**Linux for Hackers 5: Controlling file and directory permissions**

\*\*Different types of users : developers, network administrators, DB admins…

\*\*Granting permissions : r-read, w-write, x-execute

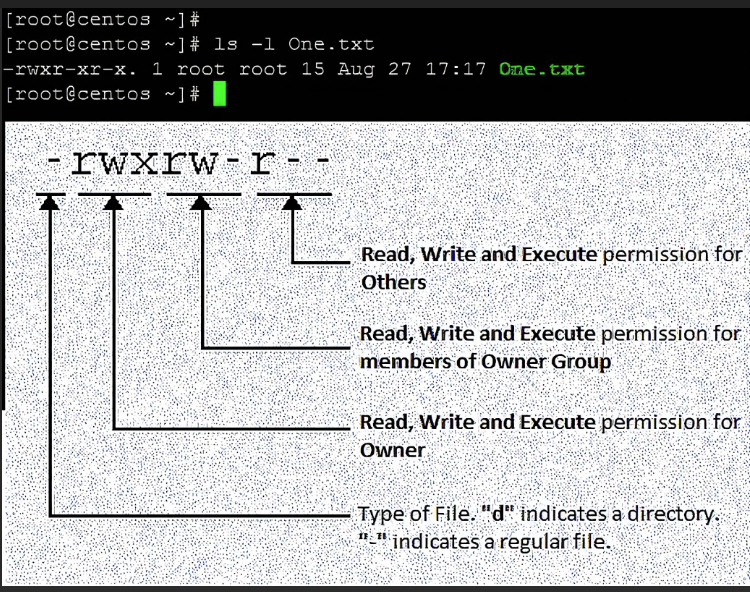
Root user can grant level of permissions depending upon what they need the files for.

* Granting ownership to individual user: **chown uday file.txt**

Chown(change owner)

* Granting ownership to a group: **chown group file.txt**

\*\*Checking permissions: **ls -l /usr/share/hashcat**



A picture containing text

Description automatically generated

Examples:

chmod 555 file.txt than ls -l

chmod u-w file.txt then ls -l

chmod u+x file.txt then ls -l

\*\*Giving root execute permissions on a newtool.

**chmod 766 newhackertool ; ls -l**

**\*\***Setting more default permissions with masks: Linux automatically sets base permissions – 666 for files and 777 for directories. Umask methods represents the permissions that you want to remove from the base permissions on a file or directory to make them more secure. umask is 022 by default. Kali default is 644 for files and 755 for directories. Every user can set a personal default umask value for the files and directory in **.profile file.** To see the current value when logged on as user simply type ***umask***.

\*\*Special permissions: SUID & SGID

1. SUID - Granting temporary root permissions to user with SUID

**chmod 4644 filename**

1. SGID – Granting the user’s group permissions with SGID

**chmod 2644 filename**

1. Stickybit – It is a permission bit that you can set on a directory to allow a user to delete or rename files within the directory.

**\*\***Special permissions, privilege escalation and the hacker:

find / -user root -perm 4000

* **cd usr/bin ; ls -l**

**observe the files and their permissions**

**Exercise**

1. Select a directory and run a long listing on it. Note the permissions on the files and directories.

2. Select a file you don’t have permission to execute and give yourself execute permissionsusing the chmod command. Try using both the numeral method (777) and the UGOmethod.

3. Choose another file and change its ownership using chown.

4. Use the find command to find all files with the SGID bit set.