

File Permissions in Linux

Prepared by: Sambou Kamissoko

LinkedIn: <https://www.linkedin.com/in/sambouk/>

Tools Used: Linux (Bash), ls -la, chmod, file system permissions

Project Description

In this project, I examined and managed Linux file and directory permissions to ensure that only authorized users had access to sensitive research files. Using Linux command-line tools, I reviewed existing permissions, identified misconfigurations, and applied corrective actions to align access with organizational security policies. This project demonstrates my ability to manage authorization, enforce least privilege, and secure file systems in a Linux environment.

Check File and Directory Details

To review existing file and directory permissions, I used the following Linux command:

```
ls -la
```

This command lists all files and directories, including hidden files, and displays detailed permission information, ownership, and group associations.

The permissions were reviewed in the following directory:

```
/home/researcher2/projects
```

Current File Permissions

The directory contained the following files and permissions:

Files

- **project_k.txt**
 - User: read, write
 - Group: read, write
 - Other: read, write
- **project_m.txt**
 - User: read, write
 - Group: read
 - Other: none
- **project_r.txt**
 - User: read, write
 - Group: read, write
 - Other: read
- **project_t.txt**
 - User: read, write
 - Group: read, write
 - Other: read
- **.project_x.txt** (hidden file)
 - User: read, write
 - Group: write
 - Other: none

Subdirectory

- **drafts/**
 - User: read, write, execute
 - Group: execute
 - Other: none

Describe the Permissions String

Linux permissions are represented by a **10-character string**, such as:

-rw-rw-r--

Explanation:

- The first character indicates file type (- for file, d for directory)
- Characters 2–4: user permissions (read, write, execute)
- Characters 5–7: group permissions
- Characters 8–10: permissions for others

For example:

- rw- = read and write
- r-- = read only
- --- = no access

Understanding this format is critical for identifying unauthorized access and enforcing least privilege.

Change File Permissions

The organization does not allow **write access for others** on files.

The file **project_k.txt** allowed write access for others, which violated policy.

To remove write permissions for others, I ran:

```
chmod o-w project_k.txt
```

After applying this command, the file permissions were successfully updated to prevent unauthorized modification.

Change File Permissions on a Hidden File

The hidden file **.project_x.txt** should:

- Allow read access for user and group
- Disallow write access for everyone

To correct the permissions, I used:

```
chmod 440 .project_x.txt
```

This ensured:

- User: read only
- Group: read only
- Other: no access

This change protects archived files from accidental or malicious modification.

Change Directory Permissions

Only the **researcher2** user should have access to the **drafts** directory and its contents.

To restrict access, I modified the directory permissions using:

```
chmod 700 drafts
```

This change ensures:

- User: full access
- Group: no access
- Other: no access

This aligns with least-privilege principles and prevents unauthorized directory traversal.

Summary

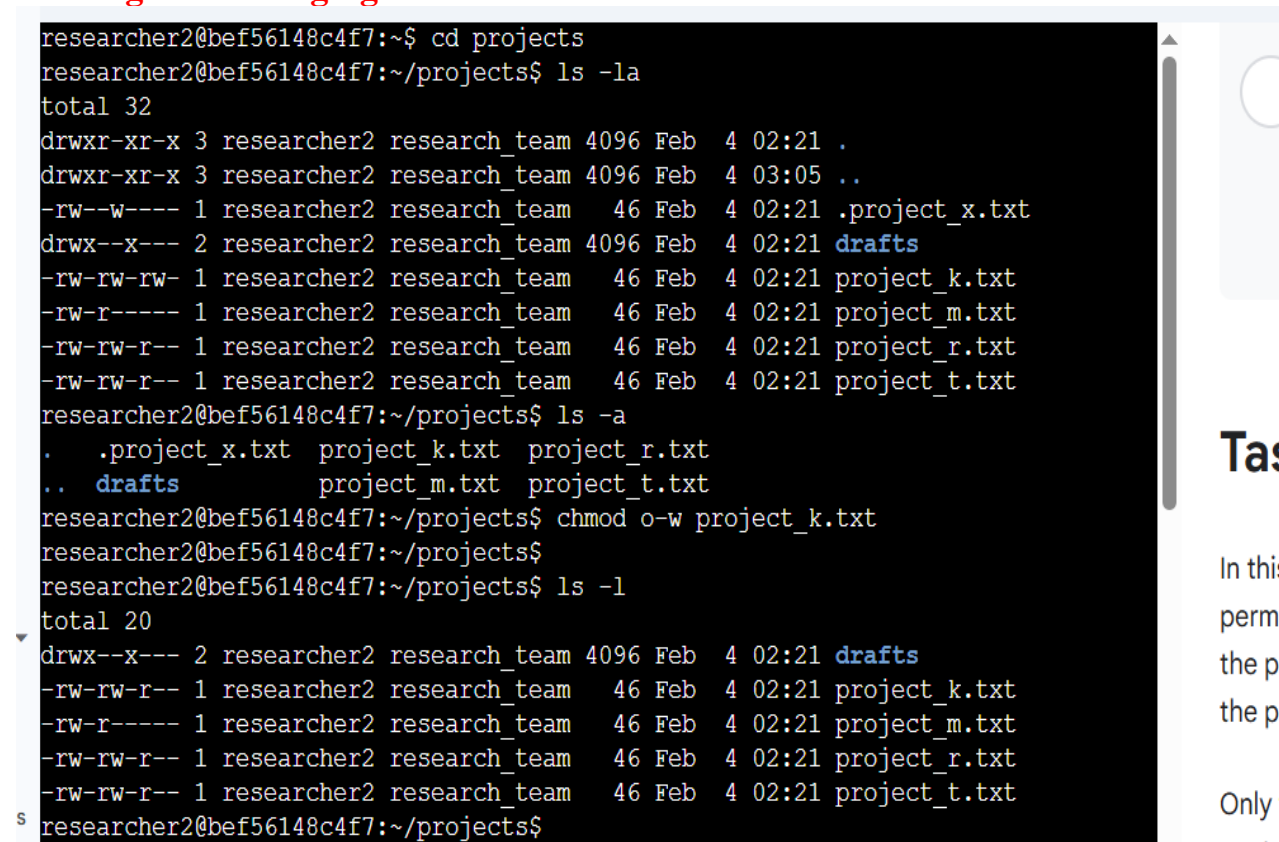
In this project, I reviewed Linux file and directory permissions, identified security misconfigurations, and corrected them using appropriate Linux commands. I

demonstrated the ability to interpret permission strings, manage access to regular and hidden files, and secure directories based on role-based authorization. These skills are essential for maintaining secure Linux systems and supporting access control requirements in enterprise environments.

Evidence

Screenshots of executed commands and outputs are included in the accompanying `screenshots/` directory to demonstrate hands-on execution and validation of changes.

Reading and Changing File Permissions in Linux



```
researcher2@bef56148c4f7:~$ cd projects
researcher2@bef56148c4f7:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb  4 02:21 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb  4 03:05 ..
-rw--w---- 1 researcher2 research_team  46 Feb  4 02:21 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb  4 02:21 drafts
-rw-rw-rw- 1 researcher2 research_team  46 Feb  4 02:21 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Feb  4 02:21 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Feb  4 02:21 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Feb  4 02:21 project_t.txt
researcher2@bef56148c4f7:~/projects$ ls -a
.  .project_x.txt  project_k.txt  project_r.txt
.. drafts        project_m.txt  project_t.txt
researcher2@bef56148c4f7:~/projects$ chmod o-w project_k.txt
researcher2@bef56148c4f7:~/projects$
researcher2@bef56148c4f7:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Feb  4 02:21 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Feb  4 02:21 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Feb  4 02:21 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Feb  4 02:21 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Feb  4 02:21 project_t.txt
researcher2@bef56148c4f7:~/projects$
```

Task

In this task, you will learn how to read and change file permissions in Linux.

Only the permissions of the files in the `projects` directory are shown.

Searching and Filtering Data Using grep and Piping

```
analyst@cfc7a5a74434:~$ cd /home/analyst/logs
analyst@cfc7a5a74434:~/logs$ grep error server_logs.txt
2022-09-28 13:56:22 error    The password is incorrect
2022-09-28 15:56:22 error    The username is incorrect
2022-09-28 16:56:22 error    The password is incorrect
2022-09-29 13:56:22 error    An unexpected error occurred
2022-09-29 15:56:22 error    Unauthorized access
2022-09-29 16:56:22 error    Unauthorized access
analyst@cfc7a5a74434:~/logs$ cd /home/analyst/reports/users
analyst@cfc7a5a74434:~/reports/users$
analyst@cfc7a5a74434:~/reports/users$ ls |grep Q1
Q1_access.txt
Q1_added_users.txt
Q1_deleted_users.txt
analyst@cfc7a5a74434:~/reports/users$ ls | grep access
Q1_access.txt
Q2_access.txt
Q3_access.txt
Q4_access.txt
analyst@cfc7a5a74434:~/reports/users$ ls
Q1_access.txt      Q1_deleted_users.txt  Q2_added_users.txt    Q3_access.txt
  Q3_deleted_users.txt  Q4_added_users.txt
Q1_added_users.txt  Q2_access.txt        Q2_deleted_users.txt  Q3_added_users.t
xt  Q4_access.txt      Q4_deleted_users.txt
analyst@cfc7a5a74434:~/reports/users$ grep jhill Q2_deleted_users.txt
1025      jhill      Sales
analyst@cfc7a5a74434:~/reports/users$
analyst@cfc7a5a74434:~/reports/users$ grep "Human Resources" Q4_added_users.txt
1151      sshah      Human Resources
1145      msosa      Human Resources
analyst@cfc7a5a74434:~/reports/users$
```

Managing Files and Directories in Linux

```
analyst@8d7798fala6a:~$ cd /home/analyst
analyst@8d7798fala6a:~$
analyst@8d7798fala6a:~$ mkdir logs
analyst@8d7798fala6a:~$
analyst@8d7798fala6a:~$ ls
logs  notes  reports  temp
analyst@8d7798fala6a:~$ rmdir temp
analyst@8d7798fala6a:~$
analyst@8d7798fala6a:~$ ls
logs  notes  reports
analyst@8d7798fala6a:~$ cd notes
analyst@8d7798fala6a:~/notes$
analyst@8d7798fala6a:~/notes$ mv Q3patches.txt ../reports
analyst@8d7798fala6a:~/notes$
analyst@8d7798fala6a:~/notes$ ls ../reports
Q1patches.txt  Q2patches.txt  Q3patches.txt
analyst@8d7798fala6a:~/notes$
analyst@8d7798fala6a:~/notes$ rm tempnotes.txt
analyst@8d7798fala6a:~/notes$
analyst@8d7798fala6a:~/notes$ ls
analyst@8d7798fala6a:~/notes$ touch tasks.txt
analyst@8d7798fala6a:~/notes$
analyst@8d7798fala6a:~/notes$ ls
tasks.txt
analyst@8d7798fala6a:~/notes$
```

```
analyst@0907b8cfc750:~$ pwd
/home/analyst
analyst@0907b8cfc750:~$ ls
logs  projects  reports  temp
analyst@0907b8cfc750:~$ cd /home/analyst/reports
analyst@0907b8cfc750:~/reports$ ls
users
analyst@0907b8cfc750:~/reports$ cd users
analyst@0907b8cfc750:~/reports/users$ ls
Q1_added_users.txt  Q1_deleted_users.txt
analyst@0907b8cfc750:~/reports/users$ ls
Q1_added_users.txt  Q1_deleted_users.txt
analyst@0907b8cfc750:~/reports/users$ cat Q1_added_users.txt
employee_id  username  department
1001         bmoreno   Marketing
1026         apatel    Human Resources
1041         cgriffin  Sales
1104         mreed     Information Technology
1177         aezra     Human Resources
1188         noshiro   Finance
analyst@0907b8cfc750:~/reports/users$
analyst@0907b8cfc750:~/reports/users$ cd /home/analyst/logs
analyst@0907b8cfc750:~/logs$ ls
server_logs.txt
analyst@0907b8cfc750:~/logs$ head server_logs.txt
2022-09-28 13:55:55 info    User logged on successfully
2022-09-28 13:56:22 error   The password is incorrect
2022-09-28 13:56:48 warning The file storage is 75% full
2022-09-28 15:55:55 info    User logged on successfully
2022-09-28 15:56:22 error   The username is incorrect
2022-09-28 15:56:48 warning The file storage is 90% full
```