“root” super user is the king of the users in Linux/Unix. Having root access grant full and unlimited access to the Linux box. I will show how to allow root access to a user in a Linux system. Typically root level access used in system administration. It’s always a pain to give others (users) root access. You need to be careful and withdraw the access once need is finished.

According to Linux file system permissions root or super user has full permission read(r), write (w) and execute(x) to any file. By default root user id is 0.

I am going to create two users namely user1 and user2. Then I will give root access to user1 .

**Method : 1 Using Usermod Command**

[root@mypc Desktop]# adduser user1  
[root@mypc Desktop]# adduser user2  
[root@mypc Desktop]# groupadd test

I am going to add user1 to root group

[root@mypc Desktop]# usermod -G root user1

**Below command provide existing user the root privilege**

[root@mypc Desktop]# usermod -g 0 -o root\_user

**Method 2 : Using Useradd Command**

I have add new user user3 to root group using one single command

[root@mypc /]# useradd -m -G root user3  
[root@mypc /]# groups user3  
user3 : user3 root

**Another option using useradd command**

Useradd -c “Imitation Root” -d /home/root\_user -m -k /etc/skel -s /bin/bash -u 0 -o -g root root\_user

**Method 3 : Editing /etc/passwd file**

Edit /etc/passwd for the particular user. Change that user's UID and GID to 0 then the user will have the permissions of root.

root:x:0:0:root:/root:/bin/bash  
temproot:x:128:128:temproot

Now temproot user should have root privilege

root:x:0:0:root:/root:/bin/bash  
temproot:x:0:0:temproot

**Method 4 : Setting as Sudo User**

The sudo configuration file is /etc/sudoers and you can edit this file using visudo command: # visudo. Using visudo protects from conflicts and guarantees that the right syntax is used.

**Full Access to Specific Users**

Add below entry in the file

bob, tom ALL=(ALL) ALL

This method is not a good idea because this allows bob and tom to use the su command to grant themselves permanent root privileges thereby skipping the command logging features of sudo.

**Grant access to specific user to specific files**

This entry allows bob and all the members of the group operator to gain access to all the program files in the /sbin and /usr/sbin directories, plus the privilege of running the command /usr/oracle/backup.pl.

bob, %operator ALL= /sbin/, /usr/sbin, /usr/oracle/backup.pl