1001 #Special Permissions

1002 #suid=Set userid = set for user(owner) so that all users can execute the command as root.

1003 #Difference between suid and sudo

1004 #sudo=Particular can execute that particular command as root

1005 #suid=All users can execute that command as root

1006 #which <command> provides the absolute path of the command

1011 #s=suid is set in 4th bit in permissions column

1012 #s=indicates both suid and execute permissions are there.

1013 #S=indicates only suid permission is there.

1019 which useradd

1020 ls -l /usr/sbin/useradd

1021 su - student

1022 chmod u+s /usr/sbin/useradd

1023 ls -l /usr/sbin/useradd

1024 su – student

useradd n1

If useradd is not working try for systemctl command as follows

su – student

systemctl restart sshd

It will not allow you to execute this command

-rwsr-xr-x. 1 root root 721744 Oct 1 2020 /usr/bin/systemctl

s is added in 4th bit so suid bit is set

su – student

49 systemctl restart sshd

50 systemctl status sshd

ls -l newfile1

-rw-r--r-- 1 root root 0 Oct 8 10:56 newfile1

mkdir /newdir1

[root@server ~]# cd /newdir1

[root@server newdir1]# ls -ld /newdir1/

drwxr-xr-x 2 root prod 6 Oct 8 10:55 /newdir1/

[root@server newdir1]# touch f1 f2

[root@server newdir1]# ls -l

total 0

-rw-r--r-- 1 root root 0 Oct 8 10:57 f1

-rw-r--r-- 1 root root 0 Oct 8 10:57 f2

[root@server newdir1]# chmod 2775 /newdir1

[root@server newdir1]# ls -ld /newdir1/

drwxrwsr-x 2 root prod 26 Oct 8 10:57 /newdir1/

[root@server newdir1]# #s is added in the 7th bit indicating that sgid bit is set

[root@server newdir1]# #chmod g+s /newdir1 and chmod 2775 /newdir1 both are same

[root@server newdir1]# #Numeric or octal permission for suid is 4 , sgid 2, stickybit 1

[root@server newdir1]# #2775=1st bit is special permission,2 is sgid,7 for user(owner),7 for group,5 for others

[root@server newdir1]# ls -l

total 0

-rw-r--r-- 1 root root 0 Oct 8 10:57 f1

-rw-r--r-- 1 root root 0 Oct 8 10:57 f2

[root@server newdir1]# touch newfile1

[root@server newdir1]# ls -l newfile1

-rw-r--r-- 1 root prod 0 Oct 8 11:02 newfile1

[root@server newdir1]# #group owner is prod

#Stickybit is set for others for a dir where many users have rw permissions

If sticky bit is set only the owner or root can delete or modify the files within that dir. [root@server ~]# ls -ld /tmp

drwxrwxrwt. 33 root root 4096 Oct 8 11:09 /tmp

[root@server ~]# #t is set for others indicating sticky bit is set for /tmp dir

[root@server ~]# useradd kiran

useradd: user 'kiran' already exists

[root@server ~]# passwd kiran

Changing password for user kiran.

New password:

BAD PASSWORD: The password is shorter than 8 characters

Retype new password:

passwd: all authentication tokens updated successfully.

[root@server ~]# su - student

Last login: Wed Oct 8 10:45:53 IST 2025 on pts/0

[student@server ~]$ cd /tmp

[student@server tmp]$ touch s1

[student@server tmp]$ ls -l s1

-rw-rw-r-- 1 student student 0 Oct 8 11:14 s1

[student@server tmp]$ logout

[root@server ~]# su - kiran

[kiran@server ~]$ cd /tmp

[kiran@server tmp]$ ls -l s1

-rw-rw-r-- 1 student student 0 Oct 8 11:14 s1

[kiran@server tmp]$ rm s1

rm: remove write-protected regular empty file ‘s1’? y

rm: cannot remove ‘s1’: Operation not permitted

[kiran@server tmp]$ logout

[root@server ~]# chmod o-t /tmp

[root@server ~]# ls -ld /tmp

drwxrwxrwx. 33 root root 4096 Oct 8 11:15 /tmp

[root@server ~]# su - kiran

Last login: Wed Oct 8 11:15:10 IST 2025 on pts/0

[kiran@server ~]$ cd /tmp

[kiran@server tmp]$ ls -l s1

-rw-rw-r-- 1 student student 0 Oct 8 11:14 s1

[kiran@server tmp]$ rm s1

rm: remove write-protected regular empty file ‘s1’? y