File permissions in Linux

Project description

Linux will be used to ensure users on the team are authorized with the appropriate permissions. Existing permissions will be examined to determine if they match the authorization that should be given. If they do not match, permissions will need to be modified to authorize the appropriate users and remove any unauthorized access.

Check file and directory details

To check permissions in the **projects** subdirectory type the command **ls -la** to display permissions of all files including any hidden files. Current permissions are:

- project_k.txt
  - -rw-rw-rw-
- project_m.txt
  - -rw-r- - - -
- project_r.txt
  - -rw-rw-r- -
- project_t.txt
  - -rw-rw-r- -
- .project_x.txt
  - -rw- - w- - - -

Describe the permissions string

The 10 character string displayed under each file corresponds to the level of access for user, group, and other.
1st character: This character is either a d or hyphen (-) and indicates the file type. If it's a d, it's a directory. If it's a hyphen (-), it's a regular file.
2nd-4th characters: These characters indicate the read (r), write (w), and execute (x) permissions for the user. For example in the project_k.txt file, the user has read and write permissions but not execute permissions. This is shown as [rw-].
5th - 7th characters: These characters indicate the read (r), write (w), and execute (x) permissions for the group. A hyphen (-) for one of these characters means that permission is not granted.

8th - 10th characters: These characters indicate permissions for other users on the system excluding the user and group.

Change file permissions

Currently, the organization does not allow other to have write access to any files. To change permissions for other, type the command chmod o+w followed by the name of the file to grant write permissions. For example, to grant other write permissions for the file project_k.txt, type **chmod o+w project_k.txt**.

Change file permissions on a hidden file

The research team has archived **.project_x.txt**, which is a hidden file. This file should not have write permissions for anyone, but the user and group should be able to read the file. To correct this type the commands:
chmod u-w .project_x.txt
chmod g-w .project_x.txt
chmod g+r .project_x.txt

Afterwards, type the command **ls -la** to ensure that the correct file permission changes were made to the hidden file.

Change directory permissions

Only **researcher2** should be allowed to access the **drafts** directory and its contents. This means that permissions for group and other need to be removed within this directory. Current file permissions are: **drwx- - x - - -**
To do this type **chmod g-x drafts** to remove execute permissions for group. Then, check your work by typing the command **ls -la**.

Summary

Using the Linux operating system, existing permissions were examined to ensure that correct authorizations were given. Multiple permission changes were made to match the level of authorization my organization wanted for files and directories in the **projects** directory.