

Re: How to monitoring activity on a card?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-03/0059.html>

From: Andrew Riabtsev (*resident_at_b-o.ru*)

Date: 03/03/04

Date: Wed, 3 Mar 2004 18:23:01 +0300

To: FreeBSD Security List <freebsd-security@freebsd.org>

İðèââð Francisco,

Wednesday, March 3, 2004, 12:51:15 PM, you wrote:

FR> My setup 4.9 stable with IPFW. Machine acts as gateway for two machines.

FR> What are my options on monitoring activity on my external card?

FR> This morning I noticed my DSL modem activity light is blinking non-stop.

FR> Looking at /var/log/ don't see anything suspicious.

FR> I feel tempted to add "log" to all my ipfw pass rules, but wonder if there

FR> isn't a better way.

FR> I am mostly concerned there is either some kind of attack going on or

FR> somehow the machine was hacked and it's running something it's not

FR> supposed to.

You also may try sniffit – shows current tcp/udp streams in curses windows. Easy to undestend from where to start searching.

--

Ñ íâèèó+øèìè îîæâèâíèÿìè,

Andrew

mailto:resident@b-o.ru

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"