File permissions in Linux

Project description

I am a security professional at a large organization, working mainly with their research team. Part of my job is to ensure users on this team are authorized with the appropriate permissions to help keep the system secure.

My task is to use the concept of Least Privilege to examine existing permissions on the file system and determine if the permissions match the authorization they should be given, modifying permissions when needed.

Check file and directory details



ls -l will show all permissions for the directory and files.

Describe the permissions string

The permission string of the drafts directory shows that the "user", researcher2, has read, write, and execute permissions, the "group", research\_team, has execute permissions, and there are no permissions for "other".

Read (r) permissions allow the user/group/other to read all files on the drafts directory

Write (w) permissions allow the user/group/other to create new files and update exsisting files in the directory

Execute (x) permissions allow the user/group/other to enter into the directory and access the files and allows files to be executed if the file is an executable.

Hyphen (-) shows no permission given.

In the first character, d stands for directory, - stands for file.

in the **2nd-4th** characters are permissions for the "**user"**, the owner of the file/directory

in the **5th-7th** characters are permissions for the "**group"**, a group of users, usually in a team or department.

in the **8th-10th** characters are permissions for the "**other"**, which are any other users on the system.

Change file permissions



In the project\_k.txt file, "other" should not have write permissions. Using chmod, I revoked the write permissions to the "other". I then used ls -l to verify that the change has been made.

Change file permissions on a hidden file



The research team has archived .project\_x.txt, which is why it is a hidden file. This file should not have write permissions for anyone, however the "user" and "group" should be able to read the file. Using chmod u=r, g=r .project\_x.txt, I replaced permissions to the "user" and "group" from read and write to read only. To verify the changes on the hidden file, I used the -la option for the ls command.

Change directory permissions



The files and directories in the projects directory belong to the researcher2 user. Only this "user" should be allowed to access the drafts directory and its contents. Using chmod g=- drafts, I revoked all permissions for the research\_team. Using chmod u-w drafts, I removed the "user" permission to write, while keeping permissions to read and execute.

Summary

Using these commands, I am able to make changes to permissions to help keep the organization more secure. Using chmod with the appropriate arguments, and ls with the correct options, I can efficiently work through LinuxOS to keep sensitive information in the hands of only those who need it.