

Re: Did i get hacked?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-05/0012.html>

From: Tony Meman (*none_at_superig.com.br*)

Date: 05/02/03

Date: Fri, 02 May 2003 17:13:54 -0300

To: freebsd-security@freebsd.org

Hi Mario,

well any strange activity in the system should be taken in consideration so I really think you should audit your system.

You said the reboot occurred at 0:32am, its a good idea to search for files modified around that time. You could use the binary of some trustable system just in case /usr/bin/find got trojaned.

You said you did not find anything in the logs, they could have been erased, use chkrootkit to verify if there are wtmp/lastlog entries that may have been erased. Chkrootkit is a pretty nice utility and will be able to tell you if there're hidden processes running on the system (comparing output from ps with /proc entries) and search for well-known rootkits. The tool is not perfect but helps a lot, check it out:

<http://www.chkrootkit.org>

Good luck,

--

Marcello Azambuja

mario wrote:

```
> hello,
> i have a FreeBSD 4.8-PRERELEASE #0 that i use as a gateway / nat box for
> my home.
> It also acts as a dns / mail server to the outside world.
> I'm using ipf and basically filter for bogus networks on the way in
and out.
> I allow everything out keeping state,
> and allow this in:
> pass in proto icmp from any to any icmp-type squench group 200
> pass in proto icmp from any to any icmp-type timex group 200
> pass in proto icmp from any to any icmp-type paramprob group 200
> pass in quick proto tcp from any port > 1023 to any port = smtp group 200
> pass in quick proto udp from any port > 1023 to any port = domain
group 200
>
> on these ports i run qmail and tinydns
>
> i was a bit sloppy by leaving these w/out a password
```

FreeBSD-Security: Re: Did i get hacked?

```
> figuring they can't login anyway.
>
> gtinydns::nnnn:nnnn::0:0:tinydns:/nonexistent:/sbin/nologin
> gdnslog::nnnn:nnnn::0:0:dns logger:/nonexistent:/sbin/nologin
> gaxfrdns::nnnn:nnnn::0:0:zone transfer:/nonexistent:/sbin/nologin
>
> I've changed this now though i'm still not sure about the implications of
> this.
> Also i'm not running tripwire or any other intrusion detection.
>
> Here's my problem. When i got up this morning, i noticed that the box
> rebooted
> at 0:32 this morning. I have 3 other computers that did not reboot
leaving me
> to believe there was no power failure. I looked through all the logs
seeking
> clues as to what happened. Hardware failure? It is an old p-75 and
the hard
> drive has had issues in udma-2 but has been doing fine for months in pio4
> mode.
> I also have a cron job at 0:30 to move the apache logs to a tmp file
restart
> apache sleep 5 minutes and then move the tmp file somewhere where
newsyslog
> can catch it. According to the log
```