

Did i get hacked?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-05/0009.html>

From: mario (mario_at_schmut.com)

Date: 05/02/03

Date: Fri, 2 May 2003 12:14:38 -0700 (PDT)

To: <freebsd-security@freebsd.org>

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

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 logs, apache restarted fine but the tmp files never made it anywhere. Again nothing useful in them either.

FreeBSD–Security: Did i get hacked?

So if this was a hardware failure (harddrive), then any kernel panic statements probably would not make it to the harddrive. So it would be hard to tell. My question is, what if i got hacked? Would there be anyway to find out despite me being totally unprepared for this?

That question really messes with my head.
Any pointer and/or clue stick treatments would be greatly appreciated.

thanx

mario;>

Do you schmut!?
<http://www.schmut.com>

For a real web site try:
House Of Sites
<http://www.HouseOfSites.net>
Email: mario@HouseOfSites.net

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"