

## RE: ICMP (Ping)

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-09/0157.html>

---

*SMiller\_at\_unimin.com*

**Date:** 09/04/03

To: security-basics@securityfocus.com

Date: Thu, 4 Sep 2003 13:23:53 -0400

Regarding the oft cited admonition against "security by obscurity": according to Bruce Schneier this is "Kerckhoffs' Principle", formulated in 1883 by Auguste Kerckhoffs, and as such is narrowly applicable only to algorithms used for cryptography. It may or may not apply to other and more generalized security issues, those cases must be evaluated individually. Regarding ICMP: I can understand why it may be desirable to block this service at the gateway. However, turning it off at the device makes several common administration tasks more difficult, which in turn could potentially degrade security... Probably an amended RFC is in order, as I believe the point of the standards was/is to embrace consensus "best practices", not ivory tower ideals that few can meet in the real world. Such a revision could also address the issue of whether or not to disable ICMP inside the firewall. No, I'm ~not~ volunteering;>)

–Scott Miller

"...my opinions do not necessarily reflect those of Unimin Corporation, and I have the bruises to prove it..."

"Jay Woody"

<jay\_woody@tnb.co To: <security-basics@securityfocus.com>  
m> cc:

Fax to:

09/04/2003 12:05 Subject: RE: ICMP (Ping)  
PM

I don't think that maintaining a RFC standard for the sake of maintaining the standard is necessarily worth your company experiencing an outage. Those standards are exactly that, a standard. They are what should be done. They are put in place mainly so that everyone knows how to interact with each other. If you changed something and made yourself non-RFC compliant in something like SMTP, that would be one thing, because everyone NEEDS to know that everyone is doing it a certain way. Everyone doesn't NEED to ping me. In a perfect world, you should always

## SecurityFocus BASICS: RE: ICMP (Ping)

maintain standards obviously. However, in this world, you make changes based upon your needs and requirements and you tell your business partners, "This is how you need to do it to do business with me."

My business could care less if the entire world can ping me and know I am up. I want my customers to know and my partners. Everyone else can go take a leap. All we needed was one denial of service attack hitting us and they determined that the amount of time it took to trouble-shoot it and fix it were not worth what they got by allowing random people around the world to "test" and see if we were up.

Certain RFC's matter to the world. Certain ones don't. This is one that the world has determined it is acceptable to violate. The "Security through Obscurity" that most people rag on is trying to mask or mislead your attacker into believing that you are running something different (different OS, etc.) and most people blast that because there are 15 different ways to tell an OS, so you block one, big deal. If you are patched then you shouldn't need to obscure it. In this case I am hiding the existence of a box because even if I am patched and proper I am still vulnerable to being pinged out of existence. The time it takes me to daily enter 15 people to drop packets from just isn't worth it.

Until I have a real business reason for NEEDING a ping (other than just to maintain a RFC Standard), then I drop them. If I NEEDED the ping then I would worry about trying to manage the settings, etc. My 2 cents.

JayW

>>> Tony Kava <securityfocus@pottcounty.com> 09/03/03 11:20AM >>>

What about compliance with standards? ICMP echo is a useful diagnostic tool, and not responding to ICMP echo is not an effective means of protecting yourself. I believe members of this list have often cited the lack of value found in 'security by obscurity'. I do not wish to suggest that allowing all types of ICMP traffic is a safe practice, but ICMP echoes should be accepted and replies should be sent unless you have blocked them in order to mitigate a denial of service attack or because you believe the source of the request is malicious in nature.

== RFC 1122 snippet ==

3.2.2.6 Echo Request/Reply: RFC-792

RE: ICMP (Ping)

## SecurityFocus BASICS: RE: ICMP (Ping)

Every host **MUST** implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies. A host **SHOULD** also implement an application-layer interface for sending an Echo Request and receiving an Echo Reply, for diagnostic purposes.

An ICMP Echo Request destined to an IP broadcast or IP multicast address **MAY** be silently discarded.

== end of snippet ==

Just my two cents, as it were.

--

Tony Kava

Network Administrator

Pottawattamie County, Iowa

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

From: freeasabird\_13@gmx.net [mailto:freeasabird\_13@gmx.net]

Sent: Tuesday, 02 September, 2003 21:12

To: Paul Kurczaba; security-basics@securityfocus.com

Subject: Re: ICMP (Ping)

> Are there any security issues for allowing a firewall/router to respond to

> Ping from the internet?

>

> -Paul Kurczaba

Yes. It would not be preferable for you to allow your firewall/router to

respond to pings from the internet. Someone running a wide-scale scan of internet computers for possible attack targets would quickly be made aware

of your obvious internet presence and you could become a target for attack.

This wouldn't be such a big problem provided your firewall/router was well-configured with security in mind. If there is no overwhelming reason

for allowing your device to respond to pings then it shouldn't be configured

to do so. It is simply calling too much attention to your systems and their

possible vulnerabilities. Well anyway, that's my quick 2 cents on the matter. I'm sure others will share theirs too.

Best Wishes,

~Nathaniel Hasenfus

---

Outgoing mail is certified Virus Free.

Checked by AVG anti-virus system (<http://www.grisoft.com>).

Version: 6.0.515 / Virus Database: 313 - Release Date: 9/1/2003

-----  
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

RE: ICMP (Ping)

## SecurityFocus BASICS: RE: ICMP (Ping)

6.Visit us: [www.blackhat.com](http://www.blackhat.com)

---

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](http://www.blackhat.com)

---

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](http://www.blackhat.com)

---

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](http://www.blackhat.com)

---