

Re: Limiting closed port RST response from 381 to 200 p

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2002-04/8952.html>

From: Mike Silbersack (silby@silby.com)

Date: 04/16/02

Date: Mon, 15 Apr 2002 20:27:53 -0500 (CDT)

From: Mike Silbersack <silby@silby.com>

To: Andrew Johns <johnsa@kpi.com.au>

On Tue, 16 Apr 2002, Andrew Johns wrote:

> *Actually Sheldon I think that's a great idea – helps with*
> *syslog DoS somewhat as well. Anybody else care to contemplate*
> *making it either a default or sysctl (ICMP_BANDLIMIT_DOSLIMIT?)*
>
> AJ

As the messages are limited to once per second, it's not really a syslog DoS. Just an annoyance, as Sheldon mentions. I think that seeing the rate is useful, although having a sysctl which allows one to switch over to the format Sheldon uses could be useful. I have considered MFCing the sysctl which disables the display of these messages and making off the default, given that many people seem to panic when seeing "limiting blah".

As the rate of incoming packets seems pretty steady, I'd wager that Christoph is being scanned by nmap or some similar tool. A true DoS would probably involve a much higher packet rate.

Mike "Silby" Silbersack

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message