ARAIZ NAQVI

INCIDENT REPORT

Fly Airlines

14TH OCTOBER, 2024

2024-2025

ARAIZ NAQVI

TABLE OF CONTENT

2024-2025

ARAIZ NAQVI

DISCLAIMER

This incident report is a project-based simulation for the fictional organization *Fly Airlines*, as part of the "Fundamentals of Cybersecurity" course on Google's Coursera platform.

While the details may resemble real-world scenarios, all data, systems, and findings are entirely fictitious and created for educational purposes. This incident report does not reflect any actual incidents or vulnerabilities affecting any real organization, including Fly Airlines.

Though based on practical analysis and protocols, the assessments are conducted in a simulated environment and should not be considered representative of any real entity's security posture.

2024-2025

ARAIZ NAQVI

INCIDENT SUMMARY

Time of Incident:	2024-10-14 14:18:32.192571 (14th October, 2024 2:18:32.192571pm)
Summary of Incident:	An accidental incident of extra privileged permissions led to an insider accidentally being able to access sensitive threat.
Location of Incident:	Fly Airlines
Reported By:	Araiz Naqvi
Reported On:	2024-10-14 14:25:29.576597 (14th October, 2024 2:25:29.576597pm)

ARAIZ NAQVI

INCIDENT DETAILS

Type of Incident: Improper File Permissions

Description: Last evening, a log showed an employee accessing a file they were not authorized to view. This could have been a serious incident if the insider threat had involved someone with malicious intent.

Fortunately, the employee reported the issue, expressing confusion about why they were able to access the file.

ARAIZ NAQVI

FILE AND DIRECTORY DETAIL

The file structure of the */home/researcher2/projects* directory and the original permissions of the files and subdirectory it contained were as follows:

```
ls -l
```

```
total 20
drwx--x--- 2 researcher2 research_team 4096 Oct 14 07:13 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Oct 14 07:13 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Oct 14 07:13 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 07:13 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 07:13 project_t.txt
```

Clearly, permissions are as follows:

- project_k.txt
  - User = read, write,
  - Group = read, write
  - Other = read, write
- project_m.txt
  - User = read, write
  - Group = read
  - Other = none

(PTO)

- 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
  - User = read, write
  - Group = write
  - Other = none

Additionally,
There is also one subdirectory inside the projects directory named drafts. The permissions on drafts are:

- User = read, write, execute
- Group = execute
- Other = none

ARAIZ NAQVI

THE PERMISSIONS STRING

A 10-character string begins each entry and indicates how the permissions on the file are set.

For instance, a directory with full permissions for all owner types would be drwxrwxrwx:

- **The 1st character (file type)**: The d indicates it's a directory. When this character is a hyphen (-) or f, it's a regular file.

- **The 2nd-4th characters (read (r), write (w), and execute (x) permissions for the user)**: When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted to the user.

- **The 5th-7th characters (read (r), write (w), and execute (x) permissions for the group)**: When one of these characters is a hyphen (-) instead, it indicates that this permission is not granted for the group.

- **The 8th-10th characters (read (r), write (w), and execute (x) permissions for the owner type of other)**: This owner type consists of all other users on the system apart from the user and the group.

When one of these characters is a hyphen (-) instead, that indicates that this permission is not granted.

ARAIZ NAQVI

CHANGING FILE PERMISSIONS

All files' group ownership is observed to be under a group called *research_team.*

File *project_k.txt* does not allow other users to have write(w) permissions however they have been given, and this needs to be fixed as follows:

```
researcher2@597f03d64d03:~/projects$ chmod o-w project_k.txt
researcher2@597f03d64d03:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Oct 14 07:13 .
drwxr-xr-x 3 researcher2 research_team 4096 Oct 14 07:22 ..
-rw--w---- 1 researcher2 research_team   46 Oct 14 07:13 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Oct 14 07:13 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 07:13 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Oct 14 07:13 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 07:13 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 07:13 project_t.txt
```

(PTO)

Also, project_m.txt is not allowed to grant read access to anyone but the user. Hence this permission needs to be taken off as follow:

```
researcher2@01854ecb8024:~/projects$ chmod g-r project_m.txt
researcher2@01854ecb8024:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Oct 14 08:03 .
drwxr-xr-x 3 researcher2 research_team 4096 Oct 14 08:23 ..
-rw--w---- 1 researcher2 research_team   46 Oct 14 08:03 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Oct 14 08:03 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_k.txt
-rw------- 1 researcher2 research_team   46 Oct 14 08:03 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_t.txt
```

Additionally, a hidden file .project_x.txt must not grant write(w) access to anyone, not even the user. Hence write permission needs to be taken off from both user and group only cause others don't have them anyway as follows:

```
researcher2@01854ecb8024:~/projects$ chmod u-w,g-w .project_x.txt
researcher2@01854ecb8024:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Oct 14 08:03 .
drwxr-xr-x 3 researcher2 research_team 4096 Oct 14 08:23 ..
-r-------- 1 researcher2 research_team   46 Oct 14 08:03 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Oct 14 08:03 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_k.txt
-rw------- 1 researcher2 research_team   46 Oct 14 08:03 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_t.txt
```

(PTO)

ARAIZ NAQVI

CHANGING HIDDEN FILE PERMISSIONS

Additionally, a hidden file .project_x.txt must not grant write(w) access to anyone, not even the user. Hence write permission needs to be taken off from both user and group only cause others don't have them anyway as follows:

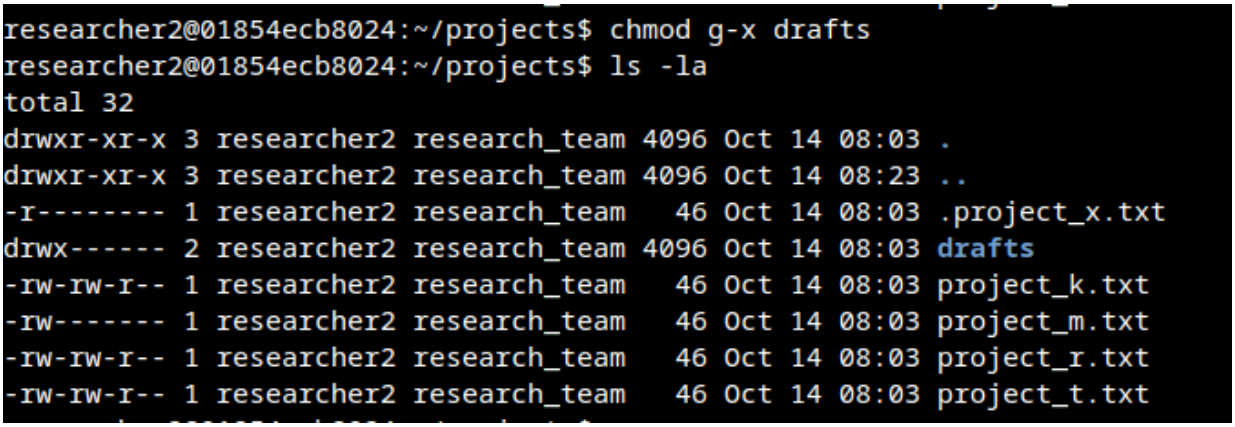
```
researcher2@01854ecb8024:~/projects$ chmod u-w,g-w .project_x.txt
researcher2@01854ecb8024:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Oct 14 08:03 .
drwxr-xr-x 3 researcher2 research_team 4096 Oct 14 08:23 ..
-r-------- 1 researcher2 research_team   46 Oct 14 08:03 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Oct 14 08:03 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_k.txt
-rw------- 1 researcher2 research_team   46 Oct 14 08:03 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Oct 14 08:03 project_t.txt
```

2024-2025

ARAIZ NAQVI

CHANGING DIRECTORY PERMISSIONS

Finally, the drafts should not be executable by group, so execute permission has been removed as follows:



ARAIZ NAQVI

UPDATED FILE AND DIRECTORY DETAIL

Clearly, permissions are as follows:

- 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
  - User = read, write
  - Group = write
  - Other = none

(PTO)

Additionally,

There is also one subdirectory inside the projects directory named drafts. The permissions on drafts are:

- User = read, write, execute
- Group = execute
- Other = none

ARAIZ NAQVI

SUMMARY

These permission changes have now neutralised any chance of an insider or outsider threat disabling critical access to critical files that the organisation can't afford to have compromised.

These regular checks are essential to understand what vulnerabilities lie in the open and need to be safeguarded as soon as possible.

(PTO)

Araiz Naqvi

Network Security Engineer

If you find this helpful, you'll love my content!

@araiz-naqvi

@araiznaqvi