

Linux File and Directory Permission Hardening (Least Privilege)

Project description

Strengthened an organization's security posture by modifying permissions using the Bash command-line interface. The principles established by least privilege were paramount in making adjustments.

Check file and directory details

```
researcher2@ff92539f5434:~$ pwd
/home/researcher2
researcher2@ff92539f5434:~$ cd /home/researcher2/projects
researcher2@ff92539f5434:~/projects$ ls
drafts  project_k.txt  project_m.txt  project_r.txt  project_t.txt
researcher2@ff92539f5434:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Nov 18 12:12 drafts
-rw-rw-rw- 1 researcher2 research_team    46 Nov 18 12:12 project_k.txt
-rw-r----- 1 researcher2 research_team    46 Nov 18 12:12 project_m.txt
-rw-rw-r-- 1 researcher2 research_team    46 Nov 18 12:12 project_r.txt
-rw-rw-r-- 1 researcher2 research_team    46 Nov 18 12:12 project_t.txt
researcher2@ff92539f5434:~/projects$ 
```

Used a command option in order to look beyond the basic details provided by the `ls` command, the command `ls -l` allows you to view directory or file permissions.

Describe the permissions string

```
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_t.txt
```

Let's break down the first string listed above.

The first character represents whether we are referencing a file or directory in this case since a hyphen is listed it is a file (d for directory, - for files).

The following characters are clustered into 3 groups containing 3 letters. The three clusters represent the owner types with the order being user, group, and other from left to right. Within said clusters we find the level of permission that each group has (r-permission to read, w-permission to write, x-permission to execute, - null).

Therefore the 10 character string reads that we are referencing a file in which users hold permission to read and write, the owner type group has permission to read and write, and finally the owner type others has permission to read.

Change file permissions

```
researcher2@ff92539f5434:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Nov 18 12:12 drafts
-rw-rw-rw- 1 researcher2 research_team 46 Nov 18 12:12 project_k.txt
-rw-r---- 1 researcher2 research_team 46 Nov 18 12:12 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_t.txt
researcher2@ff92539f5434:~/projects$ chmod o-w project_k.txt
researcher2@ff92539f5434:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Nov 18 12:12 drafts
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_k.txt
-rw-r---- 1 researcher2 research_team 46 Nov 18 12:12 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_t.txt
researcher2@ff92539f5434:~/projects$ █
```

The command ls -l was used to identify the file that had been mistakenly assigned write permissions for the owner type other.

The change mode command (chmod) was used to remove the owner type other's write permissions.

chmod o-w project_k.txt

You'll find a breakdown of that command below.

chmod (remove write permission from owner type other) (file to be modified)

Change file permissions on a hidden file

```
researcher2@ff92539f5434:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov 18 12:12 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov 18 13:30 ..
-rw--w---- 1 researcher2 research_team 46 Nov 18 12:12 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Nov 18 12:12 drafts
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_k.txt
-rw----- 1 researcher2 research_team 46 Nov 18 12:12 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_t.txt
researcher2@ff92539f5434:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@ff92539f5434:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov 18 12:12 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov 18 13:30 ..
-r--r----- 1 researcher2 research_team 46 Nov 18 12:12 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Nov 18 12:12 drafts
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_k.txt
-rw----- 1 researcher2 research_team 46 Nov 18 12:12 project_m.txt
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_r.txt
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_t.txt
researcher2@ff92539f5434:~/projects$ 
```

The file `.project_x.txt` is a hidden file that has been archived and should not be written to by anyone. The string currently reads that it is a file that grants users permission to read and write and grants the owner type group permission to write.

Using the command `chmod u-w,g-w,g+r .project_x.txt` I was able to remove the owner type user and group permission to write and then granted the owner type group the permission to read.

Change directory permissions

```
researcher2@ff92539f5434:~/projects$ pwd  
/home/researcher2/projects  
researcher2@ff92539f5434:~/projects$ ls -l  
total 20  
drwx--x--- 2 researcher2 research_team 4096 Nov 18 12:12 drafts  
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_k.txt  
-rw----- 1 researcher2 research_team 46 Nov 18 12:12 project_m.txt  
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_r.txt  
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_t.txt  
researcher2@ff92539f5434:~/projects$ chmod g-x drafts  
researcher2@ff92539f5434:~/projects$ ls -l  
total 20  
drwx----- 2 researcher2 research_team 4096 Nov 18 12:12 drafts  
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_k.txt  
-rw----- 1 researcher2 research_team 46 Nov 18 12:12 project_m.txt  
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_r.txt  
-rw-rw-r-- 1 researcher2 research_team 46 Nov 18 12:12 project_t.txt
```

The command chmod can be used to modify permissions on directories and files. In this case the directory known as drafts was mistakenly granting the owner type group the permission to execute. I went ahead removed said permission using chmod g-x drafts.

Summary

The concept of least privilege is crucial for maintaining a healthy security posture. These simple yet impactful adjustments can be the difference between a disgruntled employee altering key files or even a hacktivist intervening with business continuity. Using Linux I was able to efficiently harden this organization's security measures.