

## Re: Do ICMP re-directs actually work ?

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-10/0192.html>

---

**From:** Blake Frantz ([blake@mc.net](mailto:blake@mc.net))

**Date:** 10/30/01

Date: Tue, 30 Oct 2001 15:28:00 -0600 (CST)  
From: Blake Frantz <[blake@mc.net](mailto:blake@mc.net)>  
To: Naveed Anwar <[naveed@middleoffice.com](mailto:naveed@middleoffice.com)>  
Subject: Re: Do ICMP re-directs actually work ?  
Message-ID: <Pine.BSI.4.05L.10110301517260.2673-100000@maxx.mc.net>

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
- 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\EnableICMPRedirect

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*

Re: Do ICMP re-directs actually work ?

## SecurityFocus Penetration: Re: Do ICMP re-directs actually work

> 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 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:** [Mike Brentlinger: "Re: Using Null Session information from NAT.EXE"](#)
- **In reply to:** [Naveed Anwar: "Do ICMP re-directs actually work ?"](#)
- **Next in thread:** [foob@return0.net: "Re: Do ICMP re-directs actually work ?"](#)
- **Next in thread:** [Mike Gilles: "RE: Do ICMP re-directs actually work ?"](#)
- **Reply:** [foob@return0.net: "Re: Do ICMP re-directs actually work ?"](#)
- **Messages sorted by:** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)