SSL Audit (alpha) – Cipher suite scanner

Thierry ZOLLER
Principal Security Consultant
contact@g-sec.lu
http://www.g-sec.lu

G-SEC™ is a **vendor independent** Luxemburgish led security consulting group that offers IT Security consulting services on an organizational and technical level. Our work has been featured in New York Times, eWeek, ct', SAT1, Washington Post and at conferences ranging from Hack.lu to Cansecwest.

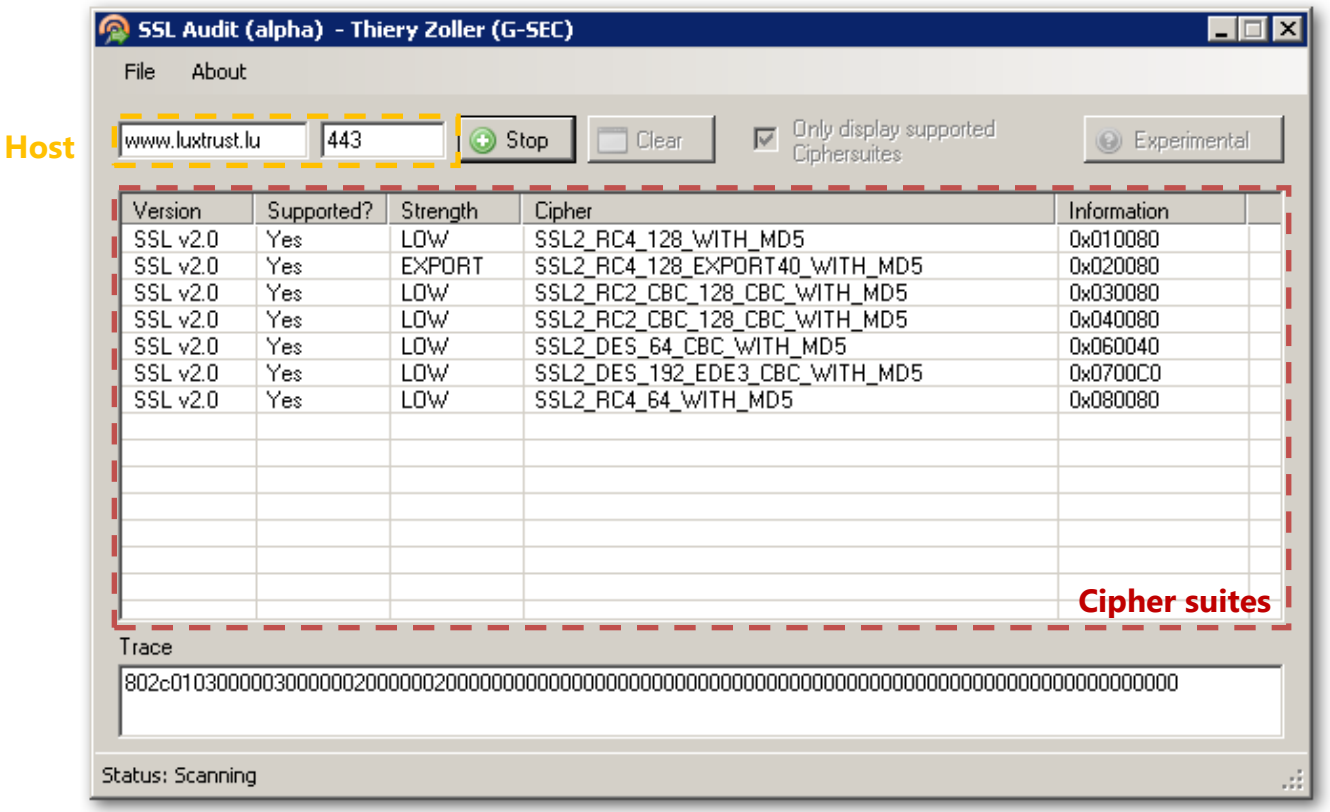
Table of Contents

About

SSL Audit scans web servers for SSL support, unlike other tools it is not limited to ciphers supported by SSL engines such as OpenSSL or NSS and can detect all known cipher suites.

Use

- Scan: Enter the host and the port the SSL service listens on.
- 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 Engine 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 – 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 – False positives
- Lacks option to export results (yes, that's pretty dumb)

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.