Antonio Shields
CYSE 270
February 02, 2023
Assignment 4

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)

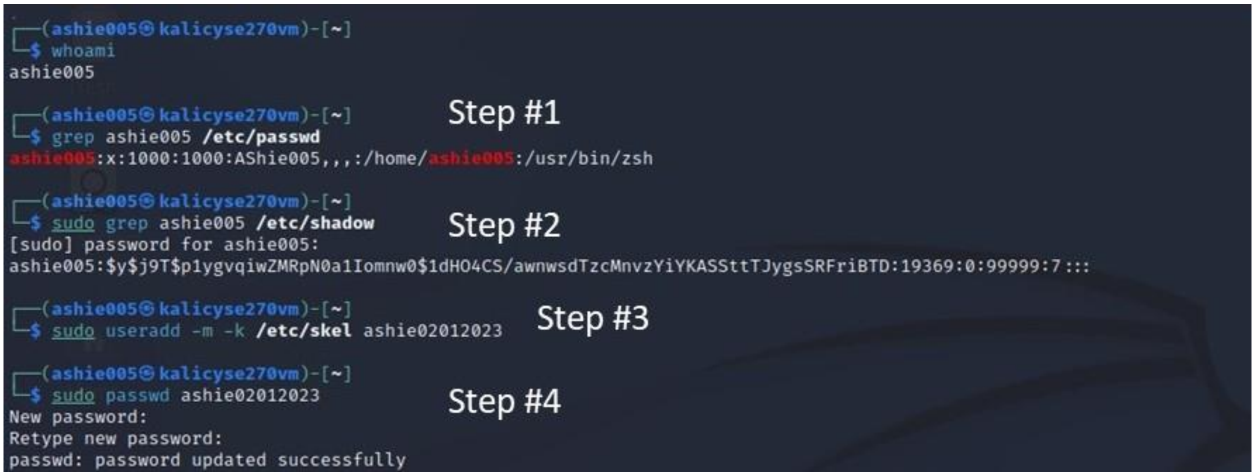
1. **Open a terminal window in VM and execute the correct command to display user account information (including the login shell and home directory) for the current user using grep.**

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

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

   /home/xxxxx for this user. ***<u>Please note that ashie005, my UID, is my original user account made for kali linux before this assignment, so ashie02012023 is the new account that was made for this assignment.</u>*******

4. **Set a password for the new user.**

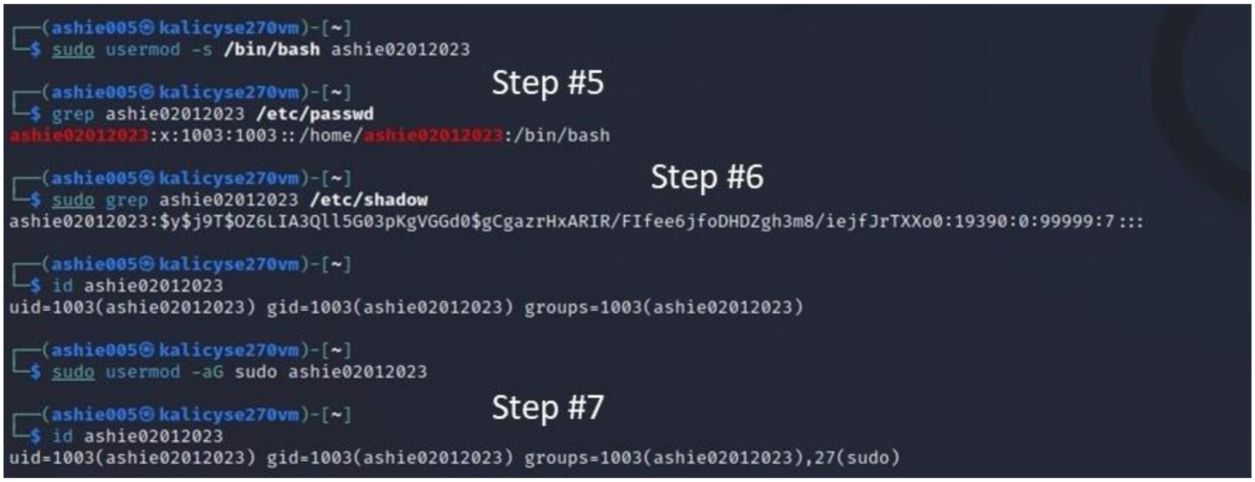


```
┌──(ashie005㉿kalicyse270vm)-[~]
└─$ whoami
ashie005

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ grep ashie005 /etc/passwd
ashie005:x:1000:1000:AShie005,,,:/home/ashie005:/usr/bin/zsh

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo grep ashie005 /etc/shadow
[sudo] password for ashie005:
ashie005:$y$j9T$p1ygvqiwZMRpN0a1Iomnw0$1dHO4CS/awnwsdTzcMnvzYiYKASSttTJygsSRFriBTD:19369:0:99999:7:::

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo useradd -m -k /etc/skel ashie02012023

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo passwd ashie02012023
New password:
Retype new password:
passwd: password updated successfully
```

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

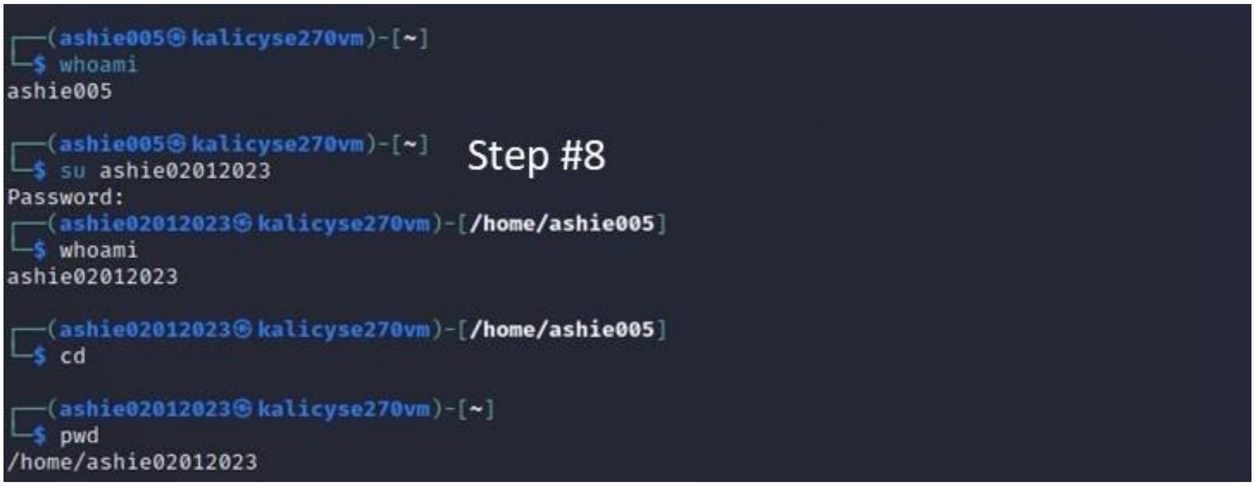
6. **Execute the correct command to display user password information (including the encrypted password and password aging) for the new user xxxxx using grep.**

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



```
┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo usermod -s /bin/bash ashie02012023

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ grep ashie02012023 /etc/passwd
ashie02012023:x:1003:1003::/home/ashie02012023:/bin/bash

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo grep ashie02012023 /etc/shadow
ashie02012023:$y$j9T$OZ6LIA3Qll5G03pKgVGGd0$gCgazrHxARIR/FIfee6jfoDHDZgh3m8/iejfJrTXXo0:19390:0:99999:7:::

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ id ashie02012023
uid=1003(ashie02012023) gid=1003(ashie02012023) groups=1003(ashie02012023)

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo usermod -aG sudo ashie02012023

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ id ashie02012023
uid=1003(ashie02012023) gid=1003(ashie02012023) groups=1003(ashie02012023),27(sudo)
```

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



```
┌──(ashie005㉿kalicyse270vm)-[~]
└─$ whoami
ashie005

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ su ashie02012023
Password:
┌──(ashie02012023㉿kalicyse270vm)-[/home/ashie005]
└─$ whoami
ashie02012023

┌──(ashie02012023㉿kalicyse270vm)-[/home/ashie005]
└─$ cd

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ pwd
/home/ashie02012023
```

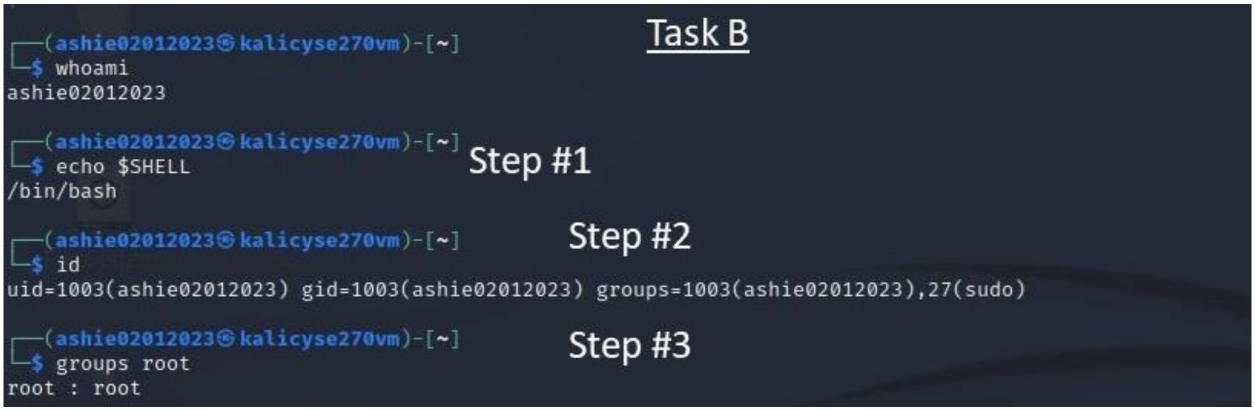
Task B – Group account management (12 * 5 = 60 points)

Use Linux commands to execute the following tasks:

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

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

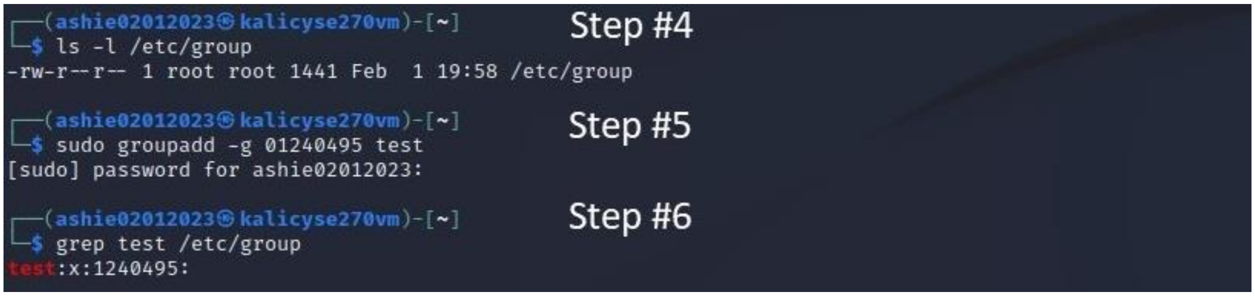
3. **Display the group membership of the root account.**



```
┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ whoami
ashie02012023

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ echo $SHELL
/bin/bash

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ id
uid=1003(ashie02012023) gid=1003(ashie02012023) groups=1003(ashie02012023),27(sudo)

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ groups root
root : root
```

4. **Run the correct command to determine the user owner and group owner of the /etc/group file.**
5. **Create a new group named test and use your UIN as the GID.**

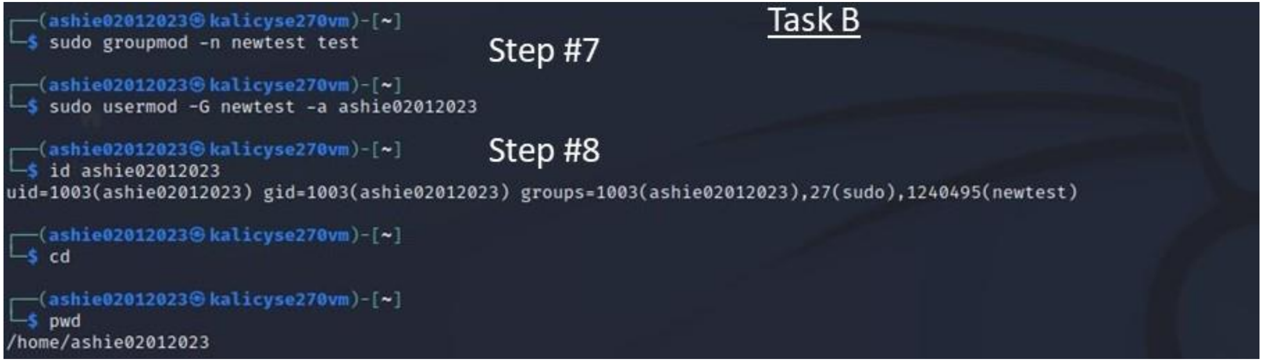
6. **Display the group account information for the test group using grep.**



```
┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ ls -l /etc/group
-rw-r--r-- 1 root root 1441 Feb  1 19:58 /etc/group

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ sudo groupadd -g 01240495 test
[sudo] password for ashie02012023:

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ grep test /etc/group
test:x:1240495:
```

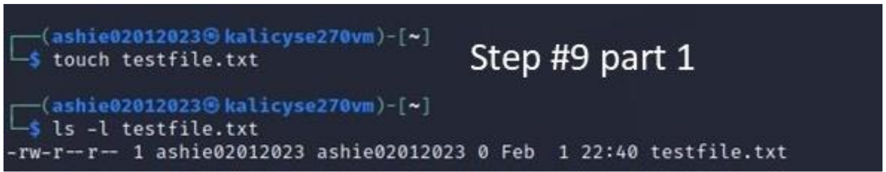
7. **Change the group name of the test group to newtest.**

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



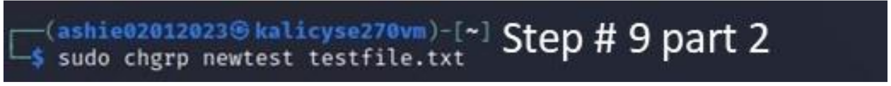
```
┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ sudo groupmod -n newtest test

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ sudo usermod -G newtest -a ashie02012023

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ id ashie02012023
uid=1003(ashie02012023) gid=1003(ashie02012023) groups=1003(ashie02012023),27(sudo),1240495(newtest)

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ cd

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ pwd
/home/ashie02012023
```

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



```
┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ touch testfile.txt

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ ls -l testfile.txt
-rw-r--r-- 1 ashie02012023 ashie02012023 0 Feb  1 22:40 testfile.txt
```

Step #9 part 1



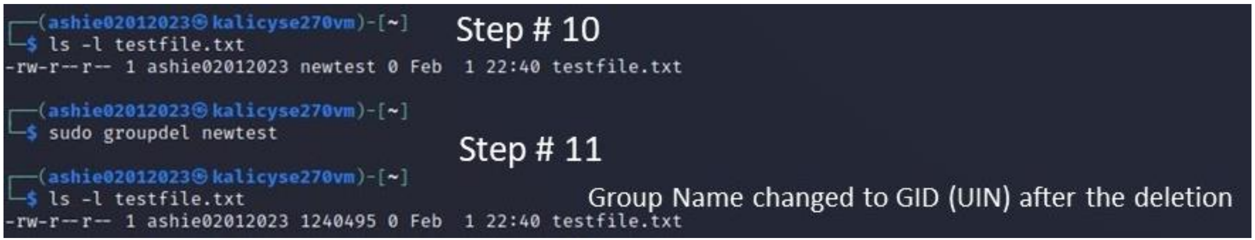
```
┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ sudo chgrp newtest testfile.txt
```

Step # 9 part 2

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?** Group Name changed to the GID assigned, which was my UIN after deletion.

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

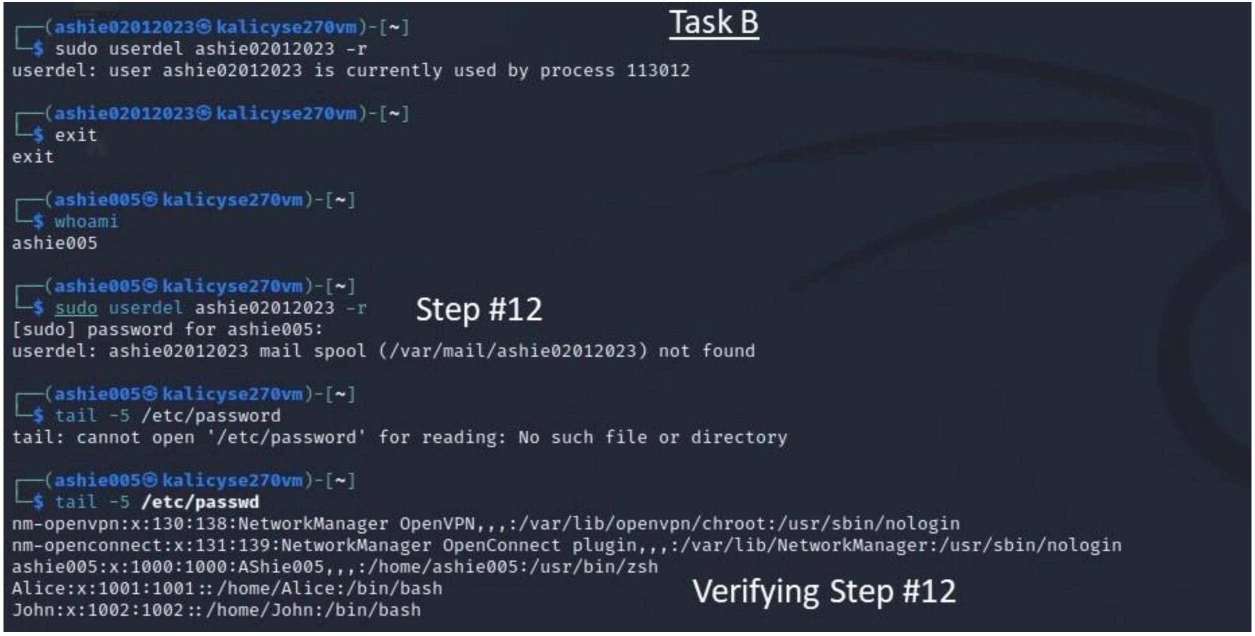


```
┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ ls -l testfile.txt
-rw-r--r-- 1 ashie02012023 newtest 0 Feb  1 22:40 testfile.txt

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ sudo groupdel newtest

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ ls -l testfile.txt
-rw-r--r-- 1 ashie02012023 1240495 0 Feb  1 22:40 testfile.txt
```

Step # 10

Step # 11

Group Name changed to GID (UIN) after the deletion



```
┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ sudo userdel ashie02012023 -r
userdel: user ashie02012023 is currently used by process 113012

┌──(ashie02012023㉿kalicyse270vm)-[~]
└─$ exit
exit

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ whoami
ashie005

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ sudo userdel ashie02012023 -r
[sudo] password for ashie005:
userdel: ashie02012023 mail spool (/var/mail/ashie02012023) not found

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ tail -5 /etc/password
tail: cannot open '/etc/password' for reading: No such file or directory

┌──(ashie005㉿kalicyse270vm)-[~]
└─$ tail -5 /etc/passwd
nm-openvpn:x:130:138:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:131:139:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
ashie005:x:1000:1000:AShie005,,,:/home/ashie005:/usr/bin/zsh
Alice:x:1001:1001::/home/Alice:/bin/bash
John:x:1002:1002::/home/John:/bin/bash
```

Task B

Step #12

Verifying Step #12