

Re: Strange pings from 127.0.0.1

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-06/0248.html>

From: Tim Schwimer (*tschwimer_at_hotmail.com*)

Date: 06/24/04

Date: 24 Jun 2004 16:23:49 -0000
To: security-basics@securityfocus.com

('binary' encoding is not supported, stored as-is) In-Reply-To:
<20040618220642.GA17943@ranjeet-pc2.zultys.com>

Thanks for the suggestions. I'll look into seeing if I can't trace down the infected device by assuming any target host is not the source.

As for the MAC, it just doesn't make any sense to me. I know that they are DEC addresses, and that we do not have any devices with DEC NIC's. Nor do they show up in the CAM table on the switch. In addition, port security is turned on for every active port on the switch. One would think that a packet with an invalid source MAC seen by the switch would cause a port violation and shut the port down.

One of the problems I'm having is the code on the switch is very old. I've been trying to get it updated but am limited being that it's a 24x7 production environment (that and the fact that no one else seems to care about the issue!!!). So I am not convinced that the issue is not being exacerbated by some anomolous behavior of the switch. Strange part about it though is that while I see the traffic on multiple segments, I do not see it on every port in those segments.

In addition, while I see it both tx and rx on all of my FW ports, tcpdump on the FW indicates that it is not seeing any of the traffic at all. Likewise, rules on the FW to block all of the traffic do not get any hits at all. Keep the thoughts coming guys. I appreciate it.

-t

>Received: (qmail 13316 invoked from network); 22 Jun 2004 15:45:39 -0000
>Received: from outgoing.securityfocus.com (HELO outgoing3.securityfocus.com) (205.206.231.27)
> by mail.securityfocus.com with SMTP; 22 Jun 2004 15:45:39 -0000
>Received: from lists.securityfocus.com (lists.securityfocus.com [205.206.231.19])
> by outgoing3.securityfocus.com (Postfix) with QMQP
> id 2014A237F39; Tue, 22 Jun 2004 03:00:50 -0600 (MDT)
>Mailing-List: contact security-basics-help@securityfocus.com; run by ezmlm
>Precedence: bulk
>List-Id: <security-basics.list-id.securityfocus.com>
>List-Post: <mailto:security-basics@securityfocus.com>
>List-Help: <mailto:security-basics-help@securityfocus.com>
>List-Unsubscribe: <mailto:security-basics-unsubscribe@securityfocus.com>
>List-Subscribe: <mailto:security-basics-subscribe@securityfocus.com>
>Delivered-To: mailing list security-basics@securityfocus.com
>Delivered-To: moderator for security-basics@securityfocus.com
>Received: (qmail 1849 invoked from network); 19 Jun 2004 00:21:45 -0000
>Date: Fri, 18 Jun 2004 15:06:42 -0700

SecurityFocus BASICS: Re: Strange pings from 127.0.0.1

>From: Ranjeet Shetye <ranjeet.shetye2@zultys.com>
>To: security-basics@securityfocus.com
>Subject: Re: Strange pings from 127.0.0.1
>Message-ID: <20040618220642.GA17943@ranjeet-pc2.zultys.com>
>Mail-Followup-To: security-basics@securityfocus.com
>References: <BAY8-F267zD5J47OksZ00087f7d@hotmail.com>
>Mime-Version: 1.0
>Content-Type: text/plain; charset=us-ascii
>Content-Disposition: inline
>In-Reply-To: <BAY8-F267zD5J47OksZ00087f7d@hotmail.com>
>User-Agent: Mutt/1.5.6i
>
>
>consider a packet of the type
>
>Eth_DST=Eth_A
>Eth_SRC=Eth_B
>Eth_Type=IP
>IP_Src=127.0.0.1
>IP_Dst=IP_D
>
>On Linux – packets from localhost to a local IP dont make it onto the
>network. Assuming the same to be the case on Windows, any target hosts
>(IP_D) that you see ICMPs for, are probably NOT the origin of THIS packet.
>This might help you narrow the possible sources of the traffic.
>
>Next, (assuming non-promiscuous mode of operation by the NIC) I fail to
>understand how the author of this attack intends to reach his/her targets,
>if the dest MAC addresses are fake! I might be missing something obvious,
>so if someone can point it out to me, that would be great. thanks.
>
>Instead of an attack, it might be that you have someone on your network
>who is learning socket or libnet programming, and is testing his/her
>networking coding skills on the corporate network. That might explain
>the non-existant destination MAC addresses – which I admit again, don't
>make a lot of sense to me.
>
>**Unless**, some kind of an ARP-poisoning scheme is being executed,
>so that switches are forced to forward all traffic on all ports cos their
>internal arp tables are messed up.
>
>In which case, maybe you need to lock down the arp tables in your managed
>switches, if you can.
>
>I am very curious about this traffic pattern, please let us know the
>answer once you've resolved it. thanks,
>
>--
>Ranjeet Shetye
>Senior Software Engineer
>Zultys Technologies

SecurityFocus BASICS: Re: Strange pings from 127.0.0.1

>Ranjeet dot Shetye at Zultys dot com

><http://www.zultys.com/>

>

>The views, opinions, and judgements expressed in this message are solely those of
>the author. The message contents have not been reviewed or approved by Zultys.

>

>* Timothy Schwimer (tschwimer@hotmail.com) wrote:

>> 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: <GAEPLEDFDDGJLBGAABCNKENBCMAA.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

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

>> >> >-0000

>> >> >Received: from outgoing.securityfocus.com (HELO

>> >> >outgoing2.securityfocus.com) (205.206.231.26)

>> >> > by mail.securityfocus.com with SMTP; 14 May 2004 15:58:54 -0000

>> >> >Received: from lists.securityfocus.com (lists.securityfocus.com

Re: Strange pings from 127.0.0.1

SecurityFocus BASICS: Re: Strange pings from 127.0.0.1

>> >[205.206.231.19])
>> >> > *by outgoing2.securityfocus.com (Postfix) with QMQP*
>> >> > *id 4018A1437B0; Fri, 14 May 2004 17:53:53 -0600 (MDT)*
>> >> > *Mailing-List: contact security-basics-help@securityfocus.com; run by*
>> > *ezmlm*
>> >> > *Precedence: bulk*
>> >> > *List-Id: <security-basics.list-id.securityfocus.com>*
>> >> > *List-Post: <mailto:security-basics@securityfocus.com>*
>> >> > *List-Help: <mailto:security-basics-help@securityfocus.com>*
>> >> > *List-Unsubscribe:*
>> > *<mailto:security-basics-unsubscribe@securityfocus.com>*
>> >> > *List-Subscribe: <mailto:security-basics-subscribe@securityfocus.com>*
>> >> > *Delivered-To: mailing list security-basics@securityfocus.com*
>> >> > *Delivered-To: moderator for security-basics@securityfocus.com*
>> >> > *Received: (qmail 13781 invoked from network); 13 May 2004 21:45:06*
>> > *-0000*
>> >> > *From: "Marc" <gg@stober.mailsnare.net>*
>> >> > *To: <security-basics@securityfocus.com>*
>> >> > *Subject: Strange pings from 127.0.0.1*
>> >> > *Date: Thu, 13 May 2004 23:55:35 -0400*
>> >> > *Message-ID: <GAEPLDFDDGJLBGAABCNKENBCMAA.gg@stober.mailsnare.net>*
>> >> > *MIME-Version: 1.0*
>> >> > *Content-Type: text/plain;*
>> >> > *charset="iso-8859-1"*
>> >> > *Content-Transfer-Encoding: 7bit*
>> >> > *X-Priority: 3 (Normal)*
>> >> > *X-MSMail-Priority: Normal*
>> >> > *X-Mailer: Microsoft Outlook IMO, Build 9.0.6604 (9.0.2911.0)*
>> >> > *X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1409*
>> >> > *Importance: Normal*
>> >> >
>> >> >
>> >> > *The networked applications I am responsible for have been performing*
>> > *slowly.*
>> >> > *When I tried to run Ethereal on my computer, I found some odd ICMP echo*
>> >> > *request (ping) packets with a source IP of 127.0.0.1, to addresses both*
>> >> > *within our 192.168.1.* network as well as to random Internet addresses.*
>> > *The*
>> >> > *source and destination Mac addresses aren't anything I can associate*
>> > *with*
>> > *a*
>> >> > *computer on our network (and they're not the real Mac address of my*
>> >> > *computer), so I think maybe these packets are spoofed? Could this be*
>> > *some*
>> >> > *sort of virus or DOS attack somewhere within our network? I've haven't*
>> > *seen*
>> >> > *anything quite like this mentioned online anywhere.*
>> >> >
>> >> > *Thanks, Marc*
>> >> >
>> >> >

SecurityFocus BASICS: Re: Strange pings from 127.0.0.1

>> >>
>>

>>-----
>> >> >*Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545*
>> >*off*
>> >> >*any course! All of our class sizes are guaranteed to be 10 students or*
>> >*less*
>> >> >*to facilitate one-on-one interaction with one of our expert*
>> >*instructors.*
>> >> >*Attend a course taught by an expert instructor with years of*
>> >*in-the-field*
>> >> >*pen testing experience in our state of the art hacking lab. Master the*
>> >*skills*
>> >> >*of an Ethical Hacker to better assess the security of your*
>> >*organization.*
>> >> >*Visit us at:*
>> >> >http://www.infosecinstitute.com/courses/ethical_hacking_training.html
>> >>

>>

>>-----
>> >-
>> >> >
>> >> >
>> >>
>> >>
>>

>-----
>> >-
>> >> *Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545*
>> >*off*
>> >> *any course! All of our class sizes are guaranteed to be 10 students or*
>> >*less*
>> >> *to facilitate one-on-one interaction with one of our expert instructors.*
>> >> *Attend a course taught by an expert instructor with years of*
>> >*in-the-field*
>> >> *pen testing experience in our state of the art hacking lab. Master the*
>> >*skills*
>> >> *of an Ethical Hacker to better assess the security of your organization.*
>> >> *Visit us at:*
>> >> http://www.infosecinstitute.com/courses/ethical_hacking_training.html
>> >>

>>

>-----
>> >--
>> >>
>> >>
>> >
>> >
>>
>>

>>-----
>> *Watch the online reality show Mixed Messages with a friend and enter to win*

>> *a trip to NY*

>> <http://www.msnmessenger-download.click-url.com/go/onm00200497ave/direct/01/>

>>

>>

>>

>> *Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off*

>> *any course! All of our class sizes are guaranteed to be 10 students or less*

>> *to facilitate one-on-one interaction with one of our expert instructors.*

>> *Attend a course taught by an expert instructor with years of in-the-field*

>> *pen testing experience in our state of the art hacking lab. Master the*

>> *skills of an Ethical Hacker to better assess the security of your*

>> *organization. Visit us at:*

>> http://www.infosecinstitute.com/courses/ethical_hacking_training.html

>>

>>

>

>

> *Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off*

> *any course! All of our class sizes are guaranteed to be 10 students or less*

> *to facilitate one-on-one interaction with one of our expert instruct*

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off

any course! All of our class sizes are guaranteed to be 10 students or less

to facilitate one-on-one interaction with one of our expert instructors.

Attend a course taught by an expert instructor with years of in-the-field

pen testing experience in our state of the art hacking lab. Master the skills

of an Ethical Hacker to better assess the security of your organization.

Visit us at:

http://www.infosecinstitute.com/courses/ethical_hacking_training.html
