rs6 v1.2 manual pages

Description

This tool is part of the IPv6 Toolkit v1.2: a security assessment suite for the IPv6 protocol developed by the UK CPNI. It allows the assessment of IPv6 implementations with respect to a variety of attacks based on ICMPv6 Router Solicitation messages.

Options

The rs6 tool takes its parameters as command-line options. Each of the options can be specified with a short name (one character preceded with the hyphen character, as e.g. “-i”) or with a long name (a string preceded with two hyphen characters, as e.g. “--interface”).

Depending on the amount of information (i.e., options and option data) to be conveyed into the Router Solicitations, it may be necessary for rs6 to split that information into more than one Router Solicitation. Also, when the rs6 tool is instructed to flood the victim with Router Solicitations from different sources (“--flood-sources” option), multiple packets may need to be generated. rs6 supports IPv6 fragmentation, which may be of use if a large amount of information needs to be conveyed within a single Router Solicitation message. IPv6 fragmentation is not enabled by default, and must be explicitly enabled with the “-y” option.

`--interface`, `-i`

This option specifies the network interface that the rs6 tool will use. The network interface must be specified (i.e., the tool does not select any network interface “by default”).

`--src-address`, `-s`

This option is meant to specify the IPv6 Source Address (or IPv6 prefix) to be used for the Router Solicitation messages. If left unspecified, a randomized link-local unicast (fe80::/64) address is selected.

`--dst-address`, `-d`

This option specifies the IPv6 Destination Address of the Router Solicitation messages. If left unspecified, but the Ethernet Destination Address is specified, the “all-routers link-local multicast” address (ff02::2) is selected as the IPv6 Destination Address.

`--hop-limit, -A`

This option specifies the IPv6 Hop Limit to be used for the Router Solicitation messages. It defaults to 255. Note that IPv6 nodes are required to check that the Hop Limit of incoming Router Solicitation messages is 255. Therefore, this option is only useful to assess whether an IPv6 implementation fails to enforce the aforementioned check.

`--frag-hdr`, `-y`

This option specifies that the resulting packet must be fragmented. The fragment size must be specified as an argument to this option.

`--dst-opt-hdr`, `-u`

This option specifies that a Destination Options header is to be included in the resulting packet. The extension header size must be specified as an argument to this option (the header is filled with padding options). Multiple Destination Options headers may be specified by means of multiple “-u” options.

`--dst-opt-u-hdr`, `-U`

This option specifies a Destination Options header to be included in the “unfragmentable part” of the resulting packet. The header size must be specified as an argument to this option (the header is filled with padding options). Multiple Destination Options headers may be specified by means of multiple “-U” options. This option is only valid if the “-y” option is specified (as the concept of “unfragmentable part” only makes sense when fragmentation is employed).

`--hbh-opt-hdr`, `-H`

This option specifies that a Hop-by-Hop Options header is to be included in the resulting packet. The header size must be specified as an argument to this option (the header is filled with padding options). Multiple Hop-by-Hop Options headers may be specified by means of multiple “-H” options.

`--src-link-address`, `-S`

This option specifies the link-layer Source Address of the Router Solicitation messages (currently, only Ethernet is supported). If left unspecified, the link-layer Source Address is randomized.

`--link-dst-address`, `-D`

This option specifies the link-layer Destination Address of the Router Solicitation messages (currently, only Ethernet is supported). If left unspecified, the link-layer Destination Address is set to “33:33:00:00:00:02” (the Ethernet address that corresponds to the “all-routers link-local multicast” address).

`--source-lla-opt`, `-E`

This option specifies the contents of a source link-layer address option to be included in the Router Solicitation messages. If more than one source link-layer address is specified (by means of multiple “-E” options), and all the resulting options cannot be conveyed into a single Router Solicitation, multiple Router Solicitations will be sent as needed.

`--add-slla-opt`, `-e`

This option instructs the rs6 tool to include a source link-layer address option in the Router Solicitation messages that it sends. The link-layer address included in the option is the same as the Ethernet Source Address used for the outgoing Router Solicitation messages.

`--flood-sources`, `-F`

This option instructs the rs6 tool to send Neighbor Solicitations from multiple (and random) IPv6 Source Addresses. The number of different sources is specified as “-F number”. The IPv6 Source Address of each Router Solicitation is a randomized from the IPv6 prefix specified with the “-s” option, and defaults to a random link-local unicast address (fe80::/64).

`--loop`, `-l`

This option instructs the rs6 tool to send periodic Router Solicitations to the destination node. The amount of time to pause between sending Neighbor Solicitations can be specified by means of the “-z” option, and defaults to 1 second.

`--sleep`, `-z`

This option instructs the rs6 tool to the amount of time to pause between sending Neighbor Solicitations. If left unspecified, it defaults to 1 second.

`--verbose`, `-v`

This option instructs the rs6 tool to be verbose.

`--help`, `-h`

Print help information for the rs6 tool.

Examples

Example #1

```
# ./rs6 -i eth0 -e
```

Use the network interface “eth0” to send a Router Solicitation using a random link-local unicast IPv6 Source Address and a random Ethernet Source Address, to the IPv6 Destination Address “ff02::2” (“all-routers link-local multicast” address, selected by default) and the Ethernet Destination Address “33:33:00:00:00:02” (selected by default). The Router Solicitation also includes a source link-layer address option, that contains the same Ethernet address as that used for the Ethernet Source Address of the packet.

Example #2

```
# ./rs6 -i eth0 -e -F 100 -l -z 10 -v
```

Send 100 Router Solicitation messages using a random Ethernet Source Address and random IPv6 Source Address for each of them, to the Ethernet Destination Address “33:33:00:00:00:02” (default) and the IPv6 Destination Address “ff02:2” (default). Each message includes a source link-layer address option that contains the same link-layer address as that used for the Ethernet Source Address of the packet. Repeat this operation every ten seconds. Be verbose.

Example #3

```
# ./rs6 -i eth0 -d fe80::1 -E ff:ff:ff:ff:ff:ff -v
```

Send one Router Solicitation message using a random Ethernet Source Address and a random link-local unicast (i.e., fe80::/64) IPv6 Source Address, to the Ethernet Destination Address “33:33:00:00:00:02” (default) and the IPv6 Destination Address “fe80::1”. Each Router Solicitation includes a source link-layer address option that contains the Ethernet address “ff:ff:ff:ff:ff:ff”. Be verbose.

Credits

The rs6 tool and related manuals were produced by Fernando Gont <fgont@si6networks.com> on behalf of the UK Centre for the Protection of National Infrastructure (CPNI) <http://www.cpni.gov.uk>.

License