# InfraGard Technology Tool Kit Disclaimer Notice:

# Created by Deborah Watson, Technology Tool Kit Program Development Manager, InfraGard - Houston Chapter; adapted from content created by Dave Armstrong, dave@bindshell.net

# IN NO EVENT SHALL INFRAGARD BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND/OR DOCUMENTATION, EVEN IF INFRAGARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# INFRAGARD SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE AND/OR ACCOMPANYING DOCUMENTATION, IF ANY, PROVIDED HEREUNDER IS PROVIDED "AS IS". INFRAGARD HAS NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

# ETrace

etrace is a configurable static port network tracing tool, similar to traceroute, but supporting ICMP, TCP, UDP and other IP protocols.

**Usage**

etrace [ -BbCcnv ] [ -p profile ] [ -F config ] [ -i interface ] [ -I icmp-type ] [ -T port ] [ -U port ] [ -P protocol ] [ -r probe-count ] [ -t timeout ] [ -1 hop ] [ -h hop ] [ -m hop ] [ -A address ] [ -s port ] [ -f flags ] [ -d data ] [ -D data-file ] [ -R count ] [ -q seq] [ -w window ] target [...]

**Options**

etrace has a wealth of options ranging in function from controlling output to the detailed construction of trace packets.

**Profile Options**

A profile is a pre-configured list of options stored in a shared, or user specific configuration file. By defining profiles, complex etrace option sets can be easily accessed with a single command line option.

-p, --profile

Specify a profile.

-C, --clear

Clear the current list of probes. This option can be used to allow a profile to inherit options from another profile, but specify it's own list of probes.

-F, --config

Specify an alternative profiles file.

Interface options

-i, --interface

Specify interface. If unspecified, etrace will examine the routing table and select the most appropriate interface for each target address.

-c, --promisc

Put in interface into promiscuous mode. As this option increases the load on the system in general, it should only be used if spoofing of source packets address is enabled with the "-A" option.

Trace Type Options

-I, --icmp

Specify an ICMP trace and the packet type to use. ICMP traces may use Echo (E or P), Timestamp (T or S), Netmask (N or M) or Info (I). The default trace probe is an ICMP Echo.

-h, --hop

Specify a specific hop to investigate.

-m, --maximum

Specify the maximum number of hops.

-r, --probes

Set the maximum number of probes to send per hop. The default is 3.

-t, --timeout

Set the maximum amount of time, in milli-seconds, to wait for a response to a probe. The default is 3000 (three seconds).

Packet Construction Options

-A, --address

Specify the source IP address of generated packets.

-s, --source

Set the source port of the generated probe packets. If unspecified, etrace uses a random high port.

-f, --flags

Specify TCP and/or IP flags. Takes a comma delimitered list of any of the following flags: RF, DF, MF, FIN, SYN, RST, PSH, ACK, URG, ECE, CWR (Default: SYN)

-d, --data

Specify the data content of generated probe packets. Standard meta-characters are recognised (e.g. "\n\t") as are binary values given in octal (e.g. "\000\x00");

-D, --data-file

Load the data content of the generated probe packets from the specified file. Filenames beginning with '@' a loaded from the etrace shared data directory (usually /usr/local/share/etrace). etrace currently ships with the following predfined packet data files: dns, ike.

-R, --random

Fill the data content of the generated probe packets with the specified number of random bytes.

-b, --badcksum

Generate and send probe packets with bad checksums.

-q, --seq

Specify the TCP sequence number.

-w, --window

Specify the TCP window size.

Output Options

-v, --verbose

Increase output verbosity.

-B, --debug

Enable debugging output.

-n, --numeric

Disable name resolution.

**Examples**

etrace www.sample.com

Launches a trace ICMP Echo, the default, trace to www.sample.com. Specifying the options "-I E" would accomplish the same results.

etrace -T 80 www.sample.com

Similar to the previous example, except the trace is performed on TCP port 80.

etrace --udp 53 --data-file @dns ns.sample.com

Starts are trace to ns.sample.com on UDP port 53 with the trace packets containing data loaded from the file /usr/local/share/etrace/dns (a file supplied with etrace that contains a simple dns request to resolve 127.0.0.1).

etrace -p dns -p fast ns.sample.com

The default profiles shipped with etrace include "dns" (which equates to the options shown in the previous example) and "fast" (which decreases both timeouts and the number of probes sent for each hop, as well as disabling name resolution). Profiles are stackable, with latter options overriding those specified in earlier profiles.

**Files**

~/.etrace

User specific profiles.

/usr/local/share/etrace/profile

System wide profiles.

**Download**

A safe version of etrace can be obtained from the InfraGard site at: [insert link] [etrace.1.1.tgz](http://bindshell.net/tools/etrace/etrace.1.1.tgz) (md5sum: 8e47908a75299e467b126b6730f88454)