fragroute

Abstract

fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" paper of January 1998.

It features a simple ruleset language to delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host, with minimal support for randomized or probabilistic behaviour.

This tool was written in good faith to aid in the testing of network intrusion detection systems, firewalls, and basic TCP/IP stack behaviour. Please do not abuse this software.

Download

Current source:

- fragroute-1.2.tar.gz

Required libraries:

- libdnet
- libpcap
- libevent (for non-Windows platforms)

Supported platforms:

- BSD (OpenBSD, FreeBSD, NetBSD, BSD/OS, MacOS X)
  - OpenBSD < 3.1 loopback patch - allow setting of loopback MTU
- Linux (Redhat, Debian, Slackware, ...)
- Solaris
  - Universal TUN/TAP driver for sparc64 - local pkg
  - Universal TUN/TAP driver for x86
- Windows 2000
  - CIPE-Win32 driver - required for fragroute
  - WinPcap driver - required for fragtest

Documentation

- INSTALL
- fragroute(8) manpage
- fragtest(8) manpage

Ideas

Sample applications:

- test network IDS timeout and reassembly parameters
- test TCP/IP scrubbing (norm, OpenBSD pf)
- test firewall stateful inspection
- simulate one-way latency, loss, reordering, and retransmissions
- implement TCP Daytona (i will not release this, sorry)
- implement TCP MSS clamping
- evade "passive OS fingerprinting" techniques

Dug Song <dugsong@monkey.org>