

Re: Best way to filter "Nachi pings"?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-10/0085.html>

From: Peter Pentchev (roam_at_ringlet.net)

Date: 10/27/03

Date: Mon, 27 Oct 2003 13:43:10 +0200
To: Jason Stone <freebsd-security@dfmm.org>

On Mon, Oct 27, 2003 at 03:12:48AM –0800, Jason Stone wrote:

[snip]

> > > *Filtering packets by length on the other hand is a very nice feature*

> > > *to have.*

>

> > > *As it happens, ipfw[2] does this anyway.*

>

> *Yes, ipfw2 (ie, on fbsd-5 boxes) has an "iplen" option that you can put in*

> *the body of your rule. From the manpage:*

>

> *iplen len*

> *Matches IP packets whose total length, including header and*

> *data, is len bytes.*

>

> *However, this isn't going to help most people with 4.x systems, so their*

> *best option is probably still to block all pings.*

Actually, ipfw2 has been backported to –STABLE for quite a while, and the iplen keyword has been present in –STABLE's src/sbin/ipfw/ipfw2.c ever since ipfw2 was MFC'd (about July 2002). You may want to take a look at the ipfw(8) manual page, and specifically (as recommended at the top of the manpage) the 'USING IPFW2 IN FreeBSD–STABLE' section to see how you can actually use ipfw2 and 'iplen' in –STABLE :)

G'luck,

Peter

--

Peter Pentchev roam@ringlet.net roam@sbnd.net roam@FreeBSD.org

PGP key: <http://people.FreeBSD.org/~roam/roam.key.asc>

Key fingerprint FDBA FD79 C26F 3C51 C95E DF9E ED18 B68D 1619 4553

If there were no counterfactuals, this sentence would not have been paradoxical.

- application/pgp–signature attachment: [stored](#)