sslscan

Check SSL/TLS protocols and ciphers supported by a server.

TLDR

Test a server on port 443

$ sslscan [example.com]

Test a specified port

$ sslscan [example.com]:[465]

Show certificate information

$ testssl --show-certificate [example.com]

SYNOPSIS

sslscan [*options*] *[host:port | host]*

DESCRIPTION

sslscan queries SSL/TLS services (such as HTTPS) and reports the protocol versions, cipher suites, key exchanges, signature algorithms, and certificates in use. This helps the user understand which parameters are weak from a security standpoint.

Terminal output is thus colour-coded as follows:

Red Background NULL cipher (no encryption)
Red Broken cipher (<= 40 bit), broken protocol (SSLv2 or SSLv3) or broken certificate signing algorithm (MD5)
Yellow Weak cipher (<= 56 bit or RC4) or weak certificate signing algorithm (SHA-1)
Purple Anonymous cipher (ADH or AECDH)

sslscan can also output results into an XML file for easy consumption by external programs.

OPTIONS

COLLAPSE ALL

--help

Show summary of options

--targets=<file>

A file containing a list of hosts to check. Hosts can be supplied with ports (i.e. host:port). One target per line

--sni-name=<name>

Use a different hostname for SNI

--ipv4, -4

Force IPv4 DNS resolution. Default is to try IPv4, and if that fails then fall back to IPv6.

--ipv6, -6

Force IPv6 DNS resolution. Default is to try IPv4, and if that fails then fall back to IPv6.

--show-certificate

Display certificate information.

--no-check-certificate

Don't flag certificates signed with weak algorithms (MD5 and SHA-1) or short (<2048 bit) RSA keys

--show-client-cas

Show a list of CAs that the server allows for client authentication. Will be blank for IIS/Schannel servers.

--show-ciphers

Show a complete list of ciphers supported by sslscan

--show-cipher-ids

Print the hexadecimal cipher IDs

--show-times

Show the time taken for each handshake in milliseconds. Note that only a single request is made with each cipher, and that the size of the ClientHello is not constant, so this should not be used for proper benchmarking or performance testing.

You might want to also use --no-cipher-details to make the output a bit clearer.

--ssl2

Only check if SSLv2 is enabled

--ssl3

Only check if SSLv3 is enabled

--tls10

Only check TLS 1.0 ciphers

--tls11

Only check TLS 1.1 ciphers

--tls12

Only check TLS 1.2 ciphers

--tls13

Only check TLS 1.3 ciphers

--tlsall

Only check TLS ciphers (versions 1.0, 1.1, 1.2, and 1.3)

--ocsp

Display OCSP status

--pk=<file>

A file containing the private key or a PKCS#12 file containing a private key/certificate pair (as produced by MSIE and Netscape)

--pkpass=<password>

The password for the private key or PKCS#12 file

--certs=<file>

A file containing PEM/ASN1 formatted client certificates

--no-ciphersuites

Do not scan for supported ciphersuites.

--no-fallback

Do not check for TLS Fallback Signaling Cipher Suite Value (fallback)

--no-renegotiation

Do not check for secure TLS renegotiation

--no-compression

Do not check for TLS compression (CRIME)

--no-heartbleed

Do not check for OpenSSL Heartbleed (CVE-2014-0160)

--no-groups

Do not enumerate key exchange groups

--show-sigs

Enumerate signature algorithms

--starttls-ftp

STARTTLS setup for FTP

--starttls-imap

STARTTLS setup for IMAP

--starttls-irc

STARTTLS setup for IRC

--starttls-ldap

STARTTLS setup for LDAP

--starttls-pop3

STARTTLS setup for POP3

--starttls-smtp

STARTTLS setup for SMTP

--starttls-mysql

STARTTLS setup for MySQL

--starttls-xmpp

STARTTLS setup for XMPP

--starttls-psql

STARTTLS setup for PostgreSQL

--xmpp-server

Perform a server-to-server XMPP connection. Try this if --starttls-xmpp is failing.

--rdp

Send RDP preamble before starting scan.

--bugs

Enables workarounds for SSL bugs

--timeout=<sec>

Set socket timeout. Useful for hosts that fail to respond to ciphers they don't understand. Default is 3s.

--sleep=<msec>

Pause between connections. Useful on STARTTLS SMTP services, or anything else that's performing rate limiting. Default is disabled.

--xml=<file>

Output results to an XML file. - can be used to mean stdout.

--version

Show version of program

--verbose

Display verbose output

--no-cipher-details

Hide NIST EC curve name and EDH/RSA key length.

--no-colour

Disable coloured output.

EXAMPLES

Scan a local HTTPS server

```
sslscan localhost
sslscan 127.0.0.1
sslscan 127.0.0.1:443
sslscan [::1]
sslscan [::1]:443
```

AUTHOR

sslscan was originally written by Ian Ventura-Whiting <fizz@titania.co.uk>.
sslscan was extended by Jacob Appelbaum <jacob@appelbaum.net>.
sslscan was extended by rbsec <robin@rbsec.net>.
This manual page was originally written by Marvin Stark <marv@der-marv.de>.