Usa comandos de Linux para administrar permisos de archivo

Escenario

Analiza el siguiente caso. Luego, completa las instrucciones paso a paso.
Eres un/a profesional de la seguridad en una gran organización. Trabajas principalmente con tu equipo de investigación. Parte de tu trabajo consiste en asegurarte de que los/las usuarios/as de este equipo disponen de los permisos adecuados. Esto ayuda a mantener el sistema seguro.
Tu tarea es examinar los permisos existentes en el sistema de archivos. Tendrás que determinar si estos coinciden con la autorización que se debe otorgar. Si no coinciden, deberás modificar los permisos para autorizar a los/las usuarios/as apropiados/as y eliminar cualquier acceso no autorizado.

Paso 1: Comprobar los permisos de archivos y directorios

Comando para verificar los permisos

Para revisar los permisos de los archivos, debes usar el comando `ls -la`, que mostrará los detalles de los archivos, incluidos los archivos ocultos (los que comienzan con un punto). El comando es:

```
ls -la /home/researcher2/projects
```

Esto mostrará algo similar a:

```
drwxr-xr-x 2 researcher2 researcher2 4096 Oct 8 10:21 drafts
-rw-rw-rw- 1 researcher2 researcher2 1024 Oct 8 10:21 project_k.txt
-rw-r--r-- 1 researcher2 researcher2 1024 Oct 8 10:21 project_m.txt
-rw-rw-r-- 1 researcher2 researcher2 1024 Oct 8 10:21 project_r.txt
```

```
-rw-rw-r-- 1 researcher2 researcher2 1024 Oct 8 10:21 project_t.txt
-rw--w---- 1 researcher2 researcher2 1024 Oct 8 10:21 .project_x.txt
```

Explicación de los permisos

Cada archivo o directorio tiene una cadena de 10 caracteres que representan sus permisos, por ejemplo:

- `-rw-rw-rw-` para `project_k.txt`.
- La primera letra indica si es un archivo (`-`) o un directorio (`d`).
- Los siguientes tres grupos de letras indican los permisos para el **usuario** (propietario), el **grupo**, y los **otros**. Cada grupo tiene 3 letras:
    - `r` es lectura,
    - `w` es escritura,
    - `x` es ejecución.

Paso 2: Identificar archivos que requieren modificación

Basado en el escenario, no se permite que "otros" tengan acceso de escritura a los archivos. En este caso, **`project_k.txt`** tiene permisos de escritura para "otros" (`rw-rw-rw-`). Esto debe corregirse.

Paso 3: Modificar permisos de archivos

Usa el comando `chmod` para cambiar los permisos. Para eliminar el permiso de escritura para "otros", el comando sería:

```
chmod o-w /home/researcher2/projects/project_k.txt
```

Explicación:

- `o-w` significa eliminar (`-`) permisos de escritura (`w`) para otros (`o`).
- Esto cambiaría los permisos de `rw-rw-rw-` a `rw-rw-r--`.

Paso 4: Cambiar permisos de un archivo oculto

El archivo `.project_x.txt` es oculto y debe configurarse para que el usuario y el grupo puedan leer el archivo, pero nadie puede escribir. Para lograrlo, usa:

```
chmod 440 /home/researcher2/projects/.project_x.txt
```

Explicación:

- `440` otorga permisos de lectura a **usuario** y **grupo** (`r--r-----`) y no permite escribir ni ejecutar.

Paso 5: Cambiar permisos de directorios

El directorio **drafts** debe estar solo accesible para el usuario. Para modificar sus permisos, el comando es:

```
chmod 700 /home/researcher2/projects/drafts
```

Explicación:

- `700` significa que solo el propietario (usuario) tiene permisos de lectura, escritura y ejecución (`rwx------`).

Descripción del Proyecto

Descripción del proyecto: En este proyecto, revisamos y ajustamos los permisos de los archivos y directorios en un entorno Linux para garantizar que cumplan con las políticas de seguridad de la organización. Usamos comandos como `ls -la` para verificar permisos y `chmod` para modificarlos, eliminando accesos no autorizados y configurando permisos para archivos y directorios ocultos.

Resumen: Realizamos un análisis detallado de los permisos de archivos en el directorio `/home/researcher2/projects`, identificamos archivos que tenían permisos inadecuados y los corregimos utilizando el comando `chmod`. También ajustamos los permisos de archivos ocultos y directorios, asegurando que solo los usuarios apropiados tuvieran acceso, en cumplimiento con las políticas de seguridad de la organización.

Estructura final en la plantilla:

1. **Comprobar permisos de archivos y directorios**:
    - Comando: `ls -la /home/researcher2/projects`

    - Explicación de la cadena de permisos: `-rw-rw-rw-` significa que el archivo puede ser leído y escrito por el usuario, el grupo y otros.
2. **Modificar permisos de archivos**:
    - Comando: `chmod o-w /home/researcher2/projects/project_k.txt`.
    - Explicación: Este comando quita permisos de escritura para "otros" en el archivo `project_k.txt`.
3. **Modificar permisos de archivos ocultos**:
    - Comando: `chmod 440 /home/researcher2/projects/.project_x.txt`.
    - Explicación: Esto otorga permisos de solo lectura a usuario y grupo y elimina la escritura.
4. **Modificar permisos de directorios**:
    - Comando: `chmod 700 /home/researcher2/projects/drafts`.
    - Explicación: El directorio `drafts` solo es accesible para el usuario propietario.