jumbo6 v1.3 manual pages

Description

This tool allows the assessment of IPv6 implementations with respect to attack vectors based on IPv6 jumbograms. This tool is part of the IPv6 Toolkit v1.3: a security assessment suite for the IPv6 protocols.

Modes of Operation

This tool has two modes of operation: active and listening. Active mode is employed if an IPv6 Destination Address is specified, while "listening" mode is employed if the "-L" option (or its long counterpart "--listen") is set. If both a target and the "-L" option are specified, IPv6 jumbograms are sent to the specified target, and then the tool enters listening mode to send IPv6 jumbograms in response to incoming packets.

In active mode, the tool sends IPv6 jumbograms to the specified target, and informs the user of any received ICMPv6 error messages (typically "ICMPv6 Parameter Problem" error messages). In "listening" mode, the tool listens to traffic on the local network, and sends IPv6 jumbograms in response to received packets.

When operating in "listening" mode, the tool can filter 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 attack packets 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 attack packets.

Options

The jumbo6 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").

jumbo6 supports IPv6 Extension Headers, including the IPv6 Fragmentation Header, which might be of use to circumvent layer-2 filtering and/or Network Intrusion Detection Systems (NIDS). However, IPv6 extension headers are not employed by default, and must be explicitly enabled with the corresponding options.

`--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-link-address, -S`

This option specifies the link-layer Source Address of the IPv6 jumbograms (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 IPv6 jumbograms (currently, only Ethernet is supported). By default, the link-layer Destination Address is automatically set to the link-layer address of the destination host (for on-link destinations) or to the link-layer of the first-hop router.

`--src-address, -s`

This option specifies the IPv6 Source Address (or IPv6 prefix) to be used for the Source Address of the attack packets. If an IPv6 prefix is specified, the IPv6 Source Address is randomized from that prefix. If left unspecified, a real IPv6 address of the specified network interface is used.

Note: When operating in “listening” mode, the Source Address is automatically set to the Destination Address of the incoming packet.

`--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 “listening” mode).

Note: When operating in “listening” mode, the Destination Address is automatically set to the Source Address of the incoming packet.

`--hop-limit, -A`

This option specifies the Hop Limit to be used for the IPv6 packets. By default, the Hop Limit is randomized.

`--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.

`--ipv6-length`, `-q`

This option specifies the value that the "Total Length" field of the IPv6 header should be set to. If this option is left unspecified, the "Total Length" field is set to 0, as required by the IPv6 jumbograms specification.

`--jumbo-length`, `-Q`

This option specifies the value to which the "Jumbo Payload Length" field of the Jumbo Payload option should be set. If this option is left unspecified, the "Jumbo Payload Length" field is set according to the real size of the jumbo payload (see the "-p" option).

`--payload-size`, `-P`

This options specifies the size of the jumbo payload. If left unspecified, the payload size is set to 0.

`--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`, `-G`

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).

`--loop, -l`

This option instructs the jumbo6 tool to send periodic IPv6 jumbograms to the victim node. The amount of time to pause between sending IPv6 jumbograms 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 IPv6 jumbograms (when the "--loop" option is set). If left unspecified, it defaults to 1 second.

`--listen`, `-L`

This option instructs the jumbo6 tool to operate in listening mode (possibly after attacking a given node, if a target was specified with the "-d" option). Note that this option cannot be used in conjunction with the "-l" ("--loop") option.

`--verbose`, `-v`

This option instructs the jumbo6 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 jumbo6 tool.

Examples

Example #1

```
# jumbo6 -i eth0 -s fc00:1::/64 -d fc00:1::1 -P 100
```

Send an IPv6 jumbogram to the host fc00:1::1. The IPv6 Source Address will be randomly selected from the prefix fc00:1::/64, and a the payload of 100 bytes is included in the packet.

Example #2

```
# jumbo6 -i eth0 -L -b 2001:db8::1 -v
```

Listen on the eth0 interface to incoming packets with the IPv6 Source Address set to “2001:db8::1”, and respond to such packets with an IPv6 jumbogram. Be verbose.

Credits

The jumbo6 tool and related manuals were produced by Fernando Gont <fgont@si6networks.com> for SI6 Networks <http://www.si6networks.com>.

License