

Old Dominion University
CYSE 270 Linux System for Cybersecurity

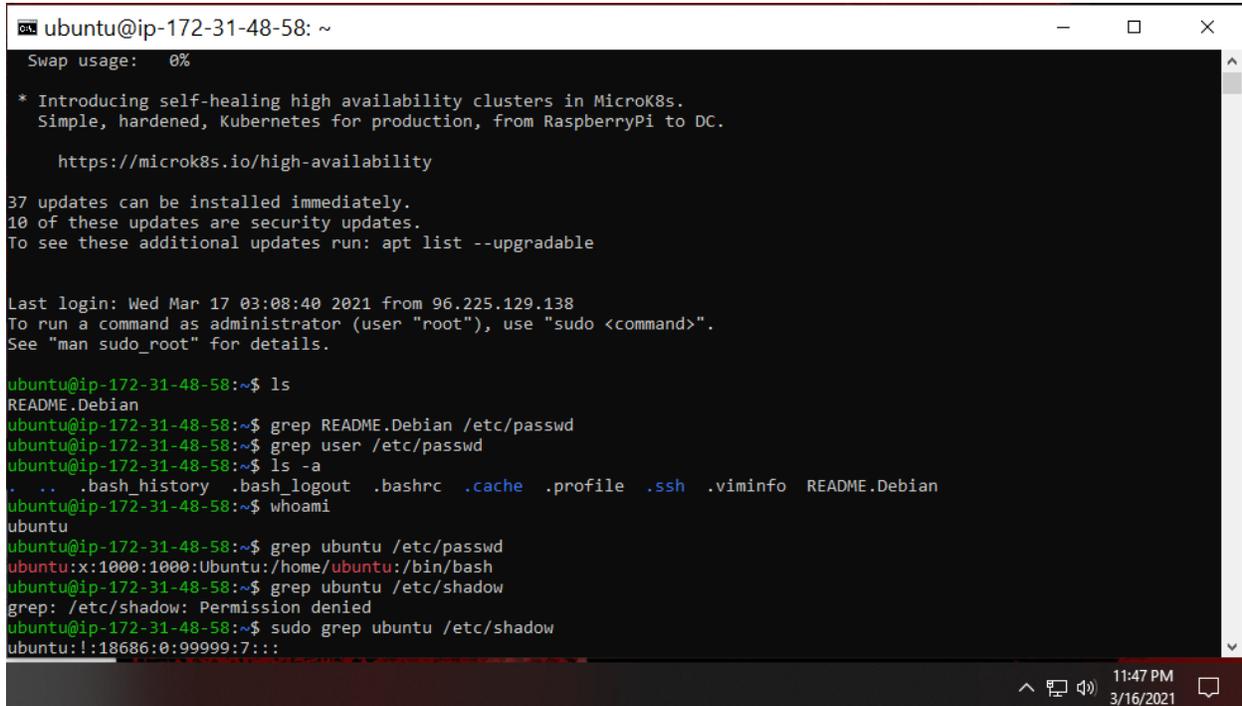
Assignment #4

Joshua Lane

01062078

Task A – User Account management (40 points)

1. Open a terminal window.
2. Execute the correct command to display user account information (including the login shell and home directory) for the current user using grep.
3. Execute the correct command to display user password information (including the encrypted password and password aging) for the current user using grep.



```
ubuntu@ip-172-31-48-58: ~
Swap usage:  0%

* Introducing self-healing high availability clusters in MicroK8s.
  Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

  https://microk8s.io/high-availability

37 updates can be installed immediately.
10 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed Mar 17 03:08:40 2021 from 96.225.129.138
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-48-58:~$ ls
README.Debian
ubuntu@ip-172-31-48-58:~$ grep README.Debian /etc/passwd
ubuntu@ip-172-31-48-58:~$ grep user /etc/passwd
ubuntu@ip-172-31-48-58:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .profile  .ssh  .viminfo  README.Debian
ubuntu@ip-172-31-48-58:~$ whoami
ubuntu
ubuntu@ip-172-31-48-58:~$ grep ubuntu /etc/passwd
ubuntu:x:1000:1000;Ubuntu:/home/ubuntu:/bin/bash
ubuntu@ip-172-31-48-58:~$ grep ubuntu /etc/shadow
grep: /etc/shadow: Permission denied
ubuntu@ip-172-31-48-58:~$ sudo grep ubuntu /etc/shadow
ubuntu:!:18686:0:99999:7:::
```

^Here is steps 2-3 using grep command

4. Create a new user named xxxxx and explicitly use options to create the home directory /home/xxxxx for this user.
5. Set a password for the new user.

SCREENSHOT IS ON NEXT PAGE

```
ubuntu@ip-172-31-48-58: ~  
ubuntu@ip-172-31-48-58:~$ ls  
README.Debian  
ubuntu@ip-172-31-48-58:~$ grep README.Debian /etc/passwd  
ubuntu@ip-172-31-48-58:~$ grep user /etc/passwd  
ubuntu@ip-172-31-48-58:~$ ls -a  
.  .. .bash_history .bash_logout .bashrc .cache .profile .ssh .viminfo README.Debian  
ubuntu@ip-172-31-48-58:~$ whoami  
ubuntu  
ubuntu@ip-172-31-48-58:~$ grep ubuntu /etc/passwd  
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash  
ubuntu@ip-172-31-48-58:~$ grep ubuntu /etc/shadow  
grep: /etc/shadow: Permission denied  
ubuntu@ip-172-31-48-58:~$ sudo grep ubuntu /etc/shadow  
ubuntu!:18686:0:99999:7:::  
ubuntu@ip-172-31-48-58:~$ sudo useradd jlane003  
ubuntu@ip-172-31-48-58:~$ sudo passwd jlane003  
New password:  
Retype new password:  
passwd: password updated successfully  
ubuntu@ip-172-31-48-58:~$ sudo userdel -r jlane003  
userdel: jlane003 mail spool (/var/mail/jlane003) not found  
userdel: jlane003 home directory (/home/jlane003) not found  
ubuntu@ip-172-31-48-58:~$ sudo userdel jlane003  
userdel: user 'jlane003' does not exist  
ubuntu@ip-172-31-48-58:~$ sudo useradd -m jlane003  
ubuntu@ip-172-31-48-58:~$ sudo passwd jlane003  
New password:  
Retype new password:  
passwd: password updated successfully
```

^Above is steps 4-5 **using sudo useradd -m**, I had to delete the one I messed up on.

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

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

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

9. Switch to the new user's account, then continue Task B.

SCREENSHOT IS ON NEXT PAGE

```
jlane003@ip-172-31-48-58: /home/ubuntu
userdel: jlane003 mail spool (/var/mail/jlane003) not found
userdel: jlane003 home directory (/home/jlane003) not found
ubuntu@ip-172-31-48-58:~$ sudo userdel jlane003
userdel: user 'jlane003' does not exist
ubuntu@ip-172-31-48-58:~$ sudo useradd -m jlane003
ubuntu@ip-172-31-48-58:~$ sudo passwd jlane003
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-48-58:~$ ls
README.Debian
ubuntu@ip-172-31-48-58:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .profile  .ssh  .sudo_as_admin_successful  .viminfo  README.Debian
ubuntu@ip-172-31-48-58:~$ sudo usermod -s /bin/bash jlane003
ubuntu@ip-172-31-48-58:~$ grep jlane003 /etc/passwd
jlane003:x:1001:1001:~/home/jlane003:/bin/bash
ubuntu@ip-172-31-48-58:~$ sudo usermod -G sudo -a jlane003
ubuntu@ip-172-31-48-58:~$ su jlane003
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jlane003@ip-172-31-48-58:~/home/ubuntu$
```

^Above is steps 6-9. I used **sudo usermod -s** to change the default login shell to bash. I checked using **grep jlane003 /etc/passwd**. I then added jlane003 to sudo using **sudo usermod -G sudo -a jlane003**. I switched users using **su jlane003**.

Task B – Group account management (60 points)

1. Open a terminal window 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.

SCREENSHOT IS ON NEXT PAGE

```
jlane003@ip-172-31-48-58: /home/ubuntu
userdel: jlane003 home directory (/home/jlane003) not found
ubuntu@ip-172-31-48-58:~$ sudo userdel jlane003
userdel: user 'jlane003' does not exist
ubuntu@ip-172-31-48-58:~$ sudo useradd -m jlane003
ubuntu@ip-172-31-48-58:~$ sudo passwd jlane003
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-48-58:~$ ls
README.Debian
ubuntu@ip-172-31-48-58:~$ ls -a
. . . .bash_history .bash_logout .bashrc .cache .profile .ssh .sudo_as_admin_successful .viminfo README.Debian
ubuntu@ip-172-31-48-58:~$ sudo usermod -s /bin/bash jlane003
ubuntu@ip-172-31-48-58:~$ grep jlane003 /etc/passwd
jlane003:x:1001:1001:~/home/jlane003:/bin/bash
ubuntu@ip-172-31-48-58:~$ sudo usermod -G sudo -a jlane003
ubuntu@ip-172-31-48-58:~$ su jlane003
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jlane003@ip-172-31-48-58:/home/ubuntu$ id
uid=1001(jlane003) gid=1001(jlane003) groups=1001(jlane003),27(sudo)
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo gid ubuntu
[sudo] password for jlane003:
sudo: gid: command not found
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo id ubuntu
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),117(netdev),118(lxd)
jlane003@ip-172-31-48-58:/home/ubuntu$
```

^Above is steps 1-3.

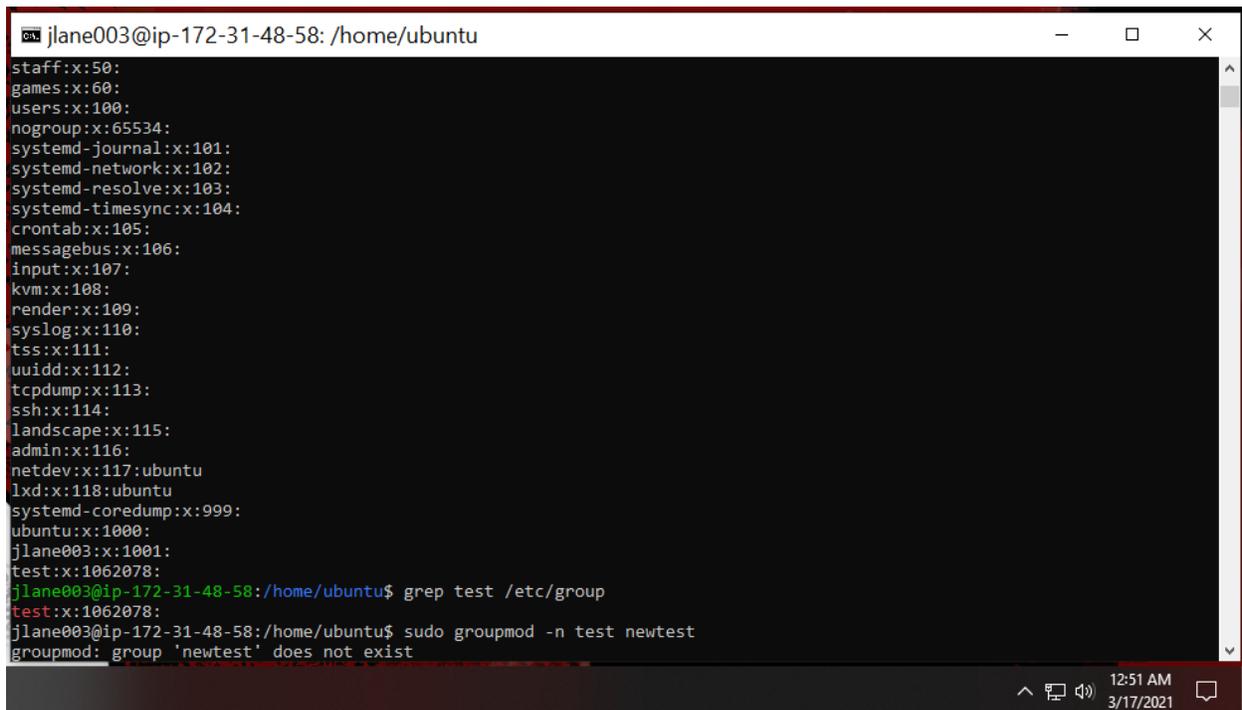
4. Run the correct command to determine the user owner and group owner of the /etc/group file.

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

```
jlane003@ip-172-31-48-58: /home/ubuntu
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-48-58:~$ ls
README.Debian
ubuntu@ip-172-31-48-58:~$ ls -a
. . . .bash_history .bash_logout .bashrc .cache .profile .ssh .sudo_as_admin_successful .viminfo README.Debian
ubuntu@ip-172-31-48-58:~$ sudo usermod -s /bin/bash jlane003
ubuntu@ip-172-31-48-58:~$ grep jlane003 /etc/passwd
jlane003:x:1001:1001:~/home/jlane003:/bin/bash
ubuntu@ip-172-31-48-58:~$ sudo usermod -G sudo -a jlane003
ubuntu@ip-172-31-48-58:~$ su jlane003
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jlane003@ip-172-31-48-58:/home/ubuntu$ id
uid=1001(jlane003) gid=1001(jlane003) groups=1001(jlane003),27(sudo)
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo gid ubuntu
[sudo] password for jlane003:
sudo: gid: command not found
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo id ubuntu
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),117(netdev),118(lxd)
jlane003@ip-172-31-48-58:/home/ubuntu$ ls -l /etc/group
-rw-r--r-- 1 root root 873 Mar 17 04:06 /etc/group
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo groupadd test -g 01062078
[sudo] password for jlane003:
jlane003@ip-172-31-48-58:/home/ubuntu$ grep test /etc/passwd
jlane003@ip-172-31-48-58:/home/ubuntu$ cat /etc/group
cat: /etc/group: No such file or directory
```

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



```
jlane003@ip-172-31-48-58: /home/ubuntu
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
systemd-timesync:x:104:
crontab:x:105:
messagebus:x:106:
input:x:107:
kvm:x:108:
render:x:109:
syslog:x:110:
tss:x:111:
uidd:x:112:
tcpdump:x:113:
ssh:x:114:
landscape:x:115:
admin:x:116:
netdev:x:117:ubuntu
lxd:x:118:ubuntu
systemd-coredump:x:999:
ubuntu:x:1000:
jlane003:x:1001:
test:x:1062078:
jlane003@ip-172-31-48-58:/home/ubuntu$ grep test /etc/group
test:x:1062078:
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo groupmod -n test newtest
groupmod: group 'newtest' does not exist
```

^Above is the group information using **grep**.

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

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

NEXT STEPS ARE ON NEXT PAGE

```
jlane003@ip-172-31-48-58: /home/ubuntu
groupmod: group 'newtest' does not exist
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo groupmod -n test newtest
groupmod: group 'newtest' does not exist
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo groupmod -n test
Usage: groupmod [options] GROUP

Options:
  -g, --gid GID           change the group ID to GID
  -h, --help              display this help message and exit
  -n, --new-name NEW_GROUP change the name to NEW_GROUP
  -o, --non-unique        allow to use a duplicate (non-unique) GID
  -p, --password PASSWORD change the password to this (encrypted)
                          PASSWORD
  -R, --root CHROOT_DIR  directory to chroot into
  -P, --prefix PREFIX_DIR prefix directory where are located the /etc/* files

jlane003@ip-172-31-48-58:/home/ubuntu$ groupmod -n test newtest
groupmod: group 'newtest' does not exist
jlane003@ip-172-31-48-58:/home/ubuntu$ groupmod -n newtest test
groupmod: Permission denied.
groupmod: cannot lock /etc/group; try again later.
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo groupmod -n newtest test
jlane003@ip-172-31-48-58:/home/ubuntu$ tail -1 /etc/group
newtest:x:1062078:
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo usermod -G newtest -a jlane003
jlane003@ip-172-31-48-58:/home/ubuntu$ id newtest
id: 'newtest': no such user
jlane003@ip-172-31-48-58:/home/ubuntu$ id jlane003
uid=1001(jlane003) gid=1001(jlane003) groups=1001(jlane003),27(sudo),1062078(newtest)
jlane003@ip-172-31-48-58:/home/ubuntu$
```

^Above is steps 7-8. I used **sudo groupmod -n newtest test** to change the group name to newtest. I then added jlane003 to newtest using **sudo usermod -G newtest -a jlane003**.

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

10. Display the user owner and group owner information.

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

SCREENSHOT IS ON NEXT PAGE

```
jlane003@ip-172-31-48-58: /home/ubuntu
groupmod: Permission denied.
groupmod: cannot lock /etc/group; try again later.
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo groupmod -n newtest test
jlane003@ip-172-31-48-58:/home/ubuntu$ tail -1 /etc/group
newtest:x:1062078:
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo usermod -G newtest -a jlane003
jlane003@ip-172-31-48-58:/home/ubuntu$ id newtest
id: 'newtest': no such user
jlane003@ip-172-31-48-58:/home/ubuntu$ id jlane003
uid=1001(jlane003) gid=1001(jlane003) groups=1001(jlane003),27(sudo),1062078(newtest)
jlane003@ip-172-31-48-58:/home/ubuntu$ touch sample.txt
touch: cannot touch 'sample.txt': Permission denied
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo touch sample.txt
jlane003@ip-172-31-48-58:/home/ubuntu$ ls -l
total 4
-rw-r--r-- 1 ubuntu ubuntu 2435 Feb 28 06:46 README.Debian
-rw-r--r-- 1 root root 0 Mar 17 05:05 sample.txt
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo chgrp newtest sample.txt
jlane003@ip-172-31-48-58:/home/ubuntu$ ls -l
total 4
-rw-r--r-- 1 ubuntu ubuntu 2435 Feb 28 06:46 README.Debian
-rw-r--r-- 1 root newtest 0 Mar 17 05:05 sample.txt
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo groupdel newtest
jlane003@ip-172-31-48-58:/home/ubuntu$ ls -l
total 4
-rw-r--r-- 1 ubuntu ubuntu 2435 Feb 28 06:46 README.Debian
-rw-r--r-- 1 root 1062078 0 Mar 17 05:05 sample.txt
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo userdel -r jlane003
userdel: user jlane003 is currently used by process 26041
jlane003@ip-172-31-48-58:/home/ubuntu$
```

^Above is steps 9-11. I used **sudo touch sample.txt** to create a new file. I used **sudo chgrp newtest sample.txt** to change group ownership. I used **sudo groupdel newtest** to delete the group and found that the group id number is shown in place of the name.

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

```
ubuntu@ip-172-31-48-58: ~
-rw-r--r-- 1 ubuntu ubuntu 2435 Feb 28 06:46 README.Debian
-rw-r--r-- 1 root newtest 0 Mar 17 05:05 sample.txt
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo groupdel newtest
jlane003@ip-172-31-48-58:/home/ubuntu$ ls -l
total 4
-rw-r--r-- 1 ubuntu ubuntu 2435 Feb 28 06:46 README.Debian
-rw-r--r-- 1 root 1062078 0 Mar 17 05:05 sample.txt
jlane003@ip-172-31-48-58:/home/ubuntu$ sudo userdel -r jlane003
userdel: user jlane003 is currently used by process 26041
jlane003@ip-172-31-48-58:/home/ubuntu$ su ubuntu
Password:
su: Authentication failure
jlane003@ip-172-31-48-58:/home/ubuntu$ su ubuntu
Password:
su: Authentication failure
jlane003@ip-172-31-48-58:/home/ubuntu$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1097 Mar 17 03:49 /etc/shadow
jlane003@ip-172-31-48-58:/home/ubuntu$ su ubuntu
Password:
su: Authentication failure
jlane003@ip-172-31-48-58:/home/ubuntu$ exit
exit
ubuntu@ip-172-31-48-58:~$ userdel -r jlane003
userdel: Permission denied.
userdel: cannot lock /etc/passwd; try again later.
ubuntu@ip-172-31-48-58:~$ sudo userdel -r jlane003
userdel: jlane003 mail spool (/var/mail/jlane003) not found
ubuntu@ip-172-31-48-58:~$
```

^Above is step 12 completed using **sudo userdel -r jlane003**.