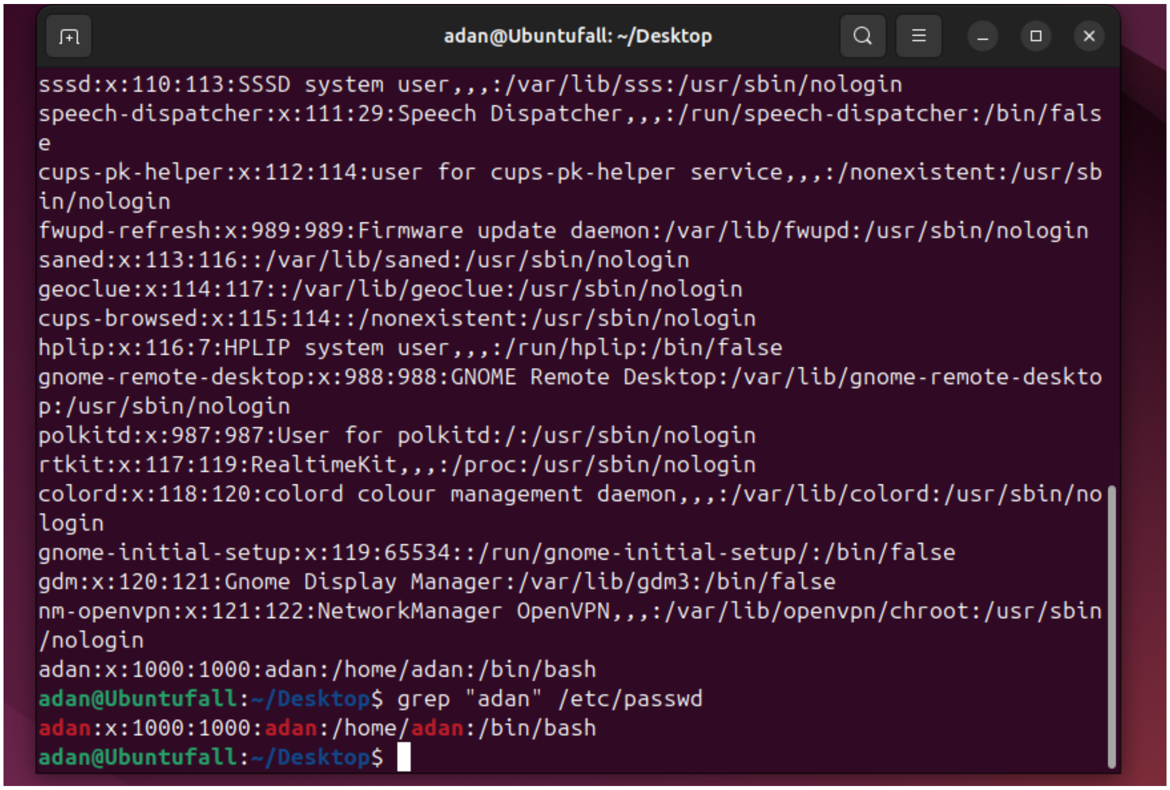
CYSE 270: Linux System for Cybersecurity Assignment: Lab 4 – User and Group Accounts

CYSE 270: Linux System for Cybersecurity

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

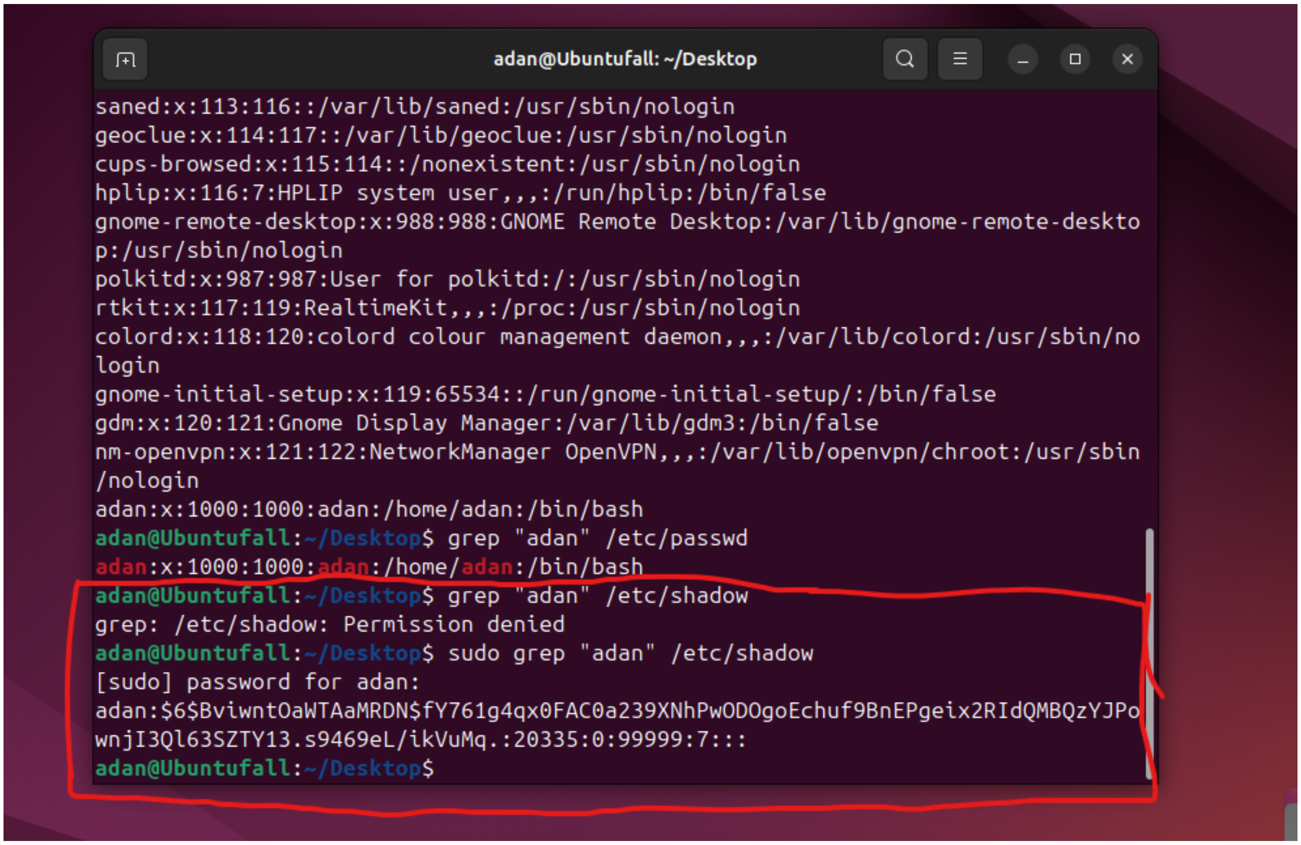
Task A – User Account management (8 * 5 = 40 points)

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.



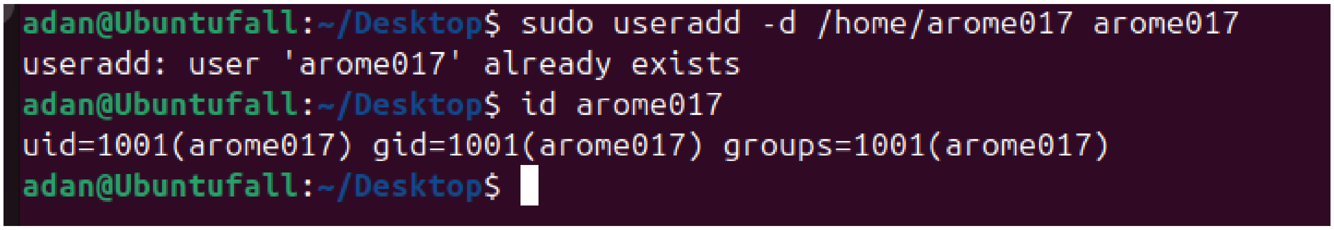
```
sssd:x:110:113:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/fals
e
cups-pk-helper:x:112:114:user for cups-pk-helper service,,,:/nonexistent:/usr/sb
in/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117::/var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114::/nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-deskto
p:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/no
login
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin
/nologin
adan:x:1000:1000:adan:/home/adan:/bin/bash
adan@Ubuntufall:~/Desktop$ grep "adan" /etc/passwd
adan:x:1000:1000:adan:/home/adan:/bin/bash
adan@Ubuntufall:~/Desktop$ 
```

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



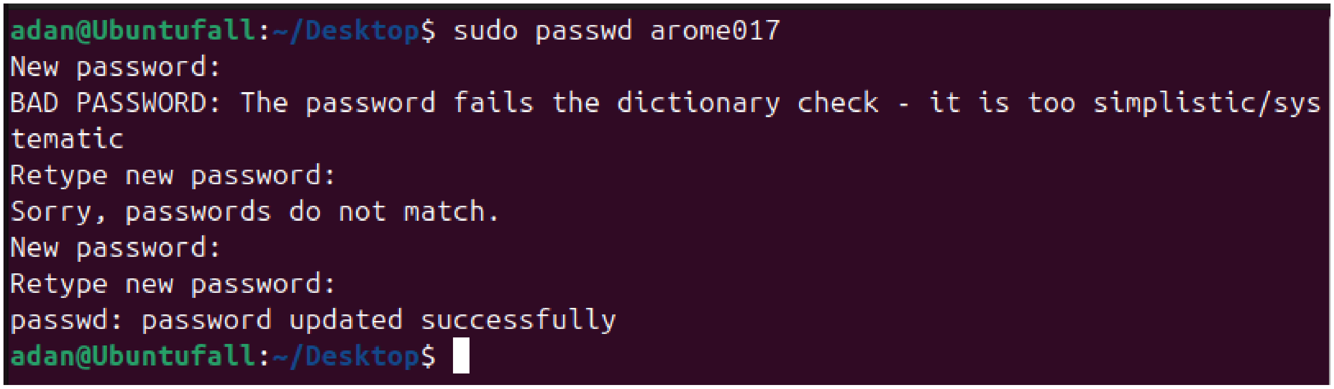
```
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117::/var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114::/nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-deskto
p:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/no
login
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin
/nologin
adan:x:1000:1000:adan:/home/adan:/bin/bash
adan@Ubuntufall:~/Desktop$ grep "adan" /etc/passwd
adan:x:1000:1000:adan:/home/adan:/bin/bash
adan@Ubuntufall:~/Desktop$ grep "adan" /etc/shadow
grep: /etc/shadow: Permission denied
adan@Ubuntufall:~/Desktop$ sudo grep "adan" /etc/shadow
[sudo] password for adan:
adan:$6$BviwntOaWTAaMRDN$fY761g4qx0FAC0a239XNhPwODOgoEchuf9BnEPgeix2RIdQMBQzYJPo
wnjI3Ql63SZTY13.s9469eL/ikVuMq.:20335:0:99999:7:::
adan@Ubuntufall:~/Desktop$
```

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



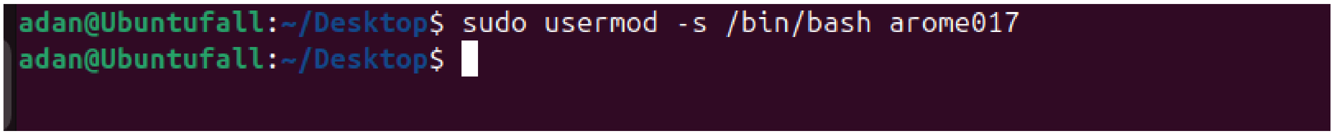
```
adan@Ubuntufall:~/Desktop$ sudo useradd -d /home/arome017 arome017
useradd: user 'arome017' already exists
adan@Ubuntufall:~/Desktop$ id arome017
uid=1001(arome017) gid=1001(arome017) groups=1001(arome017)
adan@Ubuntufall:~/Desktop$
```

4. Set a password for the new user.



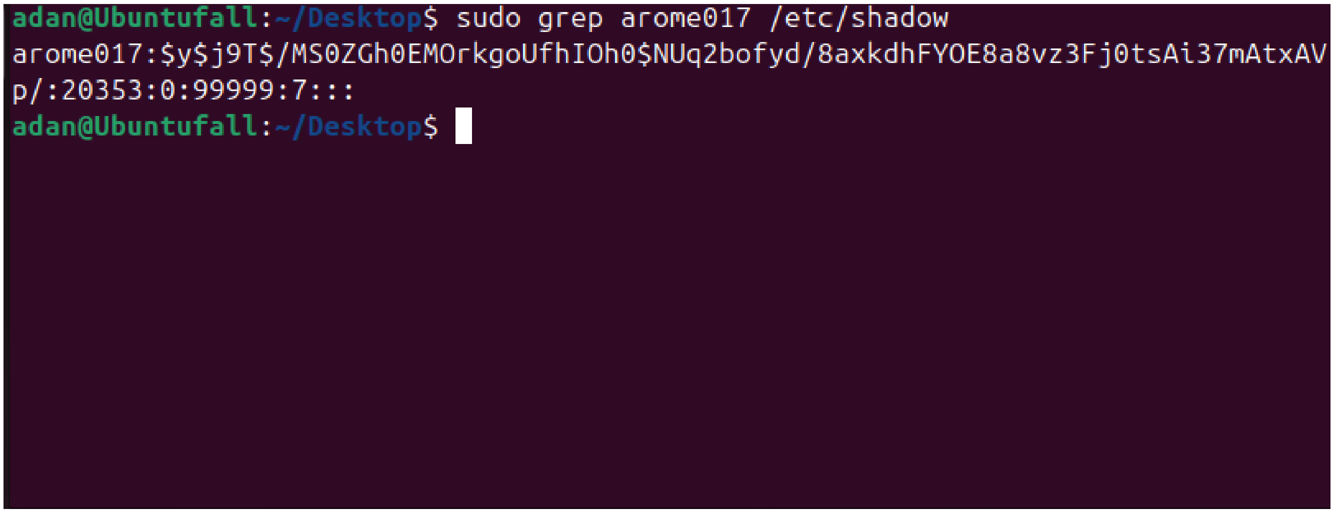
```
adan@Ubuntufall:~/Desktop$ sudo passwd arome017
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/sys
tematic
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
adan@Ubuntufall:~/Desktop$
```

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



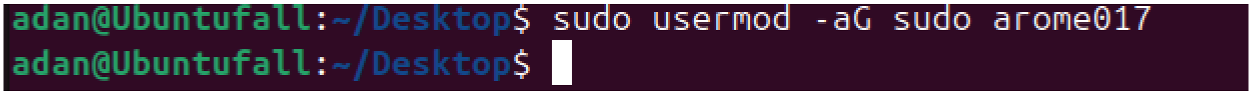
```
adan@Ubuntufall:~/Desktop$ sudo usermod -s /bin/bash arome017
adan@Ubuntufall:~/Desktop$
```

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



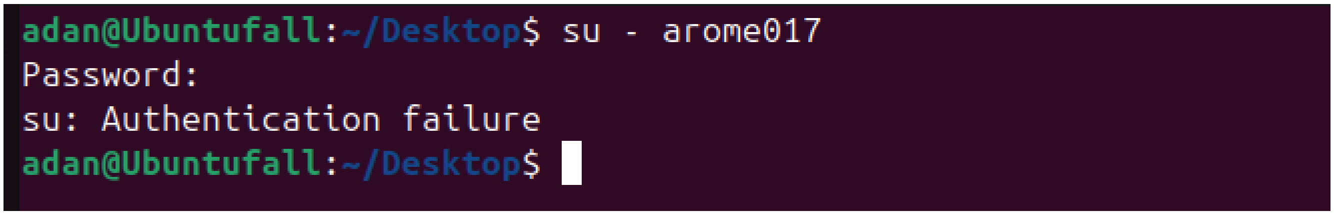
```
adan@Ubuntufall:~/Desktop$ sudo grep arome017 /etc/shadow
arome017:$y$j9T$/MS0ZGh0EMOrkgoUfhIOh0$NUq2bofyd/8axkdhFYOE8a8vz3Fj0tsAi37mAtxAV
p/:20353:0:99999:7:::
adan@Ubuntufall:~/Desktop$
```

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



```
adan@Ubuntufall:~/Desktop$ sudo usermod -aG sudo arome017
adan@Ubuntufall:~/Desktop$
```

8. Switch to the new user's account**.**



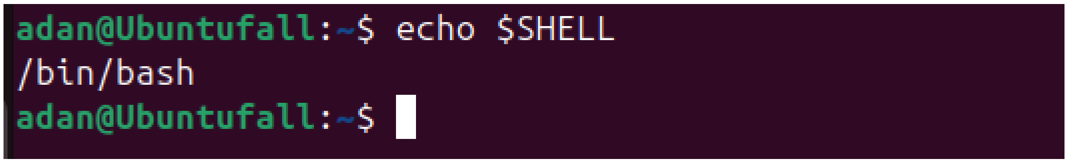
```
adan@Ubuntufall:~/Desktop$ su - arome017
Password:
su: Authentication failure
adan@Ubuntufall:~/Desktop$
```

(I forgot the password already 😵) But this would be the command to switch over.

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

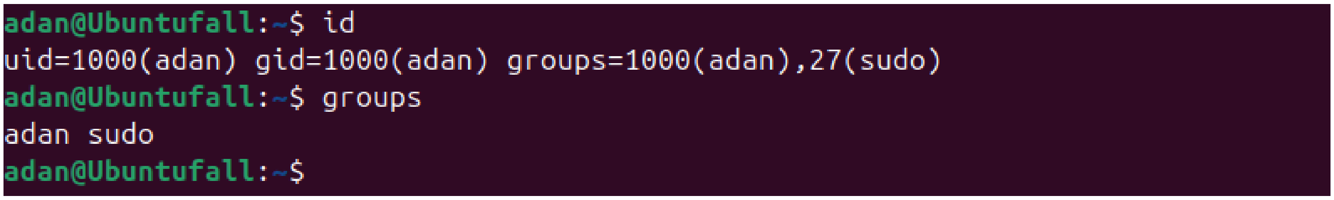
Use Linux commands to execute the following tasks:

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



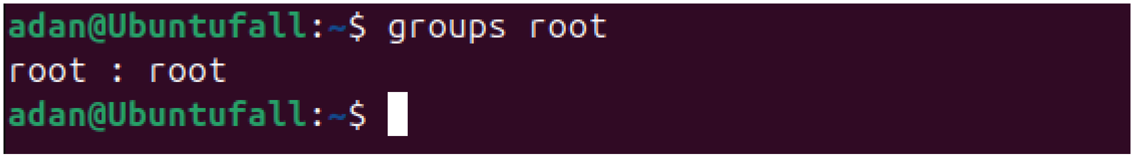
```
adan@Ubuntufall:~$ echo $SHELL
/bin/bash
adan@Ubuntufall:~$
```

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



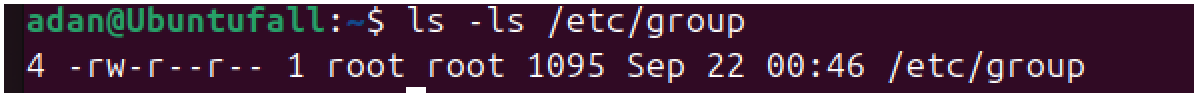
```
adan@Ubuntufall:~$ id
uid=1000(adan) gid=1000(adan) groups=1000(adan),27(sudo)
adan@Ubuntufall:~$ groups
adan sudo
adan@Ubuntufall:~$
```

3. Display the group membership of the root account.



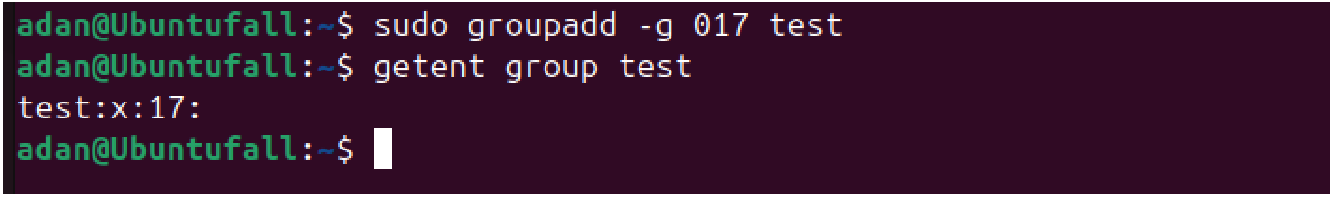
```
adan@Ubuntufall:~$ groups root
root : root
adan@Ubuntufall:~$
```

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



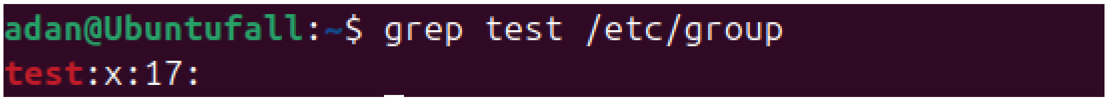
```
adan@Ubuntufall:~$ ls -ls /etc/group
4 -rw-r--r-- 1 root root 1095 Sep 22 00:46 /etc/group
```

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



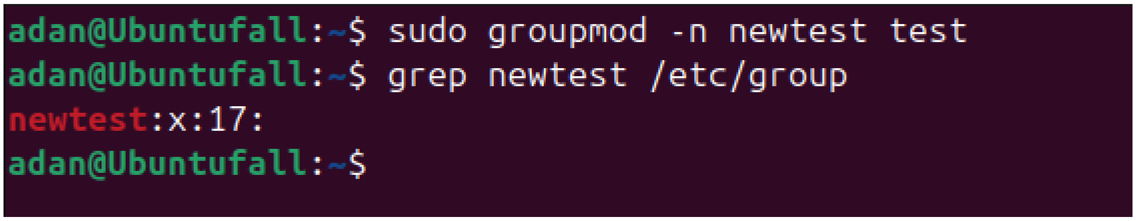
```
adan@Ubuntufall:~$ sudo groupadd -g 017 test
adan@Ubuntufall:~$ getent group test
test:x:17:
adan@Ubuntufall:~$
```

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



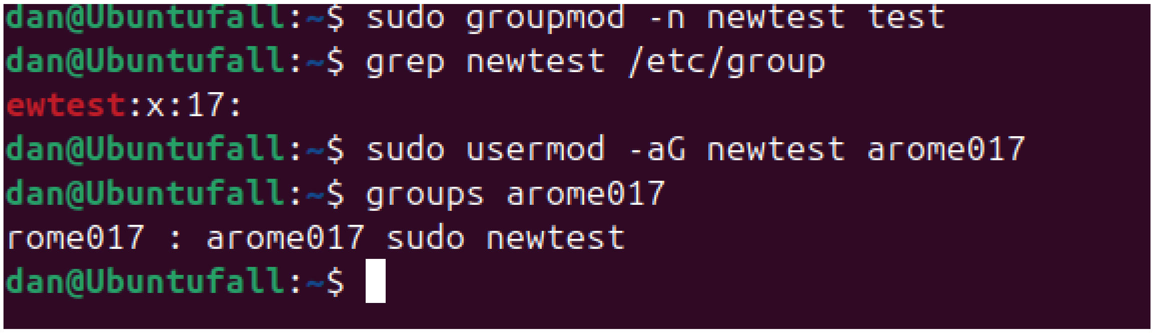
```
adan@Ubuntufall:~$ grep test /etc/group
test:x:17:
```

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



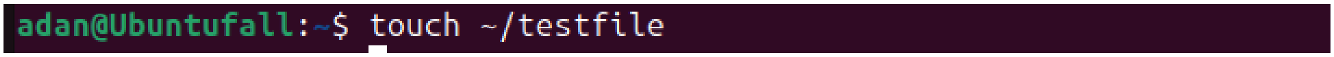
```
adan@Ubuntufall:~$ sudo groupmod -n newtest test
adan@Ubuntufall:~$ grep newtest /etc/group
newtest:x:17:
adan@Ubuntufall:~$
```

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



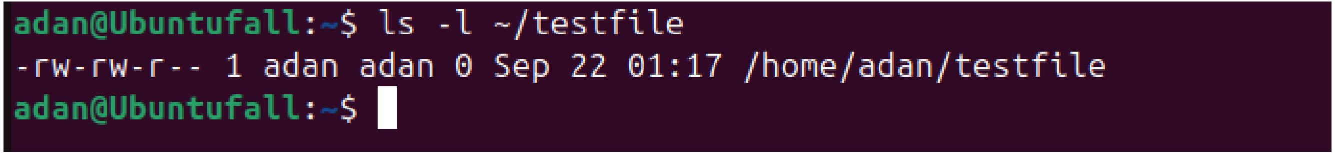
```
dan@Ubuntufall:~$ sudo groupmod -n newtest test
dan@Ubuntufall:~$ grep newtest /etc/group
ewtest:x:17:
dan@Ubuntufall:~$ sudo usermod -aG newtest arome017
dan@Ubuntufall:~$ groups arome017
rome017 : arome017 sudo newtest
dan@Ubuntufall:~$ 
```

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



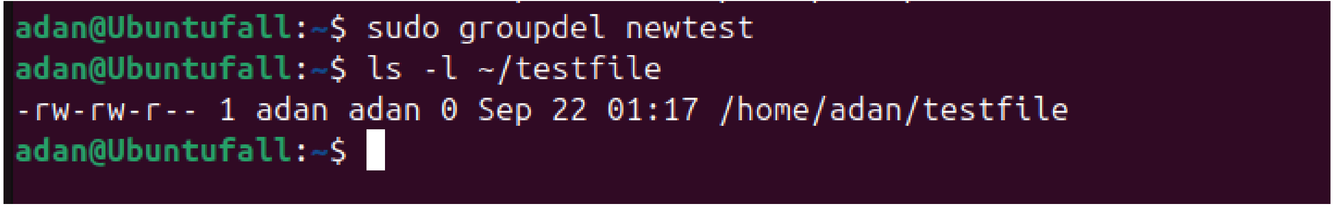
```
adan@Ubuntufall:~$ touch ~/testfile
```

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



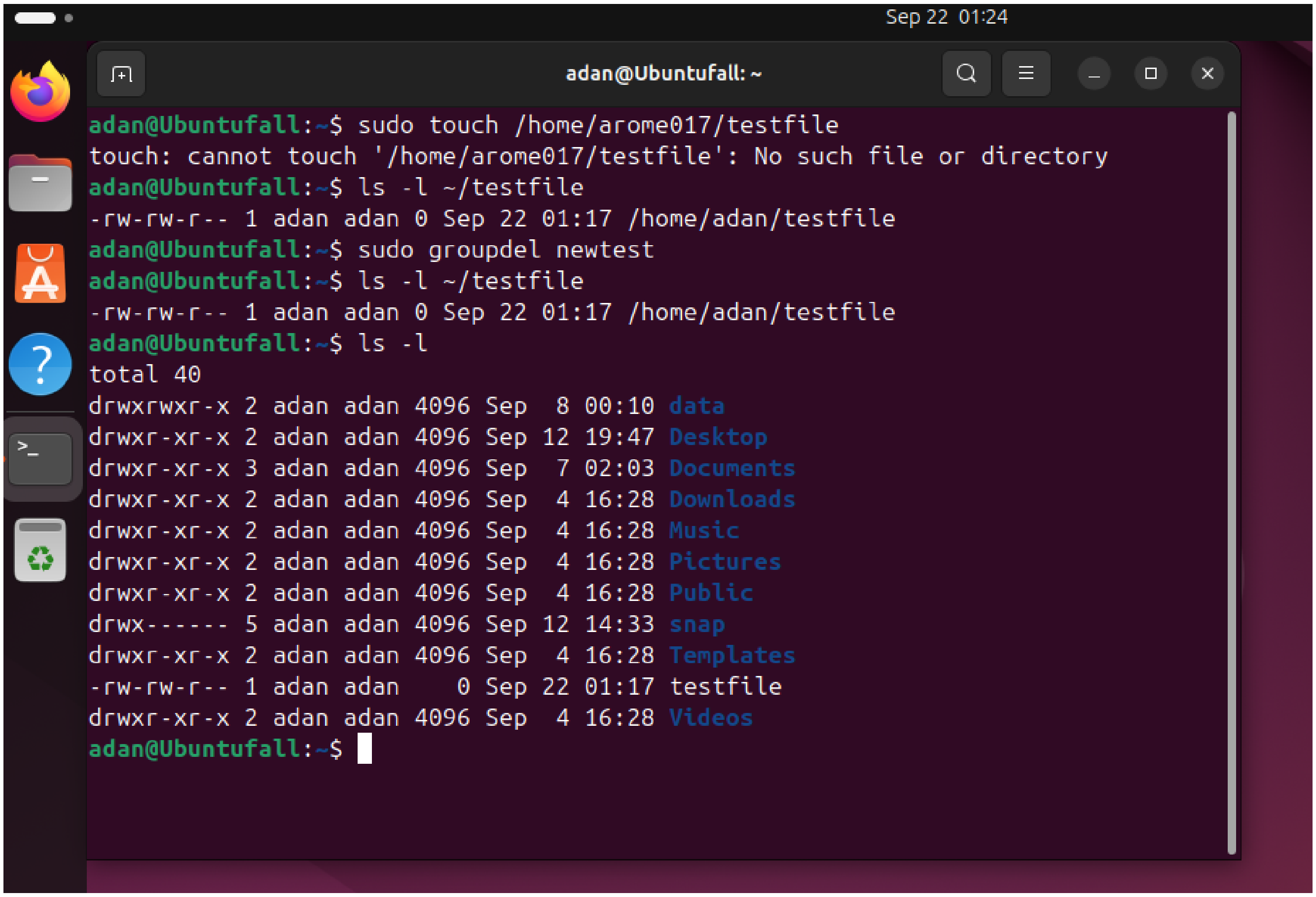
```
adan@Ubuntufall:~$ ls -l ~/testfile
-rw-rw-r-- 1 adan adan 0 Sep 22 01:17 /home/adan/testfile
adan@Ubuntufall:~$
```

10. Delete the **newtes**t group, then repeat the previous step. What do you find?



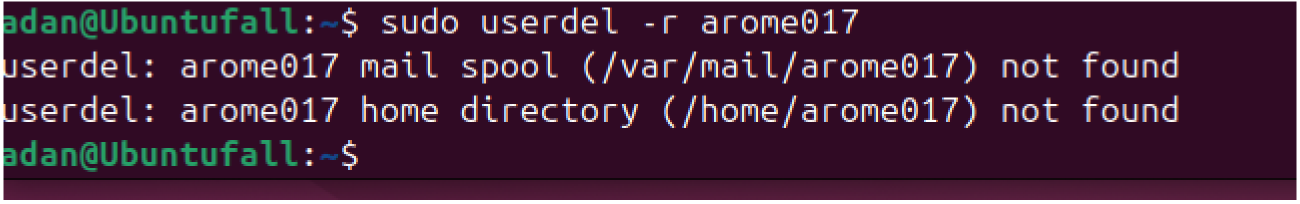
```
adan@Ubuntufall:~$ sudo groupdel newtest
adan@Ubuntufall:~$ ls -l ~/testfile
-rw-rw-r-- 1 adan adan 0 Sep 22 01:17 /home/adan/testfile
adan@Ubuntufall:~$
```

Deleting a group does not remove or change ownership of files , the files will keep the numeric GID



```
adan@Ubuntufall:~$ sudo touch /home/arome017/testfile
touch: cannot touch '/home/arome017/testfile': No such file or directory
adan@Ubuntufall:~$ ls -l ~/testfile
-rw-rw-r-- 1 adan adan 0 Sep 22 01:17 /home/adan/testfile
adan@Ubuntufall:~$ sudo groupdel newtest
adan@Ubuntufall:~$ ls -l ~/testfile
-rw-rw-r-- 1 adan adan 0 Sep 22 01:17 /home/adan/testfile
adan@Ubuntufall:~$ ls -l
total 40
drwxrwxr-x 2 adan adan 4096 Sep  8 00:10 data
drwxr-xr-x 2 adan adan 4096 Sep 12 19:47 Desktop
drwxr-xr-x 3 adan adan 4096 Sep  7 02:03 Documents
drwxr-xr-x 2 adan adan 4096 Sep  4 16:28 Downloads
drwxr-xr-x 2 adan adan 4096 Sep  4 16:28 Music
drwxr-xr-x 2 adan adan 4096 Sep  4 16:28 Pictures
drwxr-xr-x 2 adan adan 4096 Sep  4 16:28 Public
drwx------ 5 adan adan 4096 Sep 12 14:33 snap
drwxr-xr-x 2 adan adan 4096 Sep  4 16:28 Templates
-rw-rw-r-- 1 adan adan    0 Sep 22 01:17 testfile
drwxr-xr-x 2 adan adan 4096 Sep  4 16:28 Videos
adan@Ubuntufall:~$ 
```

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



```
adan@Ubuntufall:~$ sudo userdel -r arome017
userdel: arome017 mail spool (/var/mail/arome017) not found
userdel: arome017 home directory (/home/arome017) not found
adan@Ubuntufall:~$
```