

Re: Fedora Core 3 & Core 4 Password questions

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-08/0129.html>

From: Winged (*Winged_at_nofollow.com*)

Date: 08/10/05

Date: Tue, 09 Aug 2005 21:47:43 -0500

Moe Trin wrote:

> *In the Usenet newsgroup alt.computer.security, in article*
> *<xlZJe.153280\$5V4.129554@pd7tw3no>, Brandon wrote:*
>
>
>>*Is there any length of complex password that can be assigned to the ROOT*
>>*that cannot be hacked if the person hacking has console access?*
>
>
> *Console access? Why bother hacking when there are quite obvious ways*
> *around it from that point.*
>
>
>>*I am selling a software product that I do not want the users to have*
>>*access to.*
>
>
> *Then don't install it on the users hardware, or hardware that the users*
> *have access to.*
>
>
>>*The only account on the server will be ROOT. I wanted to use a password*
>>*32 characters/numbers/symbols or higher.*
>
>
> *With the modern MD-5 hash system, this is easy – after all, you want to be*
> *the only person with root, so you can set the password as you like. Of*
> *course, it only takes a few minutes AT MOST to bypass this.*
>
>
>>*Main thing is no one must get in.*
>
>
> *Physical access beats five aces. If you want the system to be totally*
> *secure, encrypt the drive, and require the password to be entered each*
> *time the system boots. You can't keep the password on the system, or*
> *allow it to be entered over the network, as either method can be compromised*
> *very easily. Not practical, you say? Neither is your desire to prevent*

alt.computer.security: Re: Fedora Core 3 & Core 4 Password questions

> *anyone from accessing the software.*

>

> *Old guy*

Old guy is right on this one. If you don't control the hardware, the software can be retrieved.

Passwords make no difference, the disk directly accessed and software copied as simply as inserting a CD (for example) with the OS that mounts the disk where one knows the password.

One can just dupe the disk and one can hack the copies to their hearts content while still using the original copy. The system manager may not even be aware this copying has occurred, it takes only a few minutes.

Even if you use hardware keys (there are several flavors on the market).

Someone who has enough patience can work their way through the locks.

You may slow them down, but in the end it will be accessed.

There are several other viable approaches, but if you are relying on a password to lock the OS down, to protect you, forget it.

Winged