

ni6 v1.0 manual pages

Description

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

Modes of Operation

This tool has two modes of operation: “active” and “listening”. In “active” mode, the tool attacks a specific target, while in “listening” mode the tool listens to ICMPv6 Node Information Query messages on the local network, and sends ICMPv6 Node Information Reply messages in response to such traffic. Active mode is employed if an IPv6 Destination Address is specified. Listening 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 listening mode to respond incoming packets with TCP segments.

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 ICMPv6 NI Reply messages are sent in response). If any “accept filter” is specified, incoming packets must match any of the specified “accept filters” in order for the tool to respond with ICMPv6 NI Reply messages.

Options

The ni6 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”).

ni6 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-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 of the ICMPv6 packets will be randomized from the specified prefix.

Note: When operating in “listening” mode, the Source Address is automatically selected depending on the IPv6 Destination Address of the ICMPv6 NI Query (unless a specific IPv6 Source Address has been specified with the “-s” option).

--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 ICMPv6 NI Query message.

--hop-limit, -A

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

--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 TCP segments (currently, only Ethernet is supported). If left unspecified, the link-layer Source Address is set to the real link-layer address of the network interface.

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

This option specifies the link-layer Destination Address of the ICMPv6 NI packets (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.

`--payload-size, -P`

This options specifies the size (in bytes) of the ICMPv6 NI payload.

`--subject-ipv6, -6`

This option specifies an IPv6 Address to be used as the Subject of ICMPv6 Node Information Query messages.

`--subject-ipv4, -4`

This option specifies an IPv4 Address to be used as the Subject of ICMPv6 Node Information Query messages.

`--subject-name, -n`

This option specifies a Name to be used as the Subject of ICMPv6 Node Information Query messages. By default, the specified name is considered to be a Fully-Qualified Domain Name (FQDN). Please consult the “--sname-slabel” option for instructions on how to specify “single-label” names.

`--subject-fname, -N`

This option instructs the ni6 tool to set the Subject of ICMPv6 NI Query messages to a forged name of the specified length.

Note: The forged name is a sequence of labels of 'a' characters, with the maximum label size being specified by means of the “--max-label-size” option.

`--subject-ename, -x`

This option instructs the ni6 tool to set the Subject of an ICMPv6 NI Query message to a malformed label of the specified length. This option is useful for including a malformed label that “spans past the end of the ICMPv6 NI Query”.

`--subject-nloop, -0`

This option specifies that the Data field should be set to a Name that contains a DNS compression loop. The loop type is specified with this option, with valid values being in the range 0-1.

`--sname-slabel, -e`

This option specifies that the specified Subject Name is a single-label name, and hence should be terminated with two (rather than one) NULL labels.

`--max-label-size, -Z`

This option specifies the maximum Name label size. It defaults to 63.

`--code, -C`

This option specifies the ICMPv6 code. For ICMPv6 NI Query messages, if specific Subject type is specified, the ICMPv6 code is automatically set to the corresponding value.

`--qtype, -q`

This option specifies the Qtype value of ICMPv6 NI messages. For ICMPv6 NI Reply messages, if specific Data type is specified, the ICMPv6 Qtype is automatically set to the corresponding value.

--flags, -X

This option specified the “Flags” field of the ICMPv6 NI messages.

For ICMPv6 NI Query messages of Qtype 3 (Node IPv6 Addresses), the “Flags” field defaults to “GSLCA”. For ICMPv6 NI Query messages of Qtype 4 (Node IPv4 Addresses), the “Flags” field defaults to “A”. For other ICMPv6 NI Query messages it defaults to 0.

For ICMPv6 Reply messages, the “Flags” field is copied from the corresponding ICMPv6 NI Query message.

--data-ipv6, -w

This option specifies an IPv6 Address to be used as the Data of ICMPv6 Node Information Reply messages.

--data-ipv4, -W

This option specifies an IPv4 Address to be used as the Data of ICMPv6 Node Information Reply messages.

--data-name, -a

This option specifies a Name to be used as the Data of ICMPv6 Node Information Reply messages. By default, the specified name is considered to be a Fully-Qualified Domain Name (FQDN). Please consult the “--dname-slabel” option for instructions on how to specify “single-label” names.

--data-fname, -A

This option instructs the ni6 tool to set the Data of the ICMPv6 NI Reply messages to a forged name of the specified length.

Note: The forged name is a sequence of labels of 'a' characters, with the maximum label size being specified by means of the “--max-label-size” option.

--data-ename, -Q

This option instructs the ni6 tool to set the Data of ICMPv6 NI Reply messages to a malformed label of the specified length. This option is useful for including a malformed label that “spans past the end of the ICMPv6 NI Reply”.

`--data-nloop, -O`

This option specifies that the Data field should be set to a Name that contains a DNS compression loop. The loop type is specified with this option, with valid values being in the range 0-2.

`--dname-slabel, -E`

This option specifies that the specified Data Name is a single-label name, and hence should be terminated with two (rather than one) NULL labels.

`--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 an 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).

`--forge-src-addr, -r`

This option instructs the ni6 tool to forge the IPv6 Source Address of ICMPv6 NI messages. Note that when operating in listening mode, unless this tool is set, ni6 will not impersonate other nodes.

`--forge-link-src-addr, -R`

This option instructs the ni6 tool to forge the link-layer Source Address of ICMPv6 NI messages.

Note: Some interface cards (or their corresponding drivers) may silently discard packets that contain a forged link-layer Source Address.

`--loop, -l`

This option instructs the tcp6 tool to send periodic TCP segments to the victim node. The amount of time to pause between sending TCP segments 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 ICMPv6 Node Information

UK CPNI (Centre for the Protection of National Infrastructure)

Query messages (when the “--loop” option is set). If left unspecified, it defaults to 1 second.

--listen, -L

This instructs the ni6 tool to operate in listening mode (possibly after attacking a specified target). Note that this option cannot be used in conjunction with the “-l” (“--loop”) option.

--verbose, -v

This option instructs the ni6 tool to be verbose. When the option is set twice, the tool is “very verbose”, and the tool also informs which packets have been discarded as a result of applying the specified filters.

--help, -h

Print help information for the ni6 tool.

Examples

Example #1

```
# ni6 -i eth0 --subject-ipv6 ff02::1 -d ff02::1 -q 2 -v
```

Send an ICMPv6 Node Information Query to the multicast address ff02::1 (“-d” option), with a Subject IPv6 Address of “ff02::1” (“--subject-ipv6” option), querying for Node names (“-q” option). Be verbose.

Example #2

```
# ni6 -i eth0 --data-fname 1000 -L --forge-src-addr -v
```

Listen to incoming ICMPv6 Node Information Query messages querying for node names, and respond with ICMPv6 NI Reply messages that contain a forged name of 700 bytes. Forge the IPv6 Source Address of the packets. Be verbose.

Credits

The ni6 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

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>>.