How to limit access to su command in Linux

If you have added Linux to your data center or are just using a single Linux machine for your business, you need to make sure it is as secure as possible.

If you have added Linux to the data center or are just using a single Linux machine for your business, you need to make sure it is as secure as possible. Of course, everyone thinks that Linux is one of the safest platforms on the planet. Although this may be true, you can still do many things to further improve the security of the Linux computer you are using.

One trick is to restrict access to su command. By using the su command, the user can change from one user account to another (if there is a password of that user account). Suppose you have some users in the admin group that have full access to certain folders (may contain sensitive data) and you do not want users who are not in the group to switch to user accounts. Other (using the su command), and then get access to that sensitive information.

This trick can be done on any Linux distribution. For example today will use Ubuntu Server. The article will create a new group, add users to that group and then restrict access to the su command for this group.

But how to limit access to su command? This is actually quite easy. Let's find out later!

Create a group

First, we will create a new group on the server (or desktop). To do this, open a terminal window and enter the command:

```
sudo groupadd admin
```

You now have a new group added to the system. If you find that the admin group already exists, you may have to create a group with a different name.

Add users to the new group

Suppose we have a user of Jack and want to add him to the new group, so that Jack has access to the su command. Please enter the following command:

```
sudo usermod -a -G admin jack
```

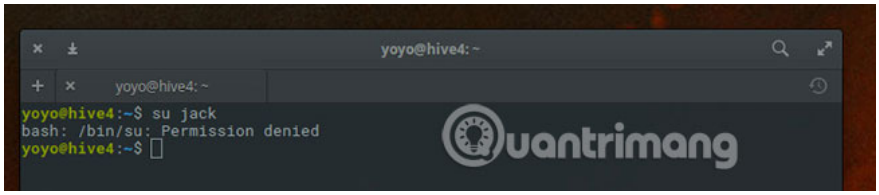
When running this command, user Jack will be a member of the admin group.

Restrict access to su commands

Now, we need to allow the admin team to access the su command. Do this with a single command. Go back to the terminal window and enter the following command:

```
sudo dpkg-statoverride --update --add root admin 4750 /bin/su
```

From the terminal window, log into Jack user account. If you try to use the su command as that user, the request will be allowed. Because Jack is a member of the admin group, has access to su command. However, if you log in as another user and try using the su command, the request will be rejected. Because only people in the admin group have access to su.



And that's all there is to do to restrict access to su command in Linux. Although this is not the only step you need to take to enhance the security of your Linux system, it will certainly prevent users from accessing the tool that can elevate their rights to unnecessary levels.

Hope you are succesful.