

Re: ICMP unreachable question

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-10/0181.html>

From: Crist J. Clark (cristjc@earthlink.net)

Date: 10/27/01

Date: Fri, 26 Oct 2001 19:50:51 -0700
From: "Crist J. Clark" <cristjc@earthlink.net>
To: Steve Culligan <stephen_culligan@hotmail.com>
Subject: Re: ICMP unreachable question
Message-ID: <20011026195051.A484@gohan.cjclark.org>

On Fri, Oct 26, 2001 at 11:05:24AM +0100, Steve Culligan wrote:

- > *I'm interested in a particular ICMP packet which seems to change the client*
- > */ servers MTU size.*
- > *The scenario is like this*
- > *client----->Router-vpn-vpn-vpn-vpn-vpn-Router ----->Firewall*
- > *----->Server*
- > *- Client initiates a connection with the server and starts to transmit data.*
- > *- Router places its ESP header on the packets coming from the server which*
- > *brings the MTU over the maximum size*
- > *- Router sends the following packet back to the server*
- > *icmp: 172.*.* unreachable - need to frag (mtu 1454)*
- > *- ICMP packet from the router gets blocked by the firewall and the*
- > *connection is eventually lost as the router cannot handle this MTU size.*
- >
- > *but*
- >
- > *If the Firewall permits the ICMP packet from the router through to the*
- > *server, the server will lower its MTU and continue the connection.*
- >
- > *So my question is , Can this be used as a denial of service attack to*
- > *continually send these ICMP packets to a server to confuse it or bring it*
- > *down.*
- > *Anybody had any experience with this or know any tools which can generate*
- > *these ICMP reachable packets ?*

It is unlikely that you could actually bring down a server with these packets. The worst you can probably do is degrade service. In order to do this, the hostile party would have to be able to sniff the data stream. There are any number of potential attacks someone can perform if they can sniff your data. This particular attack is one of the less devastating and more complicated ones so it is unlikely to be used.

I am not aware of a specific tool that builds ICMP "destination unreachable, fragmentation required and DF-bit set"-messages. You can use a tool like hping to make your own at the command line. Building a

SecurityFocus Penetration: Re: ICMP unreachable question

quick C program to build them is trivial.

IIRC, there was a recent thread about the potential for someone to flood networks by causing very small packets to be sent. I do not think the attack would work. You could degrade the performance of the connection attacked, and possibly the machine being attacked, but not the whole network (at least not without combining some other attacks with it).

--

Crist J. Clark

cjclark@alum.mit.edu

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- ***Previous message:*** [Ofir Arkin: "RE: ICMP unreachable question"](#)
- ***In reply to:*** [Steve Culligan: "ICMP unreachable question"](#)
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)