

Zyron James M. Sumulong
CYSE 270
Assignment 4 - Group and User Management
Dr. Mohammed Al kinoon
21 September 2025

Task A – User Account management

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.

Command: `grep "^kali" /etc/passwd`

-shows the username, UID, GID, home directory and login shell

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

Command: `sudo grep "kali" /etc/shadow`

```
(kali@kali)-[~]
└─$ grep "^kali" /etc/passwd
kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh

(kali@kali)-[~]
└─$ sudo grep "kali" /etc/shadow
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
kali:$y$j9T$bhPPnes6TLXf5GU5iCb/n.$0B4bwr1DwncIIyNIWQBeyLat8xRGuY500N9JqqX8LE.:19651:0:99999:7:::
```

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

Command: `sudo useradd -m -d /home/zsumu001 zsumu001`

-m creates home directory, -d /home/zsumu001 explicitly ensures the home directory follows

```
(kali@kali)-[~]
└─$ sudo useradd -m -d /home/zsumu001 zsumu001
```

4. Set a password for the new user.

Command: `sudo passwd zsumu001`

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

Command: `usermod -s /bin/bash zsumu001`

`grep "^zsumu001:" /etc/passwd`

-s specifies the login shell for user

```
(kali@kali)-[~]
└─$ sudo passwd zsumu001
New password:
Retype new password:
passwd: password updated successfully

(kali@kali)-[~]
└─$ sudo usermod -s /bin/bash zsumu001

(kali@kali)-[~]
└─$ grep "^zsumu001:" /etc/passwd
zsumu001:x:1001:1001::/home/zsumu001:/bin/bash
```

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

Command: `sudo grep "^zsumu001:" /etc/shadow`

-/etc/shadow stores password hashes

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

Command: `sudo usermod -aG sudo zsumu001`

-a adds the user to group, -G without removing from other groups

8. Switch to the new user's account.

Command: `su - zsumu001`

- su - switch user

```
(kali@kali)-[~]
└─$ sudo grep "^zsumu001:" /etc/shadow
zsumu001:$y$j9T$Pd5YBwtEft.IWTQFIw5uw.$4iEjBy7JDqh9UW.Ps40vBLen5BA/LIkbU.u8217hbVB:20352:0:99999:7:::

(kali@kali)-[~]
└─$ sudo usermod -aG sudo zsumu001

(kali@kali)-[~]
└─$ su - zsumu001
Password:
(zsumu001@kali)-[~]
└─$
```

Task B – Group account management

Use Linux commands to execute the following tasks:

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

Command: `cd ~`

`echo $SHELL`

- `cd` changes current directory to home directory, `~` is a shortcut for home
- `echo $SHELL` shows default shell for user

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

Command: `id`

- displays uid, gid, and groups

3. Display the group membership of the root account.

Command: `groups root`

- lists all groups the root user belongs to

```
(zsumu001@kali)-[~]
└─$ cd ~

(zsumu001@kali)-[~]
└─$ echo $SHELL
/bin/bash

(zsumu001@kali)-[~]
└─$ id
uid=1001(zsumu001) gid=1001(zsumu001) groups=1001(zsumu001),27(sudo)

(zsumu001@kali)-[~]
└─$ groups root
root : root
```

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

Command: `ls -l /etc/group`

- shows the user owner and group owner as root

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

Command: `sudo groupadd -g 01058957 test`

- `-g xxxxxxxx` specifies the GID

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

Command: `grep "^test:" /etc/group`

- displays `test` as group name, `x` as password placeholder, and my UIN as the GID.

```
(zsumu001@kali)-[~]
└─$ ls -l /etc/group
-rw-r--r-- 1 root root 1308 Sep 21 14:56 /etc/group

(zsumu001@kali)-[~]
└─$ sudo groupadd -g 01058957 test
[sudo] password for zsumu001:

(zsumu001@kali)-[~]
└─$ grep "^test:" /etc/group
test:x:1058957:
```

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

Command: `sudo groupmod -n newtest test`

- `groupmod` modifies existing group, `-n` sets new group name,

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

Command: `sudo usermod -aG newtest zsumu001`

- `usermod` modifies user account, `-aG` adds user to group without overriding users other group memberships

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

Command: `touch ~/testfile`

`sudo chgrp newtest ~/testfile`

- `touch` creates files (`~`) in home directory, after `/` would be name of the file

- `chgrp` changes group ownership of file, `newtest` is the new group to assign, `~/testfile`

the file that is being changed

```
(zsumu001@kali)-[~]
└─$ sudo groupmod -n newtest test

(zsumu001@kali)-[~]
└─$ sudo usermod -aG newtest zsumu001

(zsumu001@kali)-[~]
└─$ touch ~/testfile

(zsumu001@kali)-[~]
└─$ sudo chgrp newtest ~/testfile
```

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

Command: `ls -l ~/testfile`

- `ls -l` lists files in long format, showing owner, group, size etc.

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

Command: `sudo groupdel newtest`

`ls -l ~/testfile`

- `groupdel newtest` deleted the newtest group

- The group owner does not exist so, `ls -l` displayed the former GID of newtest, it being

my UIN

```
(zsumu001@kali)-[~]
└─$ ls -l ~/testfile
-rw-r--r-- 1 zsumu001 newtest 0 Sep 21 15:05 /home/zsumu001/testfile

(zsumu001@kali)-[~]
└─$ sudo groupdel newtest

(zsumu001@kali)-[~]
└─$ ls -l ~/testfile
-rw-r--r-- 1 zsumu001 1058957 0 Sep 21 15:05 /home/zsumu001/testfile
```

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

Command: `sudo userdel -r -f zsumu001`

- `userdel` deletes a user account, `-r` removes the users home directory, `-f` force deletion, `zsumu001` being the user

-I verified the account was deleted by exiting and attempting to log in to the account

```
(zsumu001@kali)-[~]
└─$ sudo userdel -r -f zsumu001
userdel: user zsumu001 is currently used by process 42525
userdel: zsumu001 mail spool (/var/mail/zsumu001) not found

(zsumu001@kali)-[~]
└─$ exit
logout

(kali@kali)-[~]
└─$ su - zsumu001
su: user zsumu001 does not exist or the user entry does not contain all the required fields
```