

RE: Do ICMP re-directs actually work ?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-10/0196.html>

From: Mike Gilles (mike.gilles@itmtech.com)

Date: 10/31/01

Message-ID: <210D139C03E0D311BF4B00500473124D3B017F@SVEN>
From: Mike Gilles <mike.gilles@itmtech.com>
To: Blake Frantz <blake@mc.net>, Naveed Anwar <naveed@middleoffice.com>
Subject: RE: Do ICMP re-directs actually work ?
Date: Wed, 31 Oct 2001 09:38:54 -0500

On a Security note: Keep in mind that ICMP redirects (ICMP type 5 packets) are unauthenticated. And when ever possible it not be used and/or filtered on any external subnet. (e.g. There's no method of authentication; meaning that a host will on blind faith accept an ICMP redirect. So someone with malicious intent could, using a third party tool, send a false redirect to a host and cause a denial of service attack against the host by messing with it's routing table.)

Just my 2 cents...

Michael John Gilles
Lead Security Engineer, MCSE
Ext. 204
616.901.9720 mobile
mike.gilles@itmtech.com

ITM Technology, LLC.
5940 Tahoe DR. S.E. Suite 110
Grand Rapids, MI 49546
616.464.1361 office
616.464.1362 fax

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

From: Blake Frantz [mailto:blake@mc.net]
Sent: Tuesday, October 30, 2001 4:28 PM
To: Naveed Anwar
Cc: pen-test@securityfocus.com; ofir@sys-security.com
Subject: Re: Do ICMP re-directs actually work ?

It's my understanding that the ICMP redirect is used in the following scenario:

- host1 sends data to gateway1
- gateway1 looks for the next hop and find gateway2
- gateway2 is on the same net as host1

RE: Do ICMP re-directs actually work ?

SecurityFocus Penetration: RE: Do ICMP re-directs actually work

- gateway1 sends redirect to host1 informing it to use gateway2
- host1 traffic now leaves via gateway2

With this in mind, I *think* the redirect has to come from "pepsi"'s gateway.

On Win2k, verify the value of:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\EnableICMP Redirect

It's set to 1 (enable) by default.

-blake

On Tue, 30 Oct 2001, Naveed Anwar wrote:

- >
- > *Hi All*
- >
- > *I have just been conducting a test in one of our labs by sending ICMP*
- > *redirects to a Windows 2000 Advanced Server using ICMPUSH. Using a*
- > *sniffer I see the packet successfully leave my machine, then again*
- > *from the target box I see the re-direct arrive. Say for example my*
- > *target machine is called Pepsi, and I tell it to redirect any packets*
- > *for a machine called Fanta to a dead gateway, hence communication to*
- > *Fanta will fail for the lifetime of the redirect.*
- >
- > *Now my understanding is that the target server (Pepsi) should now*
- > *have updated its local routing table with respect to the Fanta*
- > *machine. Then from Pepsi I try to ping/telnet/http/ftp etc..(i.e*
- > *establish communication) to Fanta I am able to. The point is since I*
- > *told Pepsi via a redirect to send all traffic for Fanta to a*
- > *blackhole, how is the communication working.*
- >
- > *One interesting point is that when I issue a netstat -rn to view the*
- > *routing table, I see no route update from the ICMP redirect.*
- >
- > *After reading Ofir's excellent paper I understand most ICMP*
- > *implementations are OS specific, therefore I guess redirects do not*
- > *work in Win2000 or Linux 6.2 which I also tested..or am I doing*
- > *something horribly wrong?*
- >
- > *Thanks*
- > *Naveed*
- >
- >

-
- > *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*

RE: Do ICMP re-directs actually work ?

SecurityFocus Penetration: RE: Do ICMP re-directs actually work

see:

> <https://alerts.securityfocus.com/>

>

>

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/>

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:** [Ian Lyte: "RE: Using Null Session information from NAT.EXE"](#)
- **Maybe in reply to:** [Naveed Anwar: "Do ICMP re-directs actually work ?"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)