

Re: Hacked or not appendice

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-06/0031.html>

From: Lupe Christoph (lupe_at_lupe-christoph.de)

Date: 06/12/04

Date: Sat, 12 Jun 2004 16:07:06 +0200

To: Peter Rosa <prosa@pro.sk>

On Saturday, 2004-06-12 at 13:44:45 +0200, Peter Rosa wrote:

> *I must add, there are no log entries after June 9, 2004. "LKM" message first*
> *appeared June 8, 2004, after this day, there is nothing in /var/messages,*
> */var/security*

Check if your syslog deamon is running. Also try to log something from the command line with logger.

> *How could I look for suspicious LKM module ? How could I find it, if the*
> *machine is hacked and I can not believe "ls", "find" etc. commands ?*

Dunno. I've turned off modules on all my FreeBSD machines. IIRC, the way to check binaries is to "make buildworld", install somewhere else and compare. Of course, you should not build on a suspect machine.

Have you turned on securelevel?

HTH,
Lupe Christoph

--

```
| lupe@lupe-christoph.de | http://www.lupe-christoph.de/ |  
| "... putting a mail server on the Internet without filtering is like |  
| covering yourself with barbecue sauce and breaking into the Charity |  
| Home for Badgers with Rabies. | Michael Lucas |
```

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"