

ns6 v1.1 manual pages

Description

This tool is part of the IPv6 Toolkit v1.1: 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 Neighbor Solicitation messages.

Options

The ns6 tool takes its parameters by means of 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) to be conveyed into the Neighbor Solicitations, it may be necessary for the ns6 tool to split that information into more than one Neighbor Solicitation message. Also, when the ns6 tool is instructed to flood the victim with Neighbor Solicitations from different sources (“--flood-sources” option), multiple packets may need to be sent. ns6 supports IPv6 fragmentation, which may be of use if a large amount of information needs to be conveyed within a single Neighbor 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 na-attack 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 to be used for the Neighbor Solicitation messages. If left unspecified, a randomized link-local (fe80::/64) address is selected.

--dst-address, -d

This option specifies the IPv6 Destination Address of the Neighbor Solicitation messages. If this option is left unspecified, but the Ethernet Destination Address is specified, the “all-nodes link-local multicast” address (ff02::1) is selected as the IPv6 Destination Address.

`--hop-limit, -A`

This option specifies the IPv6 Hop Limit to be used for the Neighbor Solicitation messages. It defaults to 255. Note that IPv6 nodes are required to check that the Hop Limit of incoming Neighbor 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 Neighbor 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 Neighbor Solicitation messages (currently, only Ethernet is supported). If left unspecified, it is set to the address “33:33:00:00:00:01” (the Ethernet address corresponding to the “all-nodes link-local multicast” IPv6 address (ff02::1)).

`--target, -t`

This option specifies the IPv6 Target Address of the Neighbor Solicitation messages.

If the “-T” (“--flood-targets”) option is specified, this option specifies an IPv6 prefix in the form “-t prefix/prefixlen”. See the description of the “-T” option for further information on how the “-t” option is processed in that specific case.

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

This option specifies the contents of a source link-layer address option to be included in the Neighbor 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 Neighbor Solicitation, multiple Neighbor Solicitations will be sent as needed.

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

This option instructs the ns6 tool to include a source link-layer address option in the Neighbor 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 Neighbor Solicitation messages.

`--flood-sources, -F`

This option instructs the ns6 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 the packets are randomly selected from the prefix specified by the “-s” option (which defaults to fe80::/64).

`--flood-targets, -T`

This option instructs the ns6 tool to send Neighbor Solicitation messages for multiple Target Addresses. The number of different Target Addresses is specified as “-T number”. The Target Address of each packet is randomly selected from the prefix ::/64, unless a different prefix has been specified by means of the “-t” option.

`--loop, -l`

This option instructs the ns6 tool to send periodic Neighbor Solicitations to the victim. 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 ns6 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 ns6 tool to be verbose.

`--help, -h`

Print help information for the ns6 tool.

Examples

Example #1

```
# ./ns6 -i eth0 -d fe80::01 -t 2001:db8::1 -e
```

Use the network interface “eth0” to send a Neighbor Solicitation message using a random link-local unicast IPv6 Source Address and a random Ethernet Source Address, to the IPv6 Destination address fe80::1 and the Ethernet Destination Address 33:33:00:00:00:01 (selected by default). The target of the Neighbor Advertisement is 2001:db8::1. The Neighbor 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

```
# ./ns6 -i eth0 -s 2001:db8::/32 -t 2001:db8::1 -F 10 -l -z 10 -e -v
```

Send 10 Neighbor Solicitation messages using random Ethernet Source Addresses and random IPv6 Source Addresses from the prefix 2001:db8::/32, to the Ethernet Destination Address 33:33:00:00:00:01 (default) and the IPv6 Destination Address ff02::1 (default). The IPv6 Target Address of the Neighbor Solicitation is 2001:db8::1, and each message includes a source link-layer

address option that contains the same address as that used for the Ethernet Source Address of the packet. Repeat this operation every ten seconds. Be verbose.

Example #3

```
# ./ns6 -i eth0 -s 2001:db8::/32 -t 2001:db8::1 -F 10 -l -z 10 -E  
ff:ff:ff:ff:ff:ff -v
```

Send 10 Neighbor Solicitation messages using random Ethernet Source Addresses and random IPv6 Source Addresses from the prefix fe80::/64 (default, link-local unicast), to the Ethernet Destination Address 33:33:00:00:00:01 (default) and the IPv6 Destination Address ff02:1 (default). The IPv6 Target Address of the Neighbor Solicitation is 2001:db8::1, and each message includes a source link-layer address option that contains the Ethernet address ff:ff:ff:ff:ff:ff. Repeat this operation every ten seconds. Be verbose.

Credits

The IPv6 Toolkit v.1.1 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

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with the Invariant Sections being just "Credits", with no Front-Cover Texts, and with no Back-Cover Texts. A copy of the license is available at <<http://www.gnu.org/licenses/fdl.html>>.