

scan6 v1.3.4 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 v1.3.4: a security assessment suite for the IPv6 protocols.

Host scanning techniques

scan6 employs a number of techniques to discover active IPv6 nodes. The following subsections discuss the different techniques employed for each type of IPv6 scan .

Local scans

For local scans, scan6 operates (roughly) as follows:

- The tool learns the local prefixes used for auto-configuration, and generates one address for each local prefix (in addition to a link-local address)
- An ICMPv6 Echo Request message destined to the all-nodes on-link multicast address (ff02::1) is sent with each of the addresses “configured” in the previous step. Probe packets are sent with different Source Addresses, such that they elicit responses from different addresses (as a result of the default IPv6 Source Address selection policy). Hence, all (or most) addresses of each node can be discovered.
- The same procedure of the previous bullet is performed, but this time with ICMPv6 packets that contain an unrecognized option of type 10xxxxxx, such that ICMPv6 Parameter Problem error messages are elicited. This allows the tool to discover e.g. Windows nodes, which otherwise do not respond to multicasted ICMPv6 Echo Request messages.
- Each time a new “alive” address is discovered, the corresponding Interface-ID is combined with all the local prefixes, and the resulting addresses are probed (with unicasted packets). This can help to discover all the SLAAC-derived and the “private addresses”, since some responses might contain e.g. Modified EUI-64 Format Identifiers, which are likely used with all the available prefixes.
- Finally, the tool removes any duplicate addresses, such that each unique address is informed to the user only once.

The aforementioned scheme can fail to discover some addresses for some implementation. For example, MacOS X employs IPv6 addresses embedding IEEE-identifiers when responding to packets destined to a link-local multicast address (and hence the temporary addresses could not be learned).

Remote scans

scan6 employs a number of bran-new techniquese for performing address scans of remote networks. Namely, it tries to mitigate a number of patterns in IPv6 addresses, such that the (theoretical) search space of 2^{64} addresses is dramatically reduced. scan6 can leverage the following address patterns:

- SLAAC addresses of specific vendors: Addresses that embedd the MAC address of the corresponding network interface card.
- virtual host addresses: Most virtualization technologies select their MAC addresses from specific IEEE OUIs (e.g., VirtualBox employs the OUI 00:50:56)
- "low-byte" addresses: in which only the lowest order (or the two lowest order) word of the IID contains a small integer (with the rest of the words being set to zero)
- IPv4-based addresses: in which the IID encodes the IPv4-address of the network interface (as in 2001:db8::192.168.1.1)
- IPv6 addresses embedding service ports, such as 2001:db8::80 (for a web server).

A thorough discussion of these address patterns can be found in: <<http://tools.ietf.org/html/draft-ietf-opsec-ipv6-host-scanning>>

Host tracking

scan6 can be employed to track IPv6 nodes across networks. Since IPv6 Stateless Address Auto-Configuration (SLAAC) typically results in globally-unique Interface Identifiers (IIDs) that are constant across networks, such identifiers can be leveraged to track nodes across a range of "known" networks, by periodically probing the IPv6 address composed of the IPv6 prefix of the target network, and the (known) Interface ID of the target node.

For host-tracking purposes, the target networks can be specified with the '-d' and/or '-m' options, while the target Interface IDs can be specified with the '-w' and/or the '-W' options (see the documentation of each option for further information).

Since for tracking purposes one will continually track the user across networks, the '-l' option will typically be set. Additionally, the '-z' option may be used to specify the number of seconds to sleep between iterations (i.e. each round of probes send to the specified targets). The value specified by the '-z' option represents a trade-off between time-liness of the tracking and bandwidth-consumption.

IPv6 host-tracking is discussed in detail in Appendix A of <<http://tools.ietf.org/html/draft-ietf-6man-stable-privacy-addresses>>.

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 down 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.

`-g, --tgt-port-embedded`

This option specifies that the target is IPv6 addresses that embed service ports (such as 2001:db8::25, 2001:db8::80, etc.). When this option is set addresses containing these ports will be probed:

- 21 (ftp)
- 22 (ssh)
- 23 (telnet)
- 25 (smtp)
- 49 (tacacs)
- 53 (dns)
- 80 (www)
- 110 (pop3)
- 123 (ntp)
- 179 (bgp)
- 220 (imap3)
- 389 (ldap)
- 443 (https)
- 547 (dhcpv6-server)
- 993 (imaps)
- 995 (pop3s)
- 1194 (openvpn)
- 3306 (mysql)
- 5060 (sip)
- 5061 (sip-tls)
- 5432 (postgresql)
- 6446 (mysql-proxy)
- 8080 (http-alt)

Note: The target IPv6 addresses are generated by concatenating the service port to an IPv6 prefix/range specified by means of the "-d" option. For each service port, four target address ranges will be generated:

PREFIX::0-5:HEX_PORT,
PREFIX::HEX_PORT:0-5,

PREFIX::0-5:DEC_PORT, and,
PREFIX::DEC_PORT:0-5

That is, IPv6 address ranges will be generated with both the service port in hexadecimal notation, and the service port in decimal notation, since both types of addresses have been found in the wild.

`--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 corresponding IEEE OUIs for such vendor, and then scan for SLAAC addresses that employ the aforementioned IEEE OUIs.

`--prefixes-file PREFIXES_FILE, -m PREFIXES_FILE`

This option specifies the name of a file containing a list of IPv6 addresses and/or IPv6 prefixes, one per line, in the same format as that used with the '-d' option. Note: The file can contain comments if they are preceded with the numeral sign ('#'), as in:

```
IPv6_address/len      # comment
# comment
IPv6_address
```

`--tgt-known-iids IIDS_FILE, -w IIDS_FILE`

This option specifies the name of a file containing one IPv6 address per line. The Interface ID of each of those IPv6 addresses will be employed, together with the network prefix specified with the '-d' option, to construct the IPv6 addresses to be probed. Since auto-configured addresses typically employ Interface IDs that are constant across networks, this option can leverage known IIDs to track such nodes across networks. Please see <<http://tools.ietf.org/html/draft-ietf-6man-stable-privacy-addresses>> for further details. Note: The file can contain comments if they are preceded with the numeral sign ('#'), as in:

```
IPv6_address          # comment
```

`--tgt-iid IID, -W IID`

This option specifies an IPv6 Interface Identifier (IID), with the same syntax as that of an IPv6 address (only the lowest-order 64 bits of the address will be employed). The specified Interface ID will be employed, together with the any network prefixes specified with the '-d' option (or with the

'-m' option), to construct the IPv6 addresses to be probed. Since auto-configured addresses typically employ Interface IDs that are constant across networks, this option can leverage known IIDs to track such nodes across networks. Please see <<http://tools.ietf.org/html/draft-ietf-6man-stable-privacy-addresses>> for further details. Note: The file can contain comments if they are preceded with the numeral sign ('#'), as in:

```
IPv6_address      # comment
```

```
--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 employing consecutive MAC/SLAAC addresses). The increment size should be that of the assumed size of the “cluster” of nodes.

```
-r, --rate-limit
```

This option specifies the rate limit to use when performing a remote address scan. “RATE” should be specified as “xbps” or “xpps” (with “x” being an unsigned integer), for rate-limits in bits per second or packets per second, respectively.

```
--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.

`--print-timestamp, -t`

This option specifies that a timestamp should be printed after the IPv6 address of each alive node.

`--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, -f`

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

```
--rand-link-src-addr, -F
```

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

```
--loop, -l
```

This option specifies that the tool should periodically loop through the specified targets. It is mostly useful to e.g. when a node disconnects from the network, or for host-tracking purposes.

```
--sleep SECONDS, -z SECONDS
```

This option specifies the amount of time (in seconds) that the tool should sleep in-between iterations over the specified targets. It is only meaningful when the '-l' option is set.

```
--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-layer addresses along with IPv6 addresses (“-e” option). Be verbose (“-v” option).

Example #2

SI6 Networks' IPv6 Toolkit v1.3.4

```
# 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 -d fc00::/64 --tgt-vendor 'Dell Inc' -p tcp
```

Use the “eth0” interface to scan for network devices manufactured by 'Dell Inc' in the target prefix fc00::/64. The tool will employ TCP segments as the probe packets (rather than the default ICMPv6 echo requests).

Example #6

```
# 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 #7

```
# scan6 -i eth0 -d 2001:db8::/64 -w KNOWN_IIDS
```

Use the “eth0” interface (“-i” option) to perform an address scan of a set of known hosts listed in the file KNOWN_IIDS, at remote network 2001:db8::/64. The target addresses are obtained by concatenating the network prefix 2001:db8::/64 with the interface IDs of each of the addresses found in the file KNOWN_IIDS.

Example #8

```
# 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).

Example #9

```
# scan6 -i eth0 -m knownprefixes.txt -w knowniids.txt -l -z 60 -t -v
```

Use the “eth0” interface (“-i” option). Build the list of targets from the IPv6 prefixes contained in the file “knownprefixes.txt” and the Interface IDs (IIDs) contained in the file “knowniids.txt”. Poll the targets periodically (“-l” option), and sleep 60 seconds after each iteration (“-z” option). Print a timestamp along the IPv6 address of each alive node (“-t” option). Be verbose (“-v” option).

Credits

The scan6 tool and related manuals were produced by Fernando Gont <fgont@si6networks.com> for SI6 Networks <<http://www.si6networks.com>>.

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>>.