格式: ike-scan [options] [hosts...]

目标主机必须在命令行上指定，除非-file选项是给定的，在这种情况下，目标是从指定的文件读取，而不是直接输入

目标主机可以被指定为IP地址或主机名。你也可以指定IP网络/位（例如192.168.1.0／24）指定在给定的所有主机网络（网络和广播地址包含，和IPstart IPend（192.168.1.3-192.168.1.27）在包容范围内指定的所有主机。

这些不同的选项用于指定目标主机上的可用的命令行，并在指定的文件中指定的文件选项。

在下面的选项中的一个字母或字的角度括号如“F”表示一个应该提供的值或字符串。相应的文本应该指示此值或字符串的含义。当提供准确的表示服或字符串，不包括角括号。方括号中的文本。

一个可选的参数

参数:

--help or -h 显示帮助文件

--file=<fn> or -f <fn> 从指定的文件中读取主机名或地址 而不是从命令行。

--sport=<p> or -s <p> 设置一个UDP端口 <p>, 默认=500, 0=随机.

一些IKE实现要求客户端使用UDP源端口500不会跟其他端口。请注意，通常需要超级用户权限使用1024以下的非零源端口。也只有一个系统上的一个进程可能绑定到一个给定的源端口在任何一个时间。使用--nat-t改变默认源端口为4500

--dport=<p> or -d <p> UDP目的端口设置为，默认值为500。

UDP端口500是分配的端口号为ISAKMP，这是用得最多的端口，如果不是所有的ike实现。使用--nat-t改变默认端口到4500

--retry=<n> or -r <n> 将主机的总次数设置为多少 默认=3.

--timeout=<n> or -t <n> Set initial per host timeout to <n> ms, default=500.

This timeout is for the first packet sent to each host.

subsequent timeouts are multiplied by the backoff

factor which is set with --backoff.

--bandwidth=<n> or -B <n> Set desired outbound bandwidth to <n>, default=56000

The value is in bits per second by default. If you

append "K" to the value, then the units are kilobits

per second; and if you append "M" to the value,

the units are megabits per second.

The "K" and "M" suffixes represent the decimal, not

binary, multiples. So 64K is 64000, not 65536.

--interval=<n> or -i <n> Set minimum packet interval to <n> ms.

The packet interval will be no smaller than this number.

The interval specified is in milliseconds by default.

if "u" is appended to the value, then the interval

is in microseconds, and if "s" is appended, the

interval is in seconds.

If you want to use up to a given bandwidth, then it is

easier to use the --bandwidth option instead.

You cannot specify both --interval and --bandwidth

because they are just different ways to change the

same underlying variable.

--backoff=<b> or -b <b> Set timeout backoff factor to <b>, default=1.50.

The per-host timeout is multiplied by this factor

after each timeout. So, if the number of retries

is 3, the initial per-host timeout is 500ms and the

backoff factor is 1.5, then the first timeout will be

500ms, the second 750ms and the third 1125ms.

--verbose or -v Display verbose progress messages.

Use more than once for greater effect:

1 - Show when each pass is completed and when

packets with invalid cookies are received.

2 - Show each packet sent and received and when

hosts are removed from the list.

3 - Display the host, Vendor ID and backoff lists

before scanning starts.

--quiet or -q Don't decode the returned packet.

This prints less protocol information so the

output lines are shorter.

--multiline or -M Split the payload decode across multiple lines.

With this option, the decode for each payload is

printed on a separate line starting with a TAB.

This option makes the output easier to read, especially

when there are many payloads.

--lifetime=<s> or -l <s> Set IKE lifetime to <s> seconds, default=28800.

RFC 2407 specifies 28800 as the default, but some

implementations may require different values.

If you specify this as a a decimal integer, e.g.

86400, then the attribute will use a 4-byte value.

If you specify it as a hex number, e.g. 0xFF, then

the attribute will use the appropriate size value

(one byte for this example).

If you specify the string "none" then no lifetime

attribute will be added at all.

You can use this option more than once in conjunction

with the --trans options to produce multiple transform

payloads with different lifetimes. Each --trans option

will use the previously specified lifetime value.

--lifesize=<s> or -z <s> Set IKE lifesize to <s> Kilobytes, default=0.

If you specify this as a a decimal integer, e.g.

86400, then the attribute will use a 4-byte value.

If you specify it as a hex number, e.g. 0xFF, then

the attribute will use the appropriate size value

(one byte for this example).

You can use this option more than once in conjunction

with the --trans options to produce multiple transform

payloads with different lifesizes. Each --trans option

will use the previously specified lifesize value.

--auth=<n> or -m <n> Set auth. method to <n>, default=1 (PSK).

RFC defined values are 1 to 5. See RFC 2409 Appendix A.

Checkpoint hybrid mode is 64221.

GSS (Windows "Kerberos") is 65001.

XAUTH uses 65001 to 65010.

This is not applicable to IKEv2.

--version or -V Display program version and exit.

--vendor=<v> or -e <v> Set vendor id string to hex value <v>.

You can use this option more than once to send

multiple vendor ID payloads.

--trans=<t> or -a <t> Use custom transform <t> instead of default set.

You can use this option more than once to send

an arbitrary number of custom transforms.

There are two ways to specify the transform:

The new way, where you specify the attribute/value

pairs, and the old way where you specify the values

for a fixed list of attributes.

For the new method, the transform <t> is specified as

(attr=value, attr=value, ...)

Where "attr" is the attribute number, and "value" is

the value to assign to that attribute. You can specify

an arbitary number of attribute/value pairs.

See RFC 2409 Appendix A for details of the attributes

and values.

Note that brackets are special to some shells, so you

may need to quote them, e.g.

--trans="(1=1,2=2,3=3,4=4)". For example,

--trans=(1=1,2=2,3=1,4=2) specifies

Enc=3DES-CBC, Hash=SHA1, Auth=shared key, DH Group=2;

and --trans=(1=7,14=128,2=1,3=3,4=5) specifies

Enc=AES/128, Hash=MD5, Auth=RSA sig, DH Group=5.

For the old method, the transform <t> is specified as

enc[/len],hash,auth,group.

Where enc is the encryption algorithm,

len is the key length for variable length ciphers,

hash is the hash algorithm, and group is the DH Group.

For example, --trans=5,2,1,2 specifies

Enc=3DES-CBC, Hash=SHA1, Auth=shared key, DH Group=2;

and --trans=7/256,1,1,5 specifies

Enc=AES-256, Hash=MD5, Auth=shared key, DH Group=5.

This option is not yet supported for IKEv2.

--showbackoff[=<n>] or -o[<n>] Display the backoff fingerprint table.

Display the backoff table to fingerprint the IKE

implementation on the remote hosts.

The optional argument specifies time to wait in seconds

after receiving the last packet, default=60.

If you are using the short form of the option (-o)

then the value must immediately follow the option

letter with no spaces, e.g. -o25 not -o 25.

--fuzz=<n> or -u <n> Set pattern matching fuzz to <n> ms, default=500.

This sets the maximum acceptable difference between

the observed backoff times and the reference times in

the backoff patterns file. Larger values allow for

higher variance but also increase the risk of

false positive identifications.

Any per-pattern-entry fuzz specifications in the

patterns file will override the value set here.

--patterns=<f> or -p <f> Use IKE backoff patterns file <f>,

default=/usr/share/ike-scan/ike-backoff-patterns.

This specifies the name of the file containing

IKE backoff patterns. This file is only used when

--showbackoff is specified.

--vidpatterns=<f> or -I <f> Use Vendor ID patterns file <f>,

default=/usr/share/ike-scan/ike-vendor-ids.

This specifies the name of the file containing

Vendor ID patterns. These patterns are used for

Vendor ID fingerprinting.

--aggressive or -A Use IKE Aggressive Mode (The default is Main Mode)

If you specify --aggressive, then you may also

specify --dhgroup, --id and --idtype. If you use

custom transforms with aggressive mode with the --trans

option, note that all transforms should have the same

DH Group and this should match the group specified

with --dhgroup or the default if --dhgroup is not used.

--id=<id> or -n <id> Use <id> as the identification value.

This option is only applicable to Aggressive Mode.

<id> can be specified as a string, e.g. --id=test or as

a hex value with a leading "0x", e.g. --id=0xdeadbeef.

--idtype=<n> or -y <n> Use identification type <n>. Default 3 (ID\_USER\_FQDN).

This option is only applicable to Aggressive Mode.

See RFC 2407 4.6.2 for details of Identification types.

--dhgroup=<n> or -g <n> Use Diffie Hellman Group <n>. Default 2.

This option is only applicable to Aggressive Mode and

IKEv2. For both of these, it is used to determine the

size of the key exchange payload.

If you use Aggressive Mode with custom transforms, then

you will normally need to use the --dhgroup option

unless you are using the default DH group.

Acceptable values are 1,2,5,14,15,16,17,18 (MODP only).

--gssid=<n> or -G <n> Use GSS ID <n> where <n> is a hex string.

This uses transform attribute type 16384 as specified

in draft-ietf-ipsec-isakmp-gss-auth-07.txt, although

Windows-2000 has been observed to use 32001 as well.

For Windows 2000, you'll need to use --auth=65001 to

specify Kerberos (GSS) authentication.

--random or -R Randomise the host list.

This option randomises the order of the hosts in the

host list, so the IKE probes are sent to the hosts in

a random order. It uses the Knuth shuffle algorithm.

--tcp[=<n>] or -T[<n>] Use TCP transport instead of UDP.

This allows you to test a host running IKE over TCP.

You won't normally need this option because the vast

majority of IPsec systems only support IKE over UDP.

The optional value <n> specifies the type of IKE over

TCP. There are currently two possible values:

1 = RAW IKE over TCP as used by Checkpoint (default);

2 = Encapsulated IKE over TCP as used by Cisco.

If you are using the short form of the option (-T)

then the value must immediately follow the option

letter with no spaces, e.g. -T2 not -T 2.

You can only specify a single target host if you use

this option.

--tcptimeout=<n> or -O <n> Set TCP connect timeout to <n> seconds (default=10).

This is only applicable to TCP transport mode.

--pskcrack[=<f>] or -P[<f>] Crack aggressive mode pre-shared keys.

This option outputs the aggressive mode pre-shared key

(PSK) parameters for offline cracking using the

"psk-crack" program that is supplied with ike-scan.

You can optionally specify a filename, <f>, to write

the PSK parameters to. If you do not specify a filename

then the PSK parameters are written to standard output.

If you are using the short form of the option (-P)

then the value must immediately follow the option

letter with no spaces, e.g. -Pfile not -P file.

You can only specify a single target host if you use

this option.

This option is only applicable to IKE aggressive mode.

--nodns or -N Do not use DNS to resolve names.

If you use this option, then all hosts must be

specified as IP addresses.

--noncelen=<n> or -c <n> Set the nonce length to <n> bytes. Default=20

This option controls the length of the nonce payload

that is sent in an aggressive mode or IKEv2 request.

Normally there is no need to use this option unless you

want to reduce the nonce size to speed up pre-shared

key cracking, or if you want to see how a particular

server handles different length nonce payloads.

RFC 2409 states that the length of nonce payload

must be between 8 and 256 bytes, but ike-scan does

not enforce this.

Specifying a large nonce length will increase the

size of the packet sent by ike-scan. A very large nonce

length may cause fragmentation, or exceed the maximum

IP packet size.

This option is only applicable to IKE aggressive mode.

--headerlen=<n> or -L <n> Set the length in the ISAKMP header to <n> bytes.

You can use this option to manually specify the value

to be used for the ISAKMP header length.

By default, ike-scan will fill in the correct value.

Use this option to manually specify an incorrect

length.

<n> can be specified as "+n" which sets the length

to n bytes more than it should be, "-n" which sets

it to n bytes less, or "n" which sets it to exactly

bytes.

Changing the header length to an incorrect value can

sometimes disrupt VPN servers.

--mbz=<n> or -Z <n> Use the value <n> for reserved (MBZ) fields, default=0.

Specifying this option makes the outgoing packet

non-RFC compliant, and should only be used if you want

to see how a VPN server will respond to invalid packets.

The value of <n> should be in the range 0-255.

--headerver=<n> or -E <n> Specify the ISAKMP header version.

The default is 0x10 (16) which corresponds to v1.0.

Specifying a non-default value will make the outgoing

packet non-RFC compliant, and should only be used if

you want to see how the VPN server reacts to strange

versions.

The value should be in the range 0-255.

--certreq=<c> or -C <c> Add the CertificateRequest payload <c>.

<c> should be specified as a hex value.

The first byte of the hex value will be interpreted as

the certificate type; the remaining bytes as the

certificate authority as described in RFC 2408 3.10.

The certificate types are listed in RFC 2408 sec 3.9.

RFC 2048 states "The Certificate Request payload MUST

be accepted at any point during the exchange"

--doi=<d> or -D <d> Set the SA DOI to <d>, default 1 (IPsec).

You will not normally want to change this unless you

want to see how the VPN server responds to a

non-standard DOI.

--situation=<s> or -S <s> Set the SA Situation to <d>, default 1.

The meaning of the situation depends on the DOI, and

is detailed in the appropriate DOI document. For the

IPsec DOI, the default Situation of 1 represents

SIT\_IDENTITY\_ONLY.

You will not normally want to change this unless you

want to see how the VPN server responds to a

non-standard situation.

--protocol=<p> or -j <p> Set the Proposal protocol ID to <p>, default 1.

The meaning of the proposal protocol ID depends on

the DOI, and is detailed in the appropriate DOI

document. For the IPsec DOI, the default proposal

protocol id of 1 represents PROTO\_ISAKMP.

You will not normally want to change this unless you

want to see how the VPN server responds to a

non-standard protocol ID.

--transid=<t> or -k <t> Set the Transform ID to <t>, default 1.

The meaning of the transform ID depends on the

DOI, and is detailed in the appropriate DOI

document. For the IPsec DOI, the default

transform id of 1 represents KEY\_IKE.

You will not normally want to change this unless you

want to see how the VPN server responds to a

non-standard transform ID.

--spisize=<n> Set the proposal SPI size to <n>. Default=0

If this is non-zero, then a random SPI of the

specified size will be added to the proposal payload.

The default of zero means no SPI.

--hdrflags=<n> Set the ISAKMP header flags to <n>. Default=0

The flags are detailed in RFC 2408 section 3.1

--hdrmsgid=<n> Set the ISAKMP header message ID to <n>. Default=0

This should be zero for IKE Phase-1.

--cookie=<n> Set the ISAKMP initiator cookie to <n>

The cookie value should be specified in hex.

By default, the cookies are automatically generated

and have unique values. If you specify this option,

then you can only specify a single target, because

ike-scan requires unique cookie values to match up

the response packets.

--exchange=<n> Set the exchange type to <n>

This option allows you to change the exchange type in

the ISAKMP header to an arbitrary value.

Note that ike-scan only supports Main and Aggressive

modes (values 2 and 4 respectively). Specifying

other values will change the exchange type value in

the ISAKMP header, but will not adjust the other

payloads.

The exchange types are defined in RFC 2408 sec 3.1.

--nextpayload=<n> Set the next payload in the ISAKMP header to <n>

Normally, the next payload is automatically set to the

correct value.

--randomseed=<n> Use <n> to seed the pseudo random number generator.

This option seeds the PRNG with the specified number,

which can be useful if you want to ensure that the

packet data is exactly repeatable when it includes

payloads with random data such as key exchange or nonce.

By default, the PRNG is seeded with an unpredictable

value.

--timestamp Display timestamps for received packets.

This option causes a timestamp to be displayed for

each received packet.

--sourceip=<s> Set source IP address for outgoing packets to <s>.

This option causes the outgoing IKE packets to have

the specified source IP address.

The address can either be an IP address in dotted

quad format, or the string "random" which will use

a different random source address for each packet that

is sent.

If this option is used, no packets will be received

This option requires raw socket support, and you

will need superuser privileges to use this option,

even if you specify a high source port.

This option does not work on all operating systems.

--shownum Display the host number for received packets.

This displays the ordinal host number of the

responding host before the IP address. It can be useful

when sending many packets to the same target IP, to

see if any probes are being ignored.

--nat-t Use RFC 3947 NAT-Traversal encapsulation.

This option adds the non-ESP marker to the beginning

of outgoing packets and strips it from received

packets, as described in RFC 3947. It also changes the

default source port to 4500 and the default destination

port to 4500, which are the ports for NAT-T IKE.

These port numbers can be changed with the --sport and

--dport options, providing they are used after the

--nat-t option.

--rcookie=<n> Set the ISAKMP responder cookie to <n>.

This sets the responder cookie to the specified hex

value. By default, the responder cookie is set to zero.

--ikev2 or -2 Use IKE version 2

This causes the outgoing packets to use IKEv2 format

as defined in RFC 4306 instead of the default IKEv1

format. Any packets returned are automatically decoded

as IKE or IKEv2 depending on their payloads irrespective

of this option.

The --ikev2 option is currently experimental. It has not

been extensively tested, and it only supports sending

the default proposal.

Report bugs or send suggestions to ike-scan@nta-monitor.com

See the ike-scan homepage at http://www.nta-monitor.com/tools/ike-scan/