

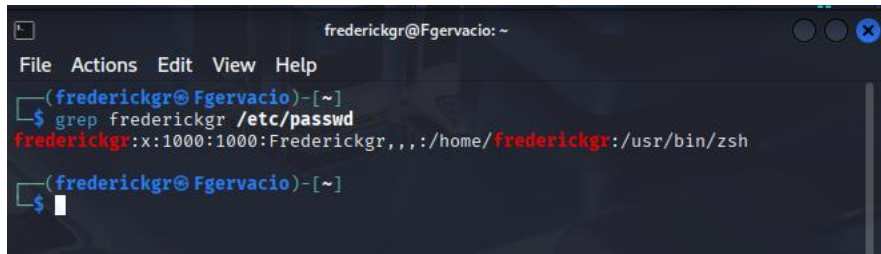
## Frederick Gervacio

### CYSE 270-17496: Linux System for Cybersecurity

#### Assignment 4

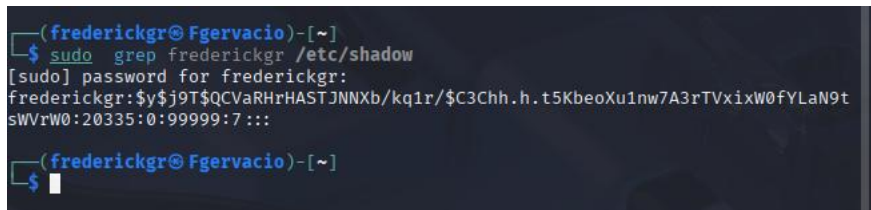
#### Task A – User Account management

- 1) Used grep to show the login shell and home directory



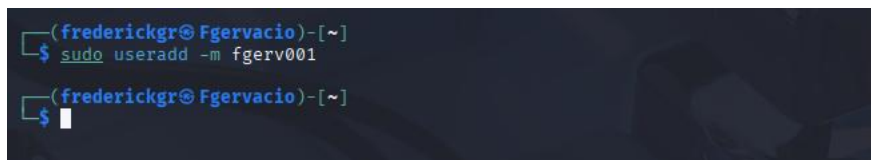
```
frederickgr@Fgervacio: ~  
File Actions Edit View Help  
(frederickgr@Fgervacio)-[~]  
$ grep frederickgr /etc/passwd  
frederickgr:x:1000:1000:Frederickgr,,,:/home/frederickgr:/usr/bin/zsh  
(frederickgr@Fgervacio)-[~]  
$
```

- 2) When using only grep would get and denied response so had to use “sudo” before the grep user /etc/shadow command to be allowed access.



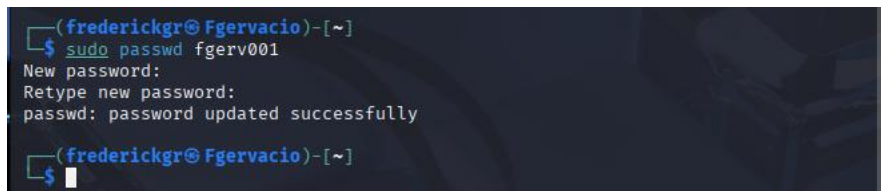
```
(frederickgr@Fgervacio)-[~]  
$ sudo grep frederickgr /etc/shadow  
[sudo] password for frederickgr:  
frederickgr:$y$j9T$QCVaRHrHASTJNNXb/kq1r/$C3Ch.h.t5KbeoXu1nw7A3rTVxixW0fYLaN9t  
sWVrW0:20335:0:99999:7 :::  
(frederickgr@Fgervacio)-[~]  
$
```

- 3) Using “sudo” command combined with useradd -m created a new user “fgerv001”



```
(frederickgr@Fgervacio)-[~]  
$ sudo useradd -m fgerv001  
(frederickgr@Fgervacio)-[~]  
$
```

- 4) Using “sudo” command with “passwd” created a password for user “fgerv001”



```
(frederickgr@Fgervacio)-[~]  
$ sudo passwd fgerv001  
New password:  
Retype new password:  
passwd: password updated successfully  
(frederickgr@Fgervacio)-[~]  
$
```

- 5) Set bash shell as the default login for fgerv001 using “sudo” usermod and /bin/bash command. Verified it using the grep user /etc/passwd.

```
(frederickgr@Fgervacio)-[~]
└─$ sudo grep fgerv001 /etc/passwd
\fgerv001:x:1001:1001::/home/fgerv001:/bin/sh

(frederickgr@Fgervacio)-[~]
└─$ sudo usermod -s /bin/bash fgerv001

(frederickgr@Fgervacio)-[~]
└─$ grep fgerv001 /etc/passwd
fgerv001:x:1001:1001::/home/fgerv001:/bin/bash

(frederickgr@Fgervacio)-[~]
└─$
```

- 6) used “sudo” grep user /etc/shadow command to display password information for the user

```
(frederickgr@Fgervacio)-[~]
└─$ sudo grep fgerv001 /etc/shadow
fgerv001:$y$j9T$IoSsIElAj.7MtZkmznKB0$o5DQeiW2IvUQTFUIBAT4/ukzIRcvr89QgCjuJXys
VT1:20352:0:99999:7:::

(frederickgr@Fgervacio)-[~]
└─$
```

- 7) Added the user to a new group while maintaining the existing group membership using the usermod -aG command

```
(frederickgr@Fgervacio)-[~]
└─$ sudo usermod -aG sudo fgerv001

(frederickgr@Fgervacio)-[~]
└─$ id fgerv001
uid=1001(fgerv001) gid=1001(fgerv001) groups=1001(fgerv001),27(sudo)

(frederickgr@Fgervacio)-[~]
└─$
```

- 8) Used the “su” command to switch user to the new account.

```
(frederickgr@Fgervacio)-[~]
└─$ su fgerv001
Password:
(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ whoami
fgerv001

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$
```

## Task B – Group account management

1. Returned to home directory and used the echo \$SHELL command to determine my previous command.

```
(frederickgr@Fgervacio)-[~]
└─$ grep frederickgr /etc/passwd
frederickgr:x:1000:1000:Frederickgr,,,:/home/frederickgr:/usr/bin/zsh

(frederickgr@Fgervacio)-[~]
└─$ echo $SHELL
/usr/bin/zsh

(frederickgr@Fgervacio)-[~]
└─$
```

2. Displayed the user's ID group membership with ID and username command

```
(frederickgr@Fgervacio)-[~]
└─$ id frederickgr
uid=1000(frederickgr) gid=1000(frederickgr) groups=1000(frederickgr),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(kaboxer)

(frederickgr@Fgervacio)-[~]
└─$
```

3. Used the “groups” command to display group membership of root account.

```
(frederickgr@Fgervacio)-[~]
└─$ groups
frederickgr adm dialout cdrom floppy sudo audio dip video plugdev users netdev scanner bluetooth lpadmin wireshark vboxsf kaboxer

(frederickgr@Fgervacio)-[~]
└─$
```

4. Used the ls -l command with the /etc/group to show the user owner and group owner.

```
(frederickgr@Fgervacio)-[~]
└─$ ls -l /etc/group
-rw-r--r-- 1 root root 1424 Sep 21 10:09 /etc/group

(frederickgr@Fgervacio)-[~]
└─$
```

5. Created a new group named test and used 1523 as the GID because I couldn't find my UIN.

```
(frederickgr@Fgervacio)-[~]
└─$ sudo groupadd -g 1523 test
[sudo] password for frederickgr:

(frederickgr@Fgervacio)-[~]
└─$
```

6. Displayed the group account information the test group using the `grep /etc/group` command.

```
(frederickgr@Fgervacio)-[~]
└─$ grep test /etc/group
test:x:1523:
```

7. Changed the group name of the test group to newtest using the `groupmod -n` command

```
(frederickgr@Fgervacio)-[~]
└─$ sudo groupmod -n newtest test

(frederickgr@Fgervacio)-[~]
└─$
```

8. Added the current `fgerv001` as second directory member without overwriting the user's current group membership.

```
password:
(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ id
uid=1001(fgerv001) gid=1001(fgerv001) groups=1001(fgerv001),27(sudo),1523(newtest)

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$
```

9. Created a new file using the “touch” command in the `fgerv001` account and changed the group owner to newtest using the “chgrp” command.

```
(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ sudo touch testfile

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ sudo chgrp newtest testfile

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$
```

10. Displayed the user owner and group owner information of the testfile using the `sudo ls -l` command when I didn't used “sudo” access was denied.

```
(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ ls -l testfile
ls: cannot access 'testfile': Permission denied

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ sudo ls -l testfile
-rw-r--r-- 1 root newtest 0 Sep 21 12:07 testfile

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ sudo ls -l
total 48
-rw-r--r-- 1 frederickgr frederickgr 5332 Sep 12 16:53 copyright_cyse270
drwxrwxr-x 3 frederickgr frederickgr 4096 Sep  5 11:59 data
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Desktop
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Documents
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Downloads
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Music
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Pictures
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Public
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Templates
-rw-r--r-- 1 root newtest 0 Sep 21 12:07 testfile
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Videos
drwxr-xr-x 8 frederickgr frederickgr 4096 Sep  5 11:38 w

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$
```

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

```
(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ sudo groupdel newestest

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$ sudo ls -l
total 48
-rw-r--r-- 1 frederickgr frederickgr 5332 Sep 12 16:53 copyright_cyse270
drwxrwxr-x 3 frederickgr frederickgr 4096 Sep  5 11:59 data
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Desktop
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Documents
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Downloads
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Music
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Pictures
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Public
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Templates
-rw-r--r-- 1 root          1523    0 Sep 21 12:07 testfile
drwxr-xr-x 2 frederickgr frederickgr 4096 Sep  4 15:18 Videos
drwxr-xr-x 8 frederickgr frederickgr 4096 Sep  5 11:38 w

(fgerv001@Fgervacio)-[/home/frederickgr]
└─$
```

the

file is now owned by the GID of group 1523 which remove the permission.

12. Delete the user fgerv001 along with the home directory using a single command. Sudo userdel -r fgerv001

```
(frederickgr@Fgervacio)-[~]
└─$ sudo userdel -r fgerv001
[sudo] password for frederickgr:
userdel: fgerv001 mail spool (/var/mail/fgerv001) not found

(frederickgr@Fgervacio)-[~]
└─$
```