

RE: Linux hacked

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-10/0493.html>

From: Nicholson, Dale (*DNicholson_at_APACMail.com*)

Date: 10/25/04

To: "Security Basics[List]" <security-basics@securityfocus.com>

Date: Mon, 25 Oct 2004 08:57:33 -0500

Thanks all for your support. The box remains offline for now but based on all of the good ideas provided on this list I have decided to start from scratch. I don't have the time or resources to ensure the machine is clean. Tonight I'm going to format the hard disk and start rebuilding.

Does anyone have some good ideas on how to protect the machine while it's getting setup? How about ipchains rules? The way I built the machine before took almost a week to download and compile everything and I'm paranoid about getting re-hacked while this process is going on.

One of the biggest differences from what I had set up before is I plan to install tripwire. Does anyone have a script already written to get new checksums when you upgrade a piece of software? How about experience setting up tripwire? I'm not sure how to tell it which files need to be looked at and which don't. I'm guessing this is a RTFM type of thing, but if someone has a good script already written that I could use as an example I would appreciate the help.

Dale

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

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

Sent: Sunday, October 24, 2004 6:55 AM

To: miles@mstevenson.org

Cc: Security Basics[List]; Nicholson, Dale

Subject: Re: Linux hacked

I'd just like to say that it's for mail's like this one below that I am glad that I joined up to this list. Worthwhile info, no BS, and people willing to help.

Dale, I'd also like to help out where I can on this one, feel free to get hold me off list as well. I do have a load of Linux experience, and security, so feel free.

Thanks to all for the help that I've received from you in the past as well.

xyberpix

RE: Linux hacked

SecurityFocus BASICS: RE: Linux hacked

On Thu, 2004-10-21 at 18:16, Miles Stevenson wrote:

> Dale,

>

> *First of all, I'd like to point out that you are asking all the right questions, and that I'm impressed by how far you've come without having any sysadmin experience.*

>

> *Contrary to the advice that you have been given thus far, I'm hoping that you*

> *have not interacted with the system at all so far, aside from unplugging it*

> *from the network and/or shutting it down. If this is the case, then don't.*

> *The first thing you want to do is take a forensically sound "image" of your*

> *system, from which you can work. This way, you can work from the image, and*

> *not the real system in trying to determine what happened and how you were attacked. I think the best approach, is to boot your system with a separate*

> *bootable CD, such as Knoppix STD, Phlak, or another forensics-focused bootable linux OS. After you boot up into the OS running from CD, you can connect the system back to your internal network. You can then use the dd and*

> *netcat utilities, to take a perfect forensic snapshot of your system, and send that snapshot to another system on the network.*

>

> *Instead of explaining how to do this, I will point you to another resource in*

> *order to save space:*

> *http://www.rajeevnet.com/hacks_hints/os_clone/os_cloning.html*

>

> *Once you have a forensic copy of your system, you can now safely continue your*

> *investigation of what went wrong and why. You can also choose to completely*

> *wipe and rebuild your system if that is the most appropriate course of action*

> *for you, and you decide to investigate later. But, the longer you wait to*

> *perform an investigation, the more difficult that investigation is going to*

> *be. Choose carefully.*

>

> *The most important thing for you to keep in mind here, is that once your*

> *system has been compromised, you can *no longer trust ANY of the data on your*

> *system*. Netstat might lie to you. Your kernel might lie to you. In essence,*

> *the attacker could have made any alterations to your systems to change the*

SecurityFocus BASICS: RE: Linux hacked

> way it behaves or what it reports to you. You can't trust the logs, you can't

> even trust the output of the commands. This is why you have to run these

> tools from a separate, TRUSTED source, such as from a read-only forensic CD

> like Phlak. Don't trust the "ls" command on the hacked system, but DO trust

> the "ls" command on your forensics disk. This is VERY important.

>

> This process is going to get more and more complicated as you continue, and is

> best handled by someone with experience. If you can get to this point, and

> then hand things over to someone else, I recommend it. If you are unable to

> do that, then I am willing to help you as much as I can. But I think you

> should first get to this point of taking a forensic snapshot of your system,

> and obtaining a bootable forensic cd (I personally like Phlak, but there are

> many others) that you can use as a tool. Once you get to this point, let me

> know your situation, and we can continue. If I cover too much right now, not

> only will I run the risk of "information overload", but I also have to start

> making assumptions about your system in order to recommend how to proceed,

> and these assumptions can be disastrous, even when made by those of us that

> know what we are doing. You can contact me off-list if you prefer.

>

> Good luck.

>

> On Wednesday 20 October 2004 12:52 pm, 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

RE: Linux hacked

SecurityFocus BASICS: RE: Linux hacked

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

> > *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,*

RE: Linux hacked

SecurityFocus BASICS: RE: Linux hacked

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 Open Source news:

<http://xyberpix.demon.co.uk>