

comp.security.ssh: Re: My Linux server got hacked last night -- please help!

Re: My Linux server got hacked last night -- please help!

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-11/0207.html>

From: Gandalf Parker (gandalf_at_most.of.my.favorite.sites)

Date: 11/30/04

Date: Tue, 30 Nov 2004 02:47:59 GMT

sarahd00d@yahoo.co.uk (sarah chang) wrote in
news:24d1fc75.0411291116.57cfad5b@posting.google.com:

> *I can't chmod or chown these files, even as root.*

Their scripts use chattr to lock the files from actions.

If I remember right its

chattr -i (file)

to change it back.

> *I'd appreciate any advice on*

> *1) How to cleanse my system*

> *2) How to avoid this type of attack in future.*

>

> *Right now I've powered off the server. I'll reboot using a RedHat*

> *install CD in rescue mode. Does anyone know how to force RedHat to*

> *reinstall all packages without repartitioning my hard drive?*

SSH attacks are getting common. I never get anything against my telnet or ftp anymore.

I could tell you how to clean your system but are you SURE you want to?

Its rarely recommended and the results are always questionable.

Gandalf Parker

-- email me

Gandalf@Community.Internet

(without the Inter of course)