SSL Audit _
TLS / SSL Scanner

Thierry ZOLLER
Thierry@zoller.lu
http://www.g -sec.lu
http://blog.zoller.lu

G-SEC™ is a non-commercial and independent group of Information Security Specialists based in Luxembourg. Our work has been featured in New York Times, eWeek, ct', SAT1, Washington Post and at conferences ranging from Hack.lu to Cansecwest.

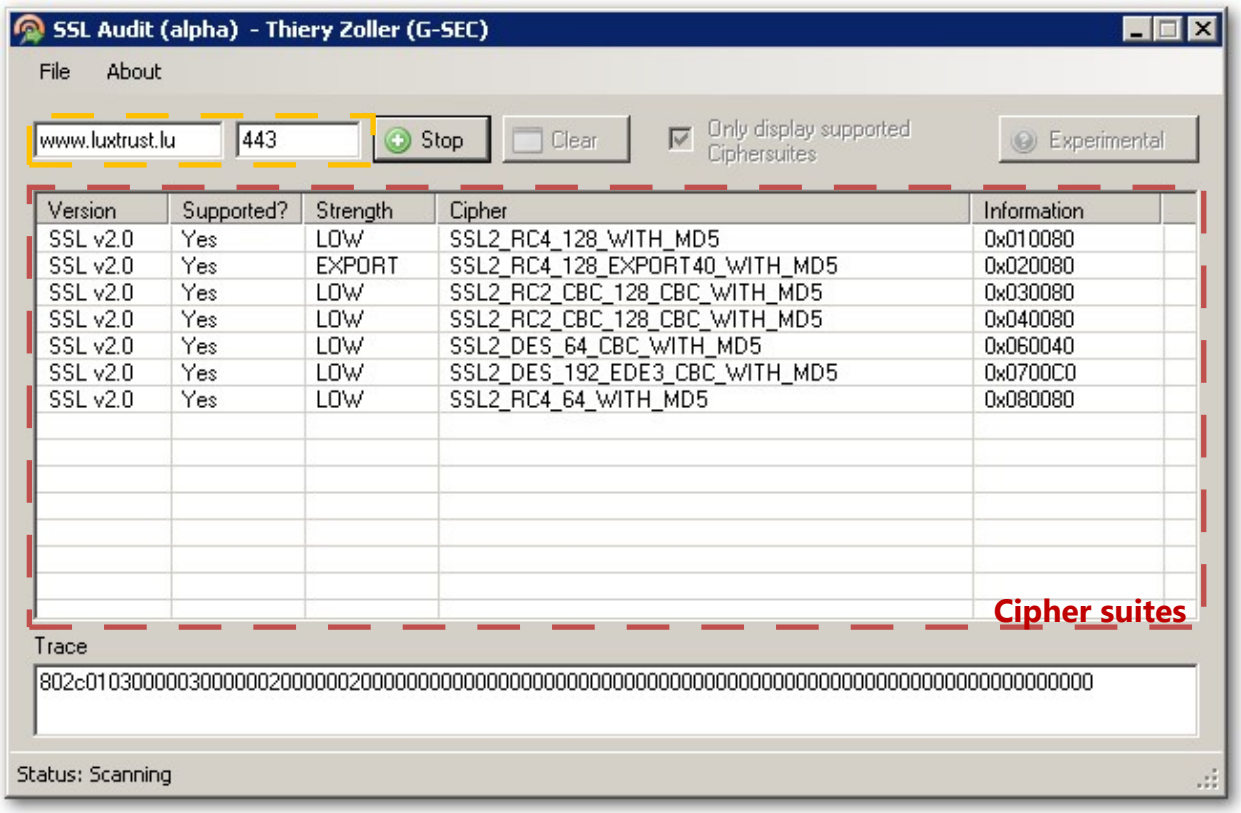
Table of Contents

About

SSL Audit scans web servers for SSL/TLS support; it implements its own rudimentary SSL/TLS Parser and is as such **not limited to ciphers supported by SSL engines such as OpenSSL or NSS** and can detect all known and RFC defined cipher suites.

Use

- Scan: Enter the host to be scanned and the appropriate port.
- Clear : Clears the results
- Option - Only display supported Cipher suites
- Experimental : Fingerprints the SSL engine (see " Fingerprint" Experimental)



Fingerprint (Experimental)

Included is an experimental fingerprint engine that tries to determine the SSL Stack used server side. It does so by **sending normal and malformed SSL packets that** can be interpreted in different ways.

It is able to distinguish

- IIS7.5 (Schannel)
- IIS7.0 (Schannel)
- IIS 6.0 (Schannel)
- Apache (Openssl)
- Apache (NSS)
- Certicom
- RSA BSAFE

The higher the Score the more likely the host is using that engine. Note: SSL accelerators/ load balancers will give unlikely results

Known limitations

- SSLv2 – SSLv2 detection is prone to false positives – Additional manual checks whether the server accepts HTTP request after negotiations are required.

  This can be done manually: *openssl s_client ssl2 -connect SERVERNAME:443 GET / HTTP1.0*

  Some servers answer correctly to an SSLv2 handshake but will output a 500 status request when actually asking for a resource over HTTPS. SSL audit is currently not able to detect this.

- Fingerprints – This is a behavioral fingerprint - False positives are common especially in environments where SSL accelerator or load balancers are used

Change log

0.9 Version

- Updated TLS 1.2 supported modes
- Added new CHACHA20 Ciphersuites (PSK, DHE, ECDHE)
- Added new ECDHE based PSK ciphersuites

0.8 Version

- Speed up SSLv2 discovery
- Added TLS 1.2 Camellia based cipher suites
- Added Aria based cipher suites (http://tools.ietf.org/html/draft-nsri-tls-aria-00)

Alpha Version

- Added option to export results to CSV
- Updated documentation

Limitation of Liability

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts), shall Thierry Zoller or G-SEC .ltd be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses),even if such Contributor has been advised of the possibility of such damages.