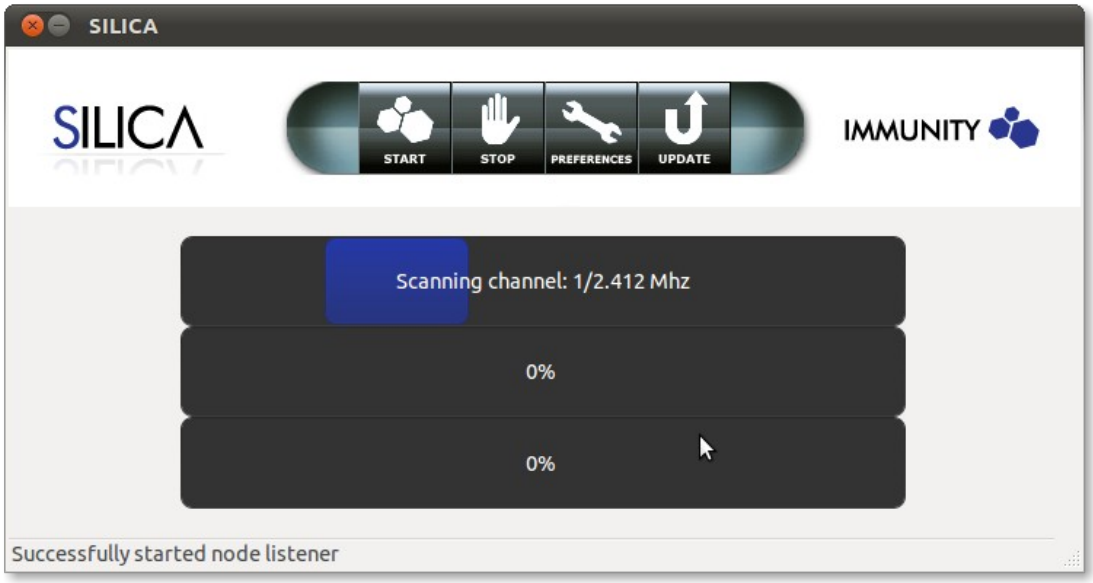
SILICA User's Manual
Feb 2011



Introduction

Immunity SILICA is a unique penetration testing and assessment solution for wireless networks. SILICA offers many features that open source utilities, or other commercial wireless assessment tools do not:

- Automation – SILICA has a one-button interface for many of the actions you will want to do during your assessment, including WEP cracking.
- Reporting – SILICA will produce HTML reports of its scanning for later perusal.
- Attack – SILICA has ready-to-use exploit modules from Immunity's CANVAS platform integrated into the attack and recon process. This means not only do you know there is a crackable network available, but you have screenshots or password hashes from the vulnerable machines on that network, all at the push of a button.

Startup

SILICA does not require any setup or install. Simply plug-in the USB drive into your computer, make sure the BIOS is configured as boot-able and let it load.

Once the license has been accepted, SILICA will start and offer you the SILICA GUI.

Make sure the card is inserted into the Express Card, PCMCIA or USB slot and the antennas are plugged in. If you notice low signal levels you may try plugging in the antenna into the other slot.

Configuration

Prior to initiating a scan, a user can use SILICA's configuration dialog to fine tune scan options. Click the preferences button to invoke the configuration dialog. Once this is done, a popup window displaying the available options will appear in the screen.

Scan

This configuration tab allows users to select a method that SILICA will use to perform a scan.

Attack Mode: Attempts to break into remote machines in a network.

MITM Mode: Actively infects hosts in the network via arp-poisoning and intercepts any traffic between the router and the active hosts.

Network Probe: Performs information gathering of the remote network such as identifying the operating system, extracting underlying details from the hosts, finding open shares etc.

Passive Session Hijacking: Allows the user to capture cookies passively without associating to a network and replay them and hijack into web sessions.

Discover key: Will attempt to recover the wireless key of the remote network. The encryption methods currently supported are WPA1/2, LEAP, WEP 64/128

Network Configuration Tab

Configuring various network options allows the user to fine tune the way the selected scan works.

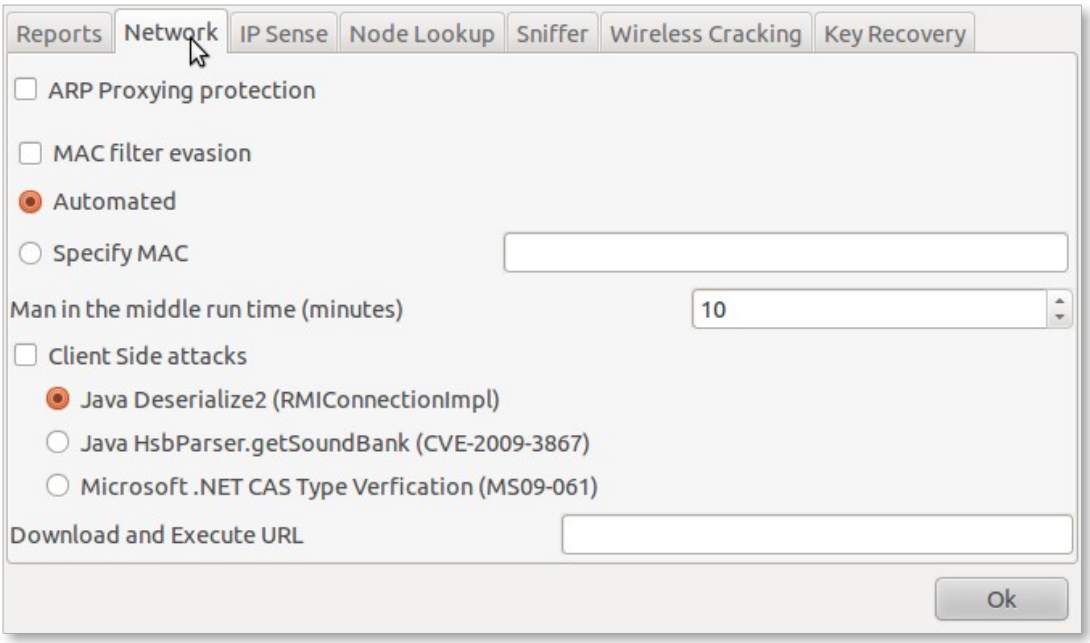


Illustration 1:

ARP Proxy Protection: If ticked this option will only scan hosts with a unique IP<->MAC address pair. If more than one hosts with the same MAC address is found then only the last IP encountered will be scanned and added to the list. This is useful when associating with Hotel, Airport, or other networks which do ARP Proxying.

Man in the middle run time: Specifies the run time in minutes.

Client Side attacks: If man in the middle is selected as an attack this will try to exploit the associated clients instead of capturing their traffic.

Download and Execute URL: Downloads and executes an executable as a post action after it exploits a client. This currently works only with win32 hosts.

MAC Filtering evasion: If ticked SILICA will attempt to bypass MAC filtering set by the access point. A MAC filter is defined as a list of certain MAC addresses that are allowed to be associated to the network.

- **Automatic:** An attempt to automatically bypass MAC filtering will be made
- **Specify MAC:** Allows to provide a custom MAC address different of the one supplied with the device.

Reports Configuration Tab

This section provides a way to configure how the reports are stored and what kind of post action result the user wants to see in the report.

Prefix Reports: The final report names will be prefixed with the string provided in the textbox area. Also the title of the final HTML will have that identification string.

Screenshot/Password hashes: If the attack scan type is selected these options will become available in the reports tab. Selecting either of the two will allow presentation of different evidence. The user can select between a screengrab or a listing of the password hashes.

Dump WIFI keys: Allows users to capture wireless keys from the Wireless Zero Configuration service.

Get browser info: Gets information from the browser if it can.

Get outlook address book: Gets information from the outlook address book.

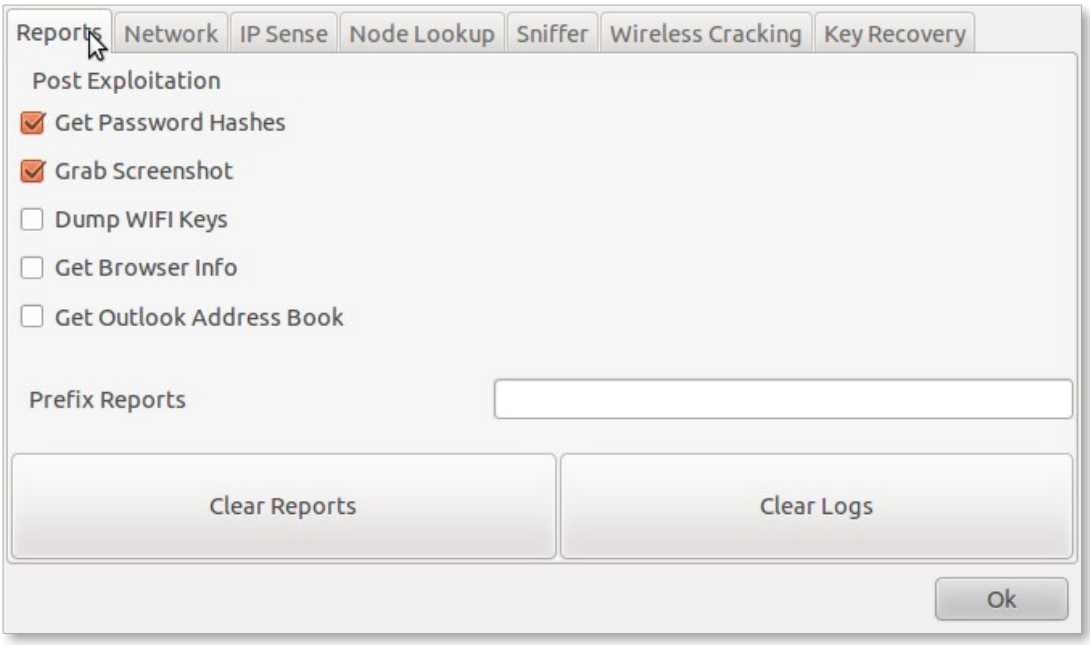


Illustration 2: Report configuration

IP Sense Configuration Tab

These options provide different methods that SILICA will use to get or assign IP address from/to the remote end.

DHCP Client: Allows a client to get an IP using a DHCP client method.

DHCP Server: Allows SILICA to act as a server and lease IP's to potential clients. This is useful for Ad-Hoc networks with automatic configuration.

ARP Force: Allows SILICA to use an ARP brute forcing method in the known local subnet ranges hoping to get back a reply from a host.

Network sense: This is a useful option that provides a stealthy way to passively listen for packets and try to sense the local IP through those.

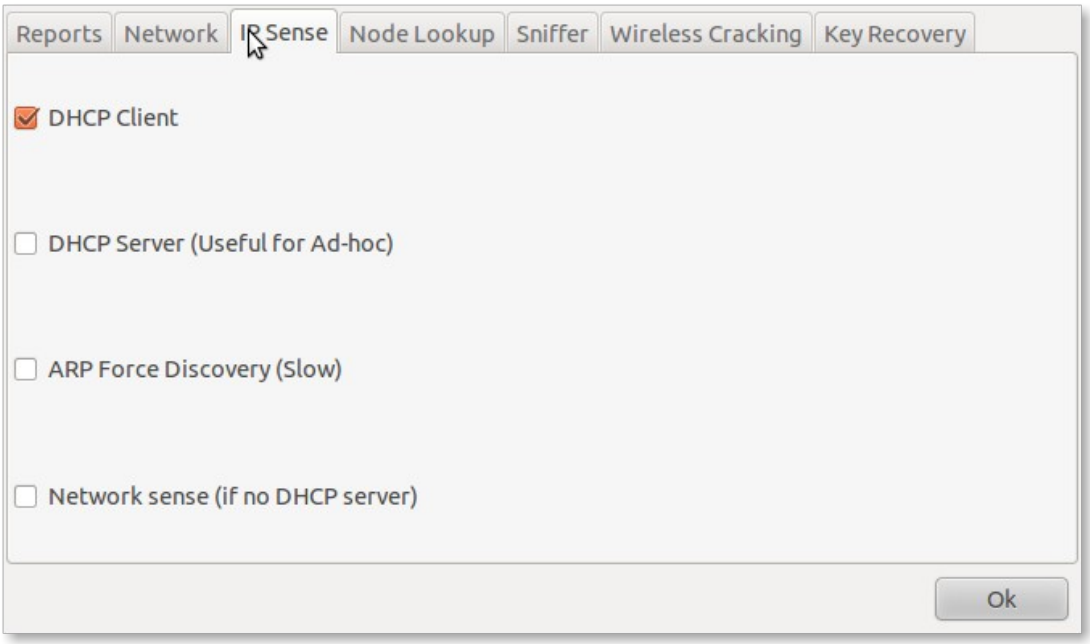


Illustration 3: Ipsense configuration

Wireless Cracking

Different options that can be used to adjust the way a WEP is recovered.

Two byte error correction: This option will check the key for a two adjacent key byte errors and correct them.

Rank table deduction correction: Corrects up to one keybyte corrections made from the probability algorithm.

ARP Packets to capture: This numerical value indicates the threshold of packets to use for the probability cracking algorithm.

Perform deauthentication: If selected SILICA will automatically try to disconnect clients when trying to recover a key. It's highly recommended that this option remains enabled.

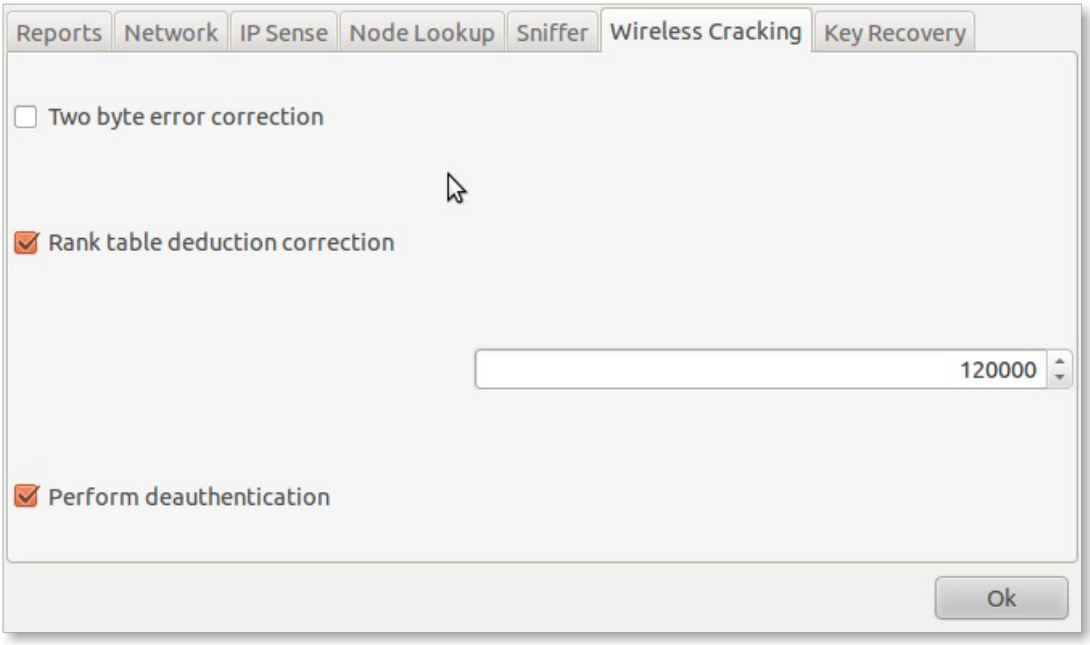


Illustration 4: Wireless cracking configuration

WPA Cracking

Cracking WPA 1 and 2 networks with SILICA is a similar process to WEP cracking in the sense that it's fully automated. However, WPA networks have a much harder encryption, and so SILICA is limited to brute forcing a password.

LEAP Cracking

Recovering LEAP credentials is an automated process and is currently supported by SILICA. It will automatically detect for active clients on the network and disconnect them to capture a handshake. Once this is done the user id and password will be saved in the report file. The code automatically senses if the network is Open WEP or LEAP WEP authentication. Optionally it can be set manually before the scan is initiated.

WEP Cracking

Similar as above WEP cracking is fully automated using the discover key option. That will attempt to get a 64 or 128bit key from the remote host if it finds an associated client.

Node Lookup

This configuration tab provides access to allow GPS selection.

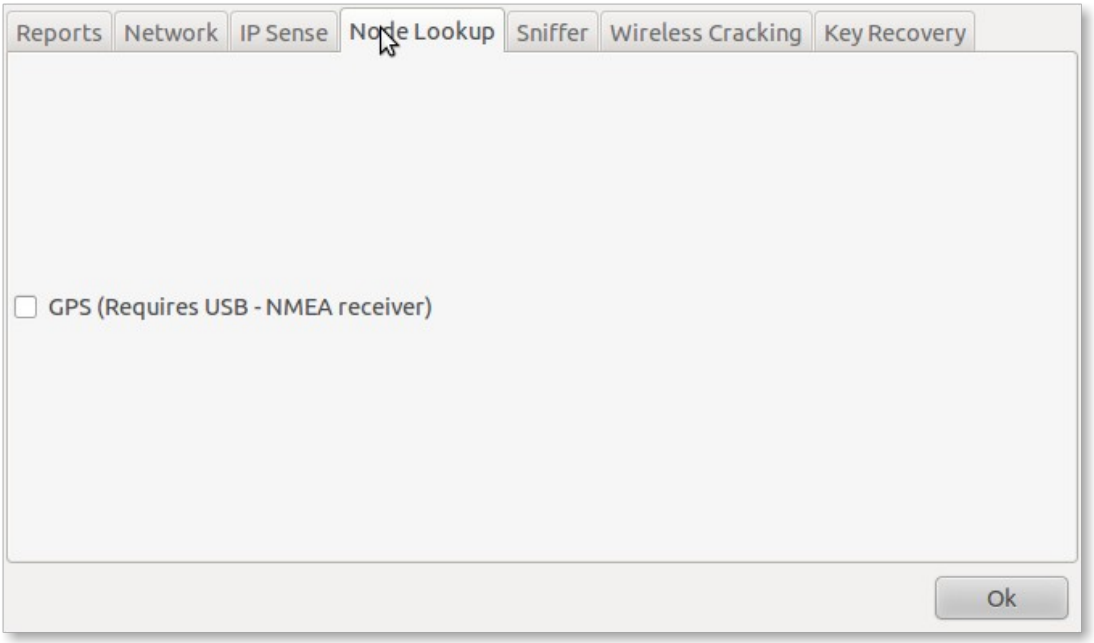


Illustration 5: Node lookup configuration

GPS: In this section of the configuration you may also modify the GPS integration. This requires a USB configured device to be attached on the machine that SILICA is running on. SILICA will automatically see if one exists and will capture the coordinates (longitude/latitude) and will add it in the reports.

Wireless Window

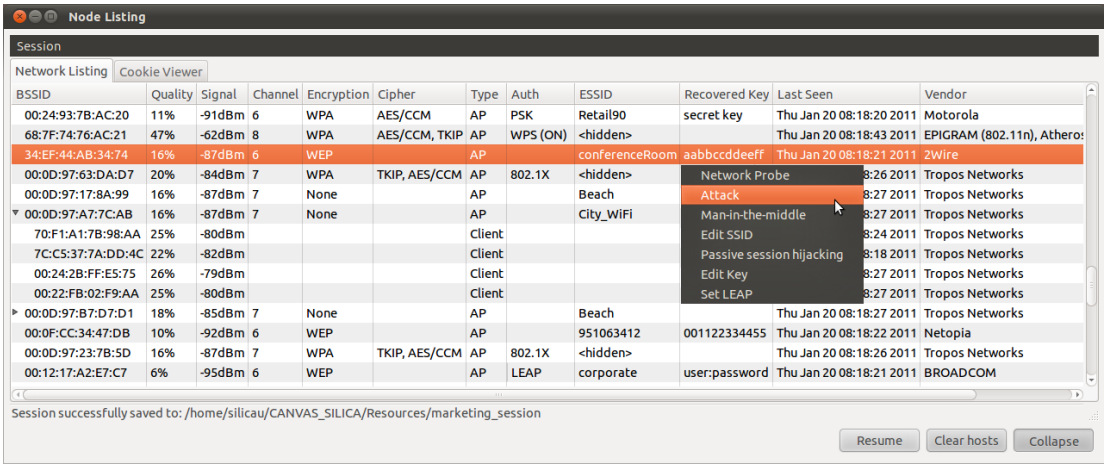


Illustration 6: Main wireless window

General Overview: This is the main window for all operations. It shows information about hosts such as MAC, Signal levels, Encryption type, Vendors etc. It further allows you to see what wireless clients are associated to a host. As shown in *Illustration 6,* clicking the triangle by a network expands a list of associated clients to it. By checking the vendor and the type a lot can be determined. For example if a client has Client/AP this means the client is also bridge but acts as an access point aswell.

If the main window remains running hosts will appear colored. In their default state they are all black. That means all hosts are active. If it's blue, green and gray accordingly that indicates that the last sign of life seen from such a network was minutes to days ago. Blue being the closest and the gray meaning it's probably a dead host/client. It must be further noted that the last seen column indicates when was the last time it saw activity from a specific host.

Actions: When you right click on a host a dynamic menu will be built. Depending on the capabilities of the host different actions will be available. For example a host that we have discovered the key for will have more actions available to a hidden network that we don't know the SSID for. The more progress is made into finding details about a host the more actions are available.

Buttons:

- *Resume/Pause*: allows the user to pause/resume the network collection in order to execute other tasks or rellocate positions.
- *Clear hosts:* Clicking this will clear out the display of the found hosts and pause the scan.
- *Expand/Collapse:* Allows the user to expand all the hosts and see what clients are associated to them without interrupting the flow of network collection. This is useful if there are many hosts being displayed on the list.

Passive session hijacking

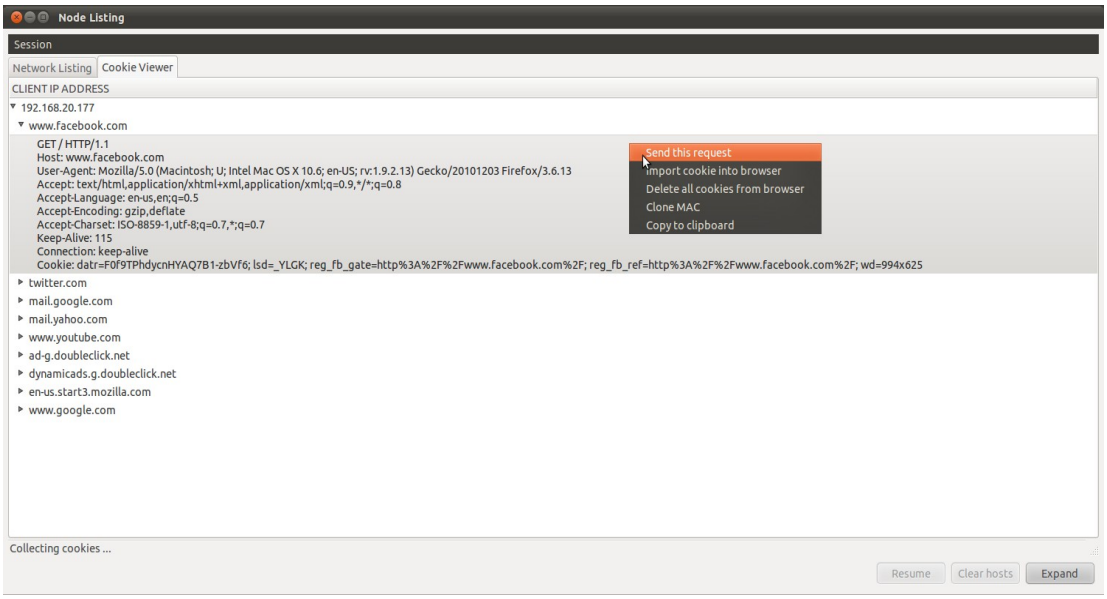


Illustration 7: Passive session hijacking

Actively listens for cookies over the air and creates a list that allows the user to directly enter a web session. This may work with popular networks such as facebook, twitter, gmail, etc. Cookies are captured over the air passively. This is less intrusive than man in the middle because there is no poisoning involved or interaction with the clients.

Key Recovery

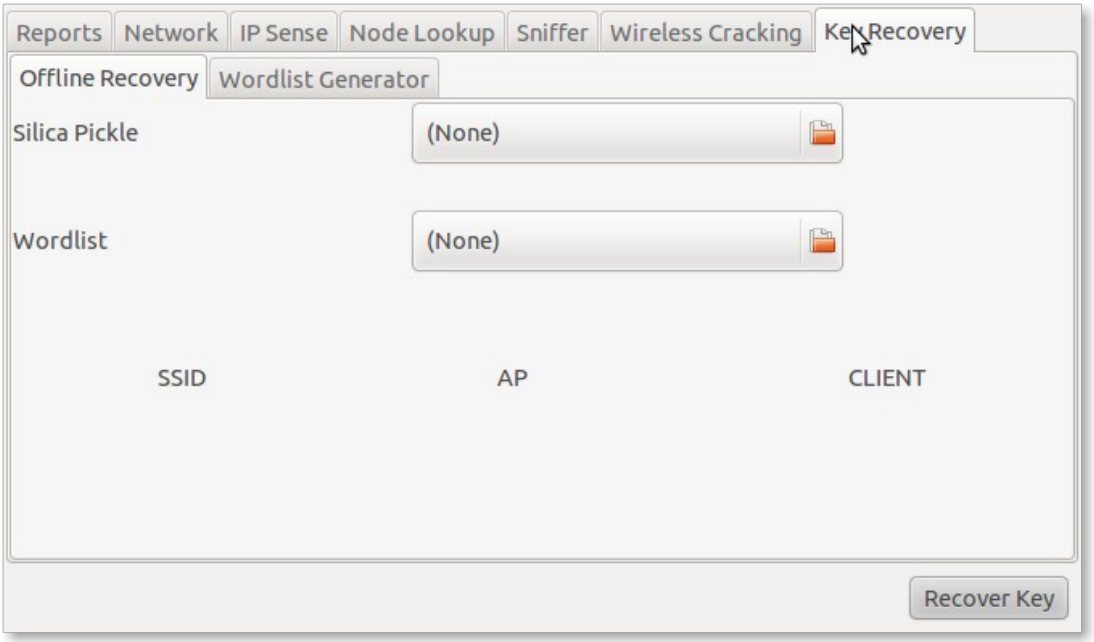


Illustration 8: Key recovery

This configuration menu is split into two main categories. One is geared towards creating word lists that will assist into recovering a encryption key and the other one to run a recovery attempt.

Key Recovery: As illustrated above it takes a pickle file which is a previously captured handshake and a word list which is used to brute force the key. Once those are loaded it populates the SSID, AP and CLIENT fields. This detects automatically if the handshake is LEAP/WPA and recovers the key.

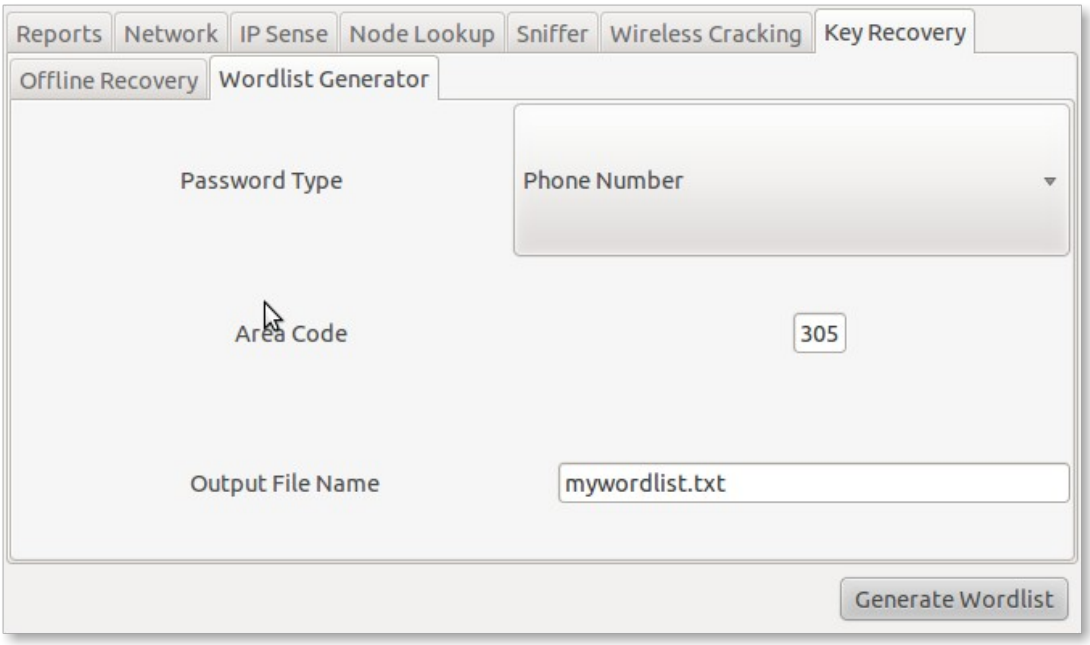


Illustration 9: Word list generator

Word list generator: This allows the user to create a phone number list of passwords if it's in an area code of interest or a numbered list. The output stores the results on the specified file to be used later by the offline cracker.

Updating

Updating SILICA adds new exploits to the unit, updates SILICA features and may introduce functionality fixes. Updates are announced on the SILICA email list. (If you are not subscribed to the list, contact Immunity.)

In order to perform an update, an Internet connection must be available.

To update, please follow the following steps **in order.**

1. Load SILICA.
2. Connect an ethernet cable with an internet connection.
3. Load up wicd (top right) and make sure the ethernet connection is active with internet.
4. Click on the update button.
5. Exit and Restart SILICA.

The most common mistake when updating is to enable your network connection before you have started SILICA.

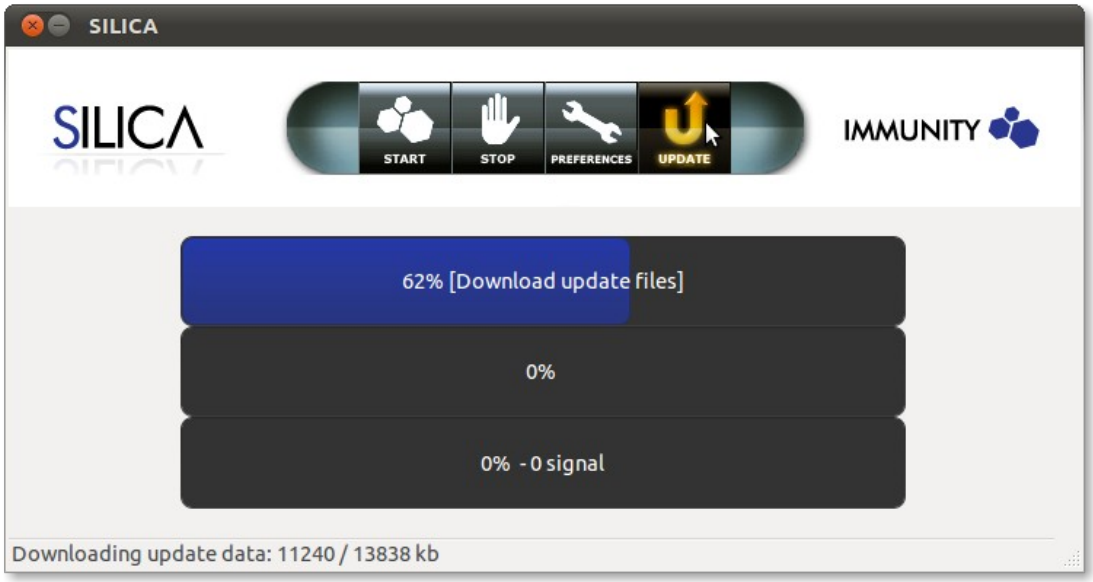


Illustration 10: SILICA update

Stopping a Scan

By clicking the stop button the scan will terminate at the next available stopping point, saving a report. This process may take a while to complete as SILICA has to wait for all the running threads to stop cleanly. Once the scan completes, the status bar will change indicating that the scan was stopped.

Viewing SILICA Reports

To view the results of a scan, open the Reports folder by clicking the Reports icon on your desktop.

Once clicked, a listing of reports in that directory will be loaded. Double-click any of these to view them. Reports starting with “VA” are probe reports; wheras reports starting with MA are “Attack” reports. Reports that start with SILICA are wireless reports and will have a list of the networks found and any encryption keys recovered during scanning.

These reports can be copied using standard Linux copy commands – you will want to make sure you also copy the header.gif and immunity.css files, which are referenced by the reports.

Feedback and Support

Immunity's SILICA developers are committed to your satisfaction. Please do not hesitate to contact the SILICA team:

silica@immunityinc.com

p 212 534 0857

f 917-591-1850

1130 Washington Ave

8th Floor

Miami Beach, FL 33139