# File permissions in Linux

## Project description

This project is part of the training course by Google for cybersecurity professionals. As an integral part of this course we learn how the file permissions work and how to amend them. This document is created by me to demonstrate skills and knowledge that we acquired during the course.

## Check file and directory details

For checking the file and directory details we use the following command within Linux:

ls -la

The first part of the command “ls” is the list command, which gives an output of the files and subdirectories of the current directory.

The second part of the command “-la” consists of 2 arguments “-l” “-a” that can be used for the ls command. The first argument “-l” shows the permissions of the items in the output of the “ls” command and the second “-a” makes sure that all files and subdirectories are displayed (also hidden files). An example of an output for the “ls -la” command is:

drwxr-xr-x 3 researcher2 research\_team 4096 Oct 6 08:54 projects

Below I will describe the output in more detail

## Describe the permissions string

The first part of the output shown above is what is called the permission string. This consists of 4 parts: [1]d [2]rwx [3]r-x [4]r-x. The first part indicates whether this is a directory, if this contains a “d” it is a directory, if it contains a “-” it is a file (thus in this example it concerns a directory). Then the other 3 parts are concerning the permissions for the file or directory, part 2 concerns the permissions of the user or owner of the file, when a file or directory is created by the user it automatically assigns the user as its owner. Part 3 concerns the user group, which can be multiple users at the same time. Creating user groups can be useful when there are multiple persons using the system at the same time. Part 4 concerns all other users in the system. There are 3 types of permissions that can be granted, r = read (allows the user to read the file or directory) w = write (allows the user to write the file or directory) and x = execute (allows the user to execute the file or directory). Lastly a “-” is used when the user or user group does not have a permission to read write or execute the file or directory. Next to the permission string you can see the user, and user group that is concerning the permissions, the number of files within the directory, the amount of bytes the file or directory has and the time of creation.

In my example:

drwxr-xr-x 3 researcher2 research\_team 4096 Oct 6 08:54 projects

The output shows the directory projects consists of 3 files which are 4096 kb in total and was created October 6 at 08:54 am. The user/owner “researcher2” has all permissions (thus read write and execute) the user group “reseach\_team” has read and execute permissions, and all other users also have read and execute permissions for the folder.

## Change file permissions

To change the file permissions the command “chmod” can be used to change the permissions of a file. This command can change the permission per category (user, usergroup or other user) by using the “u” “g” “o” argument and the permission you would like to add (+) or remove (-). For example, if we want to change the permissions for the user group and other users so they cannot execute the file we can use “ chmod g-x,o-x projects” (where projects , note that the permissions statements are separated by a comma.

N.B. It is also possible to use numeric codes to change the permissions for files and directories, for this use the following values:

0 = no permissions

1 = execute

2 = write

4 = read

If more than one type of permission is acquired then you can add those values together, eg. all permissions is 7 or only read and write permissions is 6. With the command you can give a numeric value for every individual permission category. Thus for instance “chmod 777 projects” will give all permissions to every user.

## Change file permissions on a hidden file

Similar to “normal” files it is also possible to change the permissions for hidden files.

As mentioned above the hidden files and directories are shown using the ls -a command. Hidden files in linux are displayed with a dot “.” in front of the name for instance “.projects”.

To change the permissions you can use the same method, the only difference is that the dot “.” in front of the filename should be included in the command.