**SPECIAL PERMISSIONS**

**Types of Special permissions:**

* Setuid (SUID) - 4
* Setgid (SGID) - 2
* Stickybit – 1

|  |  |  |  |
| --- | --- | --- | --- |
| **SUID** | **SGIT** | **STICKYBIT**  r-x  t | |
| rwx | r-x |
| s | s |
| rws |  | r-s | r-t |
| rwS |  | r-S | r-T |

* **SETUID(SUID): u+s**
* Setuid is a permission set in Linux that lets users run programs with the same privileges as the program's owner.
* It's used to give users temporary elevated permissions to perform specific tasks.

**SYNTAX:**

* chmod u+s file/directory

****

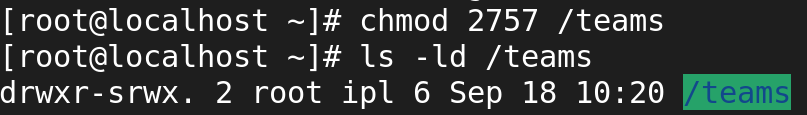
* **TO REMOVE SUID:**
* chmod u-s filename/directory

****

* **SETGIT(SGID): g+s**
* Setgid is short for "set group identity".
* It's a special permission that allows a process to run with the same group ID as the file's owner.
* This means that the user is granted access based on the permissions of the group that owns the file.

**SYNTAX:**

* chmod g+s file/directory

****

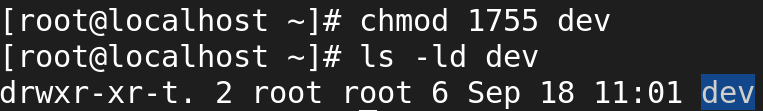
* **TO REMOVE SGID:**
* chmod g-s file/directory

****

* **STICKY BIT: o+t**
* The sticky bit is a permission bit that protects the files within a directory.
* If the directory has the sticky bit set, a file can be deleted only by the file owner, the directory owner, or by a privileged user.

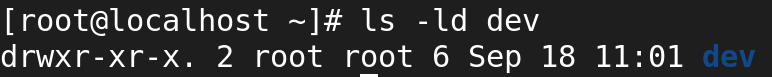
**SYNTAX:**

* chmod o+t file/directory



* **TO REMOVE STICKY BIT:**
* chmod g-s file/directory

****

****