scan6 v1.3 manual pages

Description

scan6 is an IPv6 address scanning tool that implements a number of advanced IPv6 address scanning techniques. It is part of the SI6 Networks' IPv6 Toolkit v1.3: a security assessment suite for the IPv6 protocols.

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.

`--dst-address, -d`

This option specifies the target address prefix/range of the address scan. An IPv6 prefix can be specified in the form 2001:db8::/64, or as 2001:db8:a-b:1-10 (where specific address ranges are specified for the two low order 16-bit words). This option must be specified for remote address scanning attacks.

`--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 behavior has been found in some Linux systems.

`--probe-type, -p`

This option specifies the probe packets to be used for address scanning. For local-network address scans, 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”.

For remote-network address scans, possible arguments are: “echo” (for ICMPv6 Echo Request), “unrec” (for IPv6 packets with unrecognized IPv6 options of type 10xxxxxx), and “tcp” (for using TC segments). For remote-network scans, this option defaults to “echo” (if left unspecified).

Note: For local-network address scans, 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.

`--payload-size, -P`

This options specifies the payload size of the probe packet. It defaults to 0 for TCP (i.e., empty TCP segments), and to 56 for ICMPv6.

`--src-port, -o`

This option specifies the TCP/UDP Source Port. If left unspecified, the Source Port is randomized from the range 1024-65535.

`--dst-port, -a`

This option specifies the TCP/UDP Destination Port. If left unspecified, the Destination Port is randomized from the range 1-1024.

`--tcp-flags, -X`

This option is used to set specific the TCP flags. The flags are specified as “F” (FIN), “S” (SYN), “R” (RST), “P” (PSH), “A” (ACK), “U” (URG), “X” (no flags).

If this option is left unspecified, the ACK bit is set on all probe packets.

`--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). Note: This option is only meaningful for local scans (“-l” option).

`--tgt-virtual-machines, -V`

This option specifies that the target is virtual machines. Possible options are: 'vbox' (VirtualBox), 'vmware' (vmware), and 'all' (both VirtualBox and vmware). When this option is specified, scan6 can narrow dow the search space by targetting only those IEEE OUIs employed by the aforementioned virtualization software. Note: For vmware, the search space can be further reduced if the '--ipv4-host' option is specified.

`--tgt-low-byte, -b`

This option specifies that the target is IPv6 nodes employing “low-byte” addresses.

`--tgt-ipv4-embedded, -B`

This option specifies that the target is IPv6 addresses that embed an IPv4 address. When this option is set, a prefix should be specified with the '--ipv4-host' option, such that the search space is reduced.

`--tgt-ieee-oui, -k`

This options is used to specify an IEEE OUI, such that the target of the scan is SLAAC addresses that employ the aforementioned IEEE OUI.

`--tgt-vendor, -K`

This option allows the user to specify a vendor name. scan6 will look-up all the correspoinding IEEE OUIs for such vendor, and then scan for SLAAC addresses that employ the aforementioned IEEE OUIs.

`--sort-ouis, -T`

This options, when used in conjunction with the “--tgt-vendor” option, tells the scan6 tool to “sort” the IEEE OUIs corresponding to a vendor. Namely, OUIs are employed in descending order, with the largest OUI used last (together with the smallest OUI). The rationale for this option is that when a vendor has been assigned multiple OUIs, chances are that the smaller (and “oldest”) OUI was used for devices that have already been put “out of service”, while the largest (and “newest”) OUI has probably not yet been used for deployed devices.

```
--ipv4-host, -Q
```

This options allows the user to specify an IPv4 prefix. The aforementioned prefix is employed with the “--tgt-virtual-machines” and/or “--tgc-ipv4-embeded” options to reduce the search space.

```
--inc-size, -I
```

This option is used to specify the increment size for the lowest-order 16-bit word of an IPv6 address when an IPv6 address range is to be scanned. This option is particularly useful if the target network is assumed to contain a large number of nodes with consecutive addresses (maybe because the target network employs DHCPv6, or because the target network contains a large number of devices from the same manufacturer, thus emplying consecutive MAC/SLAAC addresses). The increment size should be that of the assumed size of the “cluster” of nodes.

```
--config-file, -c
```

This option is used to specify an alternative configuration file. If left unspecified, the tool will employ '/etc/ipv6toolkit.conf'.

```
--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”. NOte: This option is only meaningful for local-network address scans.

```
--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).

Example #2

```
# ./scan6 -i eth0 -d 2001:db8::/64 –tgt-virtual-machines all –ipv4-host
10.10.10.0/24
```

Use the "eth0" interface ("-i" option) to scan for virtual machines (both VirtualBox and vmware) in the prefix 2001:db8::/64. The additional information about the IPv4 prefix employed by the host system is leveraged to reduce the search space.

Example #3

```
# ./scan6 -i eth0 -d 2001:db8::/64 –tgt-ipv4-embedded –ipv4-host
10.10.10.0/24
```

Use the "eth0" interface ("-i" option) to scan for IPv6 addresses of the network 2001:db8::/64 that embed the IPv4 prefix 10.10.10.0/24.

Example #4

```
# ./scan6 -i eth0 -d 2001:db8:0-500:0-1000
```

Use the "eth0" interface ("-i" option) to scan for IPv6 addresses of the network 2001:db8::/64, varying the two lowest order 16-bit words of the addresses in the range 0-500 and 0-1000, respectively.

Example #5

```
# ./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.

Example #6

```
# ./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 produced by Fernando Gont <fgont@si6networks.com> for SI6 Networks <http://www.si6networks.com>.

License