

Re: Urgent!!! My computer seems to be hacked, pls HELP!!!

Re: Urgent!!! My computer seems to be hacked, pls HELP!!!

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2006-09/msg00097.html>

- *From:* Randy Yates <yates@xxxxxxx>
 - *Date:* Fri, 15 Sep 2006 02:13:50 GMT
-

Grant <bugsplatter@xxxxxxx> writes:

On Thu, 14 Sep 2006 23:20:22 GMT, Randy Yates <yates@xxxxxxx> wrote:

Ayaz Ahmed Khan <ayaz@xxxxxxxxxxxxxxxx> writes:

"René Berber" typed:

Todd H. wrote:

Yup. It's the only way to get back to a known state. Wiping and reinstalling from original media.

But that's not needed, you can find which process is using that particular port and kill it (use lsof). Then run a rootkit detection and/or anti-virus detection to try to find out where that process came from (there are several to choose from). Before that I would harden ssh access, no access except your user.

Reinstalling (and rebuilding) a system is far easier and quicker than figuring out how deep and thorough the compromise is and cleaning the system to some reasonable extent.

Re: Urgent!!! My computer seems to be hacked, pls HELP!!!

Re: Urgent!!! My computer seems to be hacked, pls HELP!!!

If the OP's like me, they are loathe to do this not for the basic OS install, but for the dozens or perhaps hundreds of other upgrades/applications/tweaks that they've performed since they first installed their OS.

So?

```
tar cvzf ../backup-config.tar.gz /etc /boot/config-*
```

Ha! And you think that's all there is to it? What about all the libraries and sym links strung all over heck?

Wipe OS partition (6Ps)

6Ps?

re-install OS, unpack backup-config to /tmp
and cherry pick custom .conf files

Oh yeah – that's going to be a picnic. I just did a count in my /etc and I have 405 configuration files.

—> take me less than an hour to

reinstall router with this technique.

I'm happy for you, Grant. Really. But I don't think that would be the case for me.

Reminds me, take a backup now ;)

Always a good idea.

If i had to re-install, it would probably chew up a week of my time to reconfigure everything back just the way it was.

That's just plain pessimistic or bad planning.

Re: Urgent!!! My computer seems to be hacked, pls HELP!!!

Re: Urgent!!! My computer seems to be hacked, pls HELP!!!

And I think you're being optimistic.

If you have separate
/home and /usr/local partitions, replacing the OS is a snap...

Although I couldn't name a specific one, I bet there are more than a few local apps that install themselves in /usr/bin and whatever other non-standard locations, and they don't ask the installers permission for it.

I've been wondering lately if there's some God-send utility that would track installs for the purpose of alleviating the pain of such reinstalls.

—
% Randy Yates % "She's sweet on Wagner—I think she'd die for Beethoven.
%% Fuquay-Varina, NC % She love the way Puccini lays down a tune, and
%% % 919-577-9882 % Verdi's always creepin' from her room."
%% % <yates@xxxxxxxx> % "Rockaria", *A New World Record*, ELO
<http://home.earthlink.net/~yatescr>

Re: Urgent!!! My computer seems to be hacked, pls HELP!!!