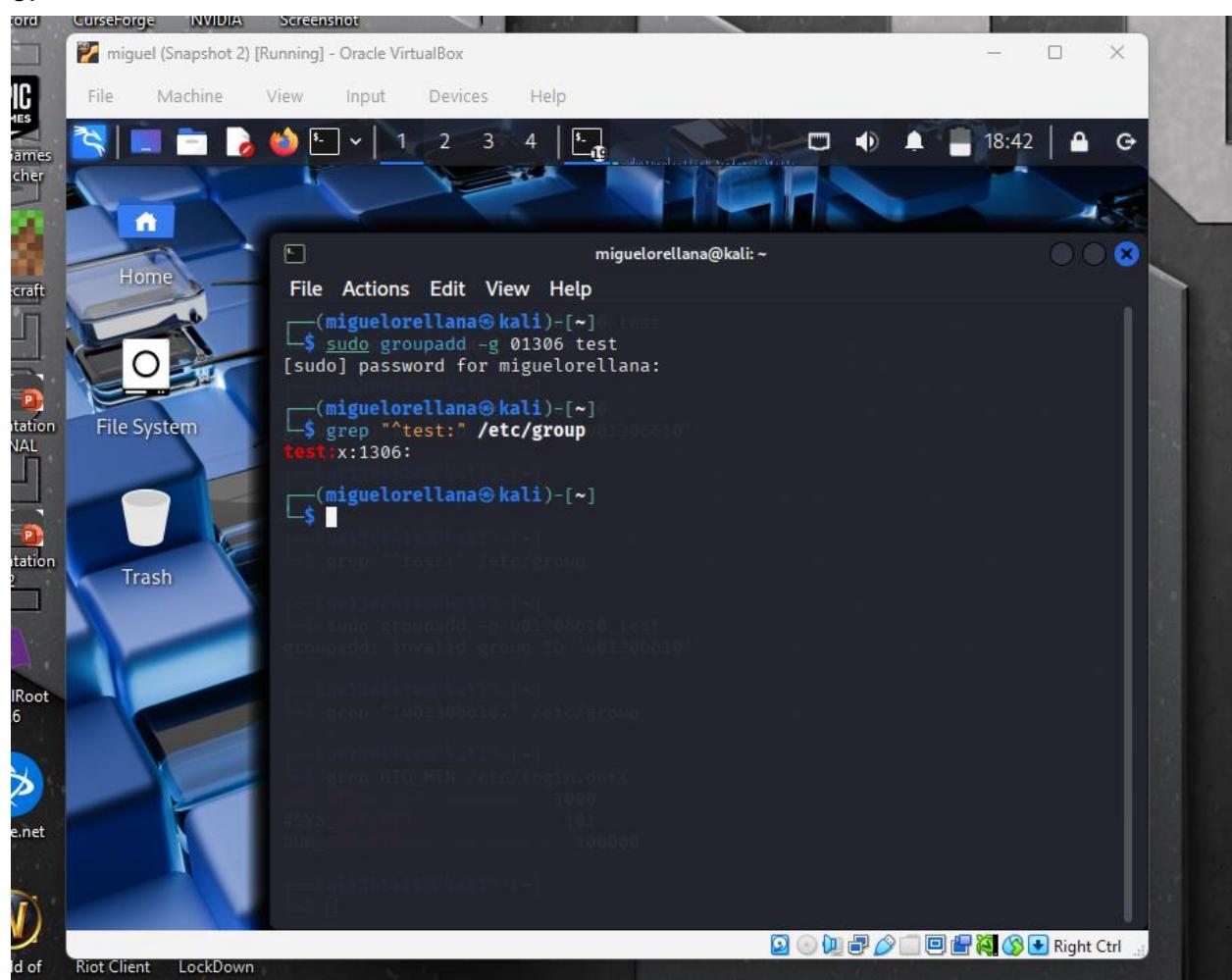


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "u01306610@kali: ~". The terminal content shows a user session starting with "su" to become root, followed by commands to check the user's home directory, shell, and groups. The desktop background is a blue keyboard image, and the taskbar at the bottom shows various application icons.

```
u01306610@kali: ~
File Actions Edit View Help
$ su - u01306610
Password:
(u01306610@kali)-[~]
$ cd ~
(u01306610@kali)-[~]
$ echo $SHELL
/bin/bash
(u01306610@kali)-[~]
$ id
uid=1001(u01306610) gid=1001(u01306610) groups=1001(u01306610),27(sudo)
(u01306610@kali)-[~]
$ 
::1      ip6-allnodes  ip6-loopback  localhost
ff02::1  ip6-allrouters kali          me name as the user
ff02::2  ip6-localhost kali.default
(u01306610@kali)-[~]
$ groups root
root : root
(u01306610@kali)-[~]
$ ls -l /etc/group
-rw-r--r-- 1 root root 1480 Sep 23 18:31 /etc/group
(u01306610@kali)-[~]
```

Shows who owns the group configuration file.

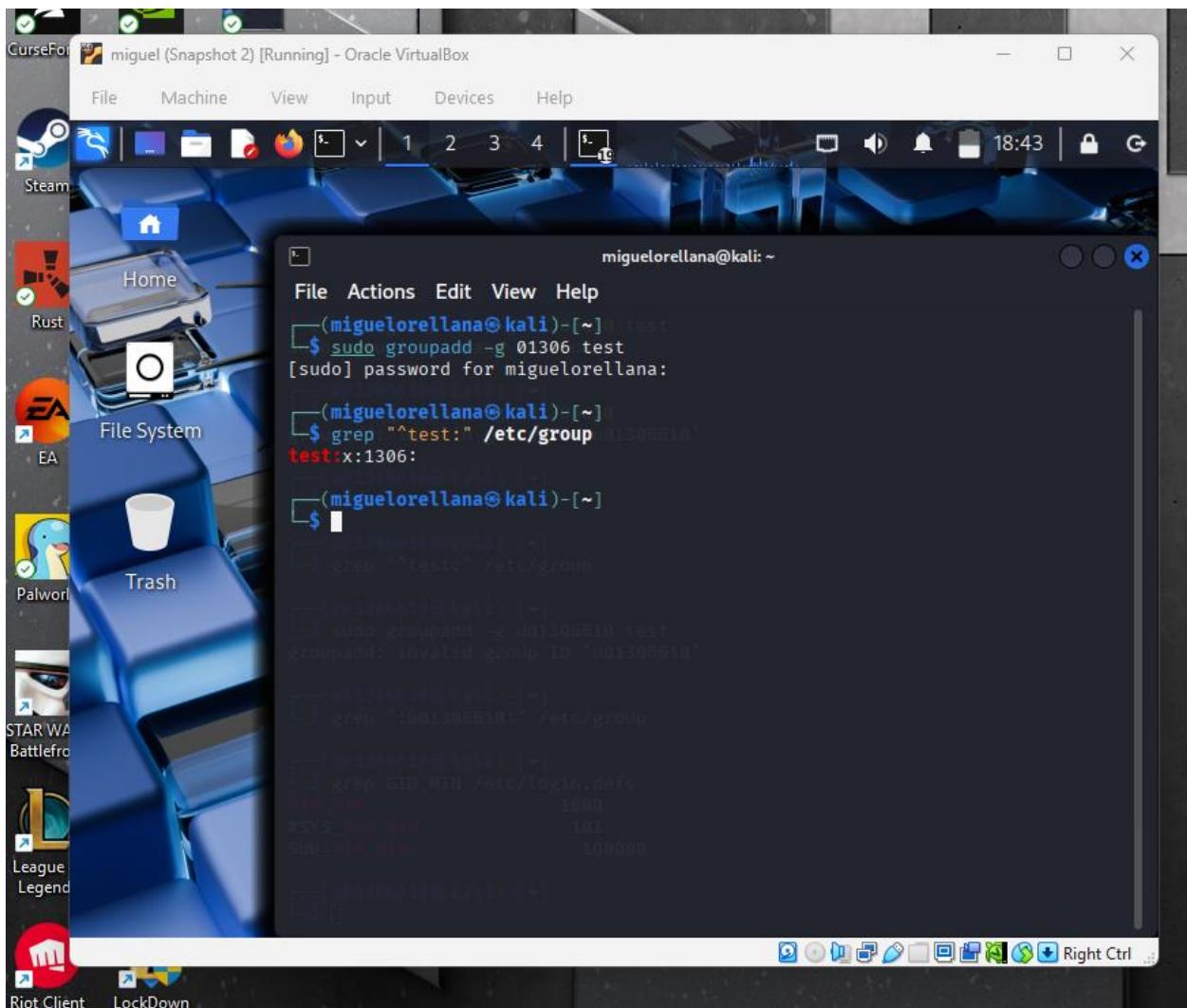
5.



Creates a group with a specific group ID

Miguel orellana

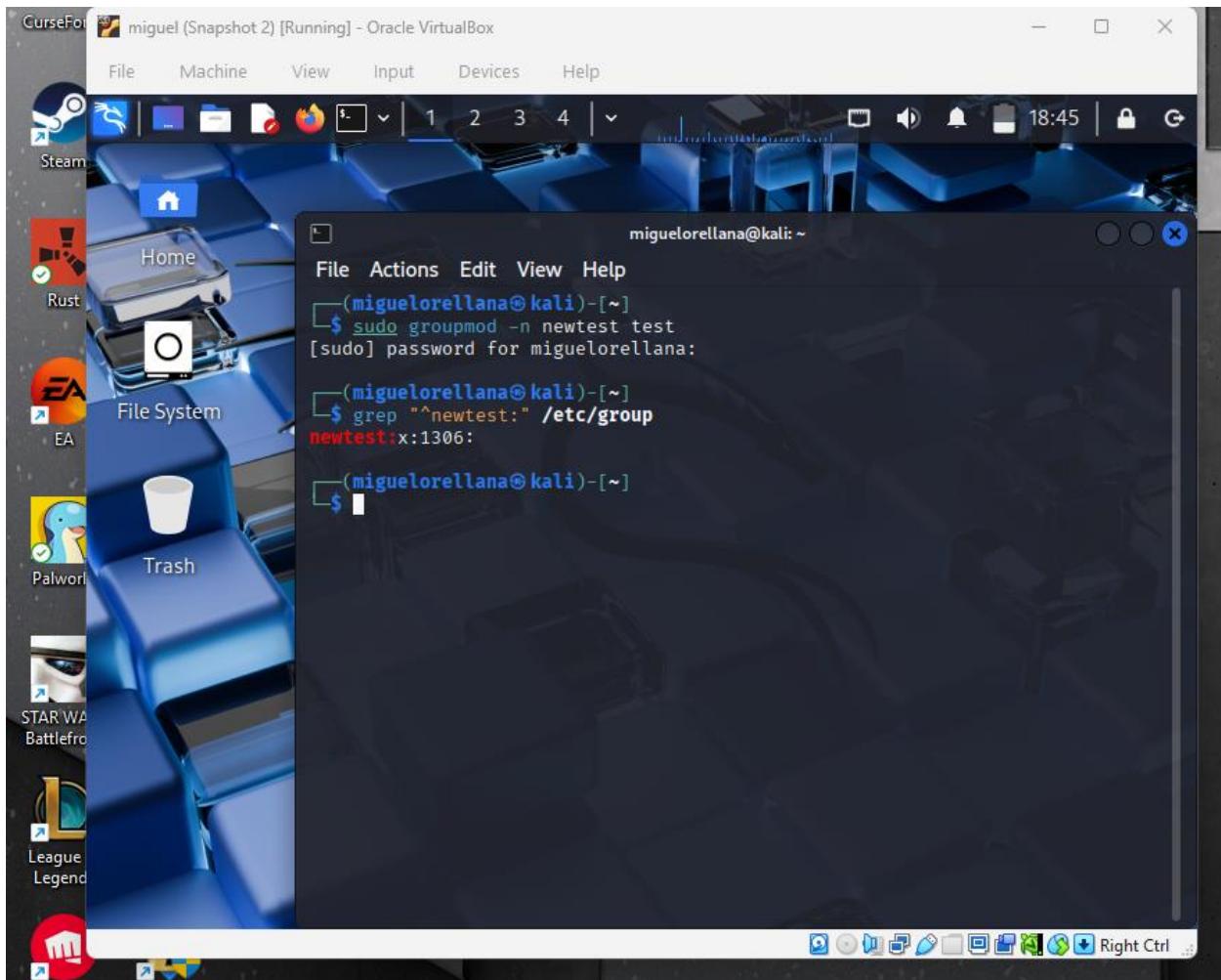
6.



```
miguelorellana@kali: ~
File Actions Edit View Help
(miguelorellana@kali)-[~] $ sudo groupadd -g 01306 test
[sudo] password for miguelorellana:
(miguelorellana@kali)-[~] $ grep "^\w+:" /etc/group
test:x:1306:
(miguelorellana@kali)-[~] $ grep "^\w+:" /etc/group
test:x:1306:
(miguelorellana@kali)-[~] $ sudo groupadd -g 001306610 test
groupadd: invalid group ID '001306610'
(miguelorellana@kali)-[~] $ grep "^\w+:" /etc/group
test:x:1306:
(miguelorellana@kali)-[~] $ grep GID_MIN /etc/login.defs
GID_MIN 1000
(miguelorellana@kali)-[~] $
```

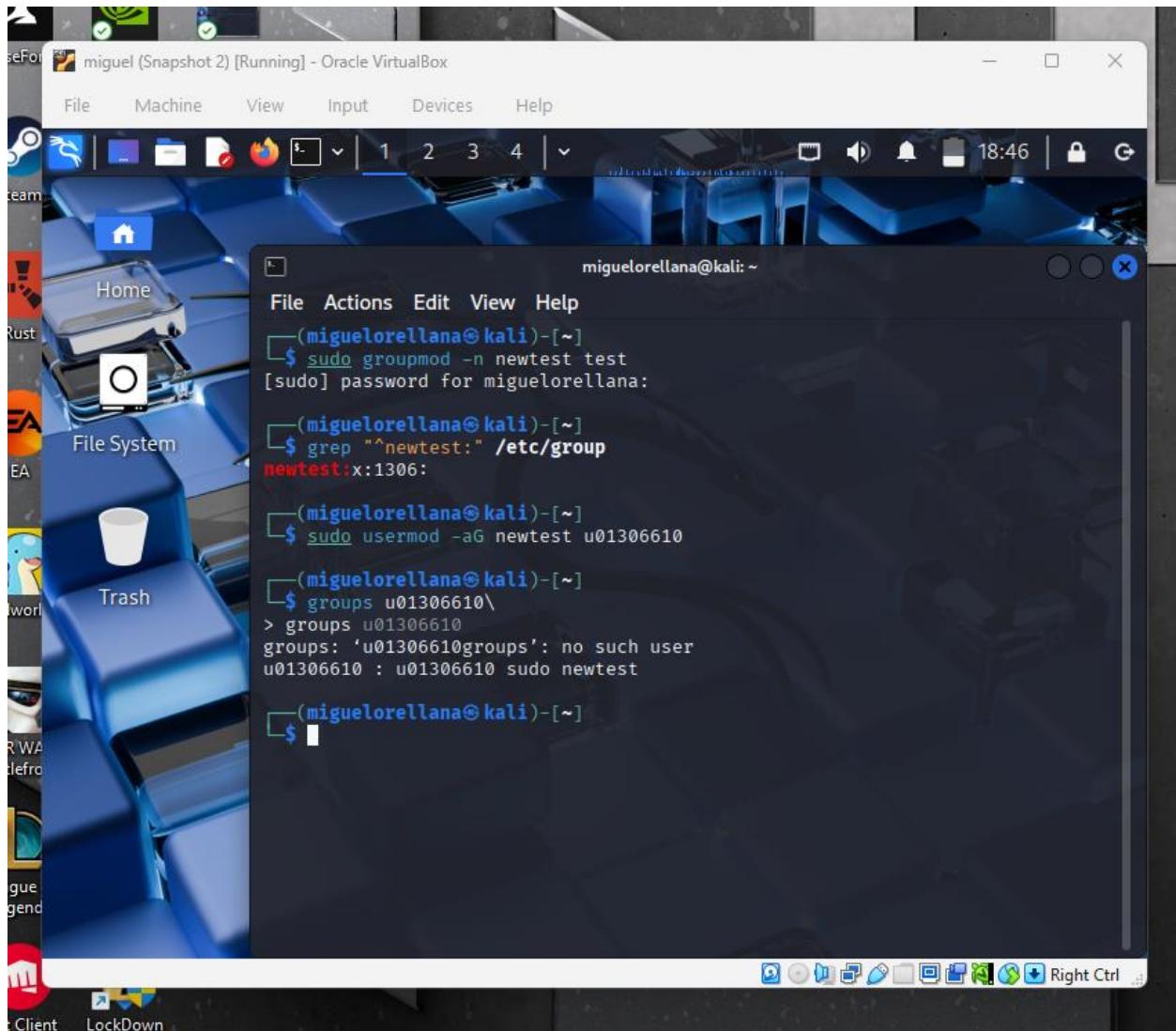
Confirms the group was created correctly

7.



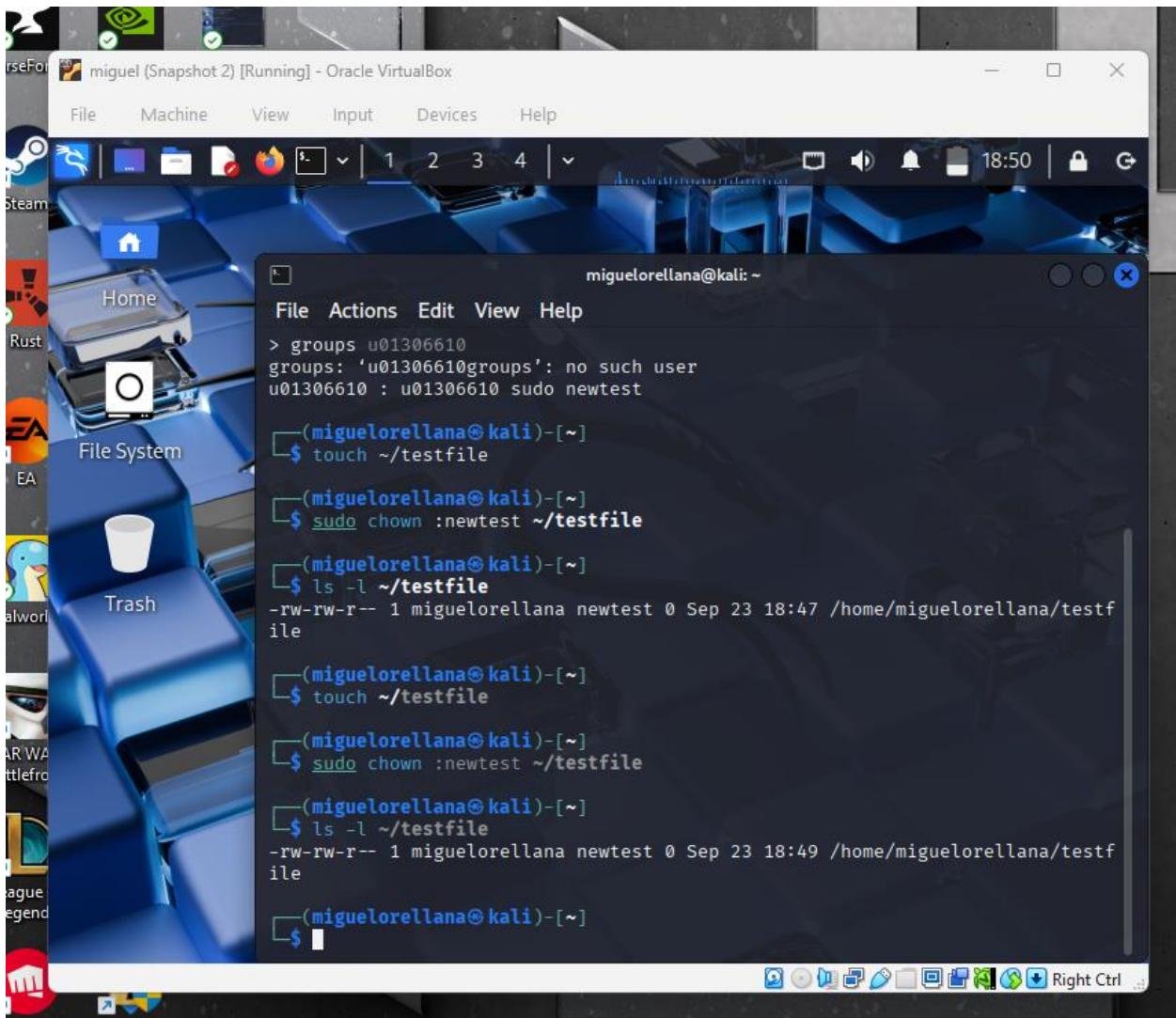
Renames the group

8.



Adds the user as a secondary member

9.



The screenshot shows a terminal window titled "miguel (Snapshot 2) [Running] - Oracle VirtualBox" running on a Kali Linux desktop. The terminal is displaying a command-line session where the user "miguelorellana" is attempting to gain root privileges. The session starts with the user checking their current groups, then creating a file named "testfile" in their home directory. They then use the "sudo chown" command to change the ownership of this file to the user "newtest". Finally, they verify the ownership change by listing the contents of the directory. The terminal window is part of a desktop environment with a blue-themed desktop background and various icons on the desktop.

```
miguelorellana@kali: ~
File Actions Edit View Help
> groups u01306610
groups: 'u01306610groups': no such user
u01306610 : u01306610 sudo newtest

[(miguelorellana@kali)-[~]
$ touch ~/testfile

[(miguelorellana@kali)-[~]
$ sudo chown :newtest ~/testfile

[(miguelorellana@kali)-[~]
$ ls -l ~/testfile
-rw-rw-r-- 1 miguelorellana newtest 0 Sep 23 18:47 /home/miguelorellana/testfile

[(miguelorellana@kali)-[~]
$ touch ~/testfile

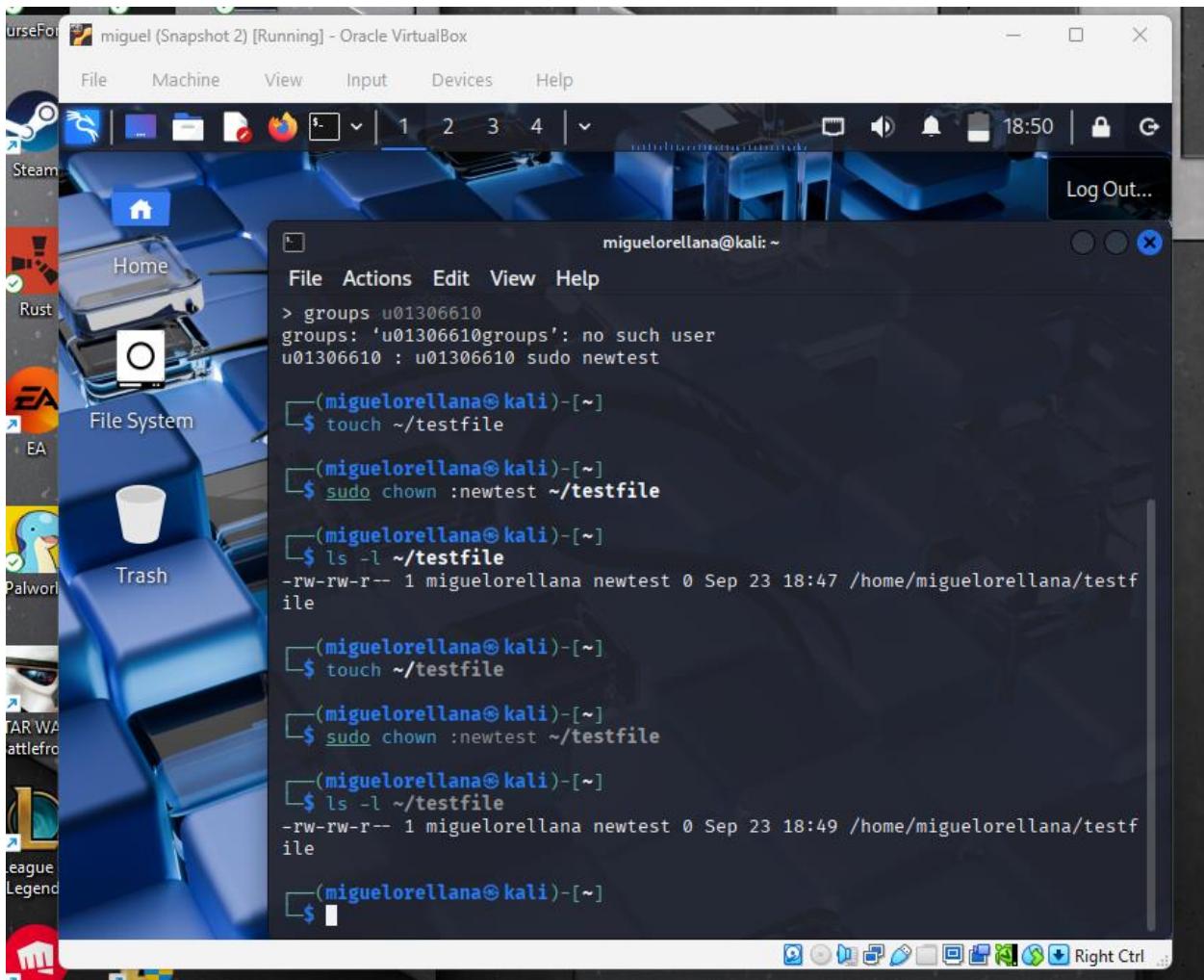
[(miguelorellana@kali)-[~]
$ sudo chown :newtest ~/testfile

[(miguelorellana@kali)-[~]
$ ls -l ~/testfile
-rw-rw-r-- 1 miguelorellana newtest 0 Sep 23 18:49 /home/miguelorellana/testfile

[(miguelorellana@kali)-[~]
$ ]
```

Creates a file and assigns group ownership

10.



```
miguelorellana@kali: ~
File Actions Edit View Help
> groups u01306610
groups: 'u01306610groups': no such user
u01306610 : u01306610 sudo newtest
  (miguelorellana@kali)-[~]
  $ touch ~/testfile

  (miguelorellana@kali)-[~]
  $ sudo chown :newtest ~testfile

  (miguelorellana@kali)-[~]
  $ ls -l ~testfile
-rw-rw-r-- 1 miguelorellana newtest 0 Sep 23 18:47 /home/miguelorellana/testfile

  (miguelorellana@kali)-[~]
  $ touch ~testfile

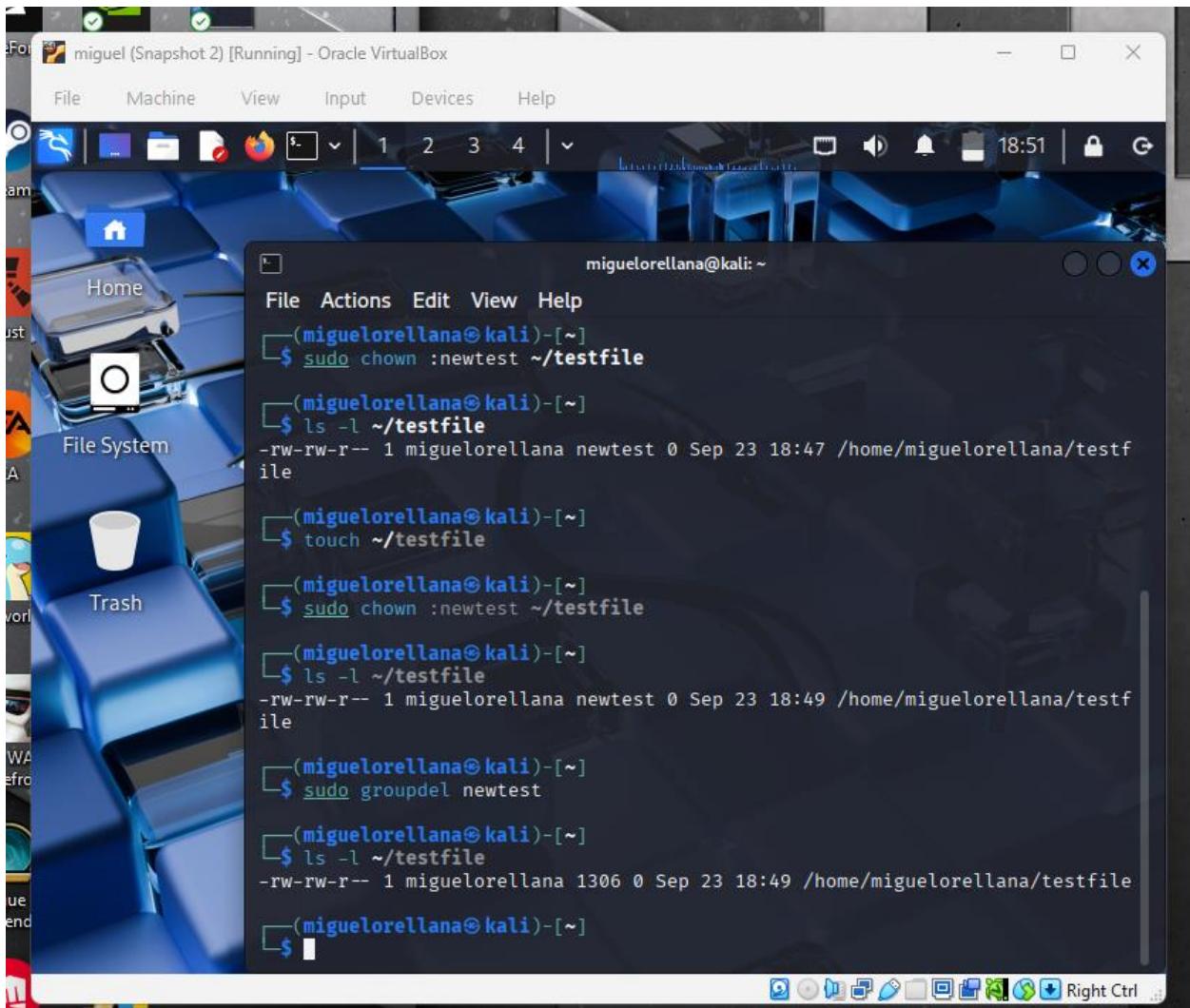
  (miguelorellana@kali)-[~]
  $ sudo chown :newtest ~testfile

  (miguelorellana@kali)-[~]
  $ ls -l ~testfile
-rw-rw-r-- 1 miguelorellana newtest 0 Sep 23 18:49 /home/miguelorellana/testfile

  (miguelorellana@kali)-[~]
  $
```

confirms the files user and group ownership

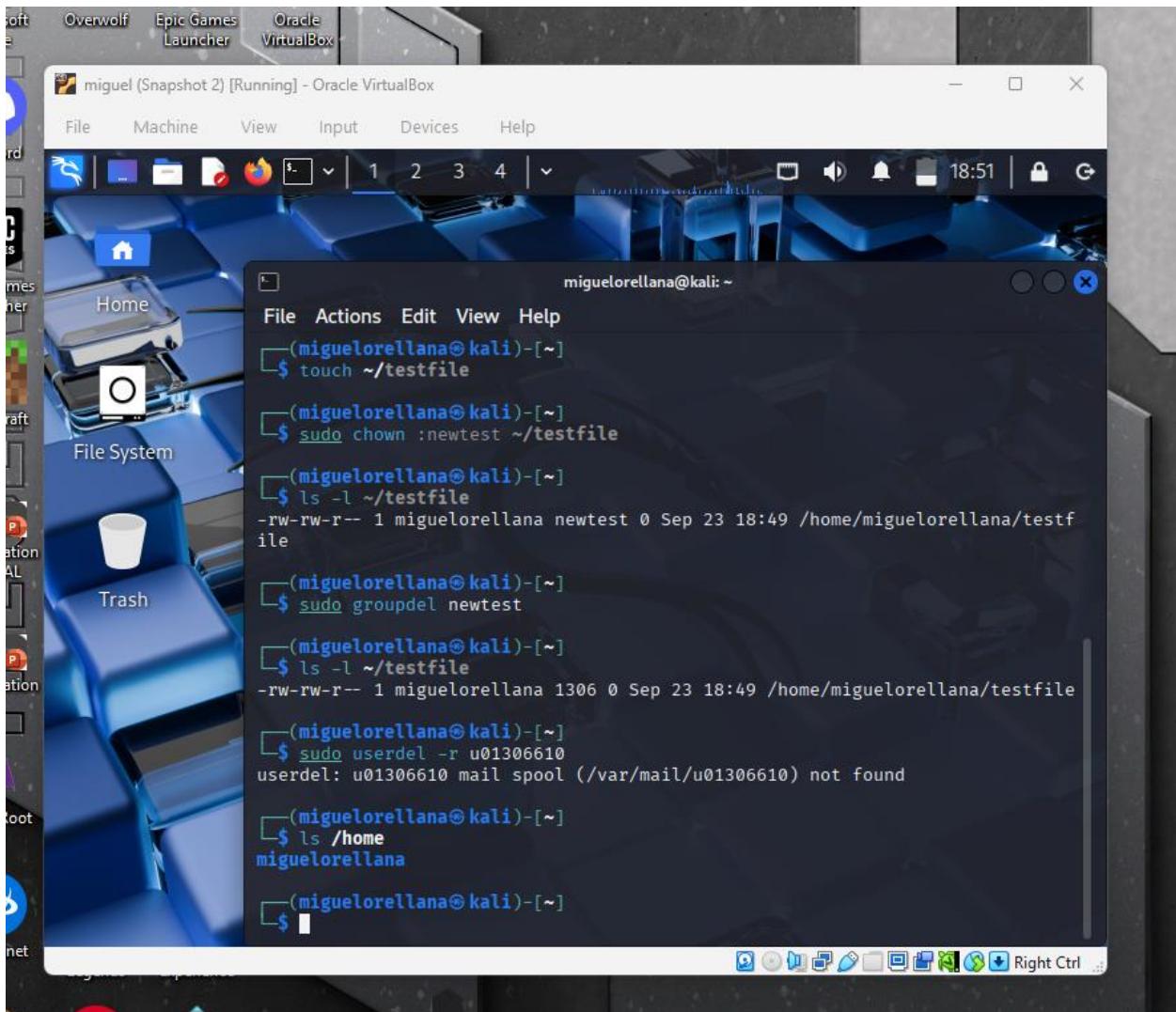
11.



```
miguelorellana@kali: ~
File Actions Edit View Help
(miguelorellana@kali)~
$ sudo chown :newtest ~/testfile
(miguelorellana@kali)~
$ ls -l ~/testfile
-rw-rw-r-- 1 miguelorellana newtest 0 Sep 23 18:47 /home/miguelorellana/testfile
(miguelorellana@kali)~
$ touch ~/testfile
(miguelorellana@kali)~
$ sudo chown :newtest ~/testfile
(miguelorellana@kali)~
$ ls -l ~/testfile
-rw-rw-r-- 1 miguelorellana newtest 0 Sep 23 18:49 /home/miguelorellana/testfile
(miguelorellana@kali)~
$ sudo groupdel newtest
(miguelorellana@kali)~
$ ls -l ~/testfile
-rw-rw-r-- 1 miguelorellana 1306 0 Sep 23 18:49 /home/miguelorellana/testfile
(miguelorellana@kali)~
$
```

Tests what happens when the group is deleted

12.



```
miguel (Snapshot 2) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File System Home Trash
miguelorellana@kali: ~
File Actions Edit View Help
(miguelorellana@kali) [~]
$ touch ~/testfile

(miguelorellana@kali) [~]
$ sudo chown :newtest ~/testfile

(miguelorellana@kali) [~]
$ ls -l ~/testfile
-rw-rw-r-- 1 miguelorellana newtest 0 Sep 23 18:49 /home/miguelorellana/testfile

(miguelorellana@kali) [~]
$ sudo groupdel newtest

(miguelorellana@kali) [~]
$ ls -l ~/testfile
-rw-rw-r-- 1 miguelorellana 1306 0 Sep 23 18:49 /home/miguelorellana/testfile

(miguelorellana@kali) [~]
$ sudo userdel -r u01306610
userdel: u01306610 mail spool (/var/mail/u01306610) not found

(miguelorellana@kali) [~]
$ ls /home
miguelorellana

(miguelorellana@kali) [~]
$
```

Remove the user and their home folder