File permissions on Linux

Project description

In this project, I acted as a security professional responsible for auditing and updating file permissions within the /home/researcher2/projects directory. The goal was to ensure that the file system adheres to the organization's security authorization policies. This involved identifying unauthorized access privileges, such as write permissions for "others," and using Linux commands to secure specific files, hidden archives, and directories to maintain system integrity.

Check file and directory details

```
researcher2@eac58ec0a0ed:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 00:38 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 02:06 ..
-rw--w---- 1 researcher2 research_team   46 Dec  2 00:38 .proje
ct_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec  2 00:38 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Dec  2 00:38 projec
t_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 00:38 projec
t_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 projec
t_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 projec
t_t.txt
researcher2@eac58ec0a0ed:~/projects$
```

The 10-character string represents the file type and permissions for proyect_k.txt file.

- **1st character (-):** Indicates that this is a regular file (a d would indicate a directory).
- **Characters 2-4 (rw-):** Represent the User (owner) permissions. They have Read and Write access.
- **Characters 5-7 (rw-):** Represent the Group permissions. The group also has Read and Write access.
- **Characters 8-10 (r--):** Represent the Other permissions. They only have Read and Write access.

Change file permissions

Upon checking the existing permissions, I identified that project_k.txt had write permissions enabled for "other" users (-rw-rw-rw-). This violates the organization's policy.

```
researcher2@eac58ec0a0ed:~/projects$ chmod o-w project_k.txt
researcher2@eac58ec0a0ed:~/projects$ ls -ul
total 20
drwx--x--- 2 researcher2 research_team 4096 Dec  2 00:38 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 00:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_t.txt
researcher2@eac58ec0a0ed:~/projects$
```

This command removes the write permission for "others." The new permissions string for this file is -rw-rw-r--.

Change file permissions on a hidden file

The hidden file .project_x.txt was archived and required strict permissions. The policy states it should have no write permissions for anyone, but the user and group must be able to read it.

```
researcher2@eac58ec0a0ed:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 00:38 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 02:06 ..
-rw--w---- 1 researcher2 research_team   46 Dec  2 00:38 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec  2 00:38 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 00:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_t.txt
researcher2@eac58ec0a0ed:~/projects$ chmod u-w,g+r-w .project_x.txt
```

This updates the permissions to read-only for the user and group, and no permissions for others. The resulting string is -r--r-----.

```
researcher2@eac58ec0a0ed:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 00:38 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 02:06 ..
-r--r----- 1 researcher2 research_team   46 Dec  2 00:38 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec  2 00:38 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 00:38 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 00:38 project_t.txt
researcher2@eac58ec0a0ed:~/projects$
```

Change directory permissions

The drafts directory currently allows group access (drwx--x---). The requirement states that only the user researcher2 should access this directory and its contents.

```
researcher2@eac58ec0a0ed:~/projects/drafts$ ls -al
total 8
drwx--x--- 2 researcher2 research_team 4096 Dec  2 00:38 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 00:38 ..
researcher2@eac58ec0a0ed:~/projects/drafts$
```

This removes the execute permission from the group. Now, only the owner has access permissions (drwx------), ensuring privacy for the directory contents.

```
researcher2@eac58ec0a0ed:~/projects/drafts$ chmod g-x /home/researcher2/projects/drafts
researcher2@eac58ec0a0ed:~/projects/drafts$ ls -al
total 8
drwx------ 2 researcher2 research_team 4096 Dec  2 00:38 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 00:38 ..
```

Summary

I successfully audited the /home/researcher2/projects directory to align file permissions with security policies. Using the ls -la command, I identified files with excessive privileges. I then used the chmod command to restrict write access for others on public files, enforce read-only access on the hidden archive .project_x.txt, and lock down the drafts directory so that only the owner can access it. These actions reduced the risk of unauthorized modification or access to sensitive data.