

How to monitoring activity on a card?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-03/0055.html>

From: Francisco Reyes (lists_at_natserv.com)

Date: 03/03/04

Date: Wed, 3 Mar 2004 09:51:15 +0000 (GMT)

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

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

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

This morning I noticed my DSL modem activity light is blinking non-stop. Looking at /var/log/ don't see anything suspicious.

I feel tempted to add "log" to all my ipfw pass rules, but wonder if there isn't a better way.

I am mostly concerned there is either some kind of attack going on or somehow the machine was hacked and it's running something it's not supposed to.

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"