

R: Removing ping/icmp from a network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-03/msg00397.html>

- *From:* "Vega – Brunello Ivan" <I.Brunello@xxxxxxxxxx>
 - *Date:* Thu, 27 Mar 2008 19:33:38 +0100
-

I let icmp flowing into internal network, but usually don't like to let outside ping my published servers.

A user could blame on "cannot open web page", but I expect an average network troubleshooter don't rely on ping on internet:

after all, I find LOTS of routers in my path to remote sites which drop traceroutes.

Everyone in between is either a script kiddie, or somebody just playing around with ping sweep/basic portscan.

I use icmp on internet just to check whether my ISP has problems going out (as it happens quite frequently :(), thus stopping after the 4th–5th hop.

Idserve (from www.grc.com) is out there, and at worst, you can make some sort of "tcp ping" (e.g. a telnet on port 80).

Ivan

-----Messaggio originale-----

Da: listbounce@xxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxx>] Per conto di Mark Owen

Inviato: giovedì 27 marzo 2008 18.09

A: Jason

Cc: Ansgar –59cobalt– Wiechers; security-basics@xxxxxxxxxxxxxxxxxx

Oggetto: Re: Removing ping/icmp from a network

On Thu, Mar 27, 2008 at 12:25 PM, Jason <securitux@xxxxxxxxxx> wrote:

snip

The idea is to limit your Internet footprint to make it as difficult as possible for an attacker. There is no need for a web server to respond to ping from the Internet for example.

It is very critical that your web server responds to ICMP on the Internet. If you go out of the way and ignore essential protocols for IP over a public network, you're just going to create a headache for all of us.

Without ICMP, it is very difficult for us to determine where a problem exists when our clients complain about slow load times or inaccessibility to your website. No ICMP means no basic trace routing, no basic latency

R: Removing ping/icmp from a network

checks, and no basic error reporting. So even if the problem is somewhere in our infrastructure that limits or prevents access to your site, you're going to get the blame and bad reputation of an unstable server. If it doesn't respond to ping, and can't be traced, its not our fault that our client can't access your site, it's yours.

--
Mark Owen