USERS AND GROUPS

Identity and Permissions

User and SuperUser

Linux puts a lot of power at your fingertips. That's the best reason to switch to Linux; it's also the most dangerous thing about the system. Linux controls how much power you can use on the computer based on your Login ID. It keeps a database of all users, and it keeps track of which user owns which files, and which users have permission to view, edit, and execute each file, folder or program. An ordinary user will not be able to do really dangerous things, like editing the user database, or deleting every file on the system.

But right now you are logged in as root. You are not just an ordinary user, you are SuperUser. (SuperUser is a real Unix term, synonymous with root.) There are no restrictions on your power. You have the ability to crash the system and make it otherwise unusable in more ways than you can imagine. As a novice it is very easy to make your system completely unusable with a single erroneous command. Believe me. I speak from experience. The first weekend after I installed Linux, I had to reinstall it FOUR times before I finally got smart and quit destroying it. And I'm a pretty savvy guy around computers, so don't think you're immune just because you know your way around a PC.

Because it is so dangerous to be logged in as root, you should never use this account unless you have to. The root account is meant to be used by the System Administrator to perform certain duties which can be destructive and therefore should only be performed by an expert. Some examples are emptying log files, mounting and unmounting file systems (more on this later under ***Getting to CD's and Floppies***), installing or removing programs, and creating or deleting user accounts.

If you are using Mandrake Linux, you will have a tool available to perform the most common administration tasks, even when logged in as a regular user. This is called the Mandrake Control Center, which you may find on your desktop or in the Configuration menu. It will ask you for the root password when you start it for security reasons. As a result of this handy tool, you may never need to actually log in as root.

Becoming SuperUser

No phone booth needed. The obvious way is simply to login as root. That may be the best way to do it if you plan on doing a bunch of system maintenance type stuff, but operating as root regularly is a bad idea, as you lose all the security protections that Linux provides. Logging in as the root user is generally discouraged and is in fact prohibited on some Linux systems by default. Fear not, there is a better way.

Try this:

```
[user]$ sudo ls

Password:*****
```

At the password prompt, type *your password*, not the root password. If it works, you will have just listed the current directory *as superuser*. Congratulations!

If you got an error about not being in the sudoers file, see the section on *configuring sudo*.

Type this:

```
[user]$ su

Password:*****

[root]#
```

Bang! Just like that, you are SuperUser! A few cautions: Although you are now SuperUser, this is not a “login” shell, so your environment hasn’t changed. The biggest way this will effect you is that some programs you normally run as root may appear to be missing. That’s because your PATH environment variable, the list of places Linux looks for executables, does not contain `/sbin` or `/usr/sbin`. If you try to run a command like `shutdown` (see below) and it complains, try typing `/sbin/shutdown` instead. That should do it.

When you are finished with your maintenance tasks you should immediately change back to normal user mode:

```
[root]# exit

[user]$
```

Notice that while you are SuperUser, your command prompt looks different. An ordinary user is prompted with the dollar sign (`$`) while SuperUser gets a pound sign or hashmark (`#`). This makes it easy to tell which mode you are in.

Source : http://www.control-escape.com/linux/users-groups.html