File permissions in Linux

Project description

In this project, I worked as a security professional responsible for managing file permissions for a research team at a large organization. My task was to ensure that users had the appropriate access to files and directories while maintaining system security. Using Linux commands, I examined and modified file permissions to align with the organization's security policies, ensuring that unauthorized users could not access sensitive information. This activity demonstrates my ability to manage file permissions effectively, a critical skill for maintaining system security in a professional environment.

Check file and directory details

To check the permissions of files and directories, I used the `ls -la` command. This command lists all files and directories, including hidden ones, along with their permissions, ownership, and modification dates.

Describe the permissions string

The 10-character string represents the file or directory permissions. For example, for the file `file1.txt`, the permissions string is `-rw-r--r--`. Here's what each character means:

1. **First character (`-`):** Indicates the type of file. `-` for a regular file, `d` for a directory.
2. **Next three characters (`rw-`):** Permissions for the owner (read and write).
3. **Middle three characters (`r--`):** Permissions for the group (read-only).
4. **Last three characters (`r--`):** Permissions for others (read-only).

In this example, the owner can read and write the file, while the group and others can only read it.

Change file permissions

The organization does not allow others to have write access to any files. In the output, `file2.txt` has the permissions `-rw-rw-r--`, which grants write access to the group. To remove write access for the group, I used the `chmod` command.

Change file permissions on a hidden file

The hidden file `.project_x.txt` should not have write permissions for anyone, but the user and group should be able to read it. Currently, its permissions are `-rw-rw-rw-`.

Change directory permissions

The `drafts` directory and its contents should only be accessible to `researcher2`. Currently, its permissions are `drwxr-xr-x`, which allows read and execute access for the group and others.

Command:

bash
Copy

```
chmod 700 drafts
```

Output:
After running the command, the permissions for `drafts` changed to `drwx------`.

Explanation:

- `700` sets permissions so that only the owner (`researcher2`) can read, write, and execute the directory.
- The group and others have no access to the directory or its contents.

Summary

Summary

In this activity, I used Linux commands to manage file and directory permissions effectively. I started by checking permissions using `ls -la`, interpreted the 10-character permissions string, and modified permissions using `chmod` to align with organizational policies. I removed write access for unauthorized users, updated permissions for a hidden file, and restricted access to a directory to ensure only the authorized user could access it. These tasks demonstrate my ability to manage file permissions and maintain system security, which are essential skills for a cybersecurity professional.