

Re[2]: icmp problem

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-05/0027.html>

From: Danil V. Gerun (*news_at_625.ru*)

Date: 05/13/05

Date: Fri, 13 May 2005 10:02:45 +0400

To: freebsd-security@freebsd.org

Hello.

Another possible solution came to my mind this morning :)
ICMP doesn't have ports like TCP and UDP do, but it does have the contents of the ICMP packets ;)

What if the contents of the ICMP Echo Request, sent by the gateway to the Internet, is for example equal to:

SHA1 (original private src_ip + some (constant) garbage)

It can be used like a NAT "port-table" by a "special" ping utility:
the real "private" sender gets all expected ICMP Replies.

Such ping utility might be found or created.

It would work with natd or with Netgraph (or with both :)).

AW> I would guess, that ICMP packets do not have a port number (just a
AW> request/response id), so that the NAT cannot distinguish multiple
AW> ICMP packet sources (I mean: The response from the ICMP requestee
AW> cannot be mapped back to the appropriate ICMP requester).

AW> Hmm... I just think, that (if you have multiple ICMP requestees)
AW> the NAT could be able to map back the ICMP requester IP by the IP
AW> of the ICMP requestee. But I do not know, how your router works...

AW> Maybe your computer-pool could elect an ICMP-master, who
AW> coordinates all the ICMP traffic through the NAT.

AW> Bye

AW> Arne

--

Best regards, Danil V. Gerun.

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"