

Re: Of mice and men

Source: <http://coding.derkeiler.com/Archive/Cobol/comp.lang.cobol/2005-05/msg00240.html>

- *From:* Donald Tees <donald_tees@xxxxxxxxxxxxx>
 - *Date:* Sat, 07 May 2005 09:16:09 -0400
-

jce wrote:

"Donald Tees" <donald_tees@xxxxxxxxxxxxx> wrote in message

So what does chmod do? Or do you somehow disable that from working?

It is the command to change permissions. I would think it fairly obvious that you cannot change a permission of a file that you do not have access to, but perhaps not. However, being able to change the permission of a file does depend on who owns the file, and what permissions they have given to others over that file. If you do not have permission to access a file, then using chmod on that file will result in the error message "you do not have permission ...", the same as any other program would.

What about services - are you sure what you're running and that they are secure (I've noticed an increasing number of questions regarding settings of sendmail etc that most users don't need in the install to prevent such problems)

What about them? Sendmail has been around for many years, and security issues have always been fixed within days of them being discovered. You have to keep your software up to date if you want to run a secure system, but that is not new, nor unique to Linux. Security updates propagate around the planet in minutes.

Please check your system for programs set with the SUID bit enabled - then tell me you cannot run something like root.

```
ls -alF `find / -perm -4000` > yoursuidreport.txt
```

Re: Of mice and men

You may have installed something as "root" that enables the program to "execute" as root. Look into something like sendmail.

I did not say you cannot run a program that gives other's access to your files. Nor did I say you cannot install a program that gives access to files owned by a group. Of course you can. You just cannot do it for someone else's files.

I can set up a program like a music player, for example, that will only play music out of the music library, and has no access to any file on the entire computer (including my own) *except* the music library. Or I could set it up so that it played music out of *my* files but other users could only access those files by playing them through *my* player. I could do the same using group ownerships using the SGID Feature instead of the SUID feature.

If I understand you rightly, you are saying if I set up a program using those methods that gives access to the root, then give users access to that program using the root User ID, then the result would be an insecure system. I'd have to do that *AS* root, of course, but as owner of the system, I do have the root password. I'm not quite sure what to say "well duh" seems appropriate, but smacks of rudeness. May I'll just ask why you would do so, then complain about a security hole.

Sendmail---user's cannot run it. It is a server. Users run a client that use it's services. A server is part of the OS, not an standard application run by a user. You install them and set up security when you do so. It is not something a user gets to change, nor do they even get to execute it, or even portions of it. It is not a library, or interface layer. They only get to send requests to it, by running a client.

That operating system application servers are not restricted by the user logged in on a specific terminal that is using them is not a security flaw. It is the way that all secure OS's work. Different permissions, based on what is being done, and who it is being done by. The server and the client are two different users, and while the OS can access the user's file, the converse is not true.

>>>I'd be less inclined to comment if you stated that its "more automatically encouraged". Many distributions will force you to use a non admin account....but this could also be done in Windows etc etc....people just

Re: Of mice and men

view windows as a "home" OS and most "home" users just don't want to deal with the fact that there are more than one way to protect yourself.

Your user ID does not change just because you do a CD command.

Nor does it in windows, OS2, DOS,Z/OS.....

Disk files do not have a user ID, how could it change?

Windows only uses the user ID for logging into an NT server, it has nothing to do with your local disk. XP will set up a profile by user ID, and 98 was getting towards that, but it has nothing to do with access rights. At the command prompt, every user is identical to every other, and the "admin" account is irrelevant. It stops you from accessing other machines, it does not protect your own a jot.

It is not a matter of how people view it. It is a matter of not existing at all.

Directories and files under Linux are *owned* by a specific user ID, That relates to your login account, not to where you happen to be sitting on the disk.

You can also do this in Windows and others

Other's yes. Windows, no.

You might be able to CD to another user's account (IF and ONLY IF you have access access), but that does *not* mean you can write to it, nor does it mean you can read it. You must, for someone else to even see the directory, give others that access.

Re: Of mice and men

You can also do this in Windows and others

You keep saying this. Are you talking about NT server? That is not windows.

Funny that my college account was windows based and I didn't have access to anything then....I wonder why Microsoft created Users/Groups and Access Control Lists and cluster servers if they didn't have any ownership protection....

Because the Unix servers they were attaching to did. They predated NT server software by several years. In fact, users's and groups were available in DOS as net user commands.

The only thing they have ever been used for in windows/DOS is to join a network. That is why the cancel button logs you in ... you are not canceling login to the computer, there is none, and there is no security. You are canceling your ability to hook into a local network as a member. The user name and group have absolutely nothing to do with the management of the disk drive on your machine, nor do they have anything to do with the ability to access your machine disk drive. If you are on the keyboard, you have access.

They also have absolutely nothing to do with the security of your machine. Their purpose is to stop *you* from harming *someone else's* network.

Security is about the ability to stop someone else's network from harming *ME*, not about stopping me from accessing something else. In fact, even when you bypass login, the other machines on the windows network can *still* access your computer, if it was set up to share anything.

That is completely ass-backwards. You do not lock your door to stop *yourself* from *leaving* your house. At least I do not.

Donald

.