File permissions in Linux

Project description

Linux commands allow cybersecurity professionals to accomplish many security tasks. In this specific task, we will increase an organizations security posture by adding and removing permissions within the organization. Data should be on a need-to-know basis and that is what we will be implementing.

Check file and directory details

To check for permissions for files and directories in linux (including hidden files), use this command:

ls -al

This command should output the following:

```
researcher2@d3bf557fd6e7:~$ pwd
/home/researcher2
researcher2@d3bf557fd6e7:~$ ls
projects
researcher2@d3bf557fd6e7:~$ cd projects
researcher2@d3bf557fd6e7:~/projects$ ls
drafts  project_k.txt  project_m.txt  project_r.txt  project_t.txt
researcher2@d3bf557fd6e7:~/projects$ ls -al
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jul 19 22:57 .
drwxr-xr-x 3 researcher2 research_team 4096 Jul 19 23:51 ..
-rw--w---- 1 researcher2 research_team   46 Jul 19 22:57 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jul 19 22:57 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Jul 19 22:57 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 19 22:57 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 19 22:57 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 19 22:57 project_t.txt
researcher2@d3bf557fd6e7:~/projects$
```

Describe the permissions string

Notice the first 10 characters in each line. The first character represents the data either being a file or directory. The second, third, and forth characters represent the USER's read, write, and execute permissions in that order. The fifth, sixth, and seventh characters are the GROUP's permissions for read. write, and execute. Lastly, the eighth, ninth, and tenth characters are the OTHER's read, write, and execute permissions.

Change file permissions

Because the organization does not allow write permissions for OTHER, we must retract that permission from project_k.txt. In order to this type in the following command:

chmod o-w project_k.txt

After execution, the list of files and directories permissions should look like this:

```
researcher2@23fe6a0f8ac4:~$ pwd
/home/researcher2
researcher2@23fe6a0f8ac4:~$ ls
projects
researcher2@23fe6a0f8ac4:~$ cd projects
researcher2@23fe6a0f8ac4:~/projects$ chmod o-w project_k.txt
researcher2@23fe6a0f8ac4:~/projects$ ls -al
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jul 20 16:56 .
drwxr-xr-x 3 researcher2 research_team 4096 Jul 20 18:10 ..
-rw--w---- 1 researcher2 research_team   46 Jul 20 16:56 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jul 20 16:56 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jul 20 16:56 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jul 20 16:56 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 20 16:56 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jul 20 16:56 project_t.txt
researcher2@23fe6a0f8ac4:~/projects$
```

Change file permissions on a hidden file

Within the hidden file, user and group should have read permissions while nobody should have write permissions. In this case, we need to take away write permissions for both user and group with the following two commands:

chmod u-w .project_x.txt
chmod g-w .project_x.txt

Next we need to add read permission to group with the following command:

chmod g+r .project_x.txt

Once those commands are executed, the following should be the output for permissions within the hidden file.

```
researcher2@23fe6a0f8ac4:~/projects$ ls -al | grep .project_x.txt
-r--r----- 1 researcher2 research_team   46 Jul 20 16:56 .project_x.txt
```

Change directory permissions

researcher2 should be the only user with access to the projects directory and its contents from within. Therefore, we need to take away any permissions the group or other have with this directory. It seems the group has permissions to read the directory so we will use this command to take that permissions away:

chmod g-x drafts

The directory permissions should now look like the following:

```
researcher2@23fe6a0f8ac4:~/projects$ ls -al | grep drafts
drwx------ 2 researcher2 research_team 4096 Jul 20 16:56 drafts
```

Summary

We have successfully checked file and directory permissions and defined the 10-character string to decypher read, write, and execute permissions for user, group, and other. On top of that, we have changed file permissions for both hidden and regular files as well as a directory. This is important in the cybersecurity workforce because it adds another easy layer of security within the organization's network.