# **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.

# **ICMPScan**

# ICMPScan scans the specified address, or addresses, for ICMP responses. Handles echo (type 8), timestamp (type 13), address mask (type 17), information (type 15) and router solicitation (type 10) requests.

# Developer: Dave Armstrong

**Usage**

icmpscan [ -EPTSNMAIRcvbn ] [ -A address ] [ -f filename ] [ -i interface ] [ -r retries ] [ -t timeout ] target [...]

**Options**

**-i, --interface**

Listen on the specified interface. If unspecified, icmpscan 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.

**-A, --address**

Specify the source IP address of generated packets.

**-t, --timeout**

Specify the timeout, in milli-seconds, before retrying.

**-r, --retries**

Specify the number of attempts to elicit a particular ICMP response.

**-f, --file**

Read target list from the specified file.

**-E, -P, --echo, --ping**

Check of ICMP Echo responses.

**-T, -S, --timestamp**

Check for ICMP Timestamp responses.

**-N, -M, --netmask**

Check for ICMP Netmask responses.

**-I, --info**

Check for ICMP Info responses.

**-R, --router**

Check for ICMP Router Solicitation responses.

**-v, --verbose**

Increase the output verbosity.

**-B, --debug**

**Target Specification**

The simplest case is listing single hostnames or IP addresses on the command line. If you want to scan a subnet of IP addresses, you can append /mask to the hostname or IP address. mask must be between 0 (scan the whole Internet) and 32 (scan the single host specified). Use /24 to scan a class "C" address and /16 for a class "B". There is also a more powerful notation which lets you specify an IP address using lists/ranges for each element. Thus you can scan the whole class "B" network 192.168.\*.\* by specifying "192.168.\*.\*" or "192.168.0-255.0-255" or even "192.168.1-50,51-255.1,2,3,4,5-255". And of course you can use the mask notation: "192.168.0.0/16". These are all equivalent. If you use asterisks ("\*"), remember that most shells require you to escape them with back slashes or protect them with quotes.

**Examples**

The following example checks the first 16 addresses in the 192.168.1.0/24 netblock for all ICMP responses. The scan speed is increased by lowering the timeout value and setting the number of retries to 1:

> icmpscan -t 500 -r 1 192.168.1.0-16

192.168.1.0: Echo (From 192.168.1.17!)

192.168.1.0: Address Mask [255.255.255.0] (From 192.168.1.17!)

192.168.1.7: Echo

192.168.1.7: Timestamp [0x03ab2db0, 0x02d4c507, 0x02d4c507]

192.168.1.7: Address Mask [255.255.255.0]

192.168.1.8: Echo

192.168.1.8: Address Mask [255.255.255.0]

To display failed probes, increase the output verbosity:

> icmpscan -v 192.168.1.1

192.168.1.1: -- No response to Echo request --

192.168.1.1: -- No response to Timestamp request --

192.168.1.1: -- No response to Netmask request --

192.168.1.1: -- No response to Info request --

192.168.1.1: -- No response to Router Solicitation request --

Individual ICMP types can be checked for by listing their corresponding flags on the command line:

> icmpscan -v --echo --netmask 192.168.1.7

192.168.1.7: Echo

192.168.1.7: Address Mask [255.255.255.0]

**Download**

A safe version of ICMPScan can be obtained from the InfraGard site at: [insert link] [icmpscan.tgz](http://bindshell.net/tools/icmpscan/icmpscan.tgz) (md5sum: 5ecfac20afb25abb630c74f2e73c86b9)

License

Target specification code (and related documentation) was extracted from nmap (by Fyodor <fyodor@insecure.org> ). icmpscam is therefore a "derived work" and release under the GNU General Public License (a copy of which should be contained within the distribution archive).