

rd-attack v1.0 manual pages

Description

This tool is part of a security assessment suite for the Neighbor Discovery protocol. It allows the assessment of IPv6 implementations with respect to a variety of attack vectors based on ICMPv6 Redirect 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 if an IPv6 Destination Address, a Redirect Destination Address, and a Redirect Target Address are specified. Passive mode is employed if the “-L” option (or its long counterpart “--listen”) is set. If both an attack target and the “-L” option are specified, the attack is launched against the specified target, and then the tool enters passive mode to respond incoming packets with ICMPv6 Redirect messages.

The tool supports filtering of incoming packets 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 packet matches any of those filters, the message is discarded (and thus no Redirect messages are sent in response). If any “accept filter” is specified, incoming packets must match the specified filters in order for the tool to respond with Redirect messages.

Options

The rd-attack 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) to be conveyed into the ICMPv6 Redirect messages, it may be necessary for the rd-attack tool to split that information into more than one Redirect message. Also, if the tool is instructed to e.g. flood the victim with Redirect messages from different sources (“--flood-sources” option), multiple packets may need to be generated. rd-attack supports IPv6 fragmentation, which might be of use to circumvent layer-2 filtering and/or Network Intrusion Detection Systems (NIDS). However, 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 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 specifies the IPv6 source address (or IPv6 prefix) to be used for the Source Address of the attack packets. This address typically corresponds to the IPv6 link-local address of the default router. If the “-F” (“--flood-sources”) option is specified, this option includes an IPv6 prefix, from which random addresses are selected. See the description of the “-F” option for further information on how the “-s” option is processed in that specific case.

Note: Instead of specifying the “Source Address” with this option, the “--learn-router” option could be set, such that the tool automatically learns the IPv6 link-local address of the default router, and uses this address for the “Source Address” of the Redirect messages.

`--dst-address, -d`

This option specifies the IPv6 Destination Address of the victim. It can be left unspecified only if the “-L” option is selected (i.e., if the tool is to operate in “Passive” mode).

When operating in passive mode (“-L” option), the IPv6 Destination Address is selected according to the IPv6 Source Address of the incoming packet.

`--hop-limit, -A`

This option specifies the Hop Limit to be used for the Redirect messages. It defaults to 255. Note that IPv6 nodes are required to check that the Hop Limit of incoming Redirect 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 Redirect messages (currently, only Ethernet is supported). If left unspecified, the link-layer Source Address is randomized. However, if this option is left unspecified, but the “--learn-router” option is set, the link-layer Source Address is set to that of the default router for the local network.

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

This option specifies the link-layer Destination Address of the Redirect messages (currently, only Ethernet is supported). If left unspecified, it is set to the “all-nodes link-local multicast” address (ff02::1).

When operating in passive mode, the link-layer Destination Address is set according to the link-layer Source Address of the incoming packet.

`--redir-target, -t`

This option specifies the Target Address of the Redirect 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.

This option can be left unspecified only if the “--make-onlink” option is selected, in which case the Redirect Target Address is set to the same value as the Redirect Destination address.

`--redir-dest, -r`

This option specifies the Redirect Destination Address. If the “-R” (“--flood-dests”) option is specified, this option specifies an IPv6 prefix in the form “-r prefix/prefixlen”. See the description of the “-R” option for further information on how the “-t” option is processed in that specific case.

`--payload-type, -p`

This option specifies the payload type to be included in the Redirect Payload. Currently supported payloads are “TCP”, “UDP”, and “ICMP6”. The payload-type defaults to “TCP”.

`--payload-size, -P`

Size of the payload to be included in the Redirect message (with the payload type being specified by the “-p” option). By default, as many bytes as possible are included, without exceeding the minimum IPv6 MTU (1280 bytes).

`--no-payload, -n`

This option specifies that no payload (i-e-, no Redirected Header option) should be included in the Redirect message.

`--ipv6-hlim, -c`

This option specifies the Hop Limit of the IPv6 packet included in the payload of the Redirect message. It defaults to 255.

`--peer-addr, -x`

This option specifies the IPv6 Source Address of the Redirect payload. If left unspecified, the IPv6 Source Address of the Redirect payload is set to the same value as the IPv6 Destination Address of the packet. This option is only employed for packets sent in “active” mode.

Note: this option might be useful to check whether an implementation validates the contents of the Redirect message.

`--redir-port, -o`

This option specifies the Destination Port of the TCP or UDP packet contained in the Redirect payload.

Note: This option is meaningful only if “TCP” or “UDP” have been specified with the “-p” option.

`--peer-port, -a`

This option specifies the Source Port of the TCP or UDP packet contained in the Redirect payload.

Note: This option is meaningful only if “TCP” or “UDP” have been specified with the “-p” option.

`--tcp-flags, -X`

This option specifies the flags of the TCP header contained in the Redirect payload. The flags are specified as “F” (FIN), “S” (SYN), “R” (RST), “P” (PSH), “A” (ACK), “U” (URG), “X” (no flags). If left unspecified, only the “ACK” bit is set.

Note: This option is meaningful only if “TCP” has been specified with the “-p” option.

`--tcp-seq, -q`

This option specifies the Sequence Number of the TCP header contained in the Redirect payload. If left unspecified, the Sequence Number is randomized.

Note: This option is meaningful only if “TCP” has been specified with the “-p” option.

`--tcp-ack, -Q`

This option specifies the Acknowledgment Number of the TCP header contained in the Redirect payload. If left unspecified, the Acknowledgment Number is randomized.

Note: This option is meaningful only if “TCP” has been specified with the “-p” option.

`--tcp-urg, -V`

This option specifies the Urgent Pointer of the TCP header contained in the Redirect payload. If left unspecified, the Urgent Pointer is set to 0.

Note: This option is meaningful only if “TCP” has been specified with the “-p” option.

`--tcp-win, -w`

This option specifies the Window of the TCP header contained in the Redirect payload. If left unspecified, the Window is randomized.

Note: This option is meaningful only if “TCP” has been specified with the “-p” option.

`--resp-mcast, -M`

This option specifies that, when operating in “passive” mode, the tool should also respond to packets sent to multicast addresses. By default, the tool does not send Redirects in response to packets sent to multicast addresses.

`--make-onlink, -O`

This option instructs the tool to set the Redirect Target Address to the same value as the Redirect Destination Address, thus causing the specified address to be considered “on-link”.

`--learn-router, -N`

This option instructs the tool to learn the link-layer and the (link-local) IPv6 addresses of the local router by means of Router Solicitation and Router Advertisement messages. If the IPv6 Source Address or the link-layer Source Address are left unspecified, the corresponding values learned with this option will be used.

Note: This option is very useful to avoid having to manually enter the IPv6 and/or Ethernet addresses of the router.

`--target-lla-opt, -E`

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

`--add-tlla-opt, -e`

This option instructs the rd-attack tool to include a target link-layer address option in the Redirect messages that it sends. When this option is employed, the link-layer Source Address must be specified, and such value will be used for the target link-layer address option. The difference between this option and the “-E” option is that the “-e” option does not specify the actual value of the option, but just instructs the tool to include a target link-layer address option (the actual value of the option is selected as explained before).

`--block-src, -j`

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

`--sanity-filters, -w`

This option automatically adds an “accept filter” for the link-layer Destination Address corresponding to the local router (either learned as a result of the “--learn-router” option, or specified by the “-S” option), and a block filter for the IPv6 Source Address fe80::/16.

Note: This option is desirable in virtually all scenarios, such that the tool does not respond to link-local traffic, etc.

`--flood-dests, -R`

This option instructs the rd-attack tool to send multiple Redirect messages for different Redirect Destination Addresses. The number of different Redirect Destination Addresses is specified as “-R number”. The Redirect Destination Address of each packet is randomly selected from the prefix ::/0, unless a different prefix has been specified by means of the “-r” option.

`--flood-targets, -T`

This option instructs the rd-attack tool to send multiple Redirect messages for different Redirect 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 fe80::/64, unless a different prefix has been specified by means of the “-t” option.

--flood-sources, -F

This option instructs the tool to send multiple Redirect messages with different Source Addresses. The number of different sources is specified as “-F number”. The Source Address of each Redirect message 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 Redirect messages whose IPv6 Source address does not match the (link-local) IPv6 address of the router used for the Redirect Destination Address.

--loop, -l

This option instructs the rd-attack tool to send periodic Redirect messages to the victim node. The amount of time to pause between sending Redirect messages 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 Redirect messages (when the “--loop” option is set). If left unspecified, it defaults to 1 second.

--listen, -L

This instructs the rd-attack tool to operate in passive mode (possibly after attacking a given node). Note that this option cannot be used in conjunction with the “-l” (“--loop”) option.

--verbose, -v

This option instructs the rd-attack tool to be verbose. When the option is set twice, the tool is “very verbose”, and the tool also informs which packets have been accepted or discarded as a result of applying the specified filters.

--help, -h

Print help information for the na-attack tool.

Examples

Example #1

```
# ./rd-attack -i eth0 --learn-router --sanity-filters -L --make-onlink -v
```

The tool uses the network interface “eth0”, and operates in passive mode (“-L” option). The IPv6 and Ethernet address of the local router is automatically learned by means of RS/RA messages. Basic filters are employed to avoid responding to incorrect/unnecessary packets (“--sanity-filters”). Each Redirect message will contain the Redirect Target Address set to the same value as the Redirect Destination Address, thus causing the corresponding address to be considered “on-link” (“--make-onlink” option). The tool will print detailed information about the attack (“-v” option).

Example #2

```
# ./rd-attack -i eth0 --learn-router -d 2001:db8::1 -r 2001:db8::/64 -t fe80::bad -R 100 -l -v
```

Flood the victim host (specified with the “-d” option) with batches of 100 Redirect messages (“-R 100” option). Each Redirect message redirects a random address from the prefix “2001:db8::/64” to the address “fe80::bad”. The IPv6 and link-layer addresses of the current local router is dynamically learned by means of RS/RA messages (“--learn-router” option). The process is repeated every second (“-l” option, with the default delay of 1 second).

Credits

The IPv6 Neighbor Discovery Tools version 1.0 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>>.