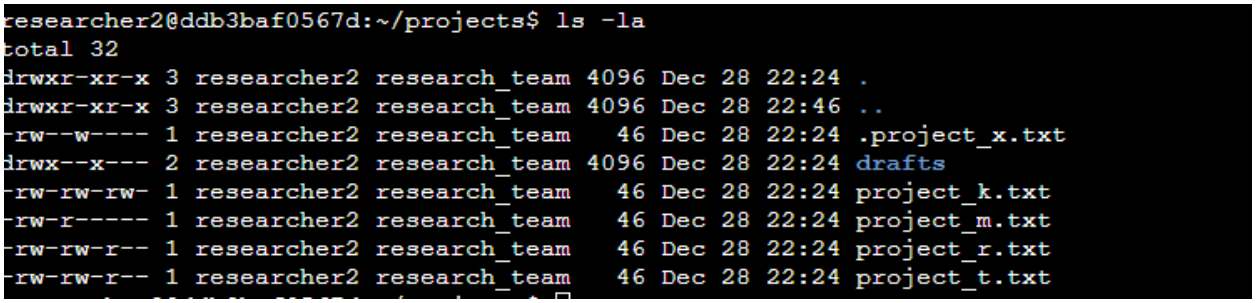
File permissions in Linux

Mubariz Saeed

Project description

I am a security professional at a large organization, working primarily with the research team. Part of my responsibilities involve regularly auditing permissions and access controls to ensure only authorized users can access sensitive research data. In this documentation, I will walk through my recent audit and changes made to properly restrict permissions for the research team.

Check file and directory details



Describe the permissions string

The `ls` command in Linux is used to list contents of a directory. The `-l` option modifies the output to display detailed information permissions, ownership, size, and modification date for each file and directory.The -a option will list all files, including hidden files and directories that start with .. So in summary, `ls -la` outputs a detailed listing of all files, including hidden ones, displaying permissions, owners, size, date, and file/directory names for the contents of the current directory.

Change file permissions

The organization does not allow others to have write access to any files. So i will change there permissions by

```
researcher2@ddb3baf0567d:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 28 22:24 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 28 22:46 ..
-rw--w---- 1 researcher2 research_team   46 Dec 28 22:24 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 28 22:24 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Dec 28 22:24 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec 28 22:24 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 28 22:24 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 28 22:24 project_t.txt
researcher2@ddb3baf0567d:~/projects$
```

I will change it by doing chmod o-w project_k.txt:

```
researcher2@ddb3baf0567d:~/projects$ chmod o-w project_k.txt
researcher2@ddb3baf0567d:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 28 22:24 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 28 22:46 ..
-rw--w---- 1 researcher2 research_team   46 Dec 28 22:24 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 28 22:24 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec 28 22:24 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec 28 22:24 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 28 22:24 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 28 22:24 project_t.txt
researcher2@ddb3baf0567d:~/projects$
```

Now write access permissions have been removed for other users.

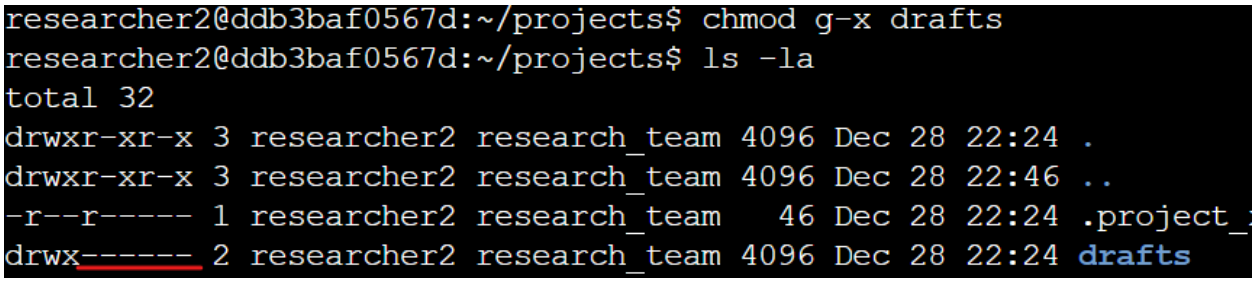
Change file permissions on a hidden file

`.project_x.txt`, should not have write permissions for anyone, but the user and group should be able to read the file. I will do this by removing write access for users,groups and others. Then i will give user and group read permissions

```
researcher2@ddb3baf0567d:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@ddb3baf0567d:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 28 22:24 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 28 22:46 ..
-r--r----- 1 researcher2 research_team   46 Dec 28 22:24 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 28 22:24 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec 28 22:24 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec 28 22:24 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 28 22:24 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 28 22:24 project_t.txt
researcher2@ddb3baf0567d:~/projects$
```

Change directory permissions

I removed the execute permissions in the drafts directory so that Only researcher2 should be allowed to access the drafts directory and its contents.



Summary

As a cybersecurity analyst, I need to properly manage file and directory permissions. Many files in our system allowed more access than necessary. This violates the principle of least privilege and poses security risks if sensitive data is leaked. To address this, I used Bash commands like "ls" and "chmod" to review and update permissions. I removed unnecessary access and aligned permissions to meet access policies.