

CYSE 270: Linux System for Cybersecurity

Assignment: Lab 4 – Group and User Accounts

CYSE 270: Linux System for Cybersecurity

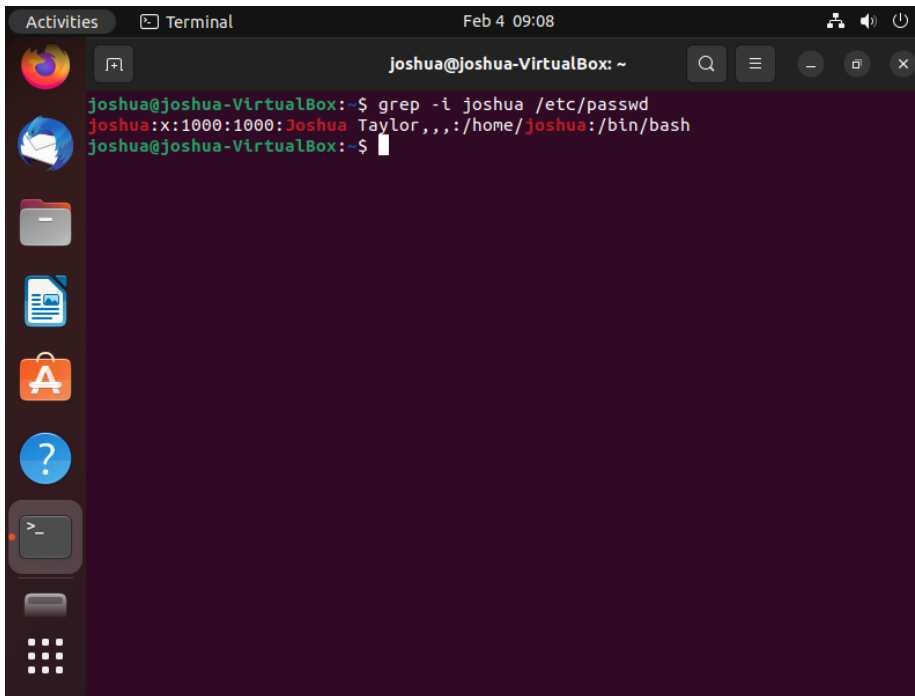
The goal of this lab is to practice basic group and account management. You can choose the Ubuntu VM on your local PC or VMware to complete this assignment.

In this assignment, you should replace **xxxxx** with your MIDAS ID in all occurrences.

Task A – User Account management (8 * 5 = 40 points)

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.

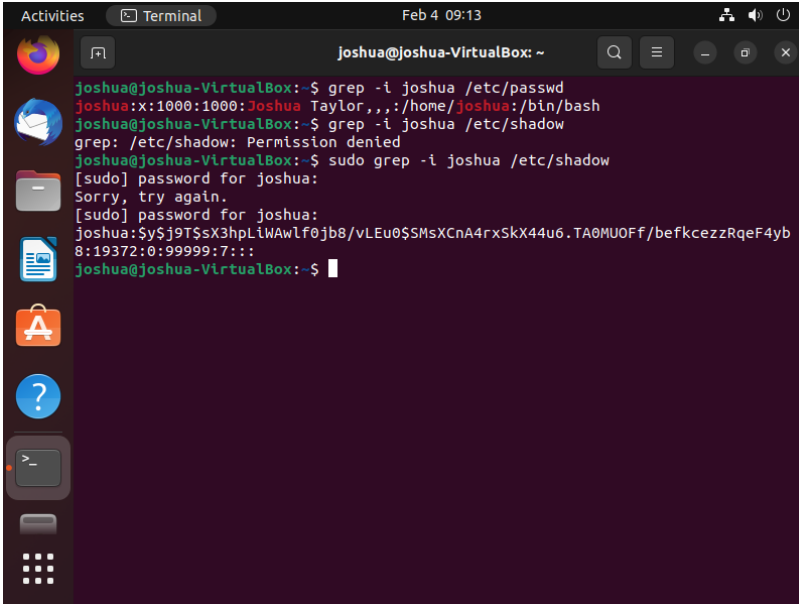
A) command is “grep -i joshua /etc/passwd”



```
Activities Terminal Feb 4 09:08
Joshua@joshua-VirtualBox: ~
joshua@joshua-VirtualBox:~$ grep -i joshua /etc/passwd
joshua:x:1000:1000:Joshua Taylor,,,:/home/joshua:/bin/bash
joshua@joshua-VirtualBox:~$
```

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

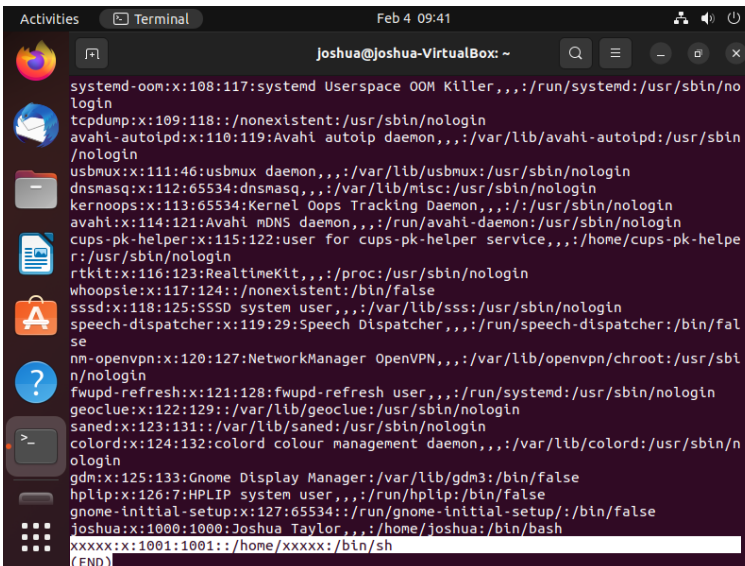
A) Command is “sudo grep -i joshua /etc/shadow “

A terminal window titled 'Joshua@Joshua-VirtualBox: ~' showing the following commands and output:

```
joshua@joshua-VirtualBox:~$ grep -i joshua /etc/passwd
joshua:x:1000:1000:Joshua Taylor,,,:/home/joshua:/bin/bash
joshua@joshua-VirtualBox:~$ grep -i joshua /etc/shadow
grep: /etc/shadow: Permission denied
joshua@joshua-VirtualBox:~$ sudo grep -i joshua /etc/shadow
[sudo] password for joshua:
Sorry, try again.
[sudo] password for joshua:
joshua:$y$j9T$Sx3hpLiWAwlf0jb8/vLEu0$SMsXCnA4rxSkX44u6.TA0MUOff/befkcezzRqeF4yb8:19372:0:99999:7:::
joshua@joshua-VirtualBox:~$
```

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

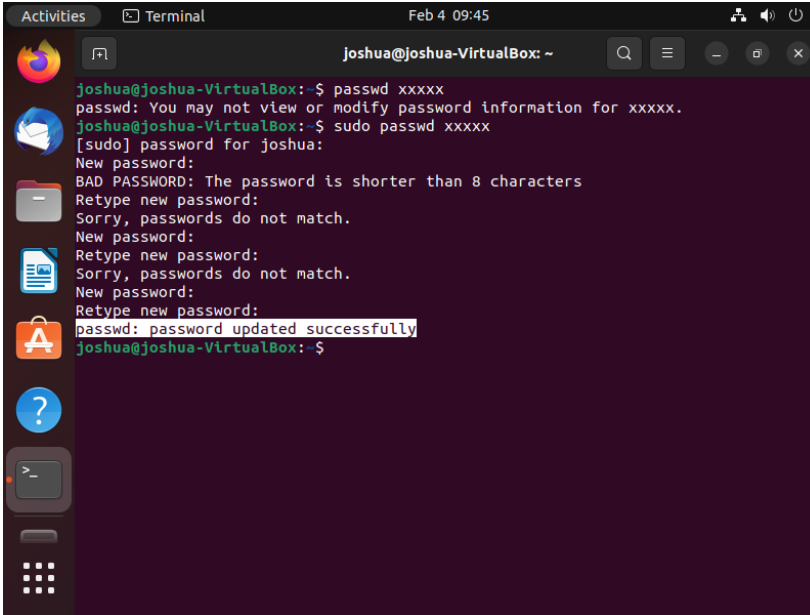
A) Command is “ sudo useradd -m xxxxx “

A terminal window titled 'Joshua@Joshua-VirtualBox: ~' showing the output of the 'cat /etc/passwd' command and the execution of 'sudo useradd -m xxxxx'.

```
systemd-oom:x:108:117:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:118:/:nonexistent:/usr/sbin/nologin
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124:/:nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
nm-openvpn:x:120:127:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
fwupd-refresh:x:121:128:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
geoclue:x:122:129:/:var/lib/geoclue:/usr/sbin/nologin
saned:x:123:131:/:var/lib/saned:/usr/sbin/nologin
colord:x:124:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
gdm:x:125:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-initial-setup:x:127:65534:/:run/gnome-initial-setup:/bin/false
joshua:x:1000:1000:Joshua Taylor,,,:/home/joshua:/bin/bash
xxxxx:x:1001:1001:/:home/xxxxx:/bin/sh
(END)
```

4. Set a password for the new user.

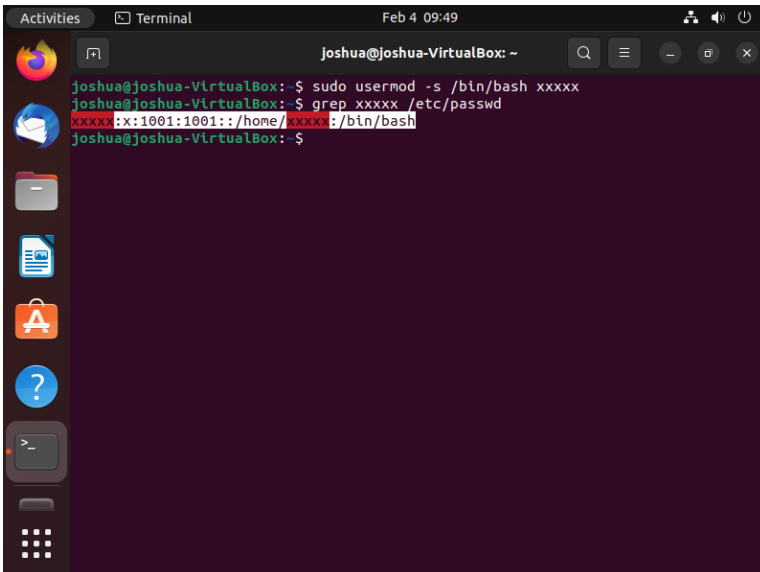
A) Command is “ sudo passwd xxxxx “



```
Activities Terminal Feb 4 09:45
joshua@joshua-VirtualBox: ~
joshua@joshua-VirtualBox:~$ passwd xxxxx
passwd: You may not view or modify password information for xxxxx.
joshua@joshua-VirtualBox:~$ sudo passwd xxxxx
[sudo] password for joshua:
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
joshua@joshua-VirtualBox:~$
```

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

A) Commands are “ `sudo usermod -s /bin/bash xxxxx`” and “ `grep xxxxx /etc/passwd` ”



```
Activities Terminal Feb 4 09:49
joshua@joshua-VirtualBox: ~
joshua@joshua-VirtualBox:~$ sudo usermod -s /bin/bash xxxxx
joshua@joshua-VirtualBox:~$ grep xxxxx /etc/passwd
xxxxx:x:1001:1001::/home/xxxxx:/bin/bash
joshua@joshua-VirtualBox:~$
```

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

A) Command is “ `sudo grep -i xxxxx /etc/shadow` ”

```
Joshua@Joshua-VirtualBox: ~  
joshua@joshua-VirtualBox:~$ sudo grep -i xxxxx /etc/shadow  
xxxxx:$y$19T$Lv.8nxpsUsnXoxZHdazj.$LN8MBnn57oyRsIBuTSkFcZhrVT.xuHV4ykVb3Bc14b9  
:19392:0:99999:7:::  
joshua@joshua-VirtualBox:~$
```

7. Add the new user **xxxxx** to sudo group without overriding the existing group membership.

A) Command is “ sudo usermod -aG sudo xxxxx “

```
Joshua@Joshua-VirtualBox: ~  
joshua@joshua-VirtualBox:~$ usermod -aG sudo xxxxx  
usermod: Permission denied.  
usermod: cannot lock /etc/passwd; try again later.  
joshua@joshua-VirtualBox:~$ sudo usermod -aG sudo xxxxx  
joshua@joshua-VirtualBox:~$
```

8. Switch to the new user’s account.

Task B – Group account management (12 * 5 = 60 points)

Use Linux commands to execute the following tasks:

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

A) command is “ grep -i xxxxx /etc/passwd “

```
xxxxx@joshua-VirtualBox: ~  
xxxxx@joshua-VirtualBox: $ grep -i xxxxx /etc/passwd  
xxxxx:x:1001:1001:/home/xxxxx:/bin/bash  
xxxxx@joshua-VirtualBox: $
```

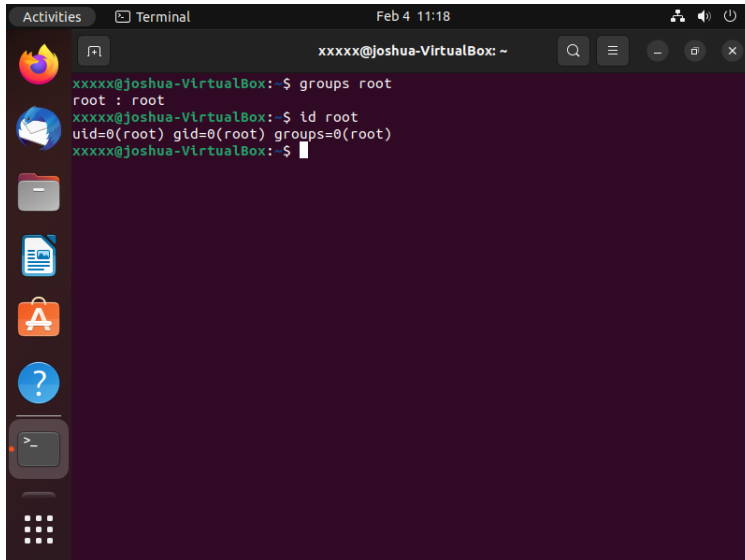
2. Display the current user's ID and group membership.

A) command is " groups "

```
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
xxxxx@joshua-VirtualBox: ~  
xxxxx@joshua-VirtualBox: $ groups  
xxxxx sudo  
xxxxx@joshua-VirtualBox: ~$
```

3. Display the group membership of the root account.

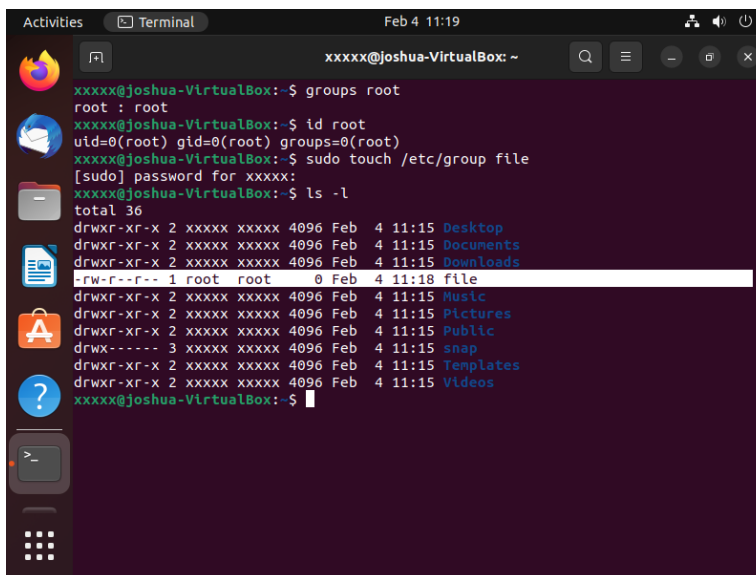
A) command is " groups root " / " id root "



```
xxxxx@joshua-VirtualBox: ~  
xxxxx@joshua-VirtualBox:~$ groups root  
root : root  
xxxxx@joshua-VirtualBox:~$ id root  
uid=0(root) gid=0(root) groups=0(root)  
xxxxx@joshua-VirtualBox:~$
```

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

A) command is “`sudo touch /etc/group file`”



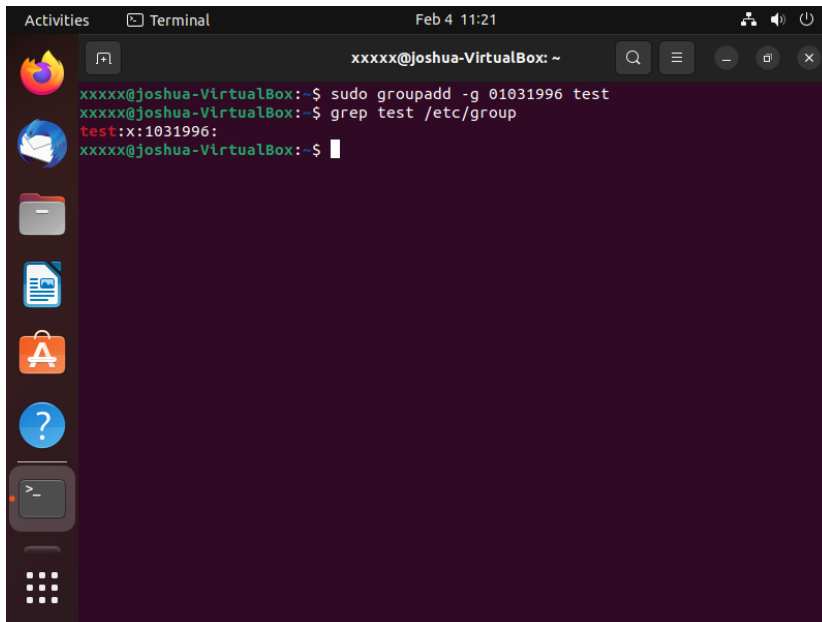
```
xxxxx@joshua-VirtualBox: ~  
xxxxx@joshua-VirtualBox:~$ groups root  
root : root  
xxxxx@joshua-VirtualBox:~$ id root  
uid=0(root) gid=0(root) groups=0(root)  
xxxxx@joshua-VirtualBox:~$ sudo touch /etc/group file  
[sudo] password for xxxxx:  
xxxxx@joshua-VirtualBox:~$ ls -l  
total 36  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Desktop  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Documents  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Downloads  
-rw-r--r-- 1 root root    0 Feb  4 11:18 file  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Music  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Pictures  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Public  
drwx----- 3 xxxxx xxxxx 4096 Feb  4 11:15 snap  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Templates  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Videos  
xxxxx@joshua-VirtualBox:~$
```

5. Create a new group named **test** and use **your UIN** as the **GID**.

A) command is “`sudo groupadd -g 01031996 test`” **screenshot in Q6 response**

6. Display the group account information for the test group using grep.

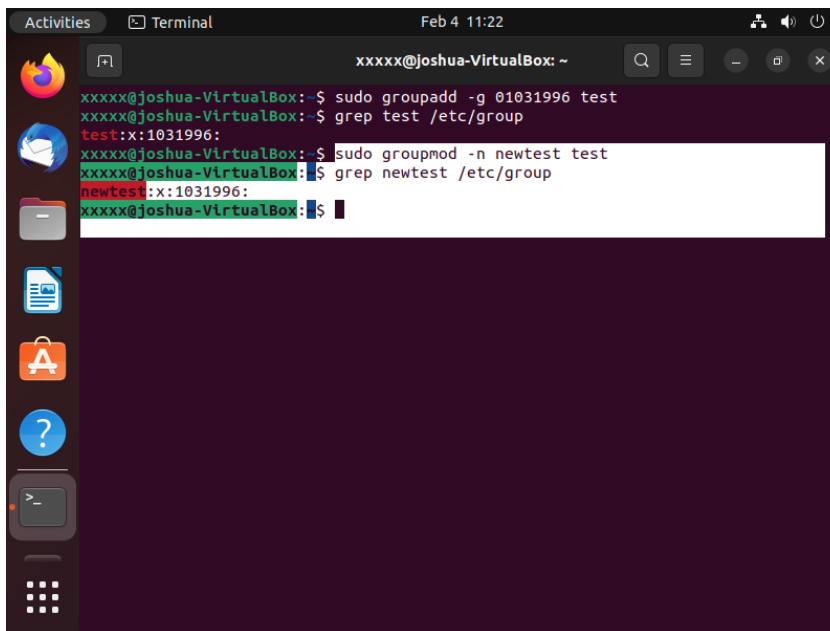
A) command is “grep test /etc/group “



```
xxxxx@joshua-VirtualBox: ~  
xxxxx@joshua-VirtualBox:~$ sudo groupadd -g 01031996 test  
xxxxx@joshua-VirtualBox:~$ grep test /etc/group  
test:x:1031996:  
xxxxx@joshua-VirtualBox:~$
```

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

A) command is “sudo groupmod -n newtest test “



```
xxxxx@joshua-VirtualBox: ~  
xxxxx@joshua-VirtualBox:~$ sudo groupadd -g 01031996 test  
xxxxx@joshua-VirtualBox:~$ grep test /etc/group  
test:x:1031996:  
xxxxx@joshua-VirtualBox:~$ sudo groupmod -n newtest test  
xxxxx@joshua-VirtualBox:~$ grep newtest /etc/group  
newtest:x:1031996:  
xxxxx@joshua-VirtualBox:~$
```

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



```
xxxxx@joshua-VirtualBox: ~  
xxxxx@joshua-VirtualBox:~$ sudo groupadd -g 01031996 test  
xxxxx@joshua-VirtualBox:~$ grep test /etc/group  
test:x:1031996:  
xxxxx@joshua-VirtualBox:~$ sudo groupmod -n newtest test  
xxxxx@joshua-VirtualBox:~$ grep newtest /etc/group  
newtest:x:1031996:  
xxxxx@joshua-VirtualBox:~$ sudo usermod -aG newtest xxxxx  
xxxxx@joshua-VirtualBox:~$ grep newtest /etc/group  
newtest:x:1031996:xxxxx  
xxxxx@joshua-VirtualBox:~$
```

9. Create a new file `testfile` in the account's home directory, then change the group owner to `newtest`.
A) commands are “`sudo touch testfile`” & “`sudo chgrp newtest testfile`”

```

Activities Terminal Feb 4 11:33
xxxxx@joshua-VirtualBox: ~
xxxxx@joshua-VirtualBox:~$ ls -l
total 36
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Desktop
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Documents
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Downloads
-rw-r--r-- 1 root root 0 Feb 4 11:18 file
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Music
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Pictures
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Public
drwx----- 3 xxxxx xxxxx 4096 Feb 4 11:15 snap
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Templates
-rw-r--r-- 1 root root 0 Feb 4 11:30 testfile
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Videos
xxxxx@joshua-VirtualBox:~$ chgrp newtest testfile
chgrp: changing group of 'testfile': Operation not permitted
xxxxx@joshua-VirtualBox:~$ sudo chgrp newtest testfile
xxxxx@joshua-VirtualBox:~$ ld-l
Command 'ld-l' not found, did you mean:
  command 'ldpl' from snap ldpl-lang (4.4)
See 'snap info <snapname>' for additional versions.
xxxxx@joshua-VirtualBox:~$ ls -l
total 36
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Desktop
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Documents
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Downloads
-rw-r--r-- 1 root root 0 Feb 4 11:18 file
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Music
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Pictures
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Public

```

```

Activities Terminal Feb 4 11:33
xxxxx@joshua-VirtualBox: ~
-rw-r--r-- 1 root root 0 Feb 4 11:18 file
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Music
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Pictures
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Public
drwx----- 3 xxxxx xxxxx 4096 Feb 4 11:15 snap
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Templates
-rw-r--r-- 1 root root 0 Feb 4 11:30 testfile
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Videos
xxxxx@joshua-VirtualBox:~$ chgrp newtest testfile
chgrp: changing group of 'testfile': Operation not permitted
xxxxx@joshua-VirtualBox:~$ sudo chgrp newtest testfile
xxxxx@joshua-VirtualBox:~$ ld-l
Command 'ld-l' not found, did you mean:
  command 'ldpl' from snap ldpl-lang (4.4)
See 'snap info <snapname>' for additional versions.
xxxxx@joshua-VirtualBox:~$ ls -l
total 36
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Desktop
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Documents
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Downloads
-rw-r--r-- 1 root root 0 Feb 4 11:18 file
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Music
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Pictures
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Public
drwx----- 3 xxxxx xxxxx 4096 Feb 4 11:15 snap
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Templates
-rw-r--r-- 1 root newtest 0 Feb 4 11:30 testfile
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb 4 11:15 Videos
xxxxx@joshua-VirtualBox:~$

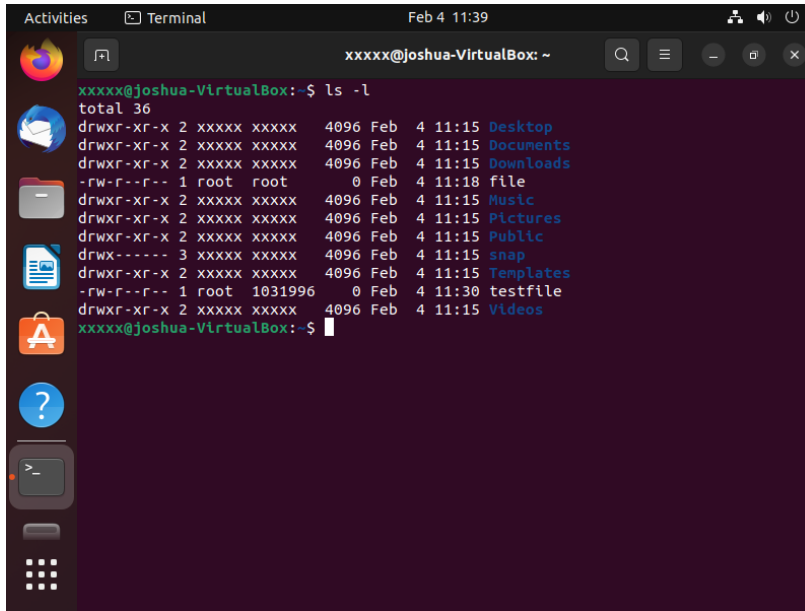
```

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

A) command is “ls -l” and **shown in previous screenshot**

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

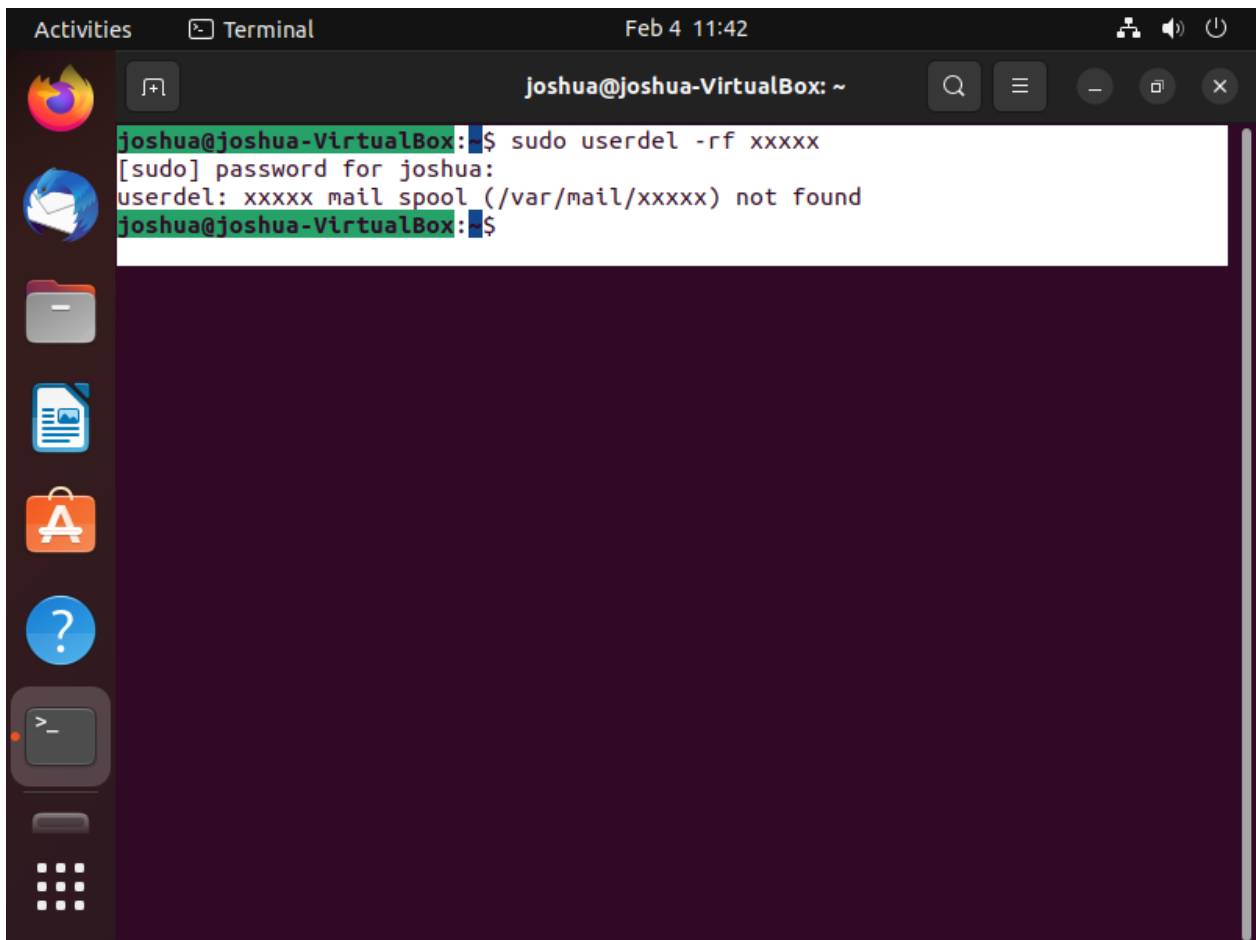
A) command is “sudo groupdel newtest” and I found that the group owner changed to the GID that was given to it; My UIN.



```
xxxxx@joshua-VirtualBox: ~  
xxxxx@joshua-VirtualBox:~$ ls -l  
total 36  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Desktop  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Documents  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Downloads  
-rw-r--r-- 1 root  root   0 Feb  4 11:18 file  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Music  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Pictures  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Public  
drwx----- 3 xxxxx xxxxx 4096 Feb  4 11:15 snap  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Templates  
-rw-r--r-- 1 root 1031996 0 Feb  4 11:30 testfile  
drwxr-xr-x 2 xxxxx xxxxx 4096 Feb  4 11:15 Videos  
xxxxx@joshua-VirtualBox:~$
```

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

A) command is “`sudo userdel -rf xxxxx`”



```
joshua@joshua-VirtualBox: ~  
joshua@joshua-VirtualBox:~$ sudo userdel -rf xxxxx  
[sudo] password for joshua:  
userdel: xxxxx mail spool (/var/mail/xxxxx) not found  
joshua@joshua-VirtualBox:~$
```