How to configure Debian to create new added users through adduser to be secure by default / Limiting access to other user's information

Author : admin

If you're about to add new users to your Debian GNU/Linux you should have certainly noticed that the defaultusers created in **/home** directory are created with a *755 chmod permissions* .
What makes it even worser is that in Debian by default the *root user home directory* **/root** has also a 755 permissons by default, you can see an example of the insecure behaviour below:

```
hipo@noah:/$ ls -ld root/
drwxr-xr-x 67 root root 4096 Aug 3 12:40 root/
```

This is quite a big security leak since every user on the system can read and copy all the documents of every other one without any constraint. Users can have read access to the **administrator root user !**
I have no clear clue why the Debian development team has taken the decision to set such an insecure permissions by default, but anyways it's probably a good practice if you're sane person with a security in mind, should certainly realize that this kind of insecure by default permissions has to be changed for a secure one.
This is probably about to save you tons of nerves of possible security info leak among users or even, security leaks coming out of your home root directory.

Changing the default permissions for the new created users on the system using the **adduser** command is pretty easy and is being controlled by */etc/adduser.conf*

the variable responsible for the persmissons of newly created user directories found within the file is: **DIR_MODE** by default in Debian this variable is set to be equal to **DIR_MODE=0755** which as I've already said is insecure thus a recommandable change value would be: **DIR_MODE=750**

So procceed and open the **vim /etc/adduser.conf** and change the **DIR_MODE=755** variable to **DIR_MODE=0750** there is plenty of more configuration options that you might want to tamper with one worthy to mention is that through the same conf file you're able to specify the range values between which a new created user's ids and gids could borrow.
This can be done via the variables **FIRST_SYSTEM_UID** LAST_SYSTEM_UID and respectively for GIDS, **FIRST_SYSTEM_GID** and **LAST_SYSTEM_GID**

Another thing to do immediately is change your root's directory default set permissions during after your Debian Linux installation is complete, to do so:

```
debian:~# chmod 750 /root
```

If you're in a position where you have already any number of users existing with alredy created insecure user home directories permissions (755) then a simple (bash shell) one liner to change all the system users permissions to 750 and hence prohibit users to be able to read among each other's directory would be:

```
debian:~# for i in /home/*; do chmod 750 $i; done
```

The default insecure behaviour that Debian Linux possess as well as the issue discussed above is well documentaed in Securing Debian Manual so check it out for a more thorough info on Debian security.