

File permissions in Linux

Project description

In this lab activity, I will utilize Linux commands to configure authorization, a crucial concept involving granting access to specific system resources. Authorization is vital for preventing unauthorized access and modification of files, reducing potential security risks. Exploring file and directory permissions in Linux, I will focus on changing ownership to restrict access, a key responsibility for a security analyst in safeguarding sensitive information and ensuring overall system security.

Check file and directory details

I use the following commands to navigate through files and directories:

- `cd` is use to change directory. Example `cd projects`
- `ls -la` is use to list all content, permission, and hiding files of a directors. `ls` command list all contents, `-la` is a combination of two commands which mean `-l` list all permissions of a file and `-a` list all hiding files projects. Example on the project directory, `ls -la` is use.

Describe the permissions string

In the `/home/researcher2/projects` directory, there are five files in chich one is a hiding file and there is also a single directory. Below are the files and directory with there current permissions:

- `.project_x.txt`
 - User = Read and Write
 - Group = Write only
 - Other = None
- `project_m.txt`
 - User = Read and Write
 - Group = Read only
 - Other = None
- `project_k.txt`
 - User = Read and Write
 - Group = Read and Write

- Other = Read and Write
- project_r.txt
 - User = Read and write
 - Group = Read and Write
 - Other = read only
- project_t.txt
 - User = Read and Write
 - Group = Read and Write
 - Other = Read only

The directory permissions

- drafts
 - User = Read, Write and execute
 - Group = Execute only
 - Other = None

```
researcher2@66402bdf13f6:~$ cd projects
researcher2@66402bdf13f6:~/projects$ ls
drafts project_k.txt project_m.txt project_r.txt project_t.txt
researcher2@66402bdf13f6:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 21:50 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 ..
-rw--w--- 1 researcher2 research_team  46 Jan 11 21:50 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan 11 21:50 drafts
-rw-rw-rw- 1 researcher2 research_team  46 Jan 11 21:50 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Jan 11 21:50 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 21:50 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 21:50 project_t.txt
researcher2@66402bdf13f6:~/projects$
```

Change file permissions

In the current permissions, the `project_k.txt` file permissions were wrongly used. The Other users should not be permitted to write to any file according to the least privilege policy.

I used this command to change the permissions `chmod o-w project_k.txt` and the `ls -la` to check if changes is successful.

```

researcher2@6b87864648fd:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 23:09 ..
-rw--w---- 1 researcher2 research_team  46 Jan 11 22:08 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan 11 22:08 drafts
-rw-rw-rw- 1 researcher2 research_team  46 Jan 11 22:08 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Jan 11 22:08 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_t.txt
researcher2@6b87864648fd:~/projects$ chmod o-w project_k.txt
researcher2@6b87864648fd:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 23:09 ..
-rw--w---- 1 researcher2 research_team  46 Jan 11 22:08 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan 11 22:08 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Jan 11 22:08 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_t.txt
researcher2@6b87864648fd:~/projects$ █

```

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 as specified in the least privilege policy. I used this command to change the permissions `chmod g-r project_m.txt` and the `ls -la` to check if changes is successful.

```

researcher2@6b87864648fd:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 23:09 ..
-rw--w---- 1 researcher2 research_team  46 Jan 11 22:08 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan 11 22:08 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Jan 11 22:08 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_t.txt
researcher2@6b87864648fd:~/projects$ chmod g-r project_m.txt
researcher2@6b87864648fd:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 23:09 ..
-rw--w---- 1 researcher2 research_team  46 Jan 11 22:08 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan 11 22:08 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_k.txt
-rw----- 1 researcher2 research_team  46 Jan 11 22:08 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_t.txt
researcher2@6b87864648fd:~/projects$ █

```

In Linux, permissions are represented with a 10-character string. Permissions include:

- **read:** for files, this is the ability to read the file contents; for directories, this is the ability to read all contents in the directory including both files and subdirectories
- **write:** for files, this is the ability to make modifications on the file contents; for directories, this is the ability to create new files in the directory
- **execute:** for files, this is the ability to execute the file if it's a program; for directories, this is the ability to enter the directory and access its files

These permissions are given to these types of owners:

- **user:** the owner of the file
- **group:** a larger group that the owner is a part of
- **other:** all other users on the system

Each character in the 10-character string conveys different information about these permissions. The following table describes the purpose of each character:

Character	Example	Meaning
1st	drwxrwxrwx	file type <ul style="list-style-type: none"> ● d for directory ● - for a regular file

2nd	drwxrwxrwx	read permissions for the user <ul style="list-style-type: none"> • r if the user has read permissions • - if the user lacks read permissions
3rd	dr w xrwxrwx	write permissions for the user <ul style="list-style-type: none"> • w if the user has write permissions • - if the user lacks write permissions
4th	drwx r wxrx	execute permissions for the user <ul style="list-style-type: none"> • x if the user has execute permissions • - if the user lacks execute permissions
5th	drwxrwxrwx	read permissions for the group <ul style="list-style-type: none"> • r if the group has read permissions • - if the group lacks read permissions
6th	drwxr w xrwx	write permissions for the group <ul style="list-style-type: none"> • w if the group has write permissions • - if the group lacks write permissions
7th	drwxrwx x rx	execute permissions for the group <ul style="list-style-type: none"> • x if the group has execute permissions • - if the group lacks execute permissions
8th	drwxrwxrwx	read permissions for other <ul style="list-style-type: none"> • r if the other owner type has read permissions • - if the other owner type lacks read permissions

- | | | | |
|------|------------|-------------------------------|---|
| 9th | drwxrwxrwx | write permissions for other | <ul style="list-style-type: none">• w if the other owner type has write permissions• - if the other owner type lacks write permissions |
| 10th | drwxrwxrwx | execute permissions for other | <ul style="list-style-type: none">• x if the other owner type has execute permissions• - if the other owner type lacks execute permissions |

Change file permissions on a hidden file

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.). I used this command to change the permissions `chmod u-w,g-w,g+r .project_x.txt` and the `ls -la` to check if changes is successful.

```
researcher2@6b87864648fd:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 23:09 ..
-rw--w---- 1 researcher2 research_team  46 Jan 11 22:08 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan 11 22:08 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_k.txt
-rw----- 1 researcher2 research_team  46 Jan 11 22:08 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_t.txt
researcher2@6b87864648fd:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@6b87864648fd:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 23:09 ..
-r--r----- 1 researcher2 research_team  46 Jan 11 22:08 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan 11 22:08 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_k.txt
-rw----- 1 researcher2 research_team  46 Jan 11 22:08 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_t.txt
researcher2@6b87864648fd:~/projects$
```

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.

Change directory permissions

Only the `researcher2` user should be allowed to access the `drafts` directory and its contents. (This means that only `researcher2` should have execute privileges.). I used this command to change the permissions `chmod g-x drafts` and the `ls -la` to check if changes is successful.

```
researcher2@6b87864648fd:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 23:09 ..
-r--r----- 1 researcher2 research_team  46 Jan 11 22:08 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan 11 22:08 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_k.txt
-rw----- 1 researcher2 research_team  46 Jan 11 22:08 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_t.txt
researcher2@6b87864648fd:~/projects$ chmod g-x drafts
researcher2@6b87864648fd:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 22:08 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan 11 23:09 ..
-r--r----- 1 researcher2 research_team  46 Jan 11 22:08 .project_x.txt
drwx----- 2 researcher2 research_team 4096 Jan 11 22:08 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_k.txt
-rw----- 1 researcher2 research_team  46 Jan 11 22:08 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan 11 22:08 project_t.txt
researcher2@6b87864648fd:~/projects$
```

Summary

In this Linux file permissions lab, the focus is on configuring authorization to prevent unauthorized access to system resources. Utilizing commands like `'cd'` and `'ls -la'`, the permissions of files and directories, such as `project_k.txt` and `drafts`, are examined. Corrections are made to align with the least privilege policy, addressing inaccuracies in file permissions through `'chmod'` commands. The concept of permissions,

encompassing read, write, and execute for user, group, and others, is elucidated. Additionally, adjustments are made to a hidden file, `.project_x.txt`, ensuring restricted writing while permitting reading. The final step involves modifying directory permissions, allowing exclusive execution access for the `researcher2` user in the `drafts` directory. Overall, the lab underscores the significance of understanding and managing permissions in Linux for enhanced system security and adherence to the least privilege principle.