

Re: Is messages showing a hack attempt?

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.misc/2005-08/2226.html>

From: Dances With Crows (danSPANceswitTRAPhcrows_at_gmail.com)

Date: 08/23/05

Date: Tue, 23 Aug 2005 15:22:34 -0500

On 23 Aug 2005 12:54:28 -0700, news@celticbear.com staggered into the Black Sun and said:

> *Unruh wrote:*

>> *Wipe yur system and then reinstall. Then install all of your distro*

>> *updates (or get a new system) Why are you running ftp?*

> *Because we have a lot of customers who have to upload files, and*

> *they're ordinary people who aren't savvy enough to know how to use*

> *SFTP.*

What the hell? <http://winscp.sourceforge.net/>; anyone who's ever used a program like WS_FTP can figure WinSCP out in less than 5 minutes. This does sort of require that the users have brains, though, and you know how well that assumption works out....

>> *>that stores the data locally for later retrieval. How do I check for*

>> *>such things?!*

>> *you don't. You wipe and reinstall.*

> *That seems a bit [like] overkill?*

"It's overkill, but you can never have too much overkill." I can't say for sure what's going on, but Unruh's "wipe and reinstall" statement is the **safest** way to go if you think you've been r00ted by a script-kiddy. It's also really annoying, but it is safe.

> *Besides, not as easy as that. We have gigs of customer files and huge database files. And a setup of ImageMagik, GhostScript, and PDFLib that takes about a day to install and configure.*

? A **day**? Installing ImageMagick and Ghostscript should take at most 15 minutes. PDFLib may take longer if you're using the non-Free parts of that library.

> *But then, going down because of a hacker certainly isn't better...but if there's an alternative to wiping and reinstalling...*

Figure out whether it's a script-kiddy who's actually done some damage to the system /+ gained account access or not. This will probably require that you find someone who's more experienced than you are and

comp.os.linux.misc: Re: Is messages showing a hack attempt?

have her look at the whole system.

Whether or not you've been compromised, *chroot your FTP/SCP users* if possible. That drastically limits the amount of damage they can do if an account or several gets compromised.

```
--  
Matt G|There is no Darkness in Eternity/But only Light too dim for us to see  
Brainbench MVP for Linux Admin /      mail: TRAP + SPAN don't belong  
http://www.brainbench.com /      "He is a rhythmic movement of the  
-----/      penguins, is Tux." --MegaHAL
```