

Re: FIN_WAIT_[1,2] and LAST_ACK

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2004-04/0061.html>

From: Chuck Swiger (cswiger_at_mac.com)

Date: 04/06/04

Date: Tue, 06 Apr 2004 12:09:11 -0400

To: Brandon Erhart <berhart@ErhartGroup.COM>

Brandon Erhart wrote:

- > *They are not timing out after 2MSL. I set my MSL to the lowest possible*
- > *setting (10) as to make TIME_WAIT connections disappear. The*
- > *FIN_WAIT_[1,2] and LAST_ACK seem to be sticking around for a while.*
- > *However, not ALL of them stick around for a "long time"(more on this in*
- > *a sec) -- e.g., after I kill my program, and say I've got 6,000*
- > *connections sitting in FIN_WAIT_[1,2] or LAST_ACK, about a minute*
- > *afterwards 90% of them have disappeared. There seem to be a few stick*
- > *around for as long as 30 minutes or more, and in fact, a few of them*
- > *stuck around until I rebooted the computer.*

People are starting to set up honeynets or tarpits which will "persist capture" TCP connections "forever" by responding with a zero window size. Such things slow down the spread of worms/virii effectively, but they also make nmap or other scanning tools (perhaps Brandon's) unhappy.

It might be interesting to retest one of these stuck connections by hand and see whether the remote machine generates a normal response.

--

-Chuck

freebsd-net@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-net>

To unsubscribe, send any mail to "freebsd-net-unsubscribe@freebsd.org"