

ra6 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 Router Advertisement messages.

Modes of Operation

This tool has two modes of operation: active and passive. In active mode, the tool attacks a specific target, while in passive mode the tool listens to traffic on the local network, and launches an attack in response to such traffic. Active mode is employed when an Ethernet destination address and/or an IPv6 destination address are specified. Passive mode is employed when the “-L” option (or its long variant “--listen”) is specified. In passive mode, the ra6 tool listens for incoming Router Solicitation messages and responds with the Router Advertisement attack messages. If both a destination address and the “-L” option are specified, the tool firstly employs active mode to attack the specified target, and then enters passive mode to respond to Router Solicitation messages with Router Advertisement attack packets.

Options

The ra6 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 Advertisements, it may be necessary for ra6 to split that information into more than one Router Advertisement message. This may be particularly the case when the “flood-prefixes”, “--flood-routes”, or “--flood-dns” options are used. Also, when the ra6 tool is instructed to flood the victim with Router Advertisements from different sources (“--flood-sources” option), multiple packets may need to be generated. ra6 supports IPv6 fragmentation, which may be of use if a large amount of information needs to be conveyed within a single Router Advertisement message. IPv6 fragmentation is not enabled by default, and must be explicitly enabled with the “-y” option.

The tool supports filtering of incoming Router Solicitation messages based on the Ethernet Source Address, the Ethernet Destination Address, the IPv6 Source Address, and the IPv6 Destination Address. There are two types of filters: “block filters” and “accept filters”. If any “block filter” is specified, and the incoming Router Solicitation message matches any of those filters, the message is discarded (and thus no Router Advertisements are sent in response). If any “accept filter” is specified, incoming Router Solicitation messages must match the specified filters in order for the ra6 tool to respond with Router Advertisement messages.

--interface, -i

This option is meant to specify the network interface to use for performing the attack. The network interface must be specified (i.e., the tool does not select any network interface “by default”).

--src-address, -s

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

--dst-address, -d

This specifies the IPv6 Destination Address of the Router Advertisement 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.

When operating in passive mode (“-L” option), the IPv6 Destination Address is selected according to the IPv6 Source Address of the Router Solicitation message. If the IPv6 Source Address of the Router Solicitation is the unspecified address (::), the “all-nodes link-local multicast” address (ff02::1) is used as the IPv6 Destination Address. Otherwise, the IPv6 Source Address of the incoming Router Solicitation message is used as the IPv6 Destination Address of the outgoing Router Advertisement messages.

--hop-limit, -A

This option specifies the Hop Limit of the Router Advertisement messages. It defaults to 255. Note that IPv6 nodes are required to check that the Hop Limit of incoming Router Advertisement 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.

`--curhop, -c`

This option specifies the CurHop value that is included in Router Advertisement messages. This is the value that nodes should use for the “Hop Limit” field of the IPv6 packets they send. If this option is not specified, the CurHop value defaults to 255.

`--lifetime, -t`

This option specifies the Router Lifetime value that is included in Router Advertisement messages. The Router Lifetime is the amount of time (in seconds) that the router can be used as a “default router”. If this option is left unspecified, a Router Lifetime value of 9000 seconds is selected.

`--reachable, -r`

This option specifies the Reachable Time value that is included in Router Advertisement messages. The Router Lifetime is the amount of time in milliseconds that a neighbor is considered “reachable” after a reachability confirmation. If this option is left unspecified, a Reachable Time of 0xffffffff (“infinity”) is selected.

`--retrans, -x`

This option specifies the Retrans Timer value that is included in Router Advertisement messages. The Retrans Timer specifies the amount of time in milliseconds between retransmitted Neighbor Solicitation messages (with ‘0’ meaning “unspecified by this router”). If this option is left unspecified, a Retrans Timer of 4000 milliseconds is selected.

--managed, -m

This option causes the ra6 tool to set the 'M' (Managed) bit in the Router Advertisement messages that it sends. The 'M' bit indicates that network configuration is "managed" (e.g., DHCPv6 should be used instead). If left unspecified, the 'M' bit is not set.

--other, -o

This option causes the ra6 tool to set the 'O' ("Other") bit in the Router Advertisement messages that it sends. The 'O' bit indicates that additional configuration information is available through other means (e.g., DHCPv6). If left unspecified, the 'O' bit is not set.

--home-agent, -a

This option causes the ra6 tool to set the 'H' ("Home Agent") bit in the Router Advertisement messages that it sends (the 'H' bit is specified in RFC 3775). If this option is left unspecified, the 'H' bit is not set.

--nd-proxy, -q

This option causes the ra6 tool to set the 'P' ("ND Proxy") bit in the Router Advertisement messages that it sends (the "P" bit is specified in RFC4389). If this option is left unspecified, the 'P' bit is not set.

--preference, -p

This option specifies the Preference field of the Router Advertisement messages, with "1" meaning "High", "0" meaning "Normal", and "-1" meaning "low" (the value "-2" is forbidden). If left unspecified, a Preference value of "1" (High) is selected.

--src-link-address, -S

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

When operating in passive mode, the link-layer Source Address is selected according to the IPv6 Destination Address of the incoming Router Solicitation messages. If the IPv6 Destination Address of the incoming Router Solicitation message is a multicast address (usually the "all-routers link-local multicast" address "ff02::02"), the link-layer Source Address is set to the address specified by the "-S" option (or to a random address if the "-S" option was left unspecified). If the IPv6

Destination Address of the incoming Router Solicitation is not a multicast address (i.e., it is a unicast address), the link-layer Source Address is set to the Ethernet Destination Address of the incoming Router Solicitation message.

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

This option is meant to specify the link-layer Destination Address of the Router Advertisement messages (currently, only Ethernet is supported). If left unspecified, it is set to “33:33:00:00:00:01” (the Ethernet multicast address corresponding to the IPv6 “all-nodes link-local multicast” address).

When operating in passive mode, the link-layer Destination Address is set depending to the IPv6 Source Address of the incoming Router Solicitation message. If the IPv6 Source Address of the incoming Router Solicitation message is the unspecified address (::), the link-layer destination address is set to “33:33:00:00:00:01” (the Ethernet multicast address corresponding to the IPv6 “all-nodes link-local multicast” address). Otherwise, the link-layer Destination Address is set to the same value as the link-layer Source Address of the incoming Router Solicitation message.

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

This option specifies the contents of a source link-layer address option to be included in the Router Advertisement messages. If a single option is specified, it is included in all the outgoing Router Advertisement messages. If more than one source link-layer address is specified, they are included only in the first packet of a set of Router Advertisements (if more than one Router Advertisement needs to be sent in order to convey all the specified information).

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

This option instructs the ra6 tool to include a source link-layer address option in the Router Advertisement messages. The link-layer address included in the option is the same as the Ethernet Source Address used for the outgoing Router Advertisement message. The difference between this option and the “-E” option is that the latter does not specify the actual value of the option, but just instructs the tool include the option (the actual value of the option is selected according to the Ethernet Source address used in the outgoing packet).

`--prefix-opt, -P`

This option specifies the contents of a Prefix Information option to be included in Router advertisement messages, with the following format: “-P prefix/length#flags#valid#preferred”. Where “prefix/length” is a mandatory field that indicates an IPv6 prefix (e.g., “2001::/16”). “flags” is an optional argument that indicates which flags should be set for this prefix (‘L’ for the “on-link” flag, ‘A’ for the “autonomous address-configuration” flag, ‘R’ for “Router Address”, and ‘-’ for indicating that no flags should be set for this prefix) -- if this field is left unspecified, the “L” and “A” flags are set for in the specified Prefix Information option. “valid” is an optional field that

indicates the “Valid Lifetime” for this prefix (the length of time in seconds during which this information can be used for on-link determination. If left unspecified, a value of 0xffffffff (infinity) is used. “preferred” is an optional argument that specifies the “Preferred Lifetime” value for this prefix (the length of time in seconds that addresses generated from this prefix via stateless address auto-configuration remain preferred). If left unspecified, a value of 0xffffffff (infinity) is used.

--route-opt, -R

This option specifies the contents of a Route Information option to be included in Router advertisement messages, with the following format: “-R prefix/length#preference#lifetime”. Where “prefix/length” is a mandatory field that indicates an IPv6 prefix (e.g., “2001::/16”). “preference” is an optional argument that indicates the preference of this prefix (with ‘1’ meaning “high”, ‘0’ meaning “normal”, ‘-1’ meaning “low”, and ‘-2’ being an invalid value). If this field is left unspecified, a value of ‘1’ (i.e., “high”) is selected. “lifetime” is an optional parameter that specifies the “Route Lifetime” for the specified route (the period of time during which this information can be used for route determination). If left unspecified, a value of 0xffffffff (infinity) is selected.

--mtu-opt, -M

This option is meant to specify the value of a MTU option that should be included in Router Advertisements. Multiple MTU options can be specified.

--rdnss-opt, -N

This option allows the advertisement of a number of recursive DNS servers by means of the RDNSS option. A “Lifetime” parameter (32 bits) indicates the amount of time (in seconds) that the specified DNS server(s) may be used for name resolution. Multiple IPv6 addresses can be specified in the same RDNSS option in the form “--dns-opt lifetime#ipv6address1#ipv6address2”. Also, more than one RDNSS option may be specified.

--flood-prefixes, -f

This option instructs the ra6 tool to flood the victim host with Prefix information options. The number of Prefix Information options to be sent is specified as “-f number”. When this option is specified, a “-P” option must be specified (with the usual syntax “-P prefix/length#flags#valid#preferred”), such that it instructs ra6 about how to generate the Prefix Information options. The “prefix/length” specifies the length of the prefixes that will be included in each Prefix Information option. While the prefix length will be constant for all options, the actual prefix will be randomized. The rest of the parameters will be shared by all the prefixes, and have the same “defaults” as indicated in the description of the “-P” option.

--flood-sources, -F

This option instructs the tool to send Router Advertisement messages from multiple addresses. The number of different sources is specified as “-F number”. The Source Address of each Router Advertisement is randomly selected from the prefix specified by the “-s” option. If the “-F” option is specified but the “-s” option is left unspecified, the Source Address of the packets is randomly selected from the prefix fe80::/64 (link-local unicast). It should be noted that hosts are required to discard Router Advertisement messages that do not have a link-local unicast address as the Source Address.

--flood-routes, -w

This option instructs the ra6 tool to flood the target with Route Information options. The number of Route Information options to be sent is specified as “-R number”. When this option is specified, a “-R” option should be specified (with the usual syntax “-R prefix/length#preference#lifetime”) such that ra6 is instructed about how to generate the Route Information options. The “prefix/length” species the length of the prefixes that will be included in each Route Information option. While the prefix length will be constant for all options, the actual prefix will be randomized. The rest of the parameters are shared by all the the options, and have the same “default values” as indicated in the description of the “-R” option.

--flood-dns, -w

This option instructs the ra6 tool to flood the target with random IPv6 addresses (supposed to correspond to recursive DNS servers), by means of the Recursive DNS Server (RDNSS) option. The number of IPv6 addresses that are to be sent to the target is specified as “-k number”. As there is a limit in the number of IPv6 addresses that can be included in a RDNSS option, it may be necessary for the tool to split those addresses into several RDNSS options.

It is possible to instruct the ra6 about the maximum number of IPv6 addresses that each RDNSS option should contain, by means of a second (and optional) parameter to the “-k” option. Namely, the tool can be instructed to send a total number of addresses (“totaladdresses”) with up to some specific number (“addrsperooption”) of addresses per RDNSS option in the form “-k totaladdresses#addrsperooption”. This might be helpful if it is believed that the target implementation enforces a limit on the number of addresses it honors on a “per RNDSS option” basis, but no limit on the aggregate number of addresses. In such a case, an implementation might e.g. survive the attack “-k 5000”, but still be vulnerable to the attack “-k 5000#3”). The “Lifetime” value for these addresses can be specified by issuing a “-N” option with the desired “Lifetime” (this is analogous to how the “--flood-routes” operates together with the “-R” option, and how the “--flood-prefixes” operates together with the “-P” option).

--block-src, -j

This option sets a block filter for the incoming Router Solicitation messages based on their IPv6 Source Address. It allows the specification of an IPv6 prefix in the form “-j prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

--block-dst, -k

This option sets a block filter for the incoming Router Solicitation messages, based on their IPv6 Destination Address. It allows the specification of an IPv6 prefix in the form “-k prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

--block-link-src, -J

This option sets a block filter for the incoming Router Solicitation messages, based on their link-layer Source Address. The option must be followed by a link-layer address (currently, only Ethernet is supported).

--block-link-dst, -K

This option sets a block filter for the incoming Router Solicitation messages, based on their link-layer Destination Address. The option must be followed by a link-layer address (currently, only Ethernet is supported).

--accept-src, -b

This option sets an accept filter for the incoming Router Solicitation messages, based on their IPv6 Source Address. It allows the specification of an IPv6 prefix in the form “-b prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

--accept-dst, -g

This option sets a accept filter for the incoming Router Solicitation messages, based on their IPv6 Destination Address. It allows the specification of an IPv6 prefix in the form “-g prefix/prefixlen”. If the prefix length is not specified, a prefix length of “/128” is selected (i.e., the option assumes that a single IPv6 address, rather than an IPv6 prefix, has been specified).

--accept-link-src, -B

This option sets an accept filter for the incoming Router Solicitation messages, based on their link-layer Source Address. The option must be followed by a link-layer address (currently, only Ethernet is supported).

`--accept-link-dst, -K`

This option sets an accept filter for the incoming Router Solicitation messages, based on their link-layer Destination Address. The option must be followed by a link-layer address (currently, only Ethernet is supported).

`--loop, -l`

This option instructs the ra6 tool to send periodic Router Advertisements to the destination node. The amount of time to pause between sending Router Advertisements can be specified by means of the “-z” option, and defaults to 1 second. Note that this option cannot be set in conjunction with the “-L” (“--listen”) option.

`--sleep, -z`

This option specifies the amount of time to pause between sending Router Advertisements. If left unspecified, it defaults to 1 second.

`--listen, -L`

This option specifies that the tool should enter the “passive” mode (possibly after operating in active mode, if the ‘-d’ or ‘-D’ options were specified).

`--verbose, -v`

This option instructs the ra6 tool to be verbose.

`--help, -h`

Print help information for the ra6 tool.

Examples

Example #1

```
# ./ra6 -i eth0 -P 2001::/64#LA -P 2002::/64#A -e -L
```

Listen (“-L”) for incoming Router Solicitations on interface eth0 (“-i eth0”), and advertise the prefix 2001::/64 for both on-link determination and auto-configuration (“-P 2001::/64#LA”) and the prefix 2002::/64 only for auto-configuration (“-P 2002::/64#A”). Include a source link-layer address option (“-e”) in the Router Advertisements.

Example #2

```
# ./ra6 -i eth0 -d fe80::1 -D 01:02:03:04:05:06 -c 5 --lifetime 100 -o  
-e -M 1400
```

Use the network interface “eth0” to send a Router Advertisement using a random link-local IPv6 Source Address and a random Ethernet Source Address, to the IPv6 Destination address fe80::1 and the Ethernet Destination Address 01:02:03:04:05:06. The Router Advertisement includes a “Router Lifetime” of 100, and advertises a CurHop value of 5 (i.e., a recommended “Hop Limit” of “5”). The ‘O’ bit is set (thus indicating that other configuration information is available via DHCP). The Router Advertisement includes a source link-layer address option (containing the same address as the Ethernet Source Address of the packet) and an MTU option with a value of 1400.

Example #3

```
# ./ra6 -i eth0 --flood-sources 10 --flood-routes 50 --flood-prefixes 40  
-R ::/64#1 -P ::/48#LA -L -e
```

Listen for incoming Router Solicitation messages on the interface “eth0”, and respond with Router Advertisements from 10 different link-local unicast IPv6 Source Addresses (randomized) and 10 different (randomized) Ethernet Source Addresses. Each Router Advertisement includes 50 Route Information options, each of them with a randomized /64 prefix and a preference of 1 (“high”). The Router Advertisements also contain 40 Prefix Information options, each with a randomized /48 prefix and the ‘A’ (auto-configuration) and ‘L’ (on-link determination) bits set. In addition, each Router Advertisement includes a source link-layer address option, containing the same (randomized) address as that used for the Ethernet Source Address field.

Example #4

```
# ./ra6 -i eth0 -N 1000#fe80::1#2001:db8::1 -L
```

Listen for incoming Router Solicitation messages, and respond with a Router Advertisement that contains one RDNSS option with two IPv6 addresses (fe80::1 and 2001:db8::1), with a Lifetime of

“1000”. All Router Solicitation messages sent to multicast addresses will be responded using the same (randomized) IPv6 Source Address and the same (randomized) Ethernet Source Address. Router Solicitation messages destined to unicast addresses will be responded with Router Advertisements using the IPv6 Destination Address and the Ethernet Destination Address of the incoming Router Solicitation message for the IPv6 Source Address and the Ethernet Source Address of the Router Advertisement, respectively.

Example #5

```
# ./ra6 -i eth0 -s fe80::1234 -S 00:01:02:03:04:05 -d fe80::1 -N 900  
--flood-dns 1000#10 -L
```

Flood the target (fe80::1) with 1000 random IPv6 addresses of Recursive DNS Servers, with a maximum of 10 addresses per RDNSS option. Each RDNSS option has a “Lifetime” of 900. Packets are sent with an IPv6 Source Address of “fe80::1234” and an Ethernet Source Address of “00:01:02:03:04:05”. Once the target has been attacked, listen for incoming Router Solicitation messages and respond with the same “flood” packets (the Ethernet Source Address and the IPv6 Source Address will change if the Router Solicitation messages have been sent to a unicast address, though).

Credits

The IPv6 Toolkit version 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>>.