**SPECIAL PERMISSIONS**

**There are three types of special permissions:**

**1. setuid (SUID) - 4**

**2. setgid (SGID) - 2**

**3. stickybit - 1**

**suid sgid stickybit**

**rwx r-x r-x**

**s s t**

**rws r-s r-t**

**rwS r-S r-T**

**It used change in symbolic format**

**chmod u+s file/directory**

**chmod g+s file/directory**

**chmod o+t file/directory**

**It is used to change in numeric format**

**chmod 4755 file**

**chmod 2755**

**chmod 1744 file**

**It is used to remove the special permission of specific dirctory/file which is (4,2,1)**

**chmod 0755**

**1.Setuid**

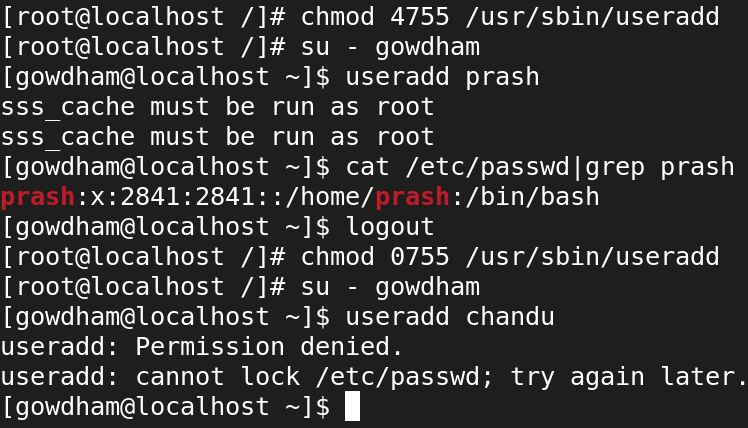
**Set User ID/SETUID : Whenever SETUID permission has set on executable files, anyone executing that command (file) will inherit the permissions of the owner of the file. Its numeric value is 4.**

**chmod 4755 <filename>**

**chmod u+s <filename>**

**chmod u-s <filename>**

**output:**



**These are the default file permissions**

**[root@machine-1 ~]# ls -l /usr/bin/su**

**-rwsr-xr-x. 1 root root 57840 May 26 2022 /usr/bin/su**

**[root@machine-1 ~]# ls -l /usr/bin/mount**

**-rwsr-xr-x. 1 root root 49624 May 26 2022 /usr/bin/mount**

**[root@machine-1 ~]# ls -l usr/bin/umount**

**-rwsr-xr-x. 1 root root 37256 May 26 2022**

**/usr/bin/umount**

**[root@machine-1 ~]# ls -l /usr/bin/passwd**

**-rwsr-xr-x. 1 root root 32648 Aug 10 2021 /usr/bin/passwd**

**[root@machine-1 ~]# ls -l /usr/bin/crontab**

**-rwsr-xr-x. 1 root root 57800 May 31 2022 /usr/bin/crontab**

**[root@machine-1 ~]# ls -l /usr/bin/chage**

**-rwsr-xr-x. 1 root root 74384 Apr 25 2022 /usr/bin/chage**

**[root@machine-1 ~]# ls -l /usr/bin/sudo**

**---s--x--x. 1 root root 185456 Aug 26 2021 /usr/bin/sudo**

**useradd**

**userdel**

**passwd**

**chage**

**fdisk**

**which ls**

**ls -l /root**

**[root@machine-1 ~]# which useradd**

**/usr/sbin/useradd**

**[root@machine-1 ~]# which userdel**

**/usr/sbin/userdel**

**[root@machine-1 ~]# which fdisk**

**/usr/sbin/fdisk**

**[root@machine-1 ~]# which whoami**

**/usr/bin/whoami**

**2. SGID**

**FILE:**

* **SGID / Set Group ID :- SETGID permission is similar to the SETUID, except that the process's effective group ID (GID) is changed to the group owner of the file, and a user is granted access based on permissions assigned to that group.**
* **The SetGID permission displays as an “s” in the group executable field. Its numeric value is 2.**

**DIRECTORY:**

**If you setup SGID on directores, all files or directories created inside that directory will be owned by the same common group(group owner of the directory where SGID is configured).**

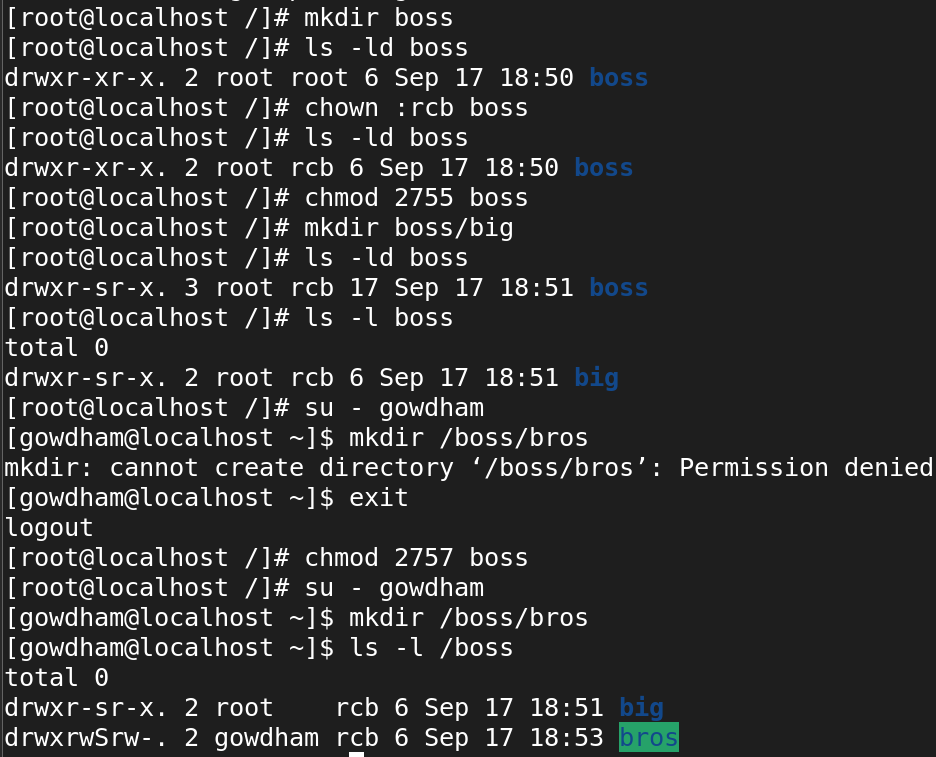
**The SetGID permission displays as an “s” in the group executable field. Its numeric value is 2.**

**chmod 2755 <file/dirname>**

**chmod g+s <file/dirname>**

**chmod g-s <file/dirname>**

**Output:**



**STICKY BIT**

**Sticky Bit :- If the directory permission have the sticky bit permission set, then the file can be deleted only by the REAL owner of the file/directory or the root user. This special permission**

**prevents to delete other user’s file from public directories. Its numeric value is 1.**

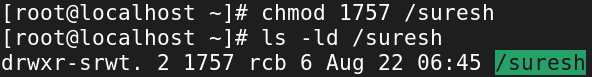
**chmod 1755 <file/dirname>**

**chmod o+t <file/dirname>**

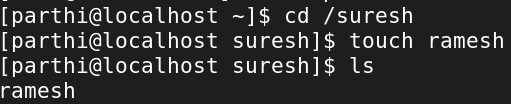
**chmod o-t <file/dirname>**

**Output:**

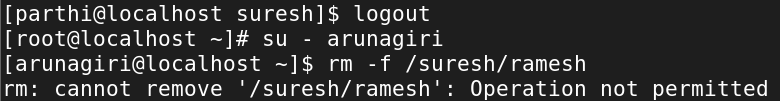
**Setting sticky permission to the directory /suresh**

****

**Switching the user from root and creating a file in the directory /suresh**

****

**Now, switching to the another user and deleting the file which was created by the user parthi, the file cannot be deleted because we set stickybit permission to the directory /suresh**

****

