



SILICA-U OVERVIEW



SILICA-U

A handheld wireless auditing and penetration testing suite, the SILICA-U leverages an automatically updated library of exploits (CANVAS) to provide a unique, automated, and always up to date testing tool.

Installed in a laptop, SILICA-U allows on-site testing with an absolute minimum footprint. SILICA-U preconfigured with a powerful toolset called the CANVAS exploit library. Installs quickly into your own PCMCIA-enabled laptop.

The CANVAS exploit library currently consists of hundreds of exploits, with new exploits added every month. The CANVAS exploits span all common platforms and applications. Please call for a demonstration or further information.

Example Use Cases

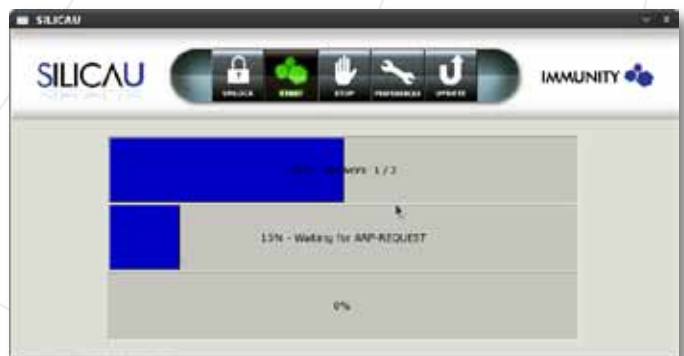
- Use as a WiFi Detection Engine
- Concealed to determine vulnerabilities in an specific area
- Tell SILICA-U to scan every machine on every wireless network for file shares and download anything of interest. Once configured, put it in your suit pocket and walk through your target's office
- Tell SILICA-U to actively penetrate any machines it can target (with any of CANVAS's exploits) and have all successfully penetrated machines connect to an external listening post running CANVAS Professional
- Use SILICA-U to conduct "man-in-the-middle" attacks against systems on a wireless network
- Use SILICA-U as you would CANVAS on your desktop – just smaller.
- Support for Bluetooth and Ethernet currently in production

Features

- + Ultra-portable form factor
- + Easy to use interface
- + Automated exploit library
- + Completely configurable
- + Cross-platform test
- + Automated report generation
- + 802.11b/g
- + Custom Linux OS

Includes

- SILICA-U Cardbus with software
- Software updates for one year
- E-mail support for one year
- User's Manual



© Copyright Transformational Security, LLC 2010. All rights reserved. Specifications subject to change.