

Re: loose source routed IP packets

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-02/0145.html>

Chris.McNab_at_trustmatta.com

Date: 02/25/04

To: pen-test@securityfocus.com
Date: Wed, 25 Feb 2004 22:23:29 +0000

Hi,

Todd MacDermid has written two excellent tools for LSRR testing, titled lsrrscan and lsrrtunnel, and available from <http://www.synacklabs.net>. You can use lsrrscan to test individual routers, firewalls, servers, etc., and see if they process LSRR packets, and if they reverse the specified route too.

For examples of lsrrscan and lsrrtunnel, along with some nice figures, see pages 61-64 of the Chapter 4 PDF from Network Security Assessment, at <http://www.oreilly.com/catalog/networksa/chapter/ch04.pdf>

Take it easy,

Chris

Chris McNab
Technical Director

Matta Consulting Limited
18 Noel Street
London W1F 8GN

08700 77 11 00
