

RE: traceroute-like tool for UDP or TCP packet

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-08/0880.html>

From: Meidinger Chris (chris.meidinger_at_badenit.de)

Date: 08/22/03

To: "'gillettdavid@fhda.edu'" <gillettdavid@fhda.edu>, "'Edward Rustin'" <ed@well.com>, "'some gu
Date: Fri, 22 Aug 2003 05:36:11 -0500

To clear the last bit up:

there is no UDP echo-request packet except (and this is a stretch) against the echo small server which is rarely running.

Linux traceroute sends UDP packets against high ports above 33000 and counts the ICMP Host-Unreachables then pings (Echo-Request) at the end to confirm the ICMP Port-Unreachable.

Windows tracert uses ICMP Echo-Request and counts ICMP Unreachables until it gets an Echo-Reply

Both increment the TTL to enumerate the next host on hand of the reply packet, whichever is being looked for.

ICMP is a separate protocol and not part of UDP (as already mentioned)

badenIT GmbH
System Support

Chris Meidinger
Tullastrasse 70
79108 Freiburg

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

From: David Gillett [<mailto:gillettdavid@fhda.edu>]
Sent: Friday, August 22, 2003 1:08 AM
To: 'Edward Rustin'; 'some guy'
Cc: security-basics@securityfocus.com
Subject: RE: traceroute-like tool for UDP or TCP packet

> > *Linux uses UDP packets to traceroute, not ICMP packets like*
> > *windows does.*
>
> *Not really.... an ICMP packet is a type of UDP packet.*

Nope. ICMP and UDP are different protocols on top of IP.

SecurityFocus BASICS: RE: traceroute-like tool for UDP or TCP packet

- > *Basically traceroute works by sending a series of ICMP ECHO*
- > *requests with increasing TTLs (time to live – how many hops*
- > *the packet can travel before it dies and aPacket*
- > *Timeout error is sent).*

What kind of packet traceroute sends depends on what the author chose to use. The two most common are UDP echo-request and ICMP echo-request, because the target host should reply with a UDP echo or ICMP echo (respectively) instead of the ICMP time-exceeded which intermediate routers will send when TTL expires.

- > *A ping is also just a ICMP ECHO message, just with*
- > *a default TTL, rather than a series of increasing TTLs.*

ICMP echo-request, actually; ICMP echo is the answer coming back.

David Gillett

This email has been scanned for all viruses by the MessageLabs Email Security System. For more information on a proactive email security service working around the clock, around the globe, visit <http://www.messagelabs.com>

Attend Black Hat Briefings & Training Federal, September 29–30 (Training), October 1–2 (Briefings) in Tysons Corner, VA; the world's premier technical IT security event. Modeled after the famous Black Hat event in Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors. Symantec is the Diamond sponsor. Early-bird registration ends September 6. Visit us: www.blackhat.com
