

Re: User access & security

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2007-10/msg00016.html>

- *From:* goarilla <"kevin DOT paulus AT skynet DOT be">
 - *Date:* Thu, 04 Oct 2007 00:57:54 +0200
-

Mark wrote:

This is a question related to my next post.

If there is a user with non-root access to their account, we are dependent on their having a good password to ward off too much nasty activity.

I am told that it is fairly easy with user access to install a rootkit of some sort and totally compromise the system.

fairly easy ? iirc a rootkit is something that replaces valuable system tools like ps, lsof, top, ipconfig, ip, ...

for this to be succesfull the user has to have access to the files in question this can be accomplished in a number of ways i know of

- a) you have fucked up your permissions and allow other to write to binaries owned by root
- b) the user account has unlimited access to or has enough access to sudo to do the same as mentionned in a)
- c) the user is rather skilled or is a script kiddie who knows where to get good tools and uses exploits in suid programs to execute the commands required to install rootkit (again you'll have to decide what you want your users to be able to do (permissions permissions permissions)). normal users have no business using suid or sgid programs
- d) the user is extremely good so after not finding the necessary sudo/sgid exploits he will try to attack running services that run as root: apache, smb, to get total access to the machine lately most attacks against webserver seem to target vulnerable php, perl script and spawn a custom script, which is located at some anonymous or compromised server, which launches a reverse (root) shell so ... it's a good idea to disallow the use of download tools like wget, curl to your users and your apache server

Now it seems to me that if this user is careless with this password, then the whole server is at risk. How true is this? Doesn't this weaken Linux to such an extent that any user access at all is guaranteed to bring down the server.

If that is the case, what do ISPs do, with their thousands of ordinary users? What does anybody do?

Re: User access & security

I ask this because I have inadvertently left an account open with a trivial password which somebody has stumbled into. (It has since been closed, but the question remains).

Assume you have been compromised and start from scratch
it's better to be safe than sorry

Thanks,

Mark

This is all i can come up with for now.

I'm not a security expert but i do like to think

i have educated myself enough, and will educate myself even further, to give some valuable advice

also remember 'security is a process not a state' and to keep up-to-date (whether it's about installed software or ... new attack vectors, tools, information, ...)

.