scan6 v1.2 manual pages

Description

scan6 is an IPv6 host scanning tool. It implements a number of IPv6-specific host scanning techniques. It is part of the IPv6 Toolkit v1.2: a security assessment suite for the IPv6 Protocol developed by the UK CPNI.

Options

The scan6 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").

`--interface, -i`

This option specifies the network interface to be used by the scan6 tool. Specification of the network interface is mandatory (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 a prefix is specified, the Source Address is randomly selected from that prefix.

If this option is left unspecified, the addresses currently configured for the specified network interface card are used.

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

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

Note: Some systems may discard packets when the link-layer address is forged. That is, even when the relevant function calls (and hence the scan6 tool itself) may return "success", packets may be discarded and not actually sent on the specified network link. In such scenarios, the real Ethernet address should be used. This type of behaviour has been found in some Linux systems.

`--probe-type, -p`

This option specifies the probe packets to be used for host scanning. The possible arguments are: "echo" (for ICMPv6 Echo Request), "unrec" (for IPv6 packets with unrecognized IPv6 options of type 10xxxxxx), and "all" (for using both ICMPv6 Echo Requests probes and unrecognized options of type 10xxxxxx). If left unspecified, this option defaults to "all".

Note: Using unrecognized IPv6 options of type 10xxxxxx enables the discovery of Windows Vista and Windows 7 systems, which otherwise do not respond to ICMPv6 Echo Requests sent to multicast addresses.

`--print-type, -P`

This option specifies the address types to be printed/informed by the scan6 tool. The possible arguments are: "local" (link-local addresses), "global" (global addresses), and "all" (print both link-local and global-addresses). If left unspecified, this option defaults to "all" (print both link-local and global-addresses).

`--print-unique, -q`

This option species that for each address scope (local and/or global) only one IPv6 address per Ethernet address should be printed. This option can be useful when interest is in identifying unique systems (e.g. for counting the number of systems connected to the local network).

Note: In the case of systems that implement "Privacy Extensions for SLAAC", more than one global unicast address will typically be found by the scan6 tool.

`--print-link-addr, -e`

This option specifies that the link-layer addresses should be printed along with the IPv6 addresses, with the format "IPV6ADDRESS @ LINKADDRESS".

`--retrans, -x`

This option specifies the number of times probe packets should be retransmitted when no response is received. Note: If left unspecified, the number of retransmission defaults to 0 (i.e., no retransmissions).

Note: this option might be useful when packets must traverse unreliable and/or congested network links.

`--timeout, -o`

This option specifies the amount of time that the tool should wait for responses to probe packets. If left unspecified, the timeout value defaults to 1 second.

Note: this option might be useful when scanning hosts on long-delay links.

```
--local, -l
```

This option specifies that host scanning should be performed on the local subnet. The type of probe packets to be used can be specified with the "-p" option.

```
--rand-src-addr, -r
```

This options specifies that the IPv6 Source Address should be randomized.

```
--rand-link-src-addr, -R
```

This options specifies that the Ethernet Source Address should be randomized.

```
--verbose, -v
```

This option selects the "verbosity" of the tool. If this option is left unspecified, only minimum information is printed. If this option is set once, additional information is printed (e.g., the tool indicates which addresses are "link-local" and which addresses are "global"). If this option is set twice, detailed information will be printed in the case the tool finds any problems when performing host scanning.

```
--help, -h
```

Print help information for the scan6 tool.

Examples

Example #1

```
# ./scan6 -i eth0 -l -e -v
```

Perform host scanning on the local network ("-l" option) using interface "eth0" ("-i" option). Use both ICMPv6 echo requests and unrecognized IPv6 options of type 10xxxxxx (default). Print link-link layer addresses along with IPv6 addresses ("-e" option). Be verbose ("-v" option).

<u>Example #2</u>

```
# ./scan6 -i eth0 -l -S 66:55:44:33:22:11 -p unrec -P global -v
```

Use the "eth0" interface ("-i" option) to perform host-scanning on the local network ("-l" option). The Ethernet Source Address is set to "66:55:44:33:22:11" ("-S" option). The probe packets will be IPv6 packets with unrecognized options of type 10xxxxxx ("-p" option). The tool will only print IPv6 global addresses ("-P" option). The tool will be verbose.

<u>Example #3</u>

```
# ./scan6 -i eth0 -l -P global –print-unique -e
```

Use the "eth0" interface ("-i" option) to perform host-scanning on the local network ("-l" option). Print only global unicast addresses ("-P" option), and at most one IPv6 address per Ethernet address ("--print-unique" option). Ethernet addresses will be printed along with the corresponding IPv6 address ("-e" option).

Credits

The scan6 tool and related manuals were originally 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>.