flow6 v1.2 manual pages

Description

This tool performs a security assessment of the Flow Label generation policy of a target node. This tool is part of the IPv6 Toolkit v1.2: a security assessment suite for the IPv6 protocol developed by the UK CPNI.

Operation

The tool sends a number of probe packets to the target node, and samples the Flow Label values of the corresponding response packets. Based on the sampled values, it tries to infer the Flow Label generation policy of the target.

The tool will first send a number of probe packets from single IPv6 address, such that the per-destination policy is determined. The tool will then send probe packets from random IPv6 addresses (from the same prefix as the first probes) such that the "global" Flow Label generation policy can be determined.

The tool computes the expected value and the standard deviation of the difference between consecutive-sampled Flow Label values ($Label_n$ – $Label_{n-1}$) with the intent of inferring the Flow Label generation algorithm of the target node.

If the standard deviation of [$Label_n$ – $Label_{n-1}$] is 0, the Flow Label is assumed to be set to a constant value, and the corresponding value is informed to the user. For small values of the standard deviation, the Flow Label is assumed to be a monotonically-increasing function with increments of the "expected value", and such "expected value" together with the standard deviation, are informed to the user. For large values of the standard deviation, the Flow Label is assumed to be randomized, and the expected value and standard deviation are informed to the user, as indicators of the "quality" of the Flow Label generation algorithm.

Options

The flow6 tool takes it 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").

`--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 probe packets. If an IPv6 prefix is specified, the IPv6 Source Address of the ICMPv6 packets will be randomized from that prefix.

`--dst-address`, `-d`

This option specifies the IPv6 Destination Address of the target node. This option cannot be left unspecified.

`--hop-limit, -A`

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

`--src-link-address`, `-S`

This option specifies the link-layer Source Address of the probe packets (currently, only Ethernet is supported). If left unspecified, the link-layer Source Address of the packets 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 probe 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 address of the first-hop router.

`--protocol`, `-P`

This option specifies the protocol type of the probe packets. Currently, both “UDP” and “TCP” are supported. If this option is left unspecified, the protocol type defaults to “TCP”.

`--dst-port`, `-p`

This option specifies the Destination Port of the probe packets. If left unspecified, the Destination Port defaults to “80” when the IPv6 payload is TCP, and to 53 if the IPv6 payload is UDP.

Note: Since it is vital for the tool to receive response packets to be able to infer the Flow Label algorithm of the target, the protocol type and Destination Port should be carefully selected (i.e., the corresponding protocol and Destination Port should not be filter, and the target should respond to packets sent to that protocol/port).

`--flow-label-policy`, `-W`

This option instructs the tool to determine the Flow Label generation policy. As of this version of the tool, this option must be specified.

`--verbose`, `-v`

This option instructs the flow6 tool to be verbose. If this option is set twice, the tool is "very verbose", and outputs the sampled Flow Label values (in addition to other information).

`--help`, `-h`

Print help information for the flow6 tool.

Examples

Example #1

```
# flow6 -i eth0 --flow-label-policy -d fe80::1 -v
```

Assess the Flow Label generation policy of the host "fe80::1", using the network interface "eth0". Probe packets are TCP segments directed to port 80 (default). Be verbose.

Example #2

```
# flow6 -i eth0 -d fe80::1 --flow-label-policy -P TCP -p 22 -vv
```

Assess the Flow Label generation policy of the host "fe80::1", using the network interface "eth0". Probe packets are TCP segments directed to port 22. Be very verbose (i.e., list the sampled Flow Label values).

Credits

The flow6 tool 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