

## RE: Traceroute

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-02/0111.html>

---

**From:** Omar Herrera (*oherrera\_at\_prodigy.net.mx*)

**Date:** 02/25/05

Date: Thu, 24 Feb 2005 19:42:29 -0600

To: pen-test@securityfocus.com

Hi, Chris

> -----Original Message-----  
> From: Chris [mailto:uid0@free.fr]  
> I've just got a little question which isn't really linked to  
> pen-testing: do you know any alternative to the normal UDP/TCP/ICMP  
> traceroute to trace the route of a packet? I'm already aware of the IP  
> Record Route option, but is there any other hack that you guys would be  
> aware of?

Plain IP packets, and actually anything that travels over IP or with an IP header (and of course over UDP/TCP), like OSPF, RIP or BGP. Tracerouting is done by sending a sequence of packets where the Time to Live Field (TTL) is incremented. You most probably know the rest of the story (TTL is decremented at each hop and elicits an ICMP time exceeded when reaching 0 ...).

Using other protocols, even if they run over TCP/UDP, might yield successful results even if other type of TCP/UDP traffic is discarded. Plain IP packets are usually blocked by firewalls but are still worth trying (you can add garbage after the IP header and play with the protocol field in the IP header to confuse some filters).

The best defense against tracerouting is an egress filter for the ICMP time exceeded packets because this breaks the protocol response (ingress filters for ICMP and UDP packets used by standard traceroute tools use are easily evaded by using other protocols). If this egress filter is in place you won't be able to traceroute... that is, unless your chosen protocol is able to elicit some other kind of response from the middle hops and/or the target :-)

If you can't find a specific traceroute tool for some protocol you could easily script it with Perl and some net modules, with C and libnet and libpcap or with packet building tools like hping, packit or nemesis.

This link might helpful: <http://www.networksorcery.com/enp/default0701.htm>

SecurityFocus Penetration: RE: Traceroute

Cheers,

Omar Herrera