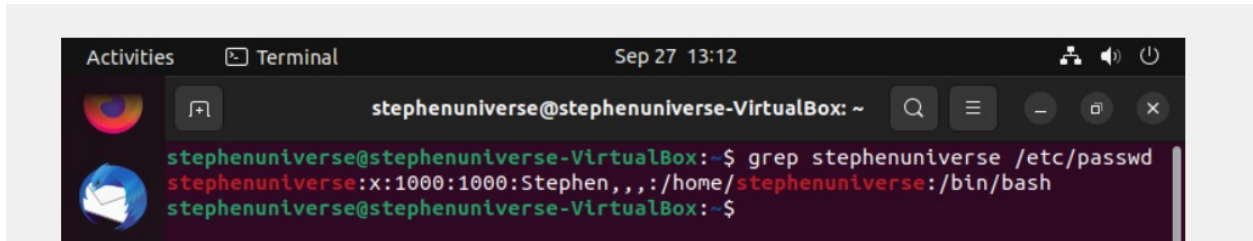


# **CYSE 270: Linux System for Cybersecurity Assignment: Lab 4 – Group and User Accounts**

Kevin Durand

### Task A – User Account management

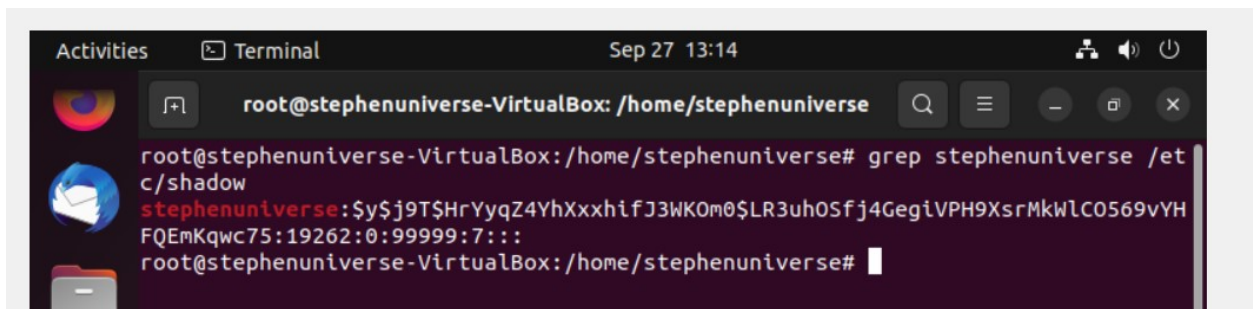
1. Open a terminal window in VM and execute the correct command to display user account information (including the login shell and home directory) for the current user using grep.



A terminal window titled 'Terminal' with the date 'Sep 27 13:12'. The prompt is 'stephenuniverse@stephenuniverse-VirtualBox: ~'. The command 'grep stephenuniverse /etc/passwd' is entered, and the output is 'stephenuniverse:x:1000:1000:Stephen,,,:/home/stephenuniverse:/bin/bash'.

```
stephenuniverse@stephenuniverse-VirtualBox:~$ grep stephenuniverse /etc/passwd
stephenuniverse:x:1000:1000:Stephen,,,:/home/stephenuniverse:/bin/bash
stephenuniverse@stephenuniverse-VirtualBox:~$
```

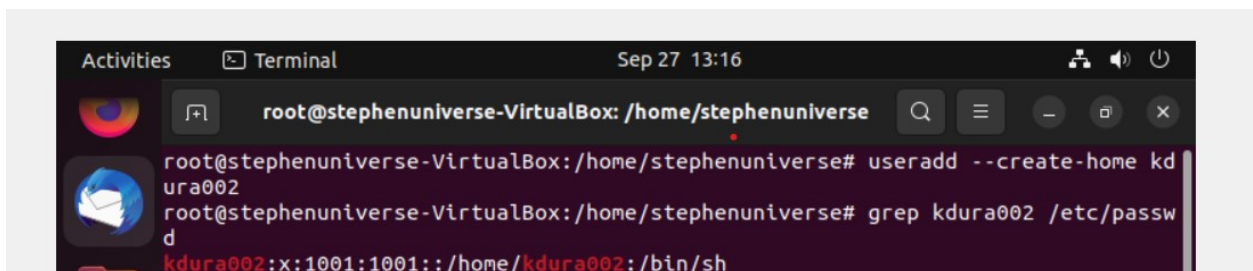
2. Execute the correct command to display user password information (including the encrypted password and password aging) for the current user using grep.



A terminal window titled 'Terminal' with the date 'Sep 27 13:14'. The prompt is 'root@stephenuniverse-VirtualBox: /home/stephenuniverse'. The command 'grep stephenuniverse /etc/shadow' is entered, and the output is 'stephenuniverse:\$y\$j9T\$HrYyqZ4YhXxxhifJ3WK0m0\$LR3uh0Sfj4GegIvPH9XsrMkWlC0569vYHFQEmKqwc75:19262:0:99999:7:::'. The prompt then returns to 'root@stephenuniverse-VirtualBox: /home/stephenuniverse#'.

```
root@stephenuniverse-VirtualBox:/home/stephenuniverse# grep stephenuniverse /etc/shadow
stephenuniverse:$y$j9T$HrYyqZ4YhXxxhifJ3WK0m0$LR3uh0Sfj4GegIvPH9XsrMkWlC0569vYHFQEmKqwc75:19262:0:99999:7:::
root@stephenuniverse-VirtualBox:/home/stephenuniverse#
```

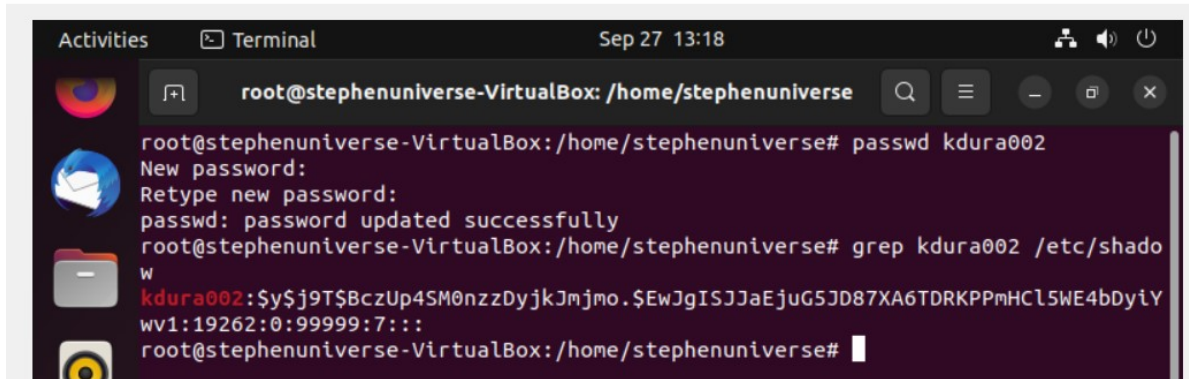
3. Create a new user named xxxxxx and explicitly use options to create the home directory /home/xxxxxx for this user.



A terminal window titled 'Terminal' with the date 'Sep 27 13:16'. The prompt is 'root@stephenuniverse-VirtualBox: /home/stephenuniverse'. The command 'useradd --create-home kdura002' is entered. The prompt then returns to 'root@stephenuniverse-VirtualBox: /home/stephenuniverse#'. The command 'grep kdura002 /etc/passwd' is entered, and the output is 'kdura002:x:1001:1001::/home/kdura002:/bin/sh'.

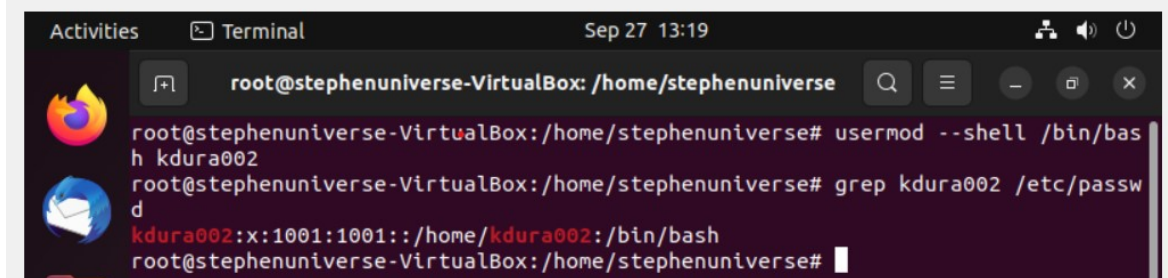
```
root@stephenuniverse-VirtualBox:/home/stephenuniverse# useradd --create-home kdura002
root@stephenuniverse-VirtualBox:/home/stephenuniverse# grep kdura002 /etc/passwd
kdura002:x:1001:1001::/home/kdura002:/bin/sh
```

- Set a password for the new user.



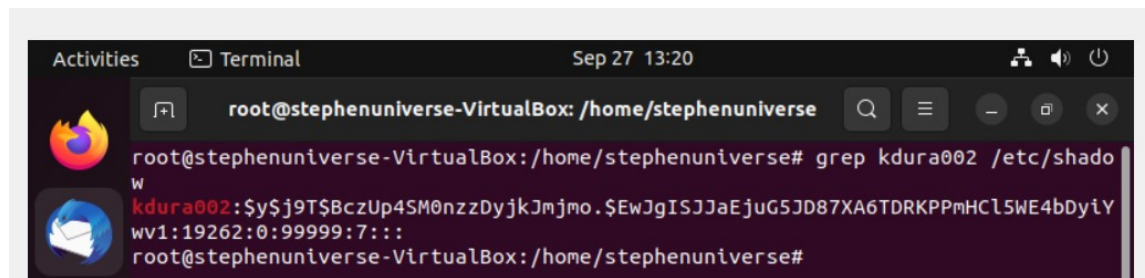
A terminal window titled 'Activities Terminal' with the date 'Sep 27 13:18'. The prompt is 'root@stephenuniverse-VirtualBox: /home/stephenuniverse'. The user enters 'passwd kdura002'. The terminal shows 'New password:', 'Retype new password:', and 'passwd: password updated successfully'. Then, the user enters 'grep kdura002 /etc/shadow', showing the user's entry: 'kdura002:\$y\$j9T\$BczUp4SM0nzzDyjkJmjmo.\$EWJgISJJJaEjuG5JD87XA6TDRKPPmHCL5WE4bDyiYwv1:19262:0:99999:7:::'. The prompt returns to 'root@stephenuniverse-VirtualBox: /home/stephenuniverse#'.

- Set bash shell as the default login shell for the new user xxxxx, then verify the change.



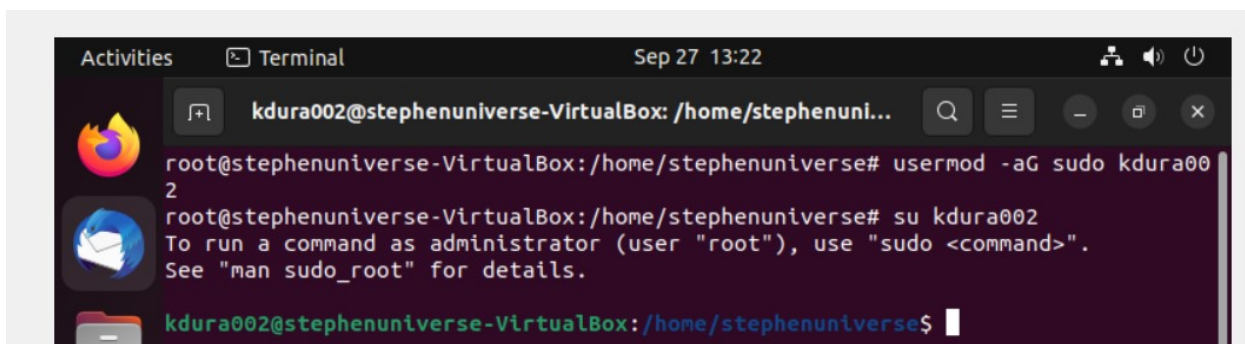
A terminal window titled 'Activities Terminal' with the date 'Sep 27 13:19'. The prompt is 'root@stephenuniverse-VirtualBox: /home/stephenuniverse'. The user enters 'usermod --shell /bin/bash kdura002'. Then, the user enters 'grep kdura002 /etc/passwd', showing the user's entry: 'kdura002:x:1001:1001::/home/kdura002:/bin/bash'. The prompt returns to 'root@stephenuniverse-VirtualBox: /home/stephenuniverse#'.

- Execute the correct command to display user password information (including the encrypted password and password aging) for the new user xxxxx using grep.



A terminal window titled 'Activities Terminal' with the date 'Sep 27 13:20'. The prompt is 'root@stephenuniverse-VirtualBox: /home/stephenuniverse'. The user enters 'grep kdura002 /etc/shadow', showing the user's entry: 'kdura002:\$y\$j9T\$BczUp4SM0nzzDyjkJmjmo.\$EWJgISJJJaEjuG5JD87XA6TDRKPPmHCL5WE4bDyiYwv1:19262:0:99999:7:::'. The prompt returns to 'root@stephenuniverse-VirtualBox: /home/stephenuniverse#'.

- Add the new user xxxxx to sudo group without overriding the existing group membership.
- Switch to the new user's account.



A terminal window titled 'Activities Terminal' with the date 'Sep 27 13:22'. The prompt is 'kdura002@stephenuniverse-VirtualBox: /home/stephenuniverse\$'. The user enters 'usermod -aG sudo kdura002'. Then, the user enters 'su kdura002', showing the message: 'To run a command as administrator (user "root"), use "sudo <command>". See "man sudo\_root" for details.'. The prompt returns to 'kdura002@stephenuniverse-VirtualBox: /home/stephenuniverse\$'.

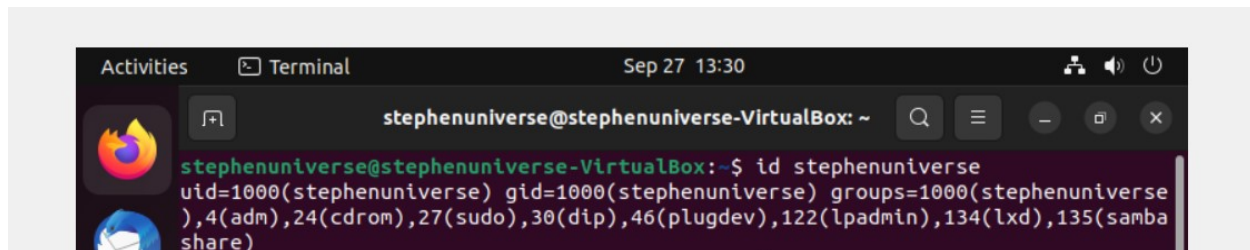
## Task B – Group account management

1. Return to your home directory and determine the shell you are using.



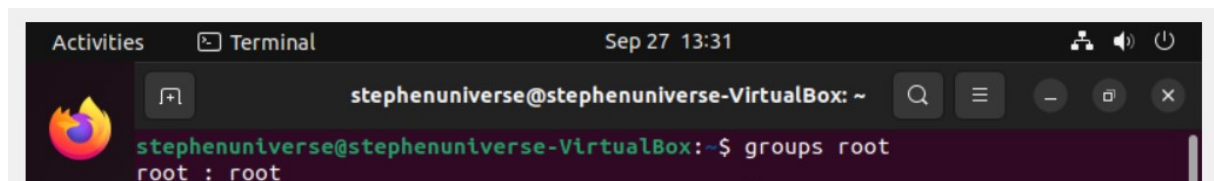
```
kdura002@stephenuniverse-VirtualBox: /home/stephenuniverse$ sudo usermod -s /bin/bash stephenuniverse
[sudo] password for kdura002:
kdura002@stephenuniverse-VirtualBox: /home/stephenuniverse$ su stephenuniverse
Password:
stephenuniverse@stephenuniverse-VirtualBox: ~$
```

2. Display the current user's ID and group membership.



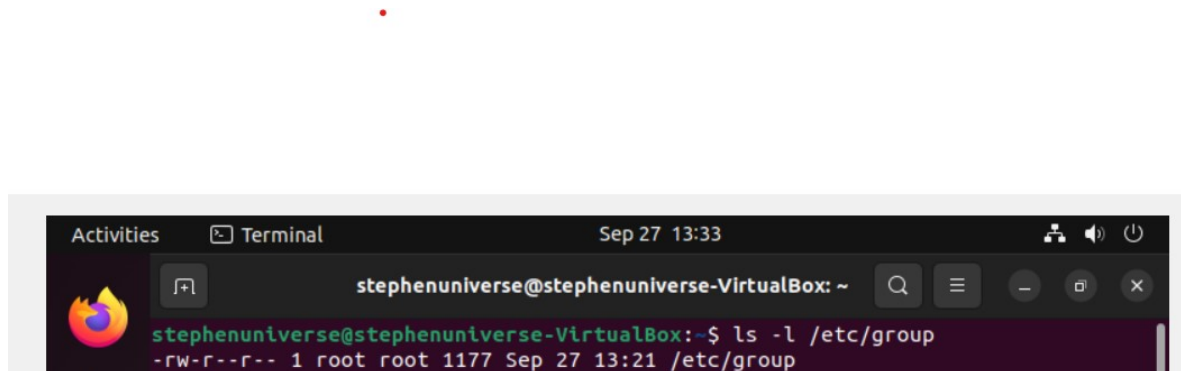
```
stephenuniverse@stephenuniverse-VirtualBox: ~$ id stephenuniverse
uid=1000(stephenuniverse) gid=1000(stephenuniverse) groups=1000(stephenuniverse),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),122(lpadmin),134(lxd),135(samba-share)
```

3. Display the group membership of the root account.



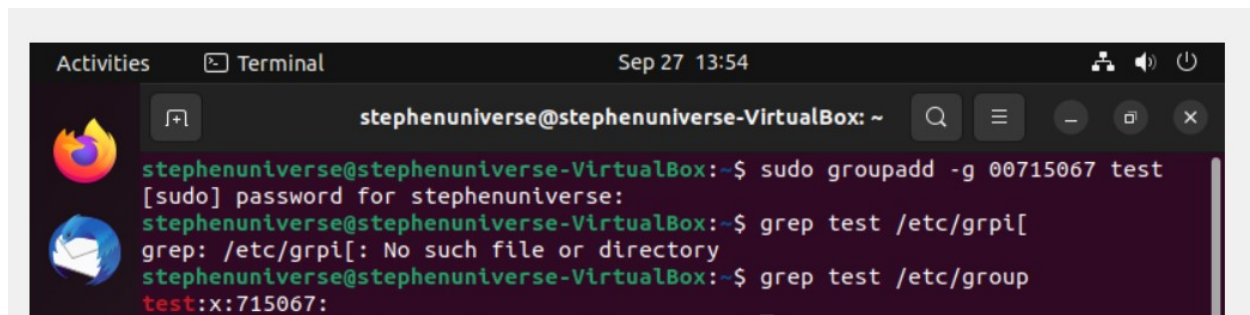
```
stephenuniverse@stephenuniverse-VirtualBox: ~$ groups root
root : root
```

4. Run the correct command to determine the user owner and group owner of the /etc/group file.



```
stephenuniverse@stephenuniverse-VirtualBox: ~$ ls -l /etc/group
-rw-r--r-- 1 root root 1177 Sep 27 13:21 /etc/group
```

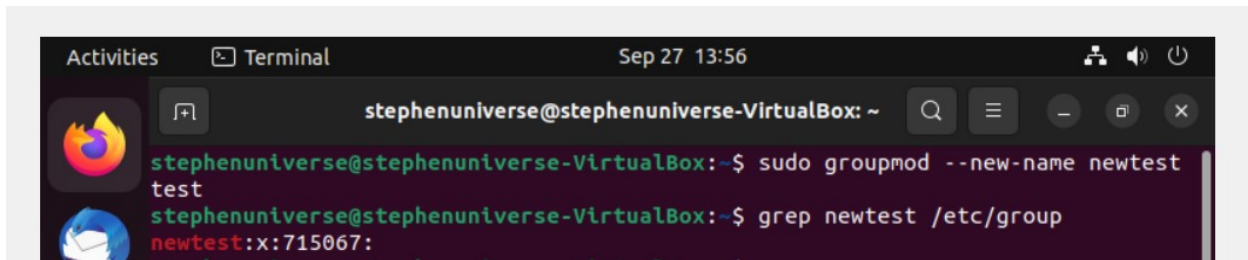
5. Create a new group named test and use your UIN as the GID.
6. Display the group account information for the test group using grep.



```
stephenuniverse@stephenuniverse-VirtualBox: ~$ sudo groupadd -g 00715067 test
[sudo] password for stephenuniverse:
stephenuniverse@stephenuniverse-VirtualBox: ~$ grep test /etc/grp[
grep: /etc/grp[[: No such file or directory
stephenuniverse@stephenuniverse-VirtualBox: ~$ grep test /etc/group
test:x:715067:
```

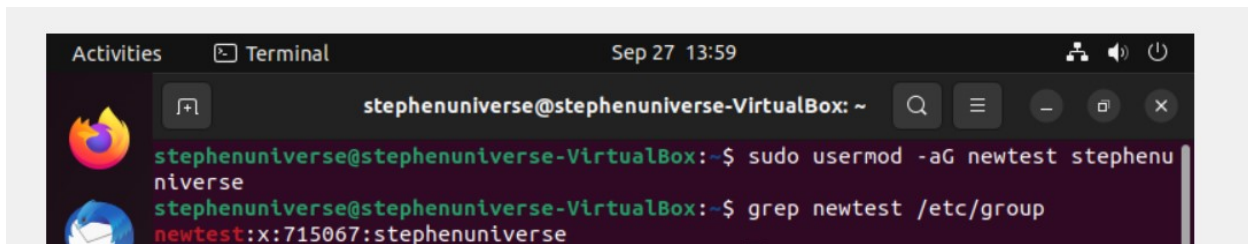


7. Change the group name of the test group to newtest.



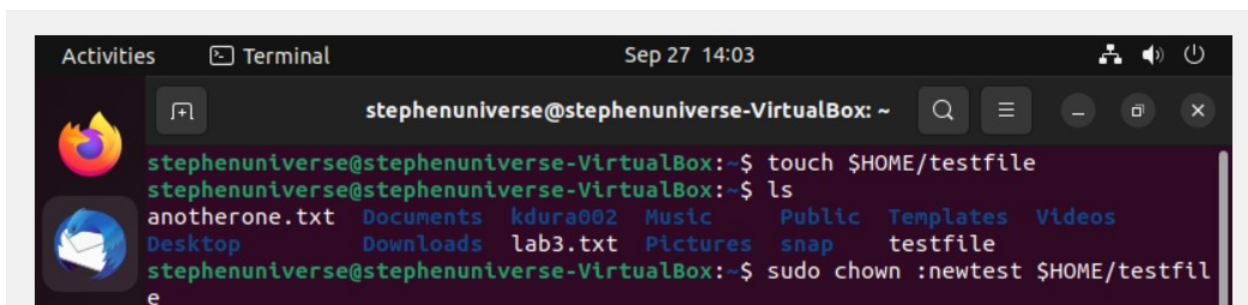
```
stephenuniverse@stephenuniverse-VirtualBox: ~  
stephenuniverse@stephenuniverse-VirtualBox:~$ sudo groupmod --new-name newtest test  
stephenuniverse@stephenuniverse-VirtualBox:~$ grep newtest /etc/group  
newtest:x:715067:
```

8. Add the current account (xxxxx) as a secondary member of the newtest group without overriding this user's current group membership.



```
stephenuniverse@stephenuniverse-VirtualBox:~$ sudo usermod -aG newtest stephenuniverse  
stephenuniverse@stephenuniverse-VirtualBox:~$ grep newtest /etc/group  
newtest:x:715067:stephenuniverse
```

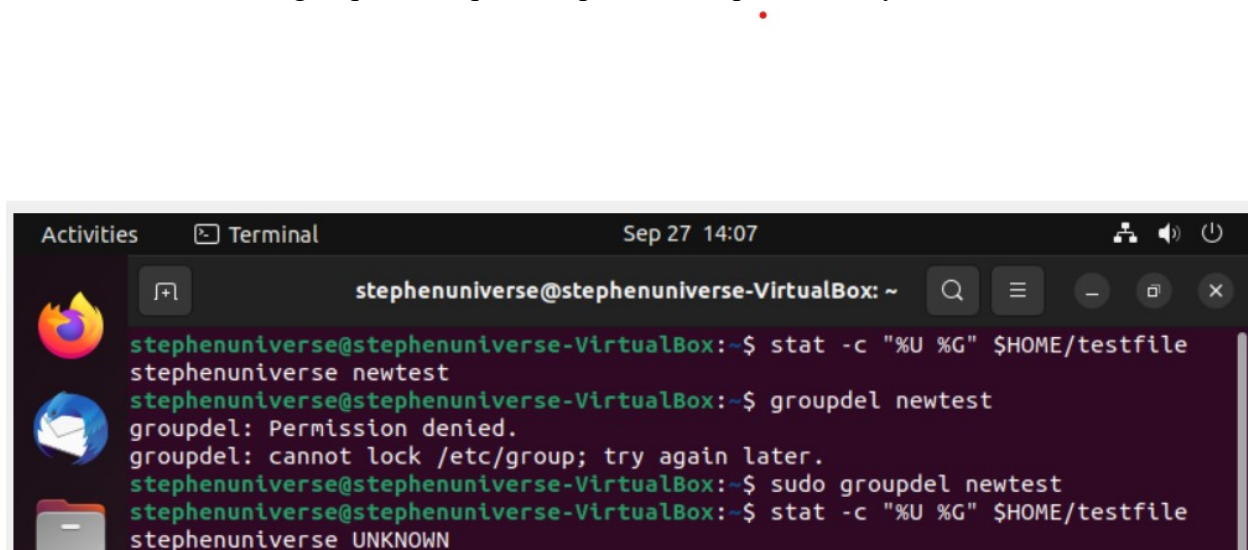
9. Create a new file testfile in the account's home directory, then change the group owner to newtest.



```
stephenuniverse@stephenuniverse-VirtualBox:~$ touch $HOME/testfile  
stephenuniverse@stephenuniverse-VirtualBox:~$ ls  
anotherone.txt  Documents  kdura002  Music      Public  Templates  Videos  
Desktop         Downloads  lab3.txt  Pictures   snap    testfile  
stephenuniverse@stephenuniverse-VirtualBox:~$ sudo chown :newtest $HOME/testfile
```

10. Display the user owner and group owner information of the file testfile.

11. Delete the newtest group, then repeat the previous step. What do you find?



```
stephenuniverse@stephenuniverse-VirtualBox:~$ stat -c "%U %G" $HOME/testfile  
stephenuniverse newtest  
stephenuniverse@stephenuniverse-VirtualBox:~$ groupdel newtest  
groupdel: Permission denied.  
groupdel: cannot lock /etc/group; try again later.  
stephenuniverse@stephenuniverse-VirtualBox:~$ sudo groupdel newtest  
stephenuniverse@stephenuniverse-VirtualBox:~$ stat -c "%U %G" $HOME/testfile  
stephenuniverse UNKNOWN
```

12. Delete the user xxxxx along with the home directory using a single command.

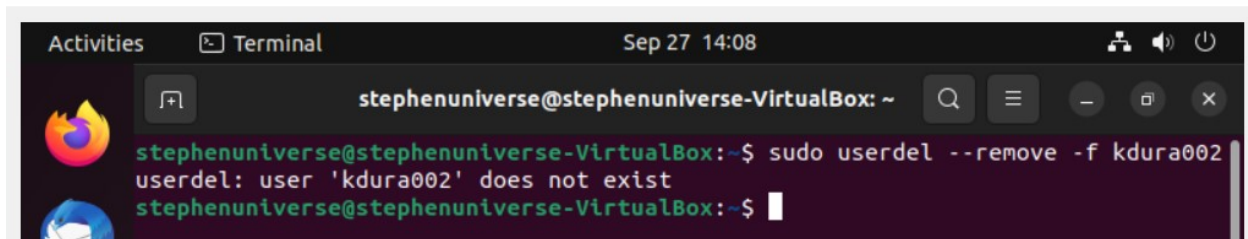
-for this I had already deleted the user, I was very reluctant to delete stephenuniverse, the base user.

-the first time I tried to delete the file it spoke of running process 1679 or some such

-I used pkill 1679 to end that process

-I then used sudo, the command found below, and I was unclear if it had been deleted.

-here is the command, and proof that kdura002 was deleted

A screenshot of a Linux terminal window. The title bar shows 'Activities', 'Terminal', and the date/time 'Sep 27 14:08'. The terminal prompt is 'stephenuniverse@stephenuniverse-VirtualBox: ~'. The user has entered the command 'sudo userdel --remove -f kdura002'. The output of the command is 'userdel: user 'kdura002' does not exist'. The prompt is now 'stephenuniverse@stephenuniverse-VirtualBox:~\$' with a cursor at the end.

```
stephenuniverse@stephenuniverse-VirtualBox: ~  
stephenuniverse@stephenuniverse-VirtualBox:~$ sudo userdel --remove -f kdura002  
userdel: user 'kdura002' does not exist  
stephenuniverse@stephenuniverse-VirtualBox:~$
```