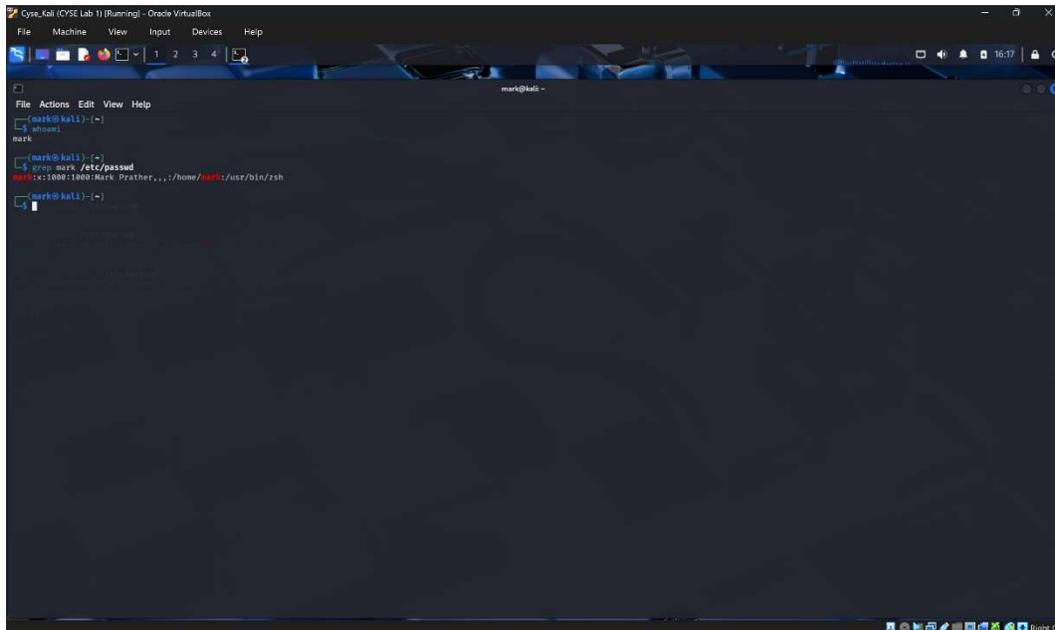


CYSE 270 Assignment 4- Task A

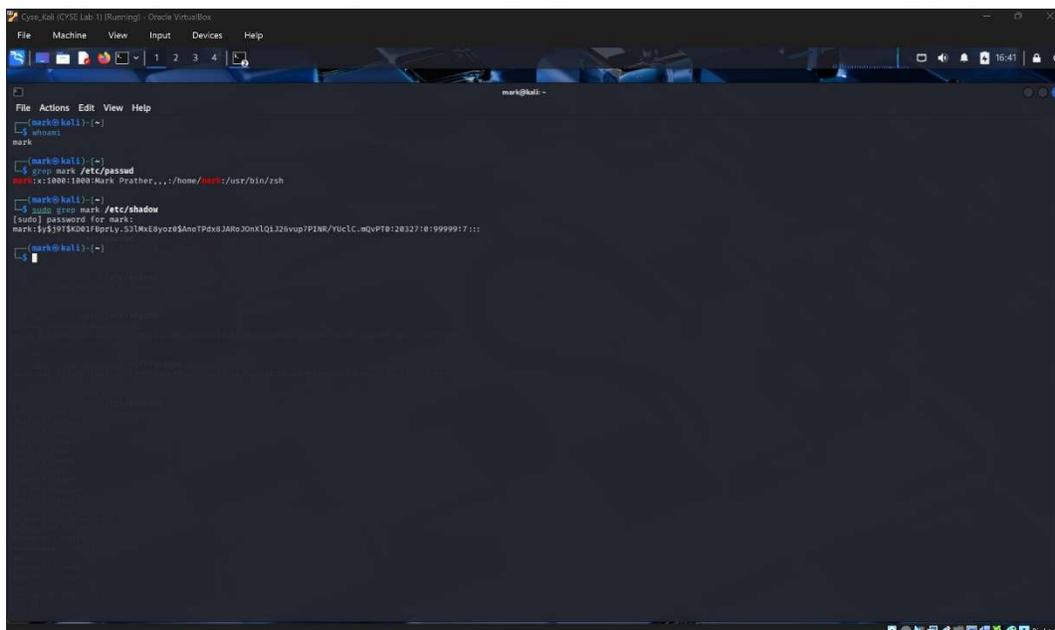
Step 1 - Execute the correct command to display user account information (including the login shell and home directory) for the current user using grep.



```
mark@kali:~$ whoami
mark
mark@kali:~$ whoens
mark
mark@kali:~$ grep mark /etc/passwd
mark:x:1000:1000:Mark Prather,,,:/home/mark:/usr/bin/zsh
mark@kali:~$
```

grep mark /etc/passwd

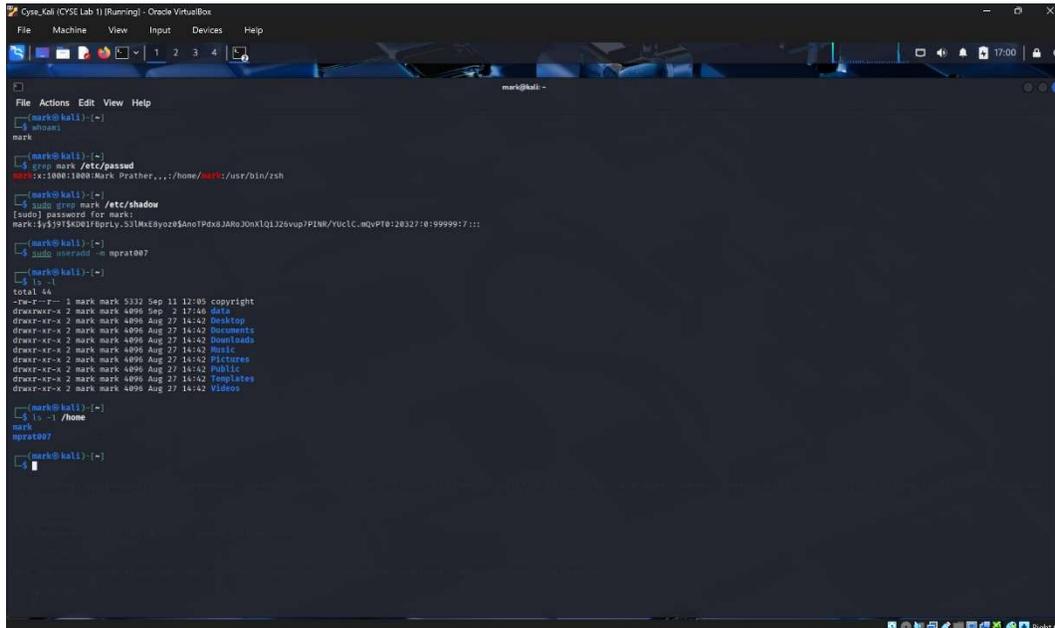
Step 2 - Execute the correct command to display user password information (including the encrypted password and password aging) for the current user using grep.



```
mark@kali:~$ whoami
mark
mark@kali:~$ whoens
mark
mark@kali:~$ grep mark /etc/passwd
mark:x:1000:1000:Mark Prather,,,:/home/mark:/usr/bin/zsh
mark@kali:~$ sudo grep mark /etc/shadow
[sudo] password for mark:
mark:$y$j91$K0eJf6pLy_52lMxEByoz$Aa0TPdx8J8Ho20xLQlJ26vup7P1WV/YuLC_mQvPT0:2032710:199999:7:::
```

sudo grep mark /etc/shadow

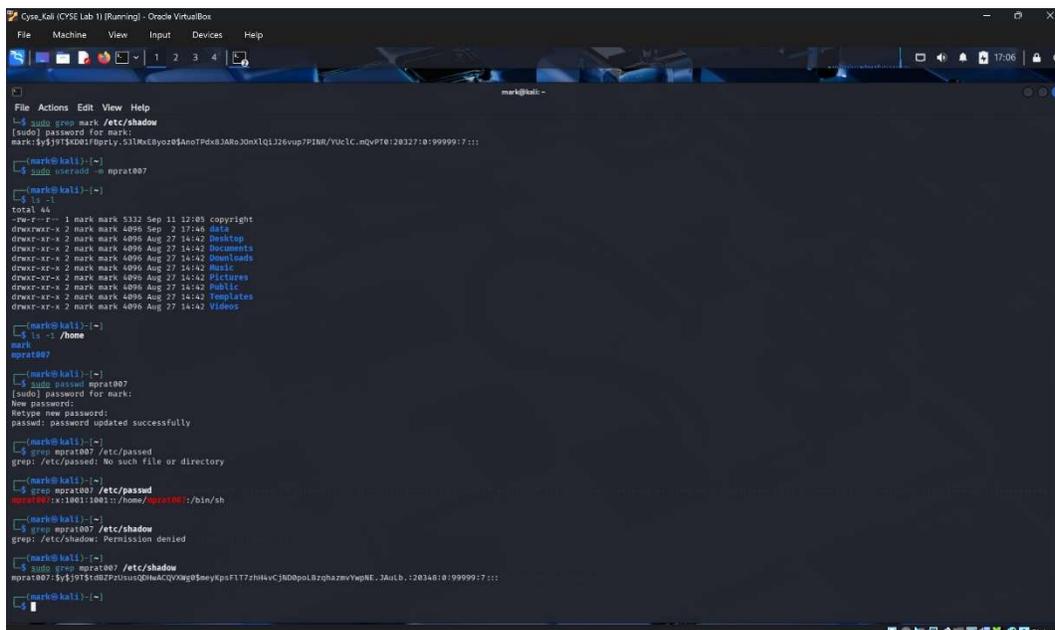
Step 3 - Create a new user named mprat007 and explicitly use options to create the home directory /home/mprat007 for this user.



```
mark@kali:~$ whoami
mark
mark@kali:~$ sudo grep mark /etc/passwd
mark:x:1000:1000:Mark Prather,,,:/home/mark:/usr/bin/zsh
mark@kali:~$ sudo grep mark /etc/shadow
mark:$y$j9T$K001F0prLy.531Mx8yoz8$AnoTPdx8JA8o.30nXlQ1J26vup7P1NR/Yu1c.mQvPT0:20327:0:99999:7:::
mark@kali:~$ sudo useradd -m mprat007
mark@kali:~$ ls -l
total 44
-rw-r--r-- 1 mark mark 5332 Sep 11 12:05 copyright
drwxrwxr-x 2 mark mark 4096 Sep  2 17:46 data
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Desktop
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Documents
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Downloads
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Music
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Pictures
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Public
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Templates
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Videos
mark@kali:~$ ls -l /home
mark
mprat007
mark@kali:~$
```

sudo useradd -m mprat007

Step 4 - Set a password for the new user.



```
mark@kali:~$ sudo grep mark /etc/shadow
mark:$y$j9T$K001F0prLy.531Mx8yoz8$AnoTPdx8JA8o.30nXlQ1J26vup7P1NR/Yu1c.mQvPT0:20327:0:99999:7:::
mark@kali:~$ sudo useradd -m mprat007
mark@kali:~$ ls -l
total 44
-rw-r--r-- 1 mark mark 5332 Sep 11 12:05 copyright
drwxrwxr-x 2 mark mark 4096 Sep  2 17:46 data
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Desktop
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Documents
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Downloads
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Music
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Pictures
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Public
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Templates
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Videos
mark@kali:~$ ls -l /home
mark
mprat007
mark@kali:~$ sudo passwd mprat007
[sudo] password for mark:
New password:
Retype new password:
passwd: password updated successfully
mark@kali:~$ grep mprat007 /etc/passwd
mprat007:x:1001:1001::/home/mprat007:/bin/sh
mark@kali:~$ grep mprat007 /etc/shadow
mprat007:$y$j9T$0BZP2Ussu@HudCQVxag8$meYkpsFL7zHhVcJ800pol8zqhzavw9E.3AulB.120346:0:99999:7:::
mark@kali:~$
```

sudo passwd mprat007 – password for mprat007 is 1234

Step 5 - Set bash shell as the default login shell for the new user mprat007, then verify the change.

```
mark@kali:~$ ls -l
total 44
-rw-r--r-- 1 mark mark 5332 Sep 11 12:05 copyright
drwxr-xr-x 2 mark mark 4096 Sep  2 17:46 data
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Desktop
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Documents
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Downloads
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Music
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Pictures
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Public
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Templates
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Videos

mark@kali:~$ sudo usermod -s /bin/bash mprat007
[sudo] password for mark:
New password:
Retype new password:
passwd: password updated successfully

mark@kali:~$ grep mprat007 /etc/passwd
mprat007:x:1801:1081::/home/mprat007:/bin/sh

mark@kali:~$ grep mprat007 /etc/shadow
grep: /etc/shadow: Permission denied

mark@kali:~$ sudo grep mprat007 /etc/shadow
mprat007:$y$9T$td2PzUssuQhMcQVWg$meYkpsFlT7zhHvCjND0pol8zqazevYpNE_3AuLb.:20348:0:99999:7:::

mark@kali:~$ sudo usermod -s /bin/bash mprat007
[sudo] password for mark:

mark@kali:~$ grep mprat007 /etc/passwd
mprat007:x:1801:1081::/home/mprat007:/bin/bash

mark@kali:~$
```

sudo usermod -s /bin/bash – set default login shell

grep mprat007 /etc/passwd – verify /bin/bash default login shell

Step 6 - Execute the correct command to display user password information (including the encrypted password and password aging) for the new user mprat007 using grep.

```
mark@kali:~$ sudo grep mprat007 /etc/shadow
mprat007:$y$9T$td2PzUssuQhMcQVWg$meYkpsFlT7zhHvCjND0pol8zqazevYpNE_3AuLb.:20348:0:99999:7:::

mark@kali:~$
```

sudo grep mprat007 /etc/shadow

CYSE 270 Assignment 4- Task B

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

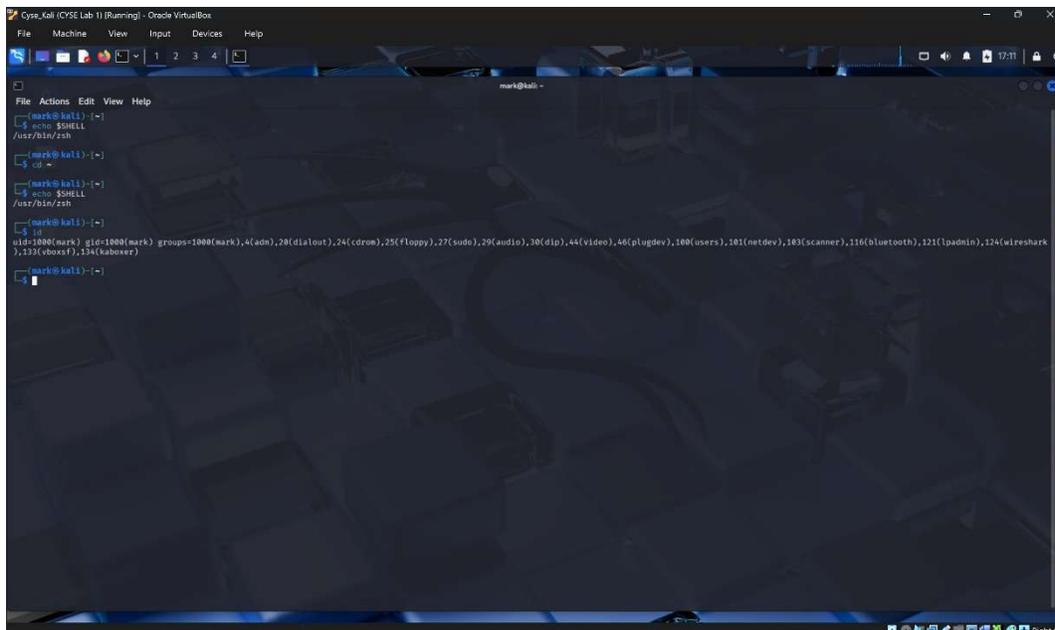


```
mark@kali: ~  
└─$ cd ~  
└─$ echo $SHELL  
/usr/bin/zsh  
└─$
```

cd ~

echo \$SHELL

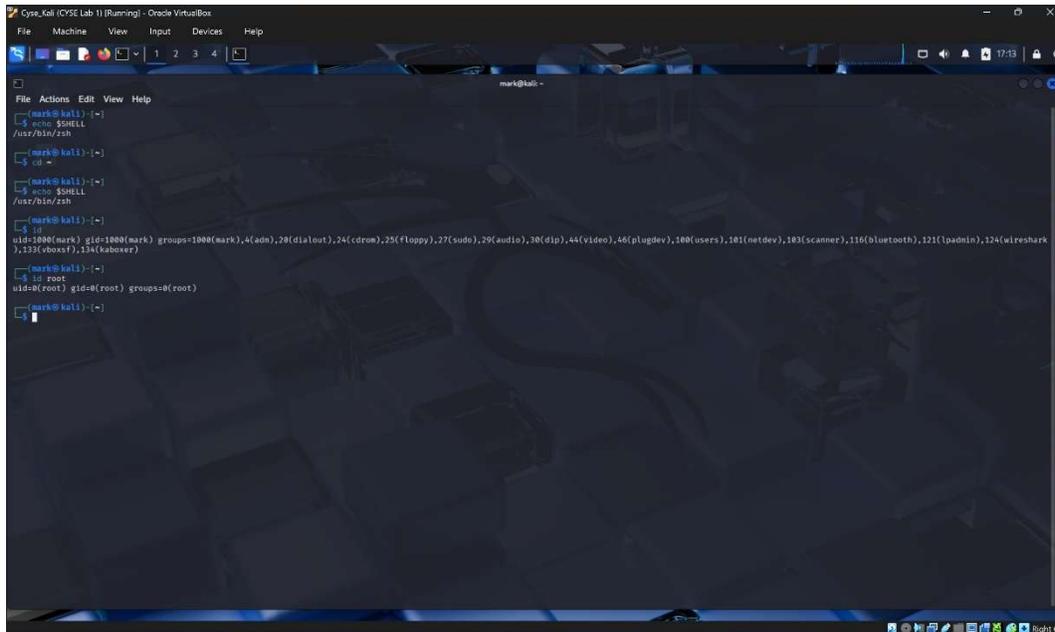
Step 2 - Display the current user's ID and group membership.



```
mark@kali: ~  
└─$ id  
uid=1000(mark) gid=1000(mark) groups=1000(mark),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),103(scanner),116(bluetooth),121(lpadmin),124(wireshark),133(vboxsf),134(kabover))  
└─$
```

id

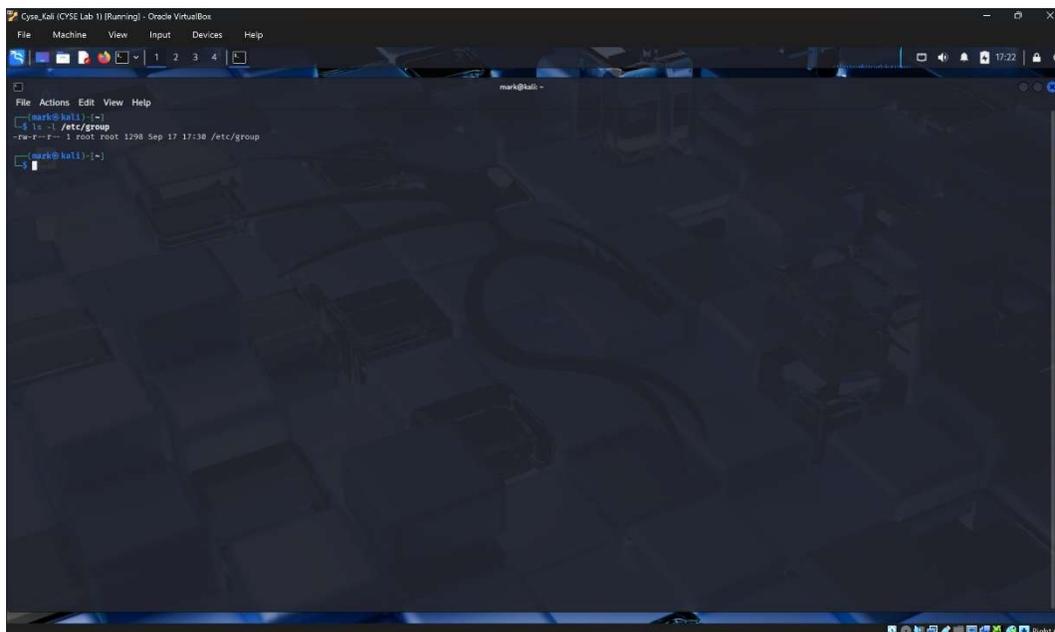
Step 3 - Display the group membership of the root account.



```
Cyax_Kali (CYSE Lab 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
mark@kali ~
┌──(mark@kali)-[~]
│   └─$ echo $SHELL
│   /usr/bin/zsh
└──(mark@kali)-[~]
      └─$ cd ~
┌──(mark@kali)-[~]
│   └─$ echo $SHELL
│   /usr/bin/zsh
└──(mark@kali)-[~]
      └─$ id
uid=1000(mark) gid=1000(mark) groups=1000(mark),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugin),100(users),101(netdev),103(scanner),116(bluetooth),121(lpadmin),124(wireshark),133(vboxsf),134(kaboxer))
┌──(mark@kali)-[~]
│   └─$ id root
uid=0(root) gid=0(root) groups=0(root)
└──(mark@kali)-[~]
      └─$
```

id root

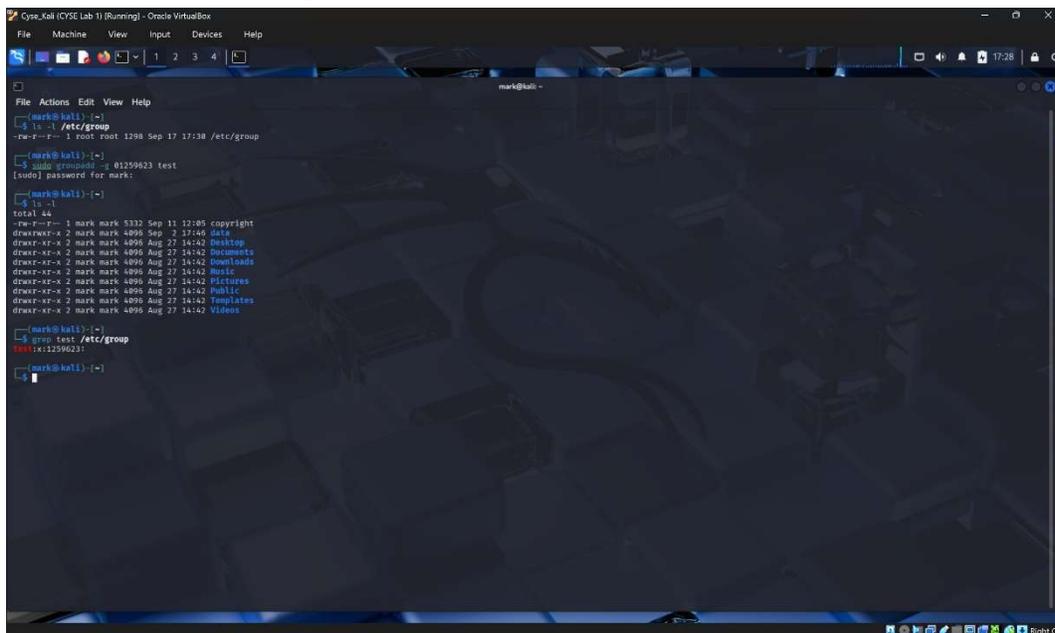
Step 4 - Run the correct command to determine the user owner and group owner of the /etc/group file.



```
Cyax_Kali (CYSE Lab 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
mark@kali ~
┌──(mark@kali)-[~]
│   └─$ ls -l /etc/group
└──(mark@kali)-[~]
      └─$
```

ls -l /etc/group

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



```
mark@kali:~$ ls -l /etc/group
-rw-r--r-- 1 root root 1298 Sep 17 17:30 /etc/group

mark@kali:~$ sudo groupadd -g 01259623 test
[sudo] password for mark:

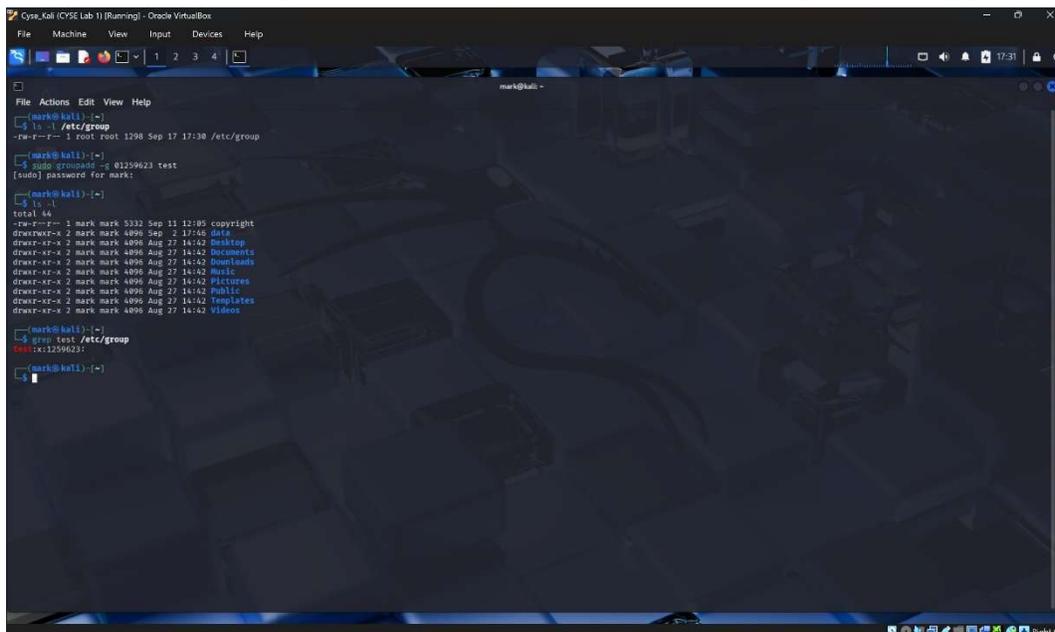
mark@kali:~$ ls -l
total 44
-rw-r--r-- 1 mark mark 5332 Sep 11 12:05 copyright
drwxr-xr-x 2 mark mark 4096 Sep  2 17:46 data
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Desktop
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Documents
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Downloads
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Music
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Pictures
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Public
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Templates
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Videos

mark@kali:~$ cat /etc/group
:x:1259623:

mark@kali:~$
```

sudo groupadd -g 01259623 test

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



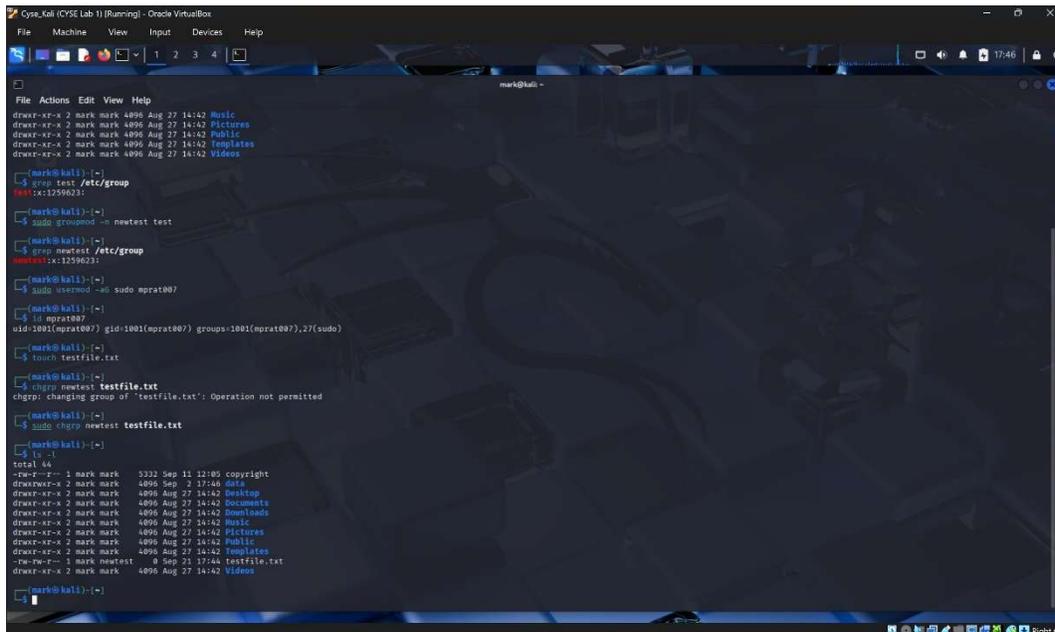
```
mark@kali:~$ cat /etc/group
:x:1259623:

mark@kali:~$ grep test /etc/group
:x:1259623:

mark@kali:~$
```

grep test /etc/group

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

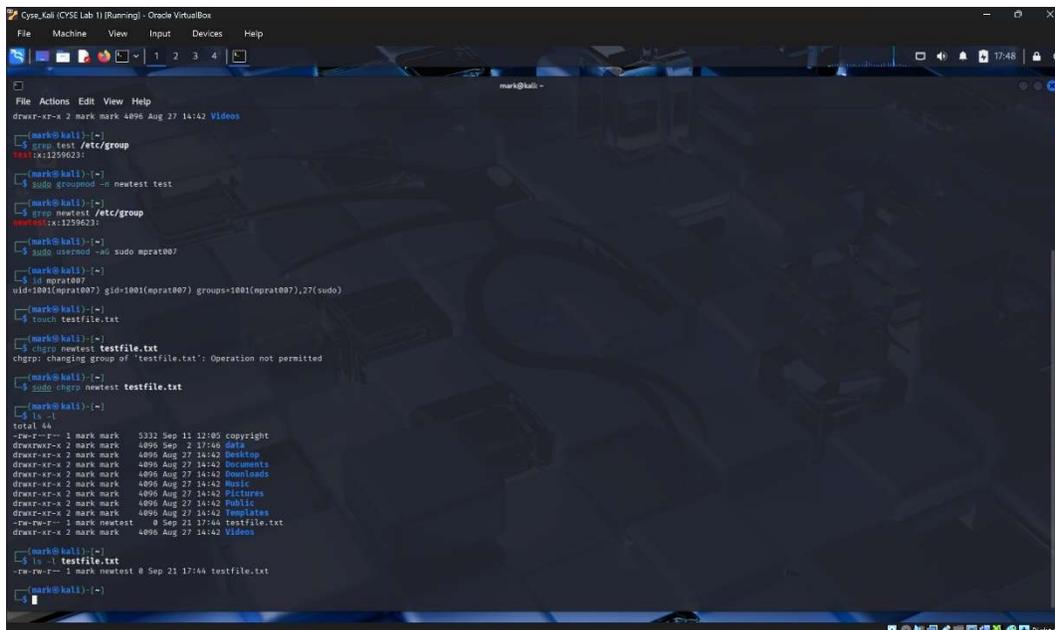


```
mark@kali:~$ touch testfile.txt
mark@kali:~$ sudo chgrp newtest testfile.txt
chgrp: changing group of 'testfile.txt': Operation not permitted
mark@kali:~$ ls -l testfile.txt
-rw-rw-r-- 1 mark newtest 0 Sep 21 17:44 testfile.txt
```

touch testfile.txt

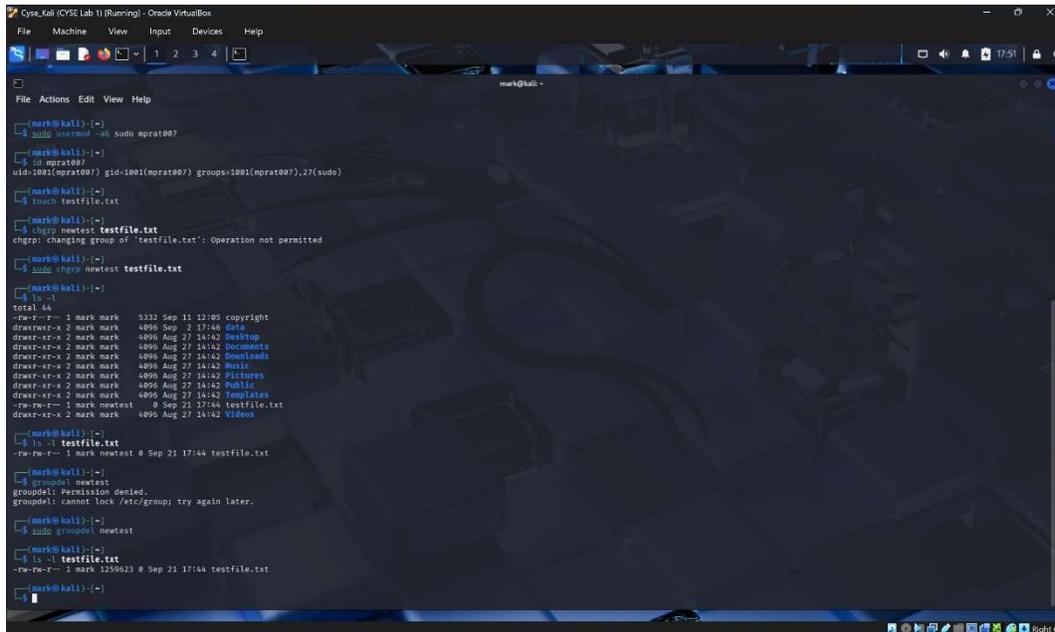
sudo chgrp newtest testfile.txt

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



```
mark@kali:~$ ls -l testfile.txt
-rw-rw-r-- 1 mark newtest 0 Sep 21 17:44 testfile.txt
```

Step 11 - Delete the newestest group, then repeat the previous step.



A terminal window showing a series of commands and their outputs. The user 'mark' is logged in. The commands and outputs are as follows:

```
mark@kali:~$ sudo userdel -r mprat007
mark@kali:~$ ls
total 44
-rw-r--r-- 1 mark mark 5332 Sep 11 12:05 copyright
drwxr-xr-x 2 mark mark 4096 Sep 2 17:46 data
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Desktop
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Documents
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Downloads
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Music
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Pictures
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Public
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Templates
-rw-rw-r-- 1 mark newestest 0 Sep 21 17:44 testfile.txt
drwxr-xr-x 2 mark mark 4096 Aug 27 14:42 Videos

mark@kali:~$ ls -l testfile.txt
-rw-rw-r-- 1 mark newestest 0 Sep 21 17:44 testfile.txt

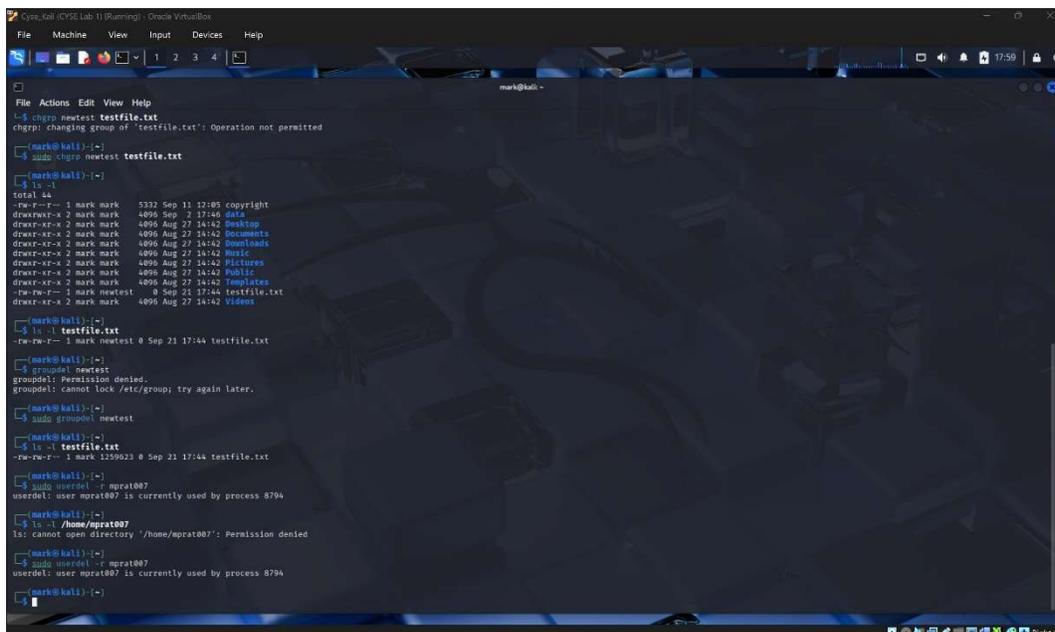
mark@kali:~$ sudo groupdel newestest
groupdel: Permission denied.
groupdel: cannot lock /etc/group; try again later.

mark@kali:~$ ls -l testfile.txt
-rw-rw-r-- 1 mark 1259623 0 Sep 21 17:44 testfile.txt
```

sudo groupdel newestest

It looks like the file reverted back to the uin group.

Step 12 - Delete the user mprat007 along with the home directory using a single command.



A terminal window showing a series of commands and their outputs. The user 'mark' is logged in. The commands and outputs are as follows:

```
mark@kali:~$ sudo userdel -r mprat007
userdel: user mprat007 is currently used by process 8794

mark@kali:~$ ls -l /home/mprat007
ls: cannot open directory '/home/mprat007': Permission denied

mark@kali:~$ sudo userdel -r mprat007
userdel: user mprat007 is currently used by process 8794
```

sudo userdel mprat007

This did not work because the user was being used in a process.