Linux File Permissions Task 2

**1. Create a folder called myteam and change its permissions to read-only for the owner:**

```bash

mkdir myteam

chmod u=r myteam

```



**2. Change the permissions of mycv 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)**  
```bash  
chmod 664 mycv # Using octal notation

chmod u=rw,g=wx,o=x mycv # Using symbolic notation  
```

**3. Maximum permission a file and a directory can have, by default when it is just created:**

The default permissions for a newly created file are 666 (read and write for owner, group, and others). The default permissions for a newly created directory are 777 (read, write, and execute for owner, group, and others), unless modified by the umask.

**4. Change your default permissions to be no permission to everyone:**

```bash

umask 0777

```

**5. Minimum permissions needed for various operations:**

- Copy a directory (source and target): rwx (read, write, execute) for both source and target directories.

- Copy a file (source and target): r (read) for the source file, rw (read and write) for the target directory.

- Delete a file: w (write) for the file.

- Change to a directory: x (execute) for the directory.

- List a directory content: r (read) for the directory.

- View a file content: r (read) for the file.

- Modify a file content: rw (read and write) for the file.

**6. Create a file with permission 444 and try to edit and remove it:**  
```bash  
touch myfile

chmod 444 myfile  
```

- You will not be able to edit or remove the file due to the lack of write permissions.

**7. Difference between "x" permission for a file and for a directory:**

- For a file: x allows execution of the file as a program.

- For a directory: x allows you to enter the directory, list its contents, and execute files within it.

**8. Create a directory with set-GID permission:**

mkdir setgiddir

chmod 775 setgiddir.