

## Re: Linux hacked

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-10/0419.html>

---

**From:** Casper the Friendly Ghost ([casper\\_at\\_camelot.homelinux.com](mailto:casper_at_camelot.homelinux.com))

**Date:** 10/21/04

Date: Wed, 20 Oct 2004 23:04:45 -0400

To: security-basics@securityfocus.com

To get back into your account you want to use, at the boot manager prompt (lilo/grub)  
init=/bin/bash

For example, if you use lilo and have 'lin' as the name to access your linux you would have to press ESC and then write at the prompt

```
lin init=/bin/bash
```

In grub you would have to edit the command and add init=/bin/bash after the kernel option

After it boots up (it will be really fast – no services) you want to do

```
mount -o remount,rw /dev/hd* (whichever your / partition is)
```

```
then you can just do passwd root  
enter the new password  
confirm
```

```
do umount /dev/hd* (the one you just mounted above)
```

hit the 3 magic buttons (Ctrl+Alt+Del)

boot normally and you should be able to login as root with your new password

My suggestion for a good rootkit finder is chkrootkit. It's the one I used for testing different rootkits and it found ~90% of them

As for what else he changed, there's no easy way to see. First thing you could do is a

```
netstat -ap -A inet
```

this will show you all your open ports and the daemons listening to them. If you see anything suspicious do some more research.

## SecurityFocus BASICS: Re: Linux hacked

Also, make copies of your logs, preferably on a different machine, and look into them deeply. Also do a lastlog and last -20 (or more) root to see if you find anybody connected from a suspicious place or anything else suspicious.

Make sure you do an emerge sync and emerge --avuU world to be up-to-date with all the packages (chances of a script kiddie to get in would be less likely with newer/patched software).

Also since you have more than a few users make sure your system wasn't compromised through THEM. A lot of times users have weak password and crackers break in their account and from there they do more damage.

Good luck!

-cos

P.S. To find out which kernel you're running do uname -r

On Wednesday 20 October 2004 12:52, Nicholson, Dale wrote:

> *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.*

Re: Linux hacked

## SecurityFocus BASICS: Re: Linux hacked

- >
- > *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*
- > *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.*

--

In Linux We TrUsT !