Completed by Sage N Clements

# File permissions in Linux

## Project description

The audit department has advised that several files, folders and directories have permissions that are not consistent with corporate guidelines.  Per the change management requests, the security team has been advised to change the permissions accordingly to avoid potential cyber incident of inappropriate access.

## Check file and directory details

```
researcher2@32d2dc59c6a4:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb  1 22:19 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb  1 23:17 ..
-rw--w---- 1 researcher2 research_team   46 Feb  1 22:19 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb  1 22:19 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Feb  1 22:19 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb  1 22:19 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb  1 22:19 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Feb  1 22:19 project_t.txt
researcher2@32d2dc59c6a4:~/projects$
```

## Describe the permissions string

Using the “ls” string with the switches “la” will display the list of files in the current directory including its associated permissions.

The current permissions for each files includes:

.project_x.txt (hidden) -owner (read, write), group (write), other (none)
Drafts (directory)- owner (read, write, execute), group (execute), other (none)
Project_k.txt - owner (read, write), group (read, write), other (read, write)
Project_m.txt- owner (read, write), group (read), other (none)
Project_r.txt - owner (read, write), group (read, write), other (read)

Completed by Sage N Clements

project_t.txt - owner (read, write), group (read, write), other (read)

The files in violation have been corrected using the following commands:
chmod o-rw project_k.txt
chmod o-r project_r.txt project_t.txt

For context, `chmod` (short for "change mode") is a Linux command used to modify file and directory permissions. It requires specifying the user type (`u` for the owner, `g` for the group, and `o` for others), an operator (`+` to add permissions and `-` to remove them), and the target file or directory.

```
researcher2@32d2dc59c6a4:~/projects$ chmod o-rw project_k.txt
researcher2@32d2dc59c6a4:~/projects$ chmod o-r project_r.txt project_t.txt
researcher2@32d2dc59c6a4:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb  1 22:19 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb  1 23:17 ..
-rw--w---- 1 researcher2 research_team   46 Feb  1 22:19 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb  1 22:19 drafts
-rw-rw---- 1 researcher2 research_team   46 Feb  1 22:19 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb  1 22:19 project_m.txt
-rw-rw---- 1 researcher2 research_team   46 Feb  1 22:19 project_r.txt
-rw-rw---- 1 researcher2 research_team   46 Feb  1 22:19 project_t.txt
researcher2@32d2dc59c6a4:~/projects$
```

## Change file permissions

The organization does not allow others to have write access to any files.  Based on current permissions the following files are out of compliance:

Project_k.txt
Project_r.txt
Project_t.txt

## Change file permissions on a hidden file

The research team has archived .project_x.txt, which is why it's a hidden file. This file should not have write permissions for anyone, but the user and group should be able to read the file.

Using the following command, this file is now in compliance: chmod u-w,g-w,g+r .project_x.txt

Completed by Sage N Clements

```
researcher2@32d2dc59c6a4:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@32d2dc59c6a4:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Feb  1 22:19 .
drwxr-xr-x 3 researcher2 research_team 4096 Feb  1 23:17 ..
-r--r----- 1 researcher2 research_team   46 Feb  1 22:19 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Feb  1 22:19 drafts
-rw-rw---- 1 researcher2 research_team   46 Feb  1 22:19 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Feb  1 22:19 project_m.txt
-rw-rw---- 1 researcher2 research_team   46 Feb  1 22:19 project_r.txt
-rw-rw---- 1 researcher2 research_team   46 Feb  1 22:19 project_t.txt
```

## Change directory permissions

The files and directories in the projects directory belong to the researcher2 user. Only researcher2 should be allowed to access the drafts directory and its contents.

Using the following command, this file is now in compliance: chmod g-rx drafts

```
researcher2@ce0b3fb2a49c:~/projects$ chmod g-rx drafts
researcher2@ce0b3fb2a49c:~/projects$ ld -la drafts
ld: cannot find -la
ld: cannot find drafts: file format not recognized
researcher2@ce0b3fb2a49c:~/projects$ ls -ld drafts/
drwx------ 2 researcher2 research_team 4096 Feb  1 23:52 drafts/
```

## Summary

The audit department identified inconsistencies in file and directory permissions that did not align with corporate security guidelines. To mitigate potential unauthorized access, the security team reviewed and adjusted permissions accordingly.

**Identified Issues:**

1. **File Permissions Violations**
    - Several files allowed write access to "others," which is against company policy.
    - The hidden file `.project_x.txt` required modifications to restrict write access while allowing read access for the user and group.
2. **Directory Permissions Violations**

    - The `Drafts` directory, owned by `researcher2`, needed to be restricted so that only `researcher2` could access its contents.

**Corrective Actions Taken:**

- Removed write access for "others" on **Project_k.txt, Project_r.txt, and Project_t.txt** to comply with security policies.
- Adjusted `.project_x.txt` to ensure only the user and group could read it, while removing unnecessary write permissions.
- Restricted group access to the **Drafts** directory, ensuring only the owner (`researcher2`) could access its contents.

These changes ensure compliance with corporate security policies and reduce the risk of unauthorized access.