

Re: Possible compromise ?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-01/0112.html>

From: Peter Rosa (*prosa_at_pro.sk*)

Date: 01/27/04

To: <freebsd-security@freebsd.org>

Date: Tue, 27 Jan 2004 21:35:15 +0100

Sorry, my syslog is not configured to save auth.* info :-(
I did not read syslog.conf carefully...

PR

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

From: "Mark Ogden" <ogden@eng.utah.edu>

To: "Peter Rosa" <prosa@pro.sk>

Cc: <freebsd-security@freebsd.org>

Sent: Tuesday, January 27, 2004 9:28 PM

Subject: Re: Possible compromise ?

> *Peter Rosa on Tue, Jan 27, 2004 at 09:23:45PM +0100 wrote:*

> > *OK, sorry for unclear previous message.*

> >

> > *In the past, one man taught me the FreeBSD basics and also installed my*

> > *gateway. In that time, I was not able to install and setup FreeBSD by*

> > *myself. He left there some holes – e.g. open virtual consoles, unset*

> > *firewall, etc. As the time went, I learned a lot about Unixes and*

> > *FreeBSD*

> > *and I tried to setup my own firewall, install and setup some programs*

> > *(with*

> > *big help of this and Questions lists, manpages and other books).*

> >

> > *When I tried to setup more security on that system, except other things,*

I

> > *disabled all virtual tty's, because there is no need to connect to this*

> > *machine remotelly (it's located 5 steps from my desk). In the past, that*

man

> > *connected to my system remotelly from various IPs.*

> >

> > *Now, when I cat /var/log/lastlog, in the very bottom of the file, I can*

read

> > *some connects from remote machines to tty0 and tty1.*

>

> *take a look at the /var/log/auth.log, it will show you everyone that*

> *remote connected and was denied.*

FreeBSD–Security: Re: Possible compromise ?

>
> *–Mark*
>
> *>It's impossible for*
> *> me to retrieve connection dates from that file. Of course, I read man*
last,
> *> man wtmp, etc., but there is nothing about /var/log/lastlog file.*
> >
> *> May be, that lines was added in the deep past, when the machine was*
open.
> *> But may be, it was done in few previous days...*
> >
> *> I know, if my machine was compromised, it is impossible to believe in*
> *> anything on that machine (also kernel, sources). So, are there some*
other
> *> ways to get information about connection dates?*
> >
> *> Peter Rosa*
> >
> > _____
> *> freebsd-security@freebsd.org mailing list*
> *> <http://lists.freebsd.org/mailman/listinfo/freebsd-security>*
> *> To unsubscribe, send any mail to*
"freebsd-security-unsubscribe@freebsd.org"
>

freebsd-security@freebsd.org mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-security>
To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"