

Re: ICMP (Ping)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-09/0337.html>

From: Jay Woody (jay_woody_at_tnb.com)

Date: 09/08/03

Date: Mon, 08 Sep 2003 12:01:02 -0500

To: <bugtraq@planetcobalt.net>, <security-basics@securityfocus.com>

That would obviously depend on how you were shedding the pings and what tools they were using. That is where I think Tim and I were crossing wires on. Obviously there are a myriad of tools out there that behave different ways. I have used a couple, I have friends that have used a bunch and all of them compile a list from people that reply and then whittle it down from there. I haven't exactly been involved in that stuff in a while now, so some tools may be nicer than others.

The only logical reason I can give is the same one that I gave Tim. They are looking for the slow, stupid ones and for whatever reason, they see that as people that respond to pings. Even not replying but acknowledging your existence I guess would tell them I am here and I am somewhat secure. They just want easy in and out, so they drop those guys and compile the list as straight-forward as possible. Again, not 100% of the time do script kiddies act like that, but a large portion of them do. 100% of the tools I have used and seen do that, so that is why I dropped them. That was the question and that was my answer.

Some of the tools now may have coded into them that an unreachable was the same as a ping response, so if you are allowing half the handshake, etc. you may still appear on those. Can't really say. My main point to Tim was that he wanted to know why some people drop them. Aside from the DoS issues that had already been discussed a large segment of the population seems to believe that script kiddies start with a ping sweep and drill down. So not being a part of the ping sweep help keeps out the clutter. Have tools changed now to take some of that into account? Probably. Are there now ways to appear as unpingable rather than unreachable? Probably. It is the constant cat and mouse game. My main point was simply that not responding to pings keeps the simple stuff from being run against you. Not the determined, vuln scanning demon, but the easy kiddie who just wants to crack as many as possible and then brag about it to his buds on IRC. You guys can look at your logs and see that most of the time, you can basically say what tool was used because it is such a pattern. These guys aren't trying their homemade zero day exploits, just the regular crap and many times the first step is pinging. That's all I am trying to get across.

SecurityFocus BASICS: Re: ICMP (Ping)

JayW

>>> Ansgar Wiechers <bugtraq@planetcobalt.net> 09/05/03 09:49PM >>>

On 2003-09-05 Jay Woody wrote:

- > *Not really, they will randomly scan and the RETURN to the ones that*
- > *replied and run a vuln scan against it. If you didn't reply to*
- begin
- > *with then they won't be RETURNING.*

Why would that be? Not replying is still telling them you're there.

Regards

Ansgar Wiechers

Captus Networks

Are you prepared for the next Sobig & Blaster?

- Instantly Stop DoS/DDoS Attacks, Worms & Port Scans
- Precisely Define and Implement Network Security
- Automatically Control P2P, IM and Spam Traffic

FIND OUT NOW – FREE Vulnerability Assessment Toolkit

<http://www.captusnetworks.com/ads/42.htm>

Captus Networks

Are you prepared for the next Sobig & Blaster?

- Instantly Stop DoS/DDoS Attacks, Worms & Port Scans
- Precisely Define and Implement Network Security
- Automatically Control P2P, IM and Spam Traffic

FIND OUT NOW – FREE Vulnerability Assessment Toolkit

<http://www.captusnetworks.com/ads/42.htm>
