

## RE: Linux hacked

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-10/0448.html>

---

**From:** Randori ([randori82\\_at\\_hotmail.com](mailto:randori82_at_hotmail.com))

**Date:** 10/21/04

To: <[security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)>

Date: Thu, 21 Oct 2004 16:05:16 -0500

Good advice from everyone. Sounds like you'd have a good idea of what's going on. For the future, for a better understanding of your system integrity, grab Tripwire. Awesome program that will check the integrity of your system per your configuration. [www.tripwire.org](http://www.tripwire.org) is where you can find the GNU one. I've been using the commercial version for about a year with great success, and will be getting Tripwire Certified over the Xmas break.

The GNU version will tell you what files have been changed (granted that it's been installed on a clean system), and as long as you keep a read-only copy of your database to compare to (dvd or possible network drive with non-write priv's), Tripwire won't get compromised.

There's one known exploit out there for the GNU version dealing with a buffer overflow in the e-mail option. I'd suggest not using the e-mail.

Best of luck rebuilding...been there...done that.

Andre Derek Protas  
Security Engineer | Electus Solutions  
[www.electussolutions.com](http://www.electussolutions.com)

-----Original Message-----

From: xyberpix [<mailto:xyberpix@xyberpix.com>]

Sent: Thursday, October 21, 2004 3:21 AM

To: Nicholson, Dale

Cc: [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)

Subject: Re: Linux hacked

Hi Dale,

To find out what kernel version you are running, type "uname -a" without the comments of course :-). That will give you a wealth of information.

As for tools to check for rootkits, one of my fav is chrootkit, do a google for it, and you'll find it, works really well.

Also, what exactly did the history file show, can you paste it into a mail for us to have a look at as well as the uname -a output, may make things easier to decipher.

RE: Linux hacked

## SecurityFocus BASICS: RE: Linux hacked

Also you say that to get in you have to boot from a CD, what happens if you don't? As the kiddie may have just messed around with your lilo.conf or grub.conf files, and that can be remedied quite easily.

If you need any help on this one, either mail me on the list, which may be better as then you can get other people's opinions on this as well, or off the list if you'd prefer.

xyberpix

On Wed, 20 October, 2004 5:52 pm, Nicholson, Dale said:

- > *First let me say I'm a security novice. Please bear with me.*
- >
- > *My home linux (gentoo) machine was hacked last Thursday. Installed active*
- > *on the box was ssh, apache, php 5, and a squirrel mail. Iptables was set up*
- > *for a firewall. The box was set up as a web server with a number of*
- > *websites and about 35 email accounts (separate passwords for the mail than*
- > *the user accounts on the box).*
- >
- > *I'm guessing it was some sort of script kiddie if the names taking credit*
- > *for the hack in the hidden folders I found are any indication. I did some*
- > *research on the person taking credit and found all kinds of information on*
- > *him, he's an 18yr old kid in Germany. I doubt he is very knowledgeable or*
- > *he would not have alerted me to the intrusion by somehow locking out all*
- > *accounts from the machine.*
- >
- > *To get in I have to boot from cd and chroot in. Everything I've tried has*
- > *been unsuccessful in getting root back.*
- >
- > *I found a hidden directory /var/tmp/.tmp that has a bunch of directories*
- > *under it with names like +\_01\_+++++++HaXorEd by ... and*
- > *+\_05\_+++++++Movies+++++++....*
- >
- > *I unplugged the machine from the internet shortly after the hack and can*
- > *find no evidence of any uploads. I do see that the person somehow was*
- > *able*
- > *to break root. I was only able to find the hidden directories because the*
- > *person forgot to clean up root's history file where I found the command*
- > *used*
- > *to create the them. The box was set up to not allow remote login of root*
- > *via ssh but you could su in once logged in as one of three users.*
- >
- > *I'm a novice at security and had been depending on my system admin to keep*
- > *the box up to date. He tells me he's been doing an emerge world every*
- > *week*
- > *but I don't know how to tell.*
- >
- > *Can someone help me with where to get a listing of everything I have*
- > *installed and the versions? I can't remember if the kernel is a 2.4 or*
- > *2.6*
- > *but I think it's 2.6. Plus I know there have been problems with ssh in*
- > *the*

RE: Linux hacked

SecurityFocus BASICS: RE: Linux hacked

- > *past but I don't know which versions have problems and I'm not sure how to*
- > *find out what version I'm running. I'm kind of stuck as my sys-admin*
- > *normally handles these things but he cannot ssh in to the box without me*
- > *first fixing the problem since he lives 13 hours from me (the box is in my*
- > *basement).*
- >
- > *Also, I need something that can detect root kits etc. on linux. I've*
- > *heard*
- > *knoppix mentioned as having good tools on this list for an example, but I*
- > *wouldn't know what tools to use for this particular case.*
- >
- > *This is what I tried so far:*
- > *I logged in using a boot CD, mounted the hard disks, chrooted in, blanked*
- > *out the root password in the /etc/shadow file, changed the root password,*
- > *rebooted and tried to log in normally. This did not work. I also checked*
- > *that the correct users were in both /etc/passwd and /etc/shadow.*
- >
- > *Note that both the email and websites were still working despite not being*
- > *able to log in, although not now of course since I unplugged the ethernet*
- > *cable.*
- >
- > *Any comments/assistance will be greatly appreciated.*
- >

--

For security and Opensource news check out:  
<http://xyberpix.demon.co.uk>