Linux File Permissions

Project Description

This project is part of the Google Cybersecurity Certificate. I take the role of a security professional working with a large organization's research team. To protect the security of projects, I manage file system authorization, in terms of ownership and permissions, to prevent unauthorised access but grant access to authorised users. To do this I ensure all files/folders, including hidden ones, have the correct owner and permissions assigned.

Linux File Permissions

In Linux, 1 is the permission to execute, 2 is the permission to write, and 4 is the permission to read. The numbers are added when multiple permissions are granted, for example a file has permission number 7 if a user is allowed to read, write and execute it. The permissions numbering system assigns three numbers to a file/folder, describing permissions granted to the user, to the group and to others outside the group respectively. For example a file has permission number 742 if the user can read, write and execute it; the group can only read it; and others outside the group can only write to it.

Both read and execute permissions are required for a directory in order to read the contents of files and folders inside it. Granting a directory permission 4 (ie: read access without execute or write access) leads to being able to list the files and folders inside it, but being unable to access the data in the files and unable to view the contents of folders inside it. Execute permissions on a directory are also required to change the permissions of files in that directory. Granting a directory permission 1 (ie: execute access without read or write access) leads to not being able to open the folder, or lists the files or folders inside it.

Execute permissions are not required to read the contents of a file. A file with permission 4 (ie: read access without execute or write access) can be read from. A file with permission 2 (ie: write access without execute or read access) can be written to but not read from.

1. Check File and Directory Details

```
researcher2@836ecc8cc3ec:~/projects$ ls
drafts          project_m.txt  project_t.txt
project_k.txt  project_r.txt
researcher2@836ecc8cc3ec:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Nov 21 07:02 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Nov 21 07:02 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Nov 21 07:02 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 21 07:02 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 21 07:02 project_t.txt
```

The ls command is used to list files and directories. The -l flag lists the assigned permissions.

The permissions are described by a 10 character string. The first character is ‘d’ if the item is a folder or ‘-‘ if the item is a file. The remaining string comprises of 3 consecutive sets of 3 characters: ‘r’, ‘w’, ‘x’ is present if read, write and execute permissions are granted respectively. A ‘-‘ in place of ‘r’, ‘w’, or ‘x’ represents that the respective permission is withheld. The 3 consecutive sets of 3 characters describe the read, write and execute permissions given to the user, the group and other users outside the group respectively.

```
researcher2@9a4d2744e91a:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov 22 05:40 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov 22 05:46 ..
-rw--w---- 1 researcher2 research_team   46 Nov 22 05:40 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Nov 22 05:40 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Nov 22 05:40 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Nov 22 05:40 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 05:40 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 05:40 project_t.txt
```

Hidden files and folders become visible when the -a flag is used. The screenshot above shows the hidden file .project_x.txt, which is hidden by default due to the dot in the front of the filename.

2. Change File Permissions

```
researcher2@7d8be59666ce:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov 22 04:38 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov 22 05:58 ..
-rw--w---- 1 researcher2 research_team   46 Nov 22 04:38 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Nov 22 04:38 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Nov 22 04:38 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Nov 22 04:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 04:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 04:38 project_t.txt
researcher2@7d8be59666ce:~/projects$ chmod o-w project_k.txt
researcher2@7d8be59666ce:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov 22 04:38 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov 22 05:58 ..
-rw--w---- 1 researcher2 research_team   46 Nov 22 04:38 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Nov 22 04:38 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 04:38 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Nov 22 04:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 04:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 04:38 project_t.txt
researcher2@7d8be59666ce:~/projects$
```

chmod o-w removes write permissions for others outside the group.

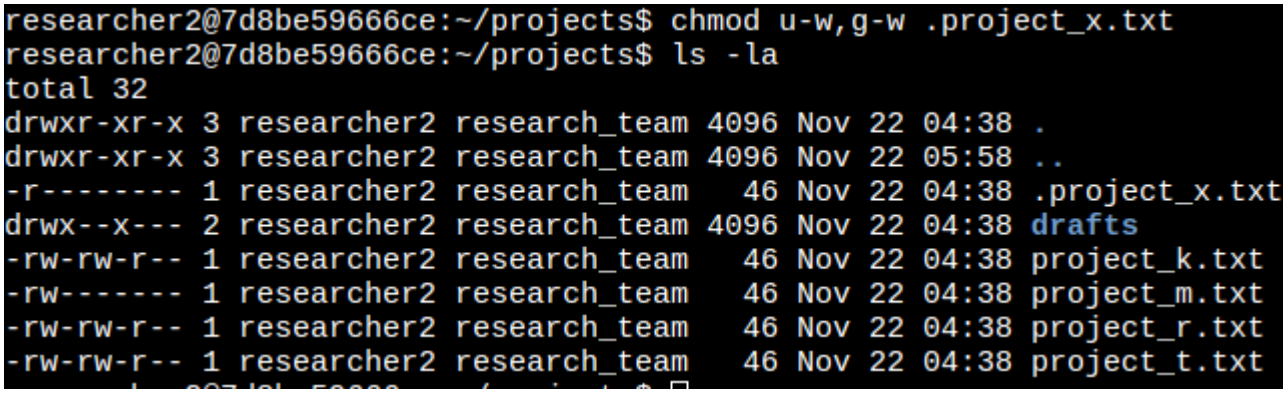
Project_m.txt is a restricted file, and group and other users outside the group should not have read access to it.

```
researcher2@7d8be59666ce:~/projects$ chmod g-r project_m.txt
researcher2@7d8be59666ce:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov 22 04:38 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov 22 05:58 ..
-rw--w---- 1 researcher2 research_team   46 Nov 22 04:38 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Nov 22 04:38 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 04:38 project_k.txt
-rw------- 1 researcher2 research_team   46 Nov 22 04:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 04:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov 22 04:38 project_t.txt
```

The chmod g-r project_m.txt command removes read privileges for the group users for project_m.txt.

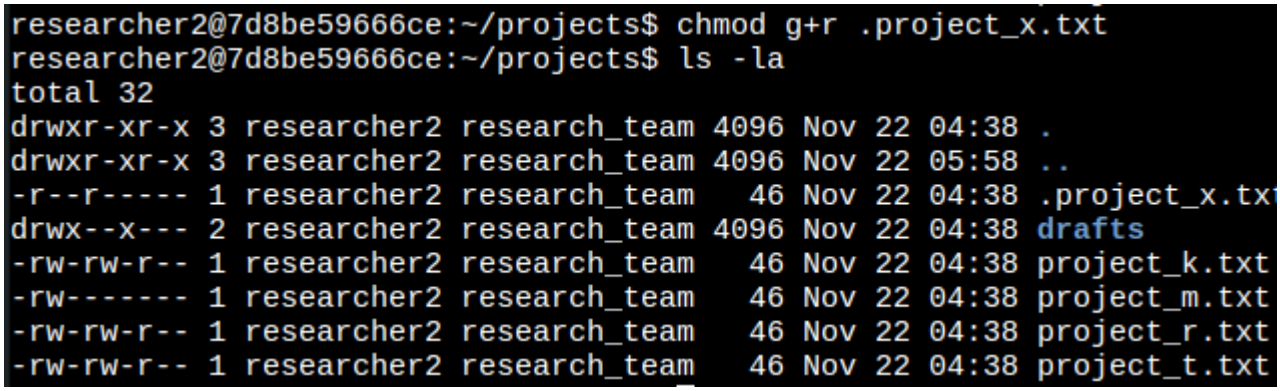
3. Change File Permissions on a Hidden File

Project X has been archived and should not be writable by anyone.



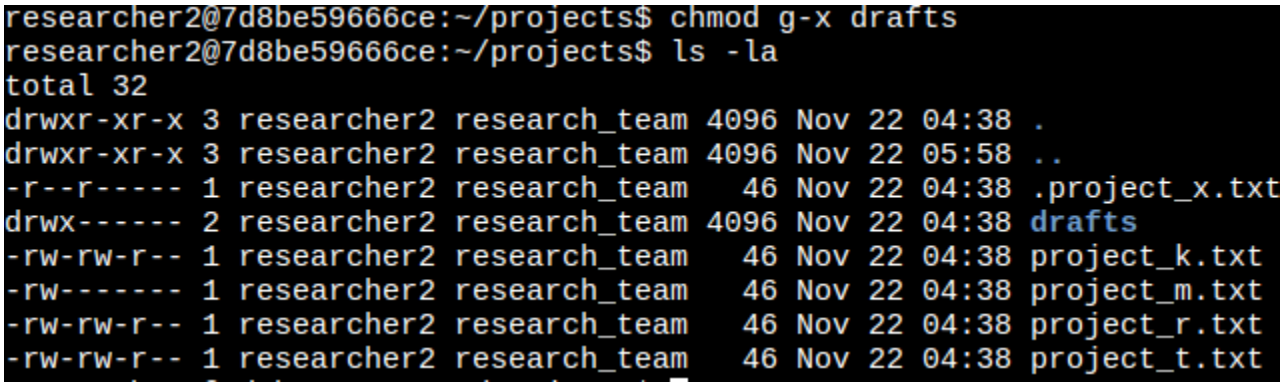
The chmod u-w,g-w .project_x.txt command removes write privileges for the user and the group for .project_x.txt.

The group should have read access to project X.



The chmod g+r .project_x.txt adds read access for the group to .project_x.txt.

4. Change Directory Permissions



The group should not have execute permissions on the drafts directory. The chmod g-x drafts command removes execute privileges for the group for the drafts directory. This is because only the researcher2 user should have access to the drafts directory.

Summary

In this lab I learned how to examine and change file and directory permissions. This is important for controlling authorizations to maintain the security of projects in the organization.