Task 1. Check file and directory details

In this task, you must explore the permissions of the `projects` directory and the files it contains. The lab starts with `/home/researcher2` as the current working directory. This is because you're changing permissions for files and directories belonging to the `researcher2` user.

1. Navigate to the `projects` directory.

The command to complete this step:

```
cd projects
```

2. List the contents and permissions of the `projects` directory.

The command to complete this step:

```
ls -l
```

The permissions of the files in the `projects` directory are as follows:

```
total 20
```

```
drwx--x--- 2 researcher2 research_team 4096 Oct 14 18:40 drafts
```

```
-rw-rw-rw- 1 researcher2 research_team   46 Oct 14 18:40 project_k.txt
```

```
-rw-r----- 1 researcher2 research_team  46 Oct 14 18:40 project_m.txt
```

```
-rw-rw-r-- 1 researcher2 research_team  46 Oct 14 18:40 project_r.txt
```

```
-rw-rw-r-- 1 researcher2 research_team  46 Oct 14 18:40 pro
```

Note: *The date and time information returned is the same as the date and time when you ran the command. Therefore, it is different from the date and time in the example.*

As you may recall from the video lesson, a 10-character string begins each entry and indicates how the permissions on the file are set. For instance, a directory with full permissions for all owner types would be `drwxrwxrwx`:

- The 1st character indicates the file type. The `d` indicates it's a directory. When this character is a hyphen (`-`), it's a regular file.
- The 2nd-4th characters indicate the read (`r`), write (`w`), and execute (`x`) permissions for the user. When one of these characters is a hyphen (`-`) instead, it indicates that this permission is not granted to the user.
- The 5th-7th characters indicate the read (`r`), write (`w`), and execute (`x`) permissions for the group. When one of these characters is a hyphen (`-`) instead, it indicates that this permission is not granted for the group.
- The 8th-10th characters indicate the read (`r`), write (`w`), and execute (`x`) permissions for the owner type of other. This owner type consists of all other users on the system apart from the user and the group. When one of these characters is a hyphen (`-`) instead, that indicates that this permission is not granted for other.

The second block of text in the expanded directory listing is the user who owns the file. The third block of text is the group owner of the file.

Task 2. Change file permissions

In this task, you must determine whether any files have incorrect permissions and then change the permissions as needed. This action will remove unauthorized access and strengthen security on the system.

None of the files should allow the other users to write to files.

1. Check whether any files in the `projects` directory have write permissions for the owner type of other.

The command to complete this step:

```
ls -l
```

2. Change the permissions of the file identified in the previous step so that the owner type of other doesn't have write permissions.

   ```
   chmod o-w project_k.txt
   ```

   Note: *Permissions are granted for three different types of owners, namely user, group, and other.*

In the `chmod` command, `u` sets the permissions for the user who owns the file, `g` sets the permissions for the group that owns the file, and `o` sets the permissions for others.

3. The file `project_m.txt` is a restricted file and should not be readable or writable by the group or other; only the user should have these permissions on this file. List the contents and permissions of the current directory and check if the group has read or write permissions.

The command to complete this step:

```
ls -l
```

4. Use the `chmod` command to change permissions of the `project_m.txt` file so that the group doesn't have read or write permissions.

The command to complete this step:

```
chmod g-r project_m.txt
```

Task 3. Change file permissions on a hidden file

In this task, you must determine if a hidden file has incorrect permissions and then change the permissions as needed. This action will further remove unauthorized access and strengthen security on the system.

The file `.project_x.txt` is a hidden file that has been archived and should not be written to by anyone. (The user and group should still be able to read this file.)

1. Check the permissions of the hidden file `.project_x.txt` and answer the question that follows.

The command to complete this step:

```
ls -la
```

2. Change the permissions of the file `.project_x.txt` so that both the user and the group can read, but not write to, the file.

Note: *Be sure to start the name of a hidden file with a period (`.`).*

The command to complete this step:

```
chmod u-w,g-w,g+r .project_x.txt
```

Task 4. Change directory permissions

In this task, you must change the permissions of a directory. First, you'll check the group permissions of the `/home/researcher2/projects/drafts` directory and then modify the permissions as required. (You should be in the `projects` directory while managing the permissions of its subdirectory `drafts`.)

Only the `researcher2` user should be allowed to access the `drafts` directory and its contents. (This means that only `researcher2` should have execute privileges.)

1. Check the permissions of the `drafts` directory and answer the following question.

The command to complete this step:

```
ls -l
```

2. Remove the execute permission for the group from the `drafts` directory.

The command to complete this step:

```
chmod g-x drafts
```