

Re: Strange pings from 127.0.0.1

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-06/0180.html>

From: Timothy Schwimer (*tschwimer_at_hotmail.com*)

Date: 06/18/04

To: talukdar_m@subway.com, security-basics@securityfocus.com

Date: Fri, 18 Jun 2004 02:26:07 +0000

Not yet. Doesn't sound like you're having the same issue though. Mine is all ICMP traffic, all sourced from the loopback, but destined to several different host IP's. In addition, the source and dest MAC are always the same regardless of the IP's.

I'm fairly certain that I've got a compromised host, but with the source IP being a loopback, I've got no way of deducing which host.

>From: Murad Talukdar <talukdar_m@subway.com>

>To: Tim Schwimer <tschwimer@hotmail.com>, security-basics@securityfocus.com

>Subject: Re: Strange pings from 127.0.0.1

>Date: Fri, 18 Jun 2004 09:43:07 +1000

>

>I've been getting this on my router logs saying that the tcp got dropped.

> Source:127.0.0.1, 80, WAN – Destination:210.80.144.150, 1912, LAN –

>'Suspicious TCP Data'

>

>Did you work out what it was with the pings? Not sure if it's similar or

>not.

>

>Murad Talukdar

>

>

>----- Original Message -----

>From: "Tim Schwimer" <tschwimer@hotmail.com>

>To: <security-basics@securityfocus.com>

>Sent: Sunday, June 13, 2004 5:24 PM

>Subject: Re: Strange pings from 127.0.0.1

>

>

>> In-Reply-To: <GAEPLDFDDGJLBGAABCNKENBCMAA.gg@stober.mailsnare.net>

>>

>> I started seeing the same thing on my DMZ segments this Friday afternoon

>at about 4:00pm (figures, huh??). Anyway, I was wondering what you found

>out

>about this. Any insight would be appreciated.

>> Thanks,

>> T

SecurityFocus BASICS: Re: Strange pings from 127.0.0.1

> > >Received: (qmail 20239 invoked from network); 14 May 2004 15:58:54
> -0000
> > >Received: fro