

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

Goal:

The goal of this lab is to familiarize students with the fundamental tasks of managing user and group accounts in Linux. By completing this lab, students will gain practical experience in creating, modifying, and deleting accounts, as well as managing group memberships and permissions, which are essential skills in system administration and cybersecurity.

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.



```
logn@kali:~$ grep $(whoami) /etc/passwd
logn:x:1000:1000:Logan Gutierrez,,:/home/logn:/usr/bin/zsh
```

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



```
lgut@kali: ~  
File Actions Edit View Help  
[lgut@kali] ~  
└─$ cat /etc/shadow  
lgut:$y$j9T$icxkkrupq11-9HakQu11/bv5kZLxpH06c16F8WVwAIPdFJ8tseADVWds1e2G1za8:20332:0:99999:7:::  
[lgut@kali] ~  
└─$
```

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



```
lgut@kali: ~  
File Actions Edit View Help  
[lgut@kali] ~  
└─$ sudo useradd -m -s /bin/bash /home/1gut1885 1gut1885  
[lgut@kali] ~  
└─$
```

4. Set a password for the new user.



```
lgut@kali: ~  
File Actions Edit View Help  
[lgut@kali] ~  
└─$ sudo passwd 1gut1885  
New password:  
Retype new password:  
passwd: password updated successfully  
[lgut@kali] ~  
└─$
```

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



```
lgtut1005@kali -
File Actions Edit View Help
(lgtut@kali) [-]
└─$ sudo passwd lgtut1005
New password:
Retype new password:
passwd: password updated successfully

(lgtut@kali) [-]
└─$ sudo usermod -s /bin/bash lgtut1005

(lgtut@kali) [-]
└─$ grep lgtut1005 /etc/passwd
lgtut1005:x:1005:1000::/home/lgtut1005:/bin/bash

(lgtut@kali) [-]
└─$ sudo grep lgtut1005 /etc/shadow
lgtut1005:$y$9T$Fm5u3fy0wrr0ug50aR1T01$zG3rFC60vLr3V5AFg8.INCuW9K7bu0P90kgF1ec8:20353:0:99999:7:::

(lgtut@kali) [-]
└─$ sudo usermod -G sudo lgtut1005

(lgtut@kali) [-]
└─$ su - lgtut1005
Password:
(lgtut1005@kali) [-]
└─$
```

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.



```
lgtut@kali -
File Actions Edit View Help
(lgtut@kali) [-]
└─$ cd ~

(lgtut@kali) [-]
└─$ echo $SHELL
/usr/bin/zsh

(lgtut@kali) [-]
└─$
```

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



```
lgut@kali: ~  
└─$ id  
uid=1000(lgut) gid=1000(lgut) groups=1000(lgut),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),181(netdev),183(scanner),116(bluetooth),121(lpadmin),324(wireshark),133(vboxsf),134(kboxer)  
└─$ groups  
lgut adm dialout cdrom floppy sudo audio dip video plugdev users netdev scanner bluetooth lpadmin wireshark vboxsf kboxer  
└─$
```

3. Display the group membership of the root account.

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



```
lgut@kali: ~  
└─$ id  
uid=0(root) gid=0(root) groups=0(root)  
└─$ ls -l /etc/group  
-rw-r--r-- 1 root root 1408 Sep 23 18:05 /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**.



```
lgut@kali: ~  
└─$ sudo groupadd -g 42223482 test  
└─$ groups test /etc/group  
test:42223482  
└─$
```

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



```
lgut@kali:~$ sudo groupmod -n newtest test
lgut@kali:~$ sudo usermod -s newtest lgut1885
lgut@kali:~$ touch testfile
lgut@kali:~$ sudo chgrp newtest ~/testfile
lgut@kali:~$
```


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



```
lgut@kali:~$ ls -l testfile
-rw-rw-r-- 1 lgut newtest 0 Sep 22 18:28 testfile
lgut@kali:~$
```

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

Newtest is no longer the group owner and now shows my UIN in its place.



```
lgut@kali:~$ sudo groupdel newtest
lgut@kali:~$ ls -l testfile
-rw-rw-r-- 1 lgut 123456 0 Sep 22 18:28 testfile
lgut@kali:~$
```

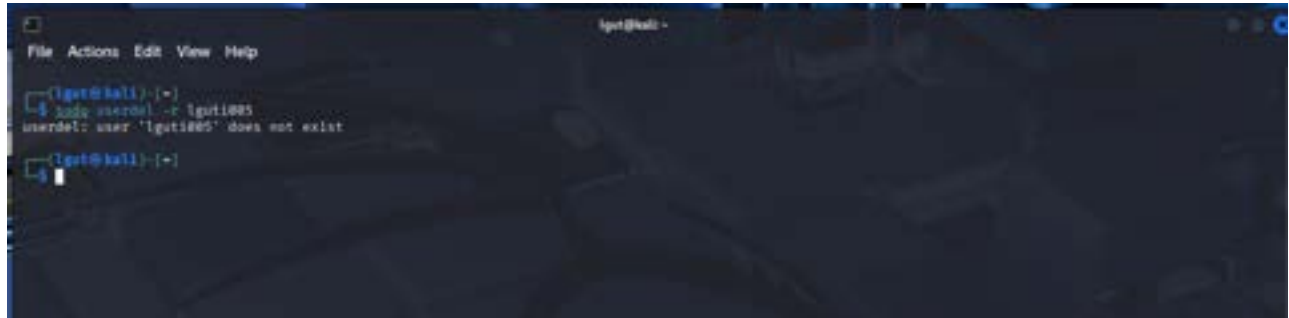
12.

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

already put the command through and typed clear, forgetting to screenshot.

But this is the command I put through. I believe it could also be `sudo rm -r`

`lguti005`



```
lguti@kali: ~  
File Actions Edit View Help  
lguti@kali: ~  
└─$ sudo userdel -r lguti005  
userdel: user 'lguti005' does not exist  
lguti@kali: ~  
└─$
```