

RE: ICMP (Ping)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-09/0212.html>

From: Tony Kava (securityfocus_at_pottcounty.com)

Date: 09/05/03

To: security-basics@securityfocus.com

Date: Fri, 5 Sep 2003 09:34:46 -0500

You are correct about the kinder and gentler internet. If I had a huge network to deal with I might share your opinion. When the death penalty becomes applicable to those who initiate denial of service attacks perhaps we can all go back to responding to pings. I believe you meant ICMP echo requests (type 8) as replies are type 0 if I recall. My reference to obscurity was the general meaning of that phrase in that one can not expect increased security by simply changing their appearance.

We know why FTP proxying is no longer allowed, but that is a more serious issue. I suppose the RFC could say SHOULD or MAY instead of MUST on the next revision. The kinder and gentler internet is dead, and I believe it has taken this thread with it.

Add another \$0.02 to the pot (which is really adding up between the dollars and euros)

--

Tony Kava

Network Administrator

Pottawattamie County, Iowa

-----Original Message-----

From: Christos Gioran [<mailto:himicos@freemail.gr>]

Sent: Friday, 05 September, 2003 09:13

To: Tony Kava

Cc: security-basics@securityfocus.com

Subject: RE: ICMP (Ping)

IMHO,

Even though it will not solve all your problems, blocking ICMP echo replies (ICMP type 8) from leaving the server is a good idea. Anyone who might want to scan your machine using just a ping sweep will not see you. All other kinds of ping should be available for normal operation as it has been stated at a previous post. Your box will **not** be invisible, just a little harder to find. Still there are Syn scans, NULL, Ack and many more goodies that may tell you off.

That also is a good alternative to ICMP pinging a machine for administrating purposes. A syn ping (using, for instance, nmap) will be enough to see if the machine is alive.

PS. As for RFC compliance, does anyone still support the proxy feature on FTP servers?? No (i hope so) since it poses a great security risk. RFC's were written for a friendly Internet, where hosts would trust each other. That is no longer the case. Times change, so should ther practices we use ;-)

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

my 0.02 euro worth :-)

On Thu, 2003-09-04 at 21:07, Tony Kava wrote:

> I do like your reasoning that others do not generally have a business need
> to ping your hosts, however I still prefer to allow this service not
simply
> to conform to standards, but rather as an easy indicator that our network
> link is up. In my previous work at a broadband ISP I was often annoyed at
> how many hosts do not respond to ICMP echo. On a LAN that uses DHCP it
can
> be a true pain because hosts can use an IP address in the dynamic range
and
> when the DHCP server double-checks that the IP is available with a ping it
> finds that the IP is not in use and allocates it to the DHCP client. The
> DHCP server should be able to assume that if the IP were in use a host
would
> respond to ICMP echo.
>
> Of course, we're talking about public IP addresses on the internet. The
> DHCP example does not apply, however it is still a useful service to other
> administrators out there. When your users are unable to reach a certain
> destination it is a quick check for connectivity. Of course there are
> numerous other methods to determine whether a host is up or not, but ping
is
> designed for this purpose. There are steps that can be taken to prevent
the
> misuse of the protocol, and those should be preferred to simply dropping
the
> packets.
>
> Others on the internet do share your opinion, and I can see why. However,
> there are still many of us who do accept ICMP echoes. Including yahoo.com
> and google.com. Yes, I know, microsoft.com and ebay.com do not. If you
> keep watch on your network and you have taken reasonable steps to diminish
> the success of a DoS attack then you should be able to safely accept ICMP
> echoes.
>
> ... my two cents, of course.
>
> --
> Tony Kava
> Network Administrator
> Pottawattamie County, Iowa

<http://www.freemail.gr> - äùñáŰí òðçñáóßá çěăêõñííéêïý ôá+ôãñííáßíõ.

<http://www.freemail.gr> - free email service for the Greek-speaking.

Attend Black Hat Briefings & Training Federal, September 29-30 (Training),
October 1-2 (Briefings) in Tysons Corner, VA; the world's premier
technical IT security event. Modeled after the famous Black Hat event in
Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors.

Symantec is the Diamond sponsor. Early-bird registration ends September 6. Visit us: www.blackhat.com