1. Create a folder called myteam in your home directory and change its permissions to read only for the owner.

```
shaher@shaher-SATELLITE-C850-A786:~$ mkdir myteam
shaher@shaher-SATELLITE-C850-A786:~$ ls -l
total 44
drwxrwxr-x 6 shaher shaher 4096 Dec  4 21:05 01_Embedded_Linux
drwxr-xr-x 2 shaher shaher 4096 Nov 23 04:31 Desktop
drwxr-xr-x 2 shaher shaher 4096 Nov 23 04:53 Documents
drwxr-xr-x 2 shaher shaher 4096 Dec 21 08:03 Downloads
drwxr-xr-x 2 shaher shaher 4096 Nov 23 04:31 Music
drwxrwxr-x 2 shaher shaher 4096 Dec 21 21:48 myteam
drwxr-xr-x 3 shaher shaher 4096 Nov 23 04:56 Pictures
drwxr-xr-x 2 shaher shaher 4096 Nov 23 04:31 Public
drwx------ 5 shaher shaher 4096 Dec  1 05:19 snap
drwxr-xr-x 2 shaher shaher 4096 Nov 23 04:31 Templates
drwxr-xr-x 2 shaher shaher 4096 Nov 23 04:31 Videos
```

```
shaher@shaher-SATELLITE-C850-A786:~$ chmod u=r myteam
shaher@shaher-SATELLITE-C850-A786:~$ ls -l | grep myteam
dr--rwxr-x 2 shaher shaher 4096 Dec 21 21:48 myteam
shaher@shaher-SATELLITE-C850-A786:~$
```

2. Log out and log in by another user.

3. Try to access (by cd command) the folder (myteam).

```
shaher@shaher-SATELLITE-C850-A786:~$ su khaled
Password:
khaled@shaher-SATELLITE-C850-A786:/home/shaher$ cd /myteam
bash: cd: /myteam: No such file or directory
khaled@shaher-SATELLITE-C850-A786:/home/shaher$ ls
ls: cannot open directory '.': Permission denied
khaled@shaher-SATELLITE-C850-A786:/home/shaher$ cd ./myteam
bash: cd: ./myteam: Permission denied
khaled@shaher-SATELLITE-C850-A786:/home/shaher$
```

4. Using the command Line

a. Change the permissions of oldpasswd file to give owner read and write permissions and for group write and execute and execute only for the others (using chmod in 2 different ways).

```
shaher@shaher-SATELLITE-C850-A786:~$ ls
01_Embedded_Linux  Documents  Music    Pictures  snap       Videos
Desktop            Downloads  myteam   Public    Templates
shaher@shaher-SATELLITE-C850-A786:~$ touch oldpasswd
shaher@shaher-SATELLITE-C850-A786:~$ ls -l | grep oldpasswd
-rw-rw-r-- 1 shaher shaher    0 22:32 21 س oldpasswd
shaher@shaher-SATELLITE-C850-A786:~$ chmod u=rw,g=wx,o=x oldpasswd
shaher@shaher-SATELLITE-C850-A786:~$ ls -l | grep oldpasswd
-rw--wx--x 1 shaher shaher    0 22:32 21 س oldpasswd
shaher@shaher-SATELLITE-C850-A786:~$ chmod u=rw,g=rw,o=r oldpasswd
shaher@shaher-SATELLITE-C850-A786:~$ ls -l | grep oldpasswd
-rw-rw-r-- 1 shaher shaher    0 22:32 21 س oldpasswd
shaher@shaher-SATELLITE-C850-A786:~$ chmod 631  oldpasswd
shaher@shaher-SATELLITE-C850-A786:~$ ls -l | grep oldpasswd
-rw--wx--x 1 shaher shaher    0 22:32 21 س oldpasswd
shaher@shaher-SATELLITE-C850-A786:~$
```

b. Change your default permissions to be as above.

you cannot set these permissions to be the default in case of the files, you cannot make them to be executable by default, but you can do so for the directories.

c. What is the maximum permission a file can have, by default when it is just created? And what is that for directory.

For a file, it can have maximum default permissions as rw_- rw_ - rw_, in other words: (666).

For a directory, it can have maximum default permissions as rwx – rwx – rwx, in other words: (777).

d. Change your default permissions to be no permission to everyone then create a directory and a file to verify.

```
shaher@shaher-SATELLITE-C850-A786:~$ umask
0002
shaher@shaher-SATELLITE-C850-A786:~$ umask 0777
shaher@shaher-SATELLITE-C850-A786:~$ umask
0777
shaher@shaher-SATELLITE-C850-A786:~$ touch testfile
shaher@shaher-SATELLITE-C850-A786:~$ mkdir testdir
shaher@shaher-SATELLITE-C850-A786:~$ ls -l | grep test
d--------- 2 shaher shaher 4096 22:45 21 س testdir
---------- 1 shaher shaher    0 22:45 21 س testfile
shaher@shaher-SATELLITE-C850-A786:~$ umask 0002
shaher@shaher-SATELLITE-C850-A786:~$ umask
0002
```

e. State who can access this file if any with proof.

The root and any user inside the sudo group.

5. Create a file with permission 444. Try to edit in it and to remove it? Note what happened.

```
shaher@shaher-SATELLITE-C850-A786:~$ touch testfile
shaher@shaher-SATELLITE-C850-A786:~$ chmod 444 testfile
shaher@shaher-SATELLITE-C850-A786:~$ ls -l | grep testfile
-r--r--r-- 1 shaher shaher    0 22:51 21 س testfile
shaher@shaher-SATELLITE-C850-A786:~$ vi testfile
```

As we can see, there is a warning that this file is a read only file.

```
~
~
~
"testfile" [readonly] 0 lines, 0 bytes
```

Also, when deleting it, it is mentioned that it is protected, (me4 awy ya3ny ☹).

```
shaher@shaher-SATELLITE-C850-A786:~$ rm testfile
rm: remove write-protected regular empty file 'testfile'?
```

6. What is the difference between the “x” permission for a file and for a directory?

For files, it allows the user to execute the file if it is executable.

For directories, it allows the user to access and navigate that directory.

But I think for both files and directories they must have read permission too to be able to get the benefit of “x” permission.

PART 2:

1. Set the sticky bit on the newly created directory.

chmod o+t testdir

2. set the setgui bit on the created directory

chmod g+s testdir

3. Create multiple user accounts.

sudo useradd user1
sudo useradd user2
.
.
.

4. Allow these users to create files within the directory and directory.

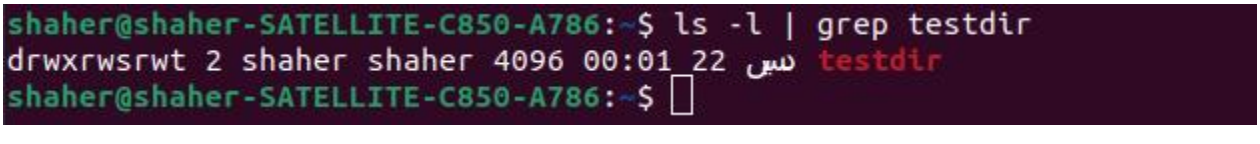
chmod o=rwxt testdir

5. Attempt to delete or rename each other's files.

6. Provide a clear output demonstrating the impact of the sticky bit on file deletion and renaming within the directory.

They can not delete each other' files because of the effect of the sticky bit on all files inside that directory, they are all protected from any user except the one who created it.

7. Provide a clear output for the directory created.



List the permission passwd command has and explain why it has S

```
shaher@shaher-SATELLITE-C850-A786:/bin$ ls -l | grep passwd
-rwsr-xr-x 1 root root     72072 2022  24 نف gpasswd
-rwxr-xr-x 1 root root    262352 2022  18 سي grub-mkpasswd-pbkdf2
-rwsr-xr-x 1 root root     59976 2022  24 نف passwd
shaher@shaher-SATELLITE-C850-A786:/bin$
```

It allows the user the ability to change his own password without giving it any unnecessary privileges for other system operations.