Assignment 6

SUID Use Case

SUID is nothing but the **special permission** given to **a user** to a **program/file** with the permission of the **file owner**. SUID stands for set user ID.

Normal User → having limited command access

So SUID is specially used to give access to execute particular commands from normal users. IT means that with the help of SUID we can permit the normal user to execute a particular command that the normal user does not have permission.

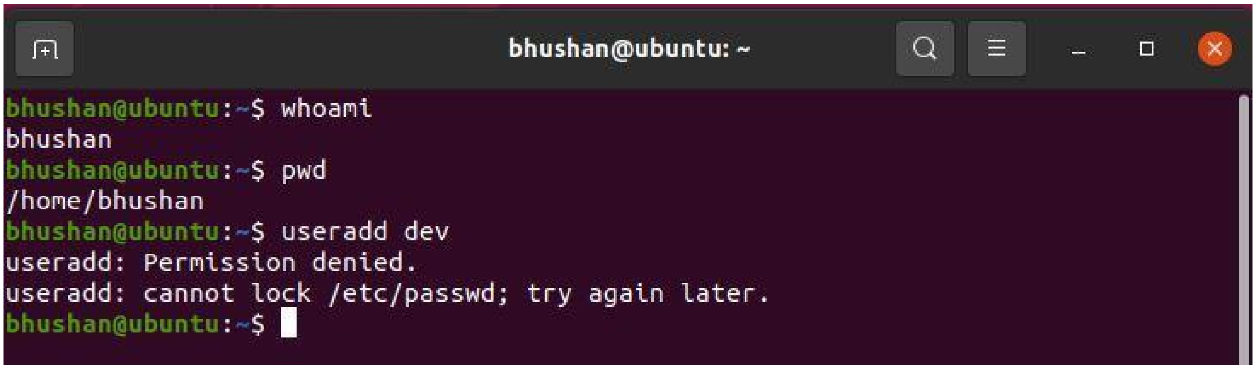
We can **apply** SUID by using 2 methods :

1) Symbolic Method → chmod u+s <command file path>
2) Numeric Method → chmod 4755 <command file path>

We can **remove** SUID by using 2 methods :

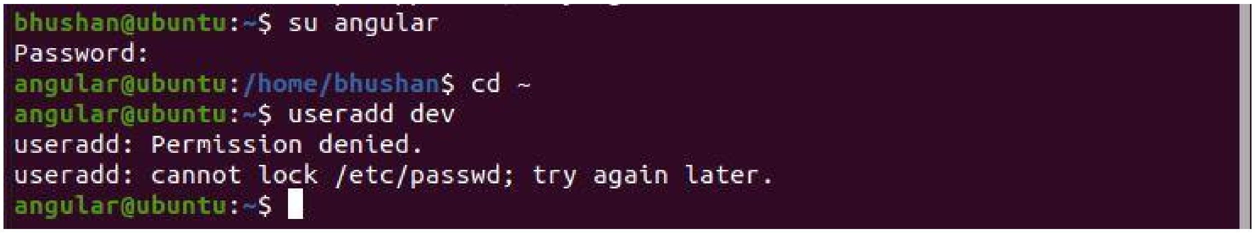
1) Symbolic Method → chmod u-s <command file path>
2) Numeric Method → chmod 755 <command file path>

Point 1: If we login with a normal user and try to execute useradd command then we get an error message. Because normal users didn't have permission to run or execute useradd commands are as follows :-



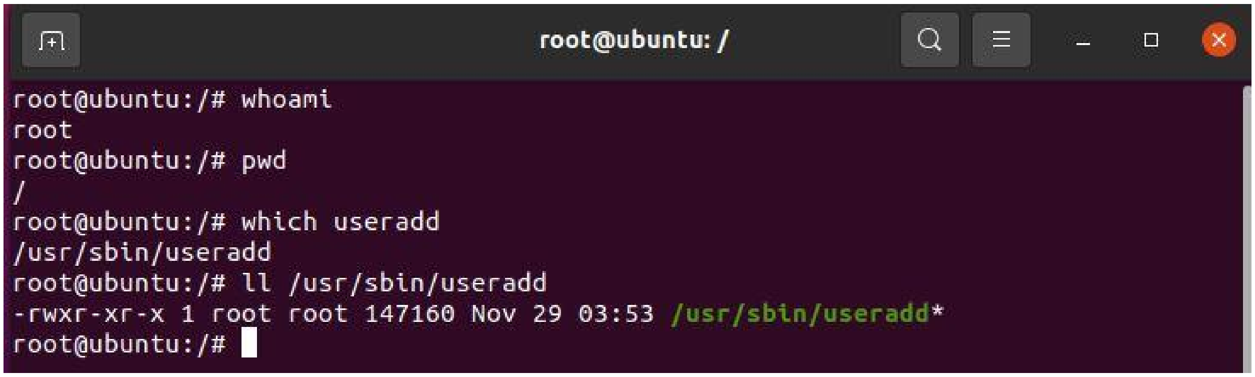
```
bhushan@ubuntu:~$ whoami
bhushan
bhushan@ubuntu:~$ pwd
/home/bhushan
bhushan@ubuntu:~$ useradd dev
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
bhushan@ubuntu:~$ 
```

If we login with another normal user angular and try to execute useradd command then we get an error message. Because normal users didn't have permission to run or execute useradd commands are as follows :-



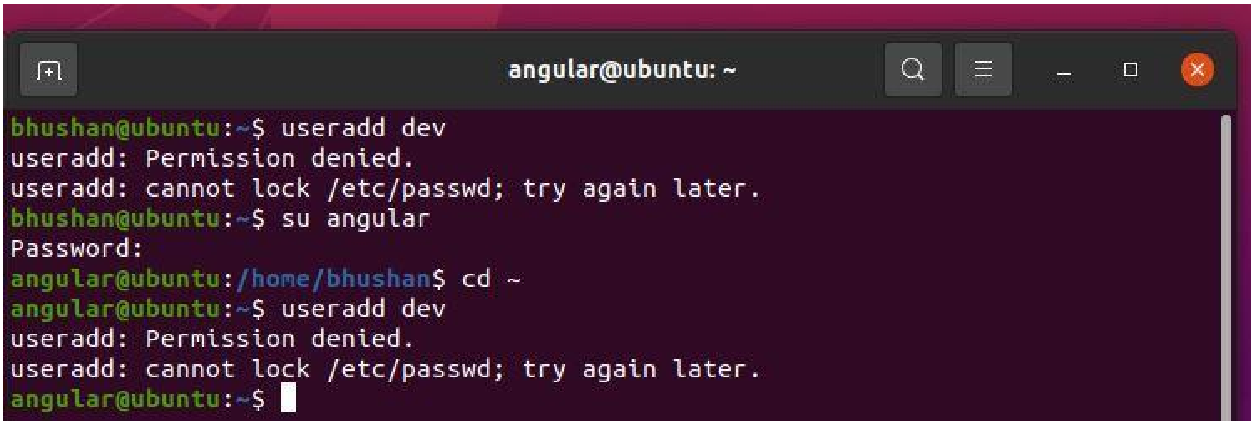
```
bhushan@ubuntu:~$ su angular
Password:
angular@ubuntu:/home/bhushan$ cd ~
angular@ubuntu:~$ useradd dev
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
angular@ubuntu:~$ 
```

Point 2: Now , Login with root user and try to check from where the useradd command will get executed or run with the help of which command and check the permission of the file or directory only the user has execute permission,group and others have execute permission.



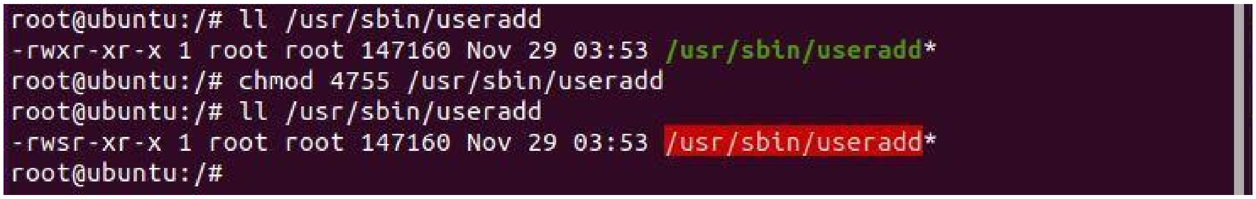
```
root@ubuntu:/# whoami
root
root@ubuntu:/# pwd
/
root@ubuntu:/# which useradd
/usr/sbin/useradd
root@ubuntu:/# ll /usr/sbin/useradd
-rwxr-xr-x 1 root root 147160 Nov 29 03:53 /usr/sbin/useradd*
root@ubuntu:/# 
```

Point 3: The user ,group and others have execute permission. Login with a normal user and try to execute useradd command. First we logged in with bhushan user and then with angular. From both we are unable to run this command.



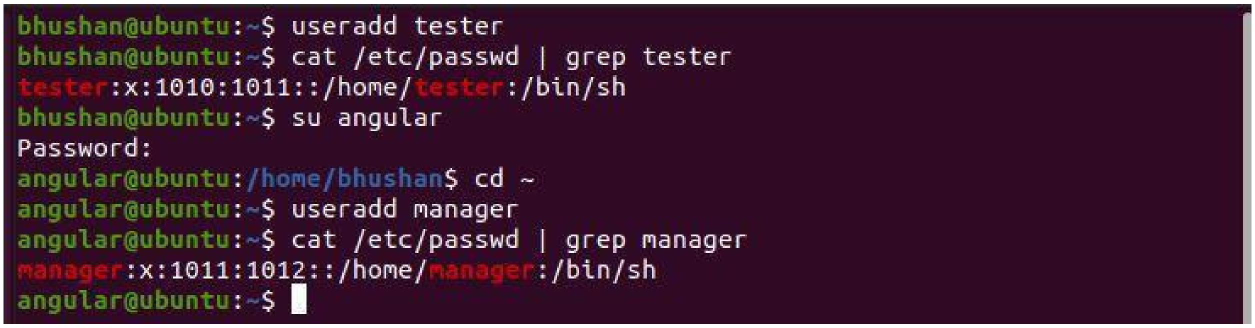
```
bhushan@ubuntu:~$ useradd dev
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
bhushan@ubuntu:~$ su angular
Password:
angular@ubuntu:/home/bhushan$ cd ~
angular@ubuntu:~$ useradd dev
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
angular@ubuntu:~$ 
```

Point 4: So to solve the above problem or to give special permission we use SUID. so here login with root user and give special permission to users with numeric mode with the help of chmod command.



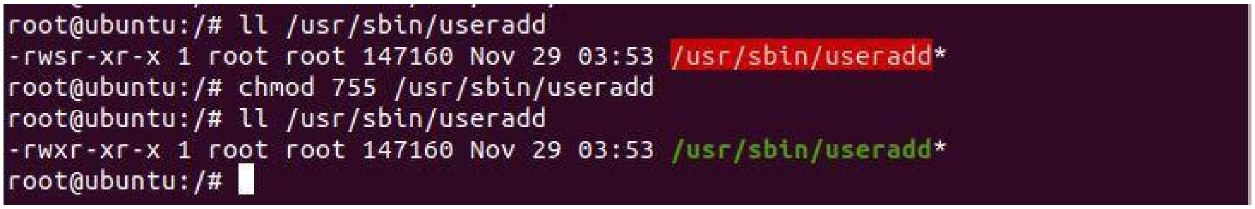
```
root@ubuntu:/# ll /usr/sbin/useradd
-rwxr-xr-x 1 root root 147160 Nov 29 03:53 /usr/sbin/useradd*
root@ubuntu:/# chmod 4755 /usr/sbin/useradd
root@ubuntu:/# ll /usr/sbin/useradd
-rwsr-xr-x 1 root root 147160 Nov 29 03:53 /usr/sbin/useradd*
root@ubuntu:/#
```

Point 5: After giving the permission, log in with a normal user and try to execute useradd command. First we logged in with bhushan user and then with angular. From both we are able to run this command.



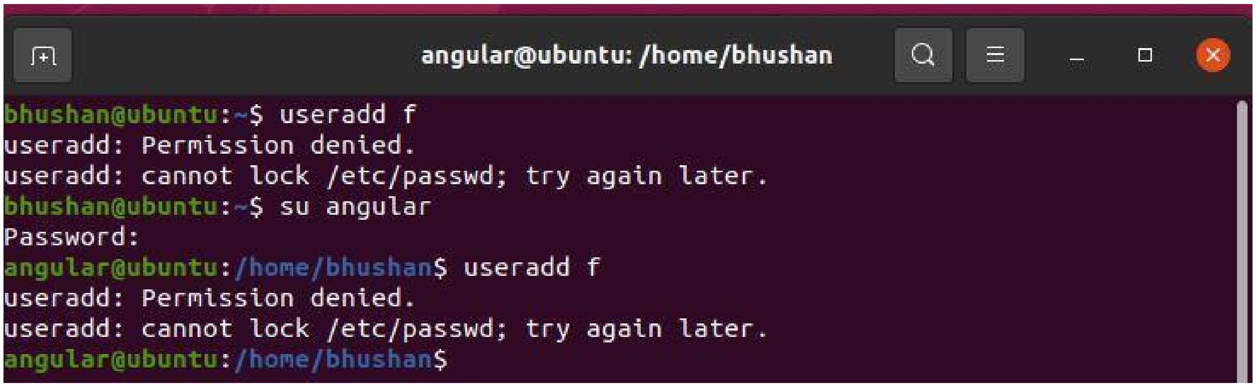
```
bhushan@ubuntu:~$ useradd tester
bhushan@ubuntu:~$ cat /etc/passwd | grep tester
tester:x:1010:1011::/home/tester:/bin/sh
bhushan@ubuntu:~$ su angular
Password:
angular@ubuntu:/home/bhushan$ cd ~
angular@ubuntu:~$ useradd manager
angular@ubuntu:~$ cat /etc/passwd | grep manager
manager:x:1011:1012::/home/manager:/bin/sh
angular@ubuntu:~$ 
```

Point 6: Now , we remove the SUID from the user. We use the chmod command in numeric mode from the root.



```
root@ubuntu:/# ll /usr/sbin/useradd
-rwsr-xr-x 1 root root 147160 Nov 29 03:53 /usr/sbin/useradd*
root@ubuntu:/# chmod 755 /usr/sbin/useradd
root@ubuntu:/# ll /usr/sbin/useradd
-rwxr-xr-x 1 root root 147160 Nov 29 03:53 /usr/sbin/useradd*
root@ubuntu:/# 
```

And now if we try to use the useradd command from a normal user then we are unable to execute it as we remove the SUID.



```
bhushan@ubuntu:~$ useradd f
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
bhushan@ubuntu:~$ su angular
Password:
angular@ubuntu:/home/bhushan$ useradd f
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
angular@ubuntu:/home/bhushan$
```