LINUX PERMISSION AUDIT

PREPARED BY: Biliaminu B. Salawu
Cybersecurity Analyst
November 2025

Executive Summary

The Linux Permission Audit project focused on reviewing and improving access controls on critical directories to ensure permissions comply with security policies, regulatory standards, and least-privilege best practices.
Linux permissions are a core security mechanism that controls access to files and directories.
They define who can read, write, or execute a file and are essential for maintaining system integrity, confidentiality, and availability.

1. Permission Types

Linux uses three primary permission types:

- Read (r): Allows viewing the contents of a file or listing a directory.
- Write (w): Allows modifying a file or creating/deleting files within a directory.
- Execute (x): Allows running a file as a program or accessing a directory.

2. File Permission (File System Permission or Access mode)

Permissions are assigned to three categories which are:

- Owner: The user who owns the file.
- Group: Users who belong to the file's group.
- Others: All other users on the system.

3. Permission Representation

Permissions are commonly displayed using symbolic notation:
drwxr-xr-- This breaks down as follows:

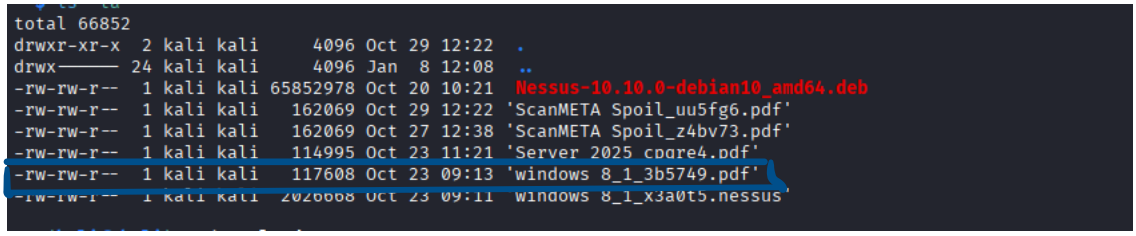
- File type (for file, d for directory)
- Owner permissions (rwx)
- Group permissions (r-x)
- Other permissions (r--)

Permissions can also be represented numerically:

Number	Permission
0	No permission
1	Execute
2	Write
4	Read
5	Read and Execute
6	Read and Write
7	Read, Write and Execute

- Example: 755 = rwxr-xr-x.

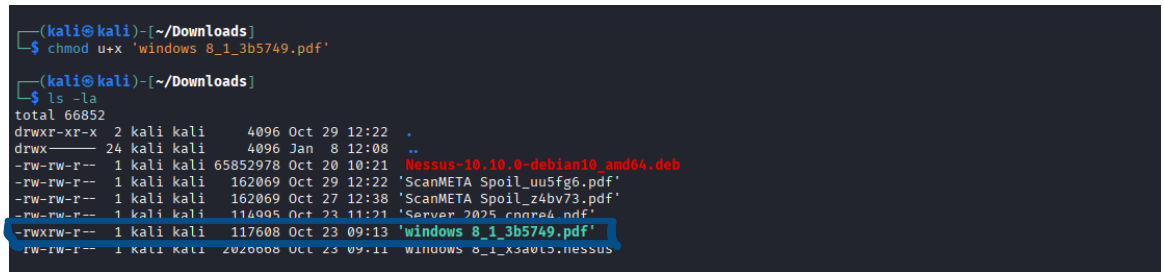
4. Changing Permission;The chmod command is used to modify permissions which is Symbolic (add or remove + or -) and Numeric methods .Examples: chmod 755 file.txt, chmod u+x script.sh where the extension .txt, .sh could be plain text file, shell script file etc. Viewing permissions to reveal the type of File Permission (File System Permission or Access mode categories using Linux.



From the screenshot above, "windows 8_1_3b5749.pdf" has -rw-rw-r—

User has read and write permission
Group has read and write permission
Others have read only permission.
Note: None of the "3 file categories" have Execute

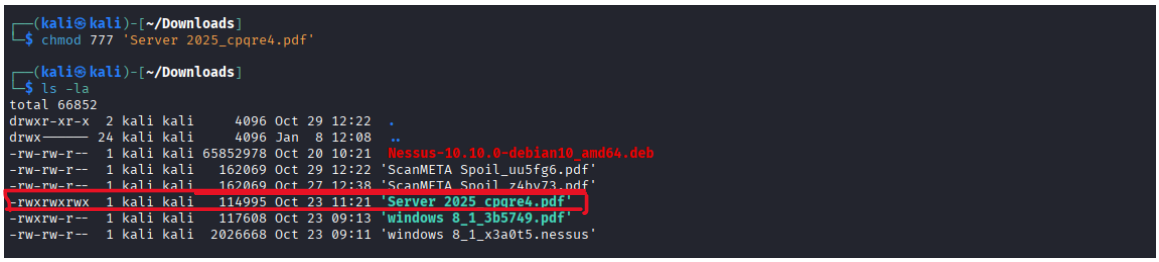
(a). To add "execute" permission to "windows 8_1_3b5749.pdf" , following command Line will be used on Linux; Chmod u+x "windows 8_1_3b5749.pdf" (Means add execute permission to the USER of the pdf).



Execution permission has been added to the "windows 8_1_3b5749.pdf" user which is now -rwx (User can read, write and execute)

rw- (Group read and write)
r— (Other can read only)

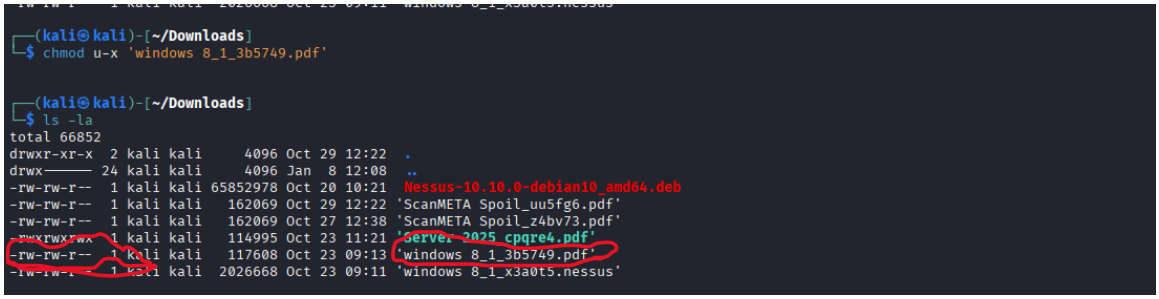
(b). Adding full permission to 'Server 2025_cpqre4.pdf', by using Numeric method following command Line will be used on Linux; Chmod 777 "windows 8_1_3b5749.pdf" (Means add execute permission to the USER, GROUP and OTHERS of the pdf).



Read, write and execute permission has been added to the 'Server 2025_cpqre4.pdf' user which is now
-rwx (User can read, write and execute).
rwx (Group can read, write and execute).
rwx (Other can read, write and execute).

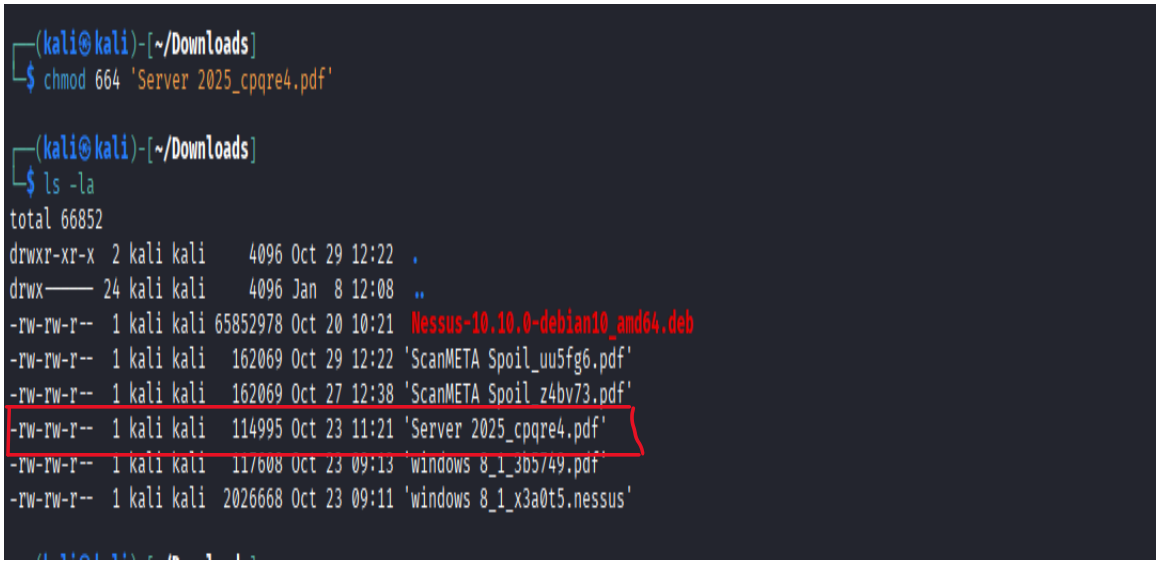
5. Removing permissions; Permission can be removed using any of the methods numeric or Symbolic e.g. "chmod u-x filename.txt", "chmod g-w book.exe" OR chmod 755 (where 7 gives full permissions to the user, 5 give read and execute to the group and 5 gives read and execute permission to other).

(a). Removing permission from the "windows 8_1_3b5749.pdf" using symbolic method



The permission has been removed and it changes to -rw-rw-r-- for 'windows 8_1_3b5749.pdf' file.

(b). Removing full permissions from 'Server 2025_cpqre4.pdf' using Numeric method



The permission has been removed and it changes to -rw-rw-r-- for 'Server 2025_cpqre4.pdf' file from full access that was given before.

6. Security Importance

Proper permission management prevents unauthorized access, limits privilege escalation, and protects critical system files from accidental or malicious modification.
Understanding Linux permission is essential for maintaining security and ensuring that users have only the necessary access to perform their tasks.

Conclusion

Linux permissions form the foundation of Linux security. Understanding and correctly applying permissions is essential for system administration, cybersecurity, and secure software deployment.