# Chapter 6

# WarDriving and Wireless Penetration Testing with OS X

**Solutions in this chapter:**

- WarDriving with Kismac
- Penetration Testing with OS X
- Other OS X Tools for WarDriving and WLAN Testing

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

# Introduction

With operating system (OS) X, WarDriving and Wireless Local Area Network (WLAN) penetration testing have excellent wireless support and several tools to make these tasks easy.

The first part of this chapter describes the steps necessary to configure and utilize the KisMAC WLAN discovery tool in order to successfully WarDrive. (For additional information regarding WarDriving, see Chapter 1.) The second part of this chapter describes how to use the information obtained during a WarDrive, and goes on to detail how a penetration tester can further utilize KisMAC to successfully penetrate a customer's wireless network.

# WarDriving with KisMAC

KisMAC is the best WarDriving and WLAN discovery and penetration testing tool available on any platform, and is available for free at *http://kismac.binaervarianz.de/*. Most WarDriving applications provide the capability to discover networks in either *active mode* or *passive mode*; KisMAC provides both. On other platforms, WarDriving tools such as Kismet for Linux and NetStumbler for Windows only provide the capability to discover WLANs. KisMAC is unique because it also includes the functionality that a penetration tester needs to attack and compromise found networks.

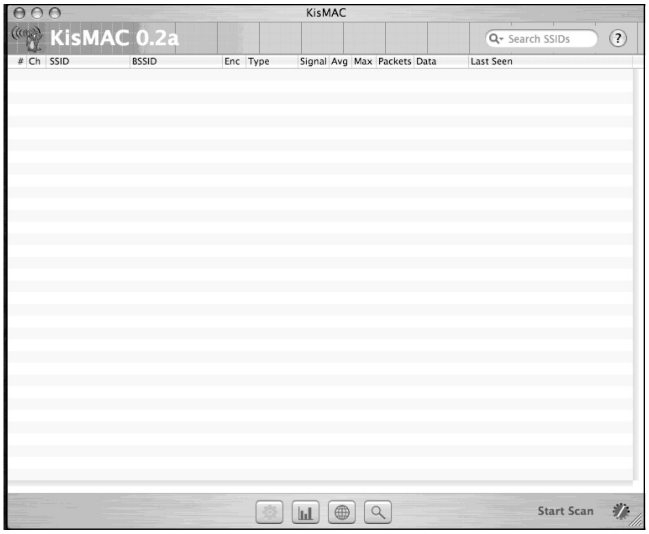
**Table 6.1** Prominent Wireless Discovery Tools and Capabilities

| Tool | Platform | Scan Type | Attack Capability |
|---|---|---|---|
| NetStumbler | Windows | Active | No |
| Kismet | Linux | Passive | No |
| KisMAC | OS X | Active/Passive | Yes |

## Starting KisMAC and Initial Configuration

Once KisMAC has been downloaded and installed, it is relatively easy-to-use. The first thing you need to do is load KisMAC, which is done by clicking on the **KisMAC** icon (see Figure 6.1). (Habitual WarDrivers will want to add KisMAC to their toolbar.)

**Figure 6.1** KisMAC


KisMAC
KisMAC 0.2a
Search SSIDs
?
# Ch SSID BSSID Enc Type Signal Avg Max Packets Data Last Seen
Start Scan

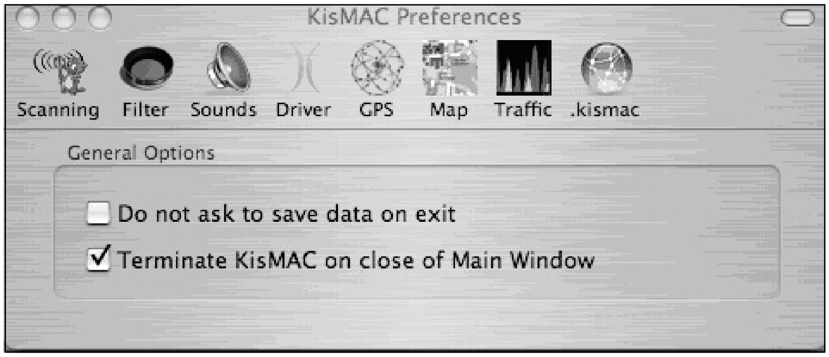
Next, you need to configure your KisMAC preferences and understand the KisMAC interface.

## Configuring the KisMAC Preferences

The KisMAC interface is very straightforward; however, because it is so robust, there are many different configuration options available. The first thing you need to do is open the "Preferences" window from the KisMAC menu by pressing **KisMAC | Preferences** (see Figure 6.2). This section covers six of the eight available preferences:

- Scanning
- Filter
- Sounds
- Driver
- Traffic
- KisMAC

**Figure 6.2** KisMAC Preferences



General Options

☐ Do not ask to save data on exit

☑ Terminate KisMAC on close of Main Window

# Scanning Options

There are two scanning options available that relate to the actions KisMAC takes when closing:

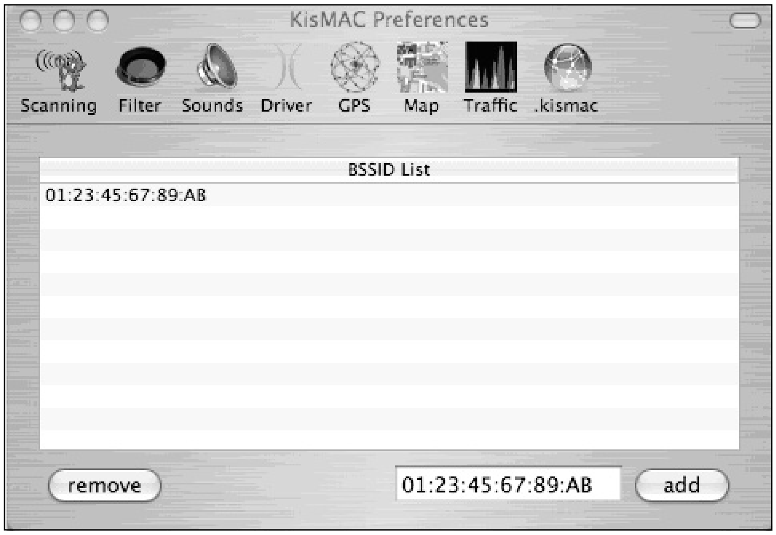
- Do not ask to save data on exit
- Terminate KisMAC on close of main window

By default, you will be prompted to save your data file unless you check the "Do not ask to save data on exit" option when closing KisMAC. It is a good idea to leave this option unchecked, thereby requiring you to manually save your data before closing KisMAC so that you do not accidentally lose data. The second option controls whether or not KisMAC terminates when you close the main window, which is a matter of personal preference. If this box is unchecked, KisMAC will be closed but remain loaded, and will continue to display in the toolbar.

# Filter Options

The Filter options allow you to designate specific MAC addresses that you *do not* want included in your results (see Figure 6.3). Enter a MAC address and press **add** to enable this functionality. This is especially useful for removing wireless networks (e.g., your home network or other boxes you are using for an attack) from your results. Additionally, if performing a penetration test, you will probably only want traffic from your target in your data sets.

**Figure 6.3** Filter Options



BSSID List

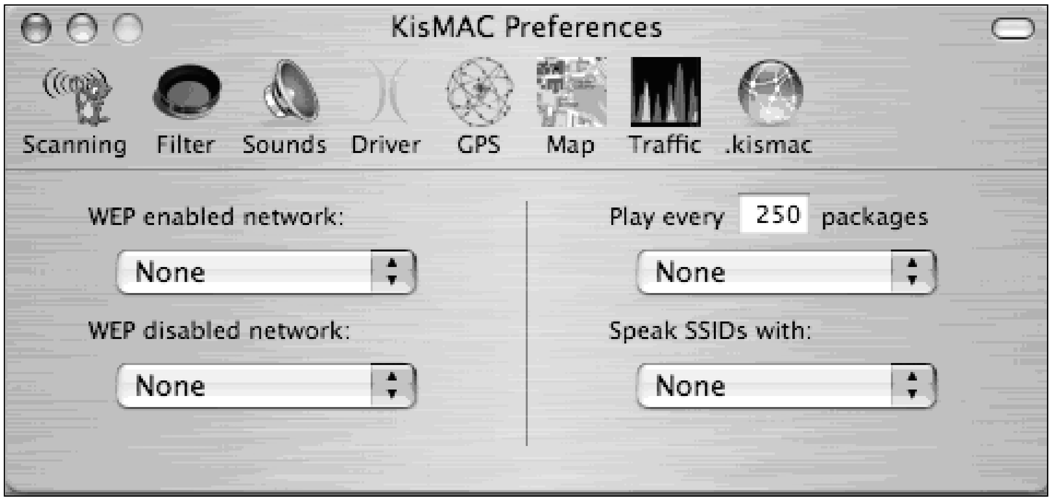
01:23:45:67:89:AB

01:23:45:67:89:AB

## Sound Preferences

Unlike its Linux counterpart, Kismet, which requires a third-party application such as Festival, KisMAC has built-in functionality for identifying the Service Set Identifier (SSID) of wireless networks (see Figure 6.4).

**Figure 6.4** Kismet Sound Preferences



WEP enabled network: None

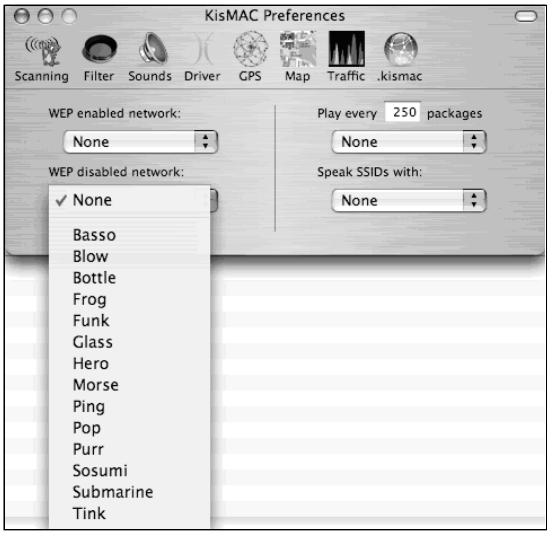
WEP disabled network: None

Play every 250 packages: None

Speak SSIDs with: None

Easy-to-use drop-down menus (see Figure 6.5) allow you to assign different sound effects to be played when a Wired Equivalent Privacy (WEP) or WiFi Protected Access (WPA) network is found. Additionally, specific sound effects can be played when a certain number of packets have been captured, and different voices can speak the network name or SSID as networks are discovered.

**Figure 6.5** Easy-to-Use Drop-Down Menus Allow You to Configure Sound Effects



KisMAC Preferences

WEP enabled network: None

WEP disabled network: ✓ None

Play every 250 packages: None

Speak SSIDs with: None

## Notes from the Underground

### Choosing a WLAN Card

KisMAC has built-in support for a wide range of WLAN cards. When choosing a card you must determine what your goals are; KisMAC has support for both active and passive scanning. Active scanning relies on the broadcast beacon to discover access points; the built-in Airport Extreme card on most iBooks and Powerbooks works in active mode only.

Passive scanning does not rely on the broadcast beacon. In order to passively scan for wireless networks, you must have a card capable of entering monitor mode (*rfmon*). Once a card has been placed in monitor mode, it can sniff all

**Continued**

traffic within range of that card (or its attached antenna) and discover any wireless networks, including those that do not broadcast from the beacon.

Kismet supports Airport or Airport Extreme cards in active mode. Atheros, Prism2, Hermes, and Prism GT chipsets support Airport and Cisco Personal Computer Memory Card International Association (PCMCIA) cards in passive mode. Additionally, Universal Serial Bus (USB) devices based on the Prism2 chipset support passive mode. Figure 6.6 displays the drop-down menu of available chipsets. Table 6.2 indicates some of the common cards and chipsets that work with KisMAC and the mode they work in.

**Table 6.2** Cards That Work with KisMAC

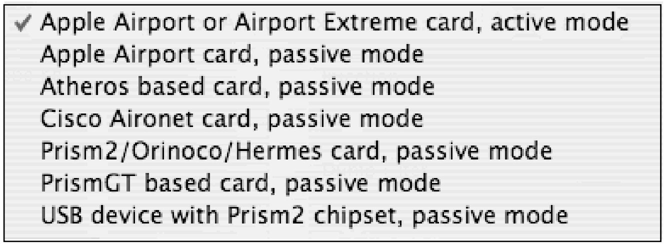
| Manufacturer | Card | Chipset | Mode |
|---|---|---|---|
| Apple | Airport | Hermes | Passive |
| Apple | Airport Express | Broadcom | Active |
| Cisco | Aironet LMC-352 | Cisco | Passive |
| Proxim | Orinoco Gold | Hermes | Passive |
| Engenius | Senao 2511CD Plus EXT2 | Prism 2 | Passive |
| Linksys | WPC11 | Prism 2 | Passive |
| Linksys | WUSB54G | Prism2 | Passive |

**NOTE**

If your adapter is not listed in Table 6.2, go to **http://linux-wlan.org/docs/wlan_adapters.html.tgz** for a more complete list of cards and their respective chipsets.

12-in. Powerbooks and all iBook models do not have PCMCIA slots, and therefore require a USB WiFi Adapter (e.g., Linksys WUSB54G or an original Airport) in order to work in passive mode. Unfortunately, there are currently no USB WiFi adapters with external antenna connectors.

**Figure 6.6** KisMAC-supported Chipsets

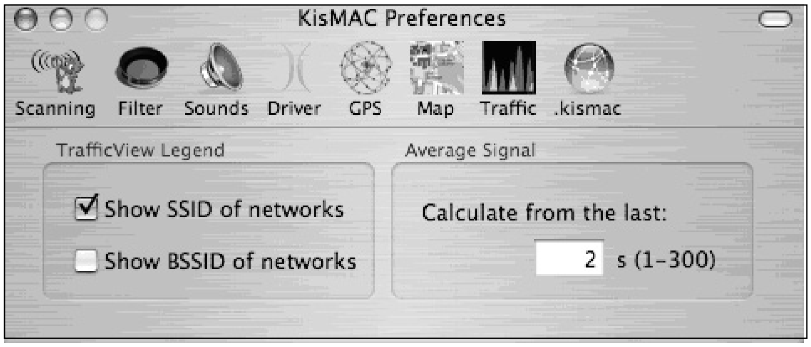


✓ Apple Airport or Airport Extreme card, active mode
Apple Airport card, passive mode
Atheros based card, passive mode
Cisco Aironet card, passive mode
Prism2/Orinoco/Hermes card, passive mode
PrismGT based card, passive mode
USB device with Prism2 chipset, passive mode

# Traffic

KisMAC also affords WarDrivers the ability to view the signal strength, number of packets transferred, and number of bytes transferred on detected networks. Networks can be displayed using the SSID or MAC address (denoted in the "Options" panel (see Figure 6.7) by Basic Service Set Identifier (BSSID). The average signal can be calculated based on the amount of traffic seen in the last 1–300 seconds, and should be adjusted depending on the degree of accuracy needed.

**Figure 6.7** Traffic Preferences



TrafficView Legend

☑ Show SSID of networks

□ Show BSSID of networks

Average Signal

Calculate from the last:

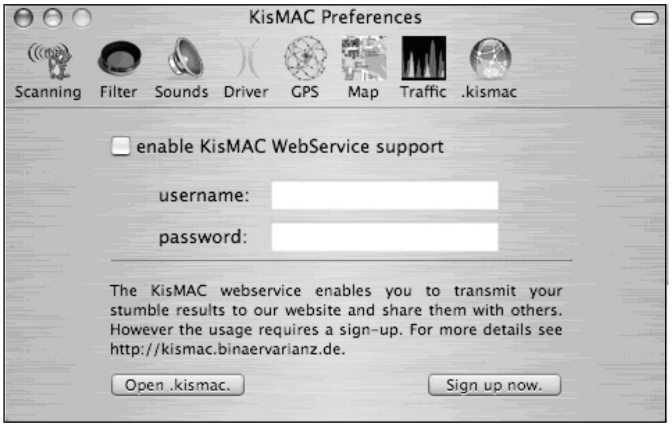
2 s (1-300)

# KisMAC Preferences

KisMAC is a built-in option that allows you to easily share your WarDrive data with other KisMAC users. In order to use KisMAC, you need a KisMAC account, which can be created from the KisMAC "Preferences" window.

Press the **Sign up now**. button to open the default browser (http://binaervarianz.de/register.php) and create your KisMAC account (see Figure 6.8). Figure 6.9 displays the KisMAC registration window.

**Figure 6.8** The KisMAC Preferences



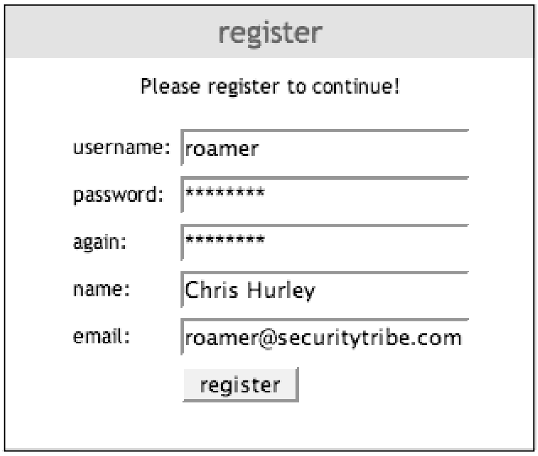
□ enable KisMAC WebService support

username:

password:

The KisMAC webservice enables you to transmit your stumble results to our website and share them with others. However the usage requires a sign-up. For more details see http://kismac.binaervarianz.de.

**Figure 6.9** KisMAC Registration Window



register

Please register to continue!

username: roamer

password: ********

again: ********

name: Chris Hurley

email: roamer@securitytribe.com

To send your data to the KisMAC server, when you have finished WarDriving select the **Export** option from the File menu by pressing **File ? Export ? Data to KisMAC Server**.

In addition to transmitting your results to the KisMAC server, a KisMAC account allows you to search the existing KisMAC database.

**NOTE**

It is a good idea to disable KisMAC prior to doing work for a customer, so that their data is not sent to a public server.

# Mapping WarDrives with KisMAC

In general, KisMAC is a very intuitive and easy-to-use tool; however, there is one exception: *mapping*. Mapping WarDrives with KisMAC can be a frustrating experience at first. This section details the steps required to successfully import a map to use with KisMAC.

## Importing a Map

The first step required in mapping WarDrives with KisMAC is importing a map. This differs from many other WLAN discovery applications (e.g., Kismet for Linux or NetStumbler for Windows) where maps are often generated at the completion of the WarDrive.

KisMAC requires the *latitude* and *longitude* of the center area of your drive in order to import a map. These coordinates can be input manually, but it is easier to connect your GPS first and get a signal lock.

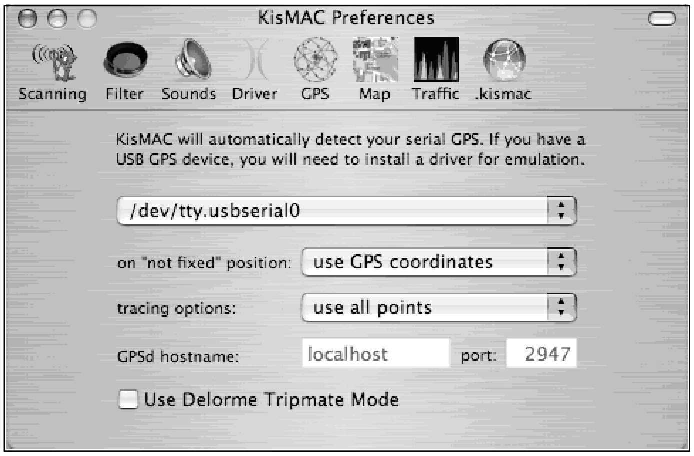
### *Using a GPS*

Most GPS devices capable of National Marine Electronics Association (NMEA) output, work with KisMAC. Many of these devices are only available with serial cables. In most cases, you will need to purchase a serial-to-USB adapter (approximately $25) in order to connect your GPS to your Mac. Most of these adapters come with drivers for OS X; thus, make sure that the one you purchase includes these drivers. Also, depending on your GPS model, you may be able to use a USB GPS cable and eliminate the need for a USB-to-serial adapter. The GPS Store sells these cables at http://www.thegpsstore.com/detail.asp?product_id=GL0997.

After you have connected your GPS, open the KisMAC Preferences and select the GPS options (see Figure 6.10). Select **/dev./tty.usbserial0** from the drop-down menu if it wasn't automatically selected.

Ensure that **use GPS coordinates** and **use all points** are selected and that the GPSd is listening on localhost port 2947. Your GPS is now configured and ready to go. To install GPS, download GPSd for OS X from *http://gpsd.berlios.de/*. Instructions for compiling and using GPSd can be found at (*http://kismac.binaervarianz.de/wiki/wiki.php/KisMAC/WiFiHacksCompileGPSd)*.

**Figure 6.10** KisMAC GPS Preferences



KisMAC will automatically detect your serial GPS. If you have a USB GPS device, you will need to install a driver for emulation.

/dev/tty.usbserial0

on "not fixed" position: use GPS coordinates

tracing options: use all points

GPSd hostname: localhost port: 2947

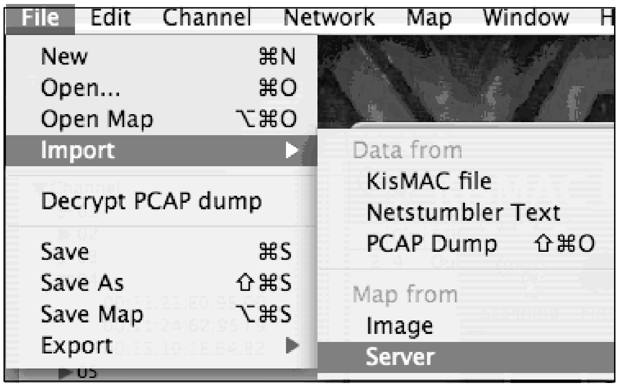
□ Use Delorme Tripmate Mode

Another option is using a Bluetooth GPS; however, according to the KisMAC Web site there is a problem with the Bluetooth stack in OS X; you still have to use GPSd with these devices.

## *Ready to Import*

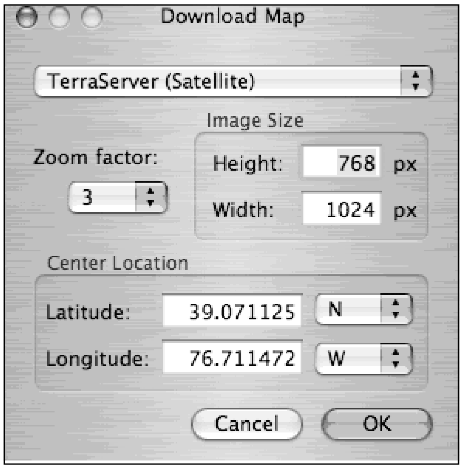
Now that your GPS device is connected, you are ready to import a map. To import a map, select **File | Import | Map from | Server** (see Figure 6.7).

**Figure 6.11** Preparing to Import a Map



This opens the "Download Map" dialog box (see Figure 6.12). Your current GPS coordinates are automatically imported into this box. Choose the server and type of map you want to import.

**Figure 6.12** Choosing the Map Server and Type of Map



Download Map

TerraServer (Satellite)

Zoom factor: 3

Image Size

Height: 768 px

Width: 1024 px

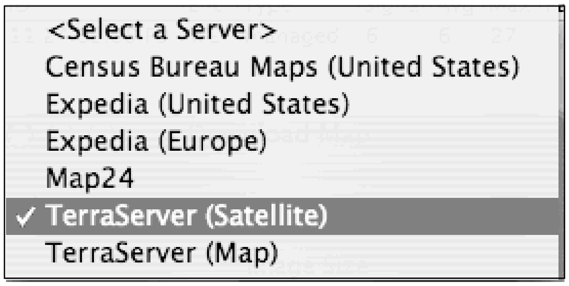
Center Location

Latitude: 39.071125 N

Longitude: 76.711472 W

There are several map servers available as well as different types of maps (i.e., *regular* or *satellite*), as shown in Figure 6.13.

**Figure 6.13** Available Map Servers and Types of Maps

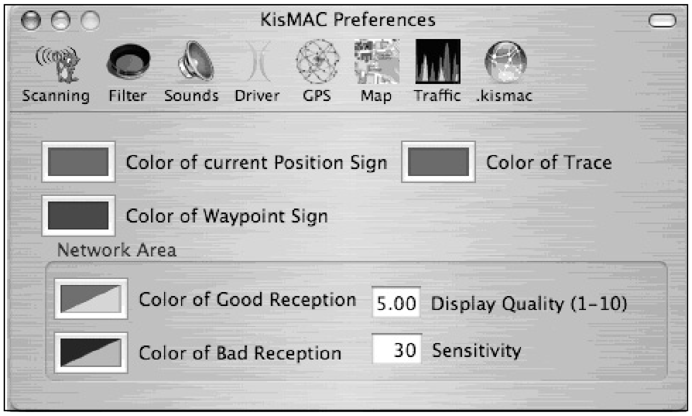


After importing your map, save it by pressing **File | Save Map** so that if KisMAC crashes during your WarDrive, you will have a local copy. KisMAC is an outstanding tool that is prone to occasionally crashing, which can happen when a large number of networks are found simultaneously. Additionally, many of the attacks included with KisMAC require significant memory and processor power. Even more unfortunate is that when KisMAC crashes, the system usually stops responding, thus requiring a complete shutdown and restart of the system to resume operations.

Waypoint 1 is set to your current position. Before beginning your WarDrive, you need to set WayPoint 2. From the OS X toolbar press **Map | Set Waypoint 2** and place the second WayPoint at your destination or any other place on the map if you are unsure of your destination.

Next, set your "Map" preferences by pressing **KisMAC | Preferences** (see Figure 6.14), which is where you set the preferences for the color scheme used on your map and the display quality and sensitivity levels some colors denote.

**Figure 6.14** KisMAC Map Preferences



Color of current Position Sign

Color of Trace

Color of Waypoint Sign

Network Area

Color of Good Reception

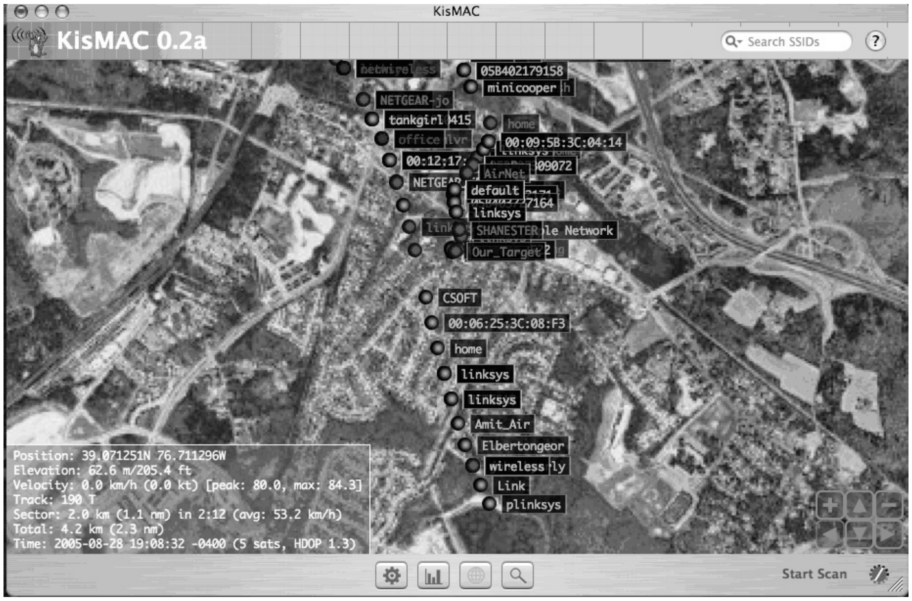
5.00 Display Quality (1-10)

Color of Bad Reception

30 Sensitivity

After all of your options are set, you are ready to WarDrive. As access points are discovered they are plotted on the map. Pressing the **Show Map** button displays your map and your access points are plotted in real time as you drive. A typical map generated by KisMAC using a satellite image, is shown in Figure 6.15.

**Figure 6.15** Typical KisMAC Satellite Map



```
Position: 39.071251N 76.711296W
Elevation: 62.6 m/205.4 ft
Velocity: 0.0 km/h (0.0 kt) [peak: 80.0, max: 84.3]
Track: 190 T
Sector: 2.0 km (1.1 nm) in 2:12 (avg: 53.2 km/h)
Total: 4.2 km (2.3 nm)
Time: 2005-08-28 19:08:32 -0400 (5 sats, HDOP 1.3)
```

KisMAC includes the ability to manipulate your map as well.

Notes from the Underground…

### Disabling the Annoying “Sleep” Function

One of the more irritating features of OS X for WarDrivers is the inability to disable the “sleep” function. In many states, driving with your laptop open is illegal. A laptop that is asleep and not collecting access points poses a difficult problem for OS X WarDrivers. Luckily, a kernel extension is available that allows you to temporarily disable the OS X sleep function.

Insomnia (**http://binaervarianz.de/projekte/programmieren/meltmac/**) is a kernel extension used to disable sleep in OS X. After downloading Insomnia, unpack the kernel extension and issue the following command:

```
sudo chown -R root:wheel Insomnia.kext
```

This correctly sets the permissions on the kernel extension. This step is required immediately after download and before using Insomnia. The kernel extension has to be loaded each time you want to disable the sleep function:

```
sudo kextload Insomnia.kext
```

Now when you close the lid on your Powerbook or iBook it will not go to sleep. When you are finished WarDriving and want to re-enable the “sleep” function, the kernel extension must be unloaded.

```
sudo kextunload Insomnia.kext
```

Your laptop is back to normal operation. It should be pointed out that Apple laptops generate a lot of heat, so it’s not a good idea to leave this kernel extension loaded all the time; just on the specific occasions when you need it.

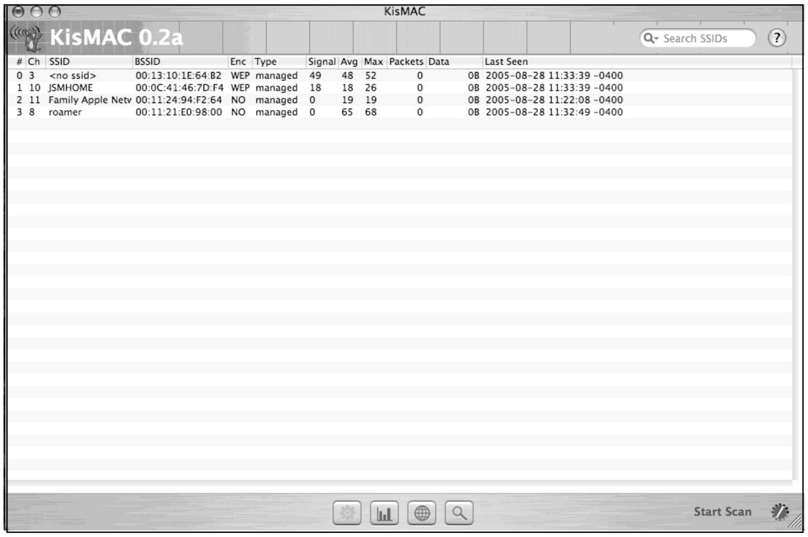
# WarDriving with KisMAC

Now that your KisMAC preferences are set, the correct driver is chosen, and your map is imported, it is time to go WarDriving. The KisMAC interface is easy to navigate and has some advanced functionality that combines the best features from other WarDriving applications, including many commercial applications.

## Using the KisMAC Interface

The KisMAC interface (see Figure 6.16) is straightforward and easy to understand. The main window displays all wireless networks that KisMAC has found, and can be sorted by number (in the order it was found); SSID; BSSID MAC address; the type of encryption used; the current, average, or maximum signal strength; the number of packets transmitted; the size of the data stream (in kilobytes or megabytes); and the time that the access point was last in range (Last Seen).

**Figure 6.16** KisMAC Graphical User Interface



| # | Ch | SSID | BSSID | Enc | Type | Signal | Avg | Max | Packets | Data | Last Seen |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 3 | <no ssid> | 00:13:10:1E:64:B2 | WEP | managed | 49 | 48 | 52 | 0 | 0B | 2005-08-28 11:33:39 -0400 |
| 1 | 10 | JSMHOME | 00:0C:41:46:7D:F4 | WEP | managed | 18 | 18 | 26 | 0 | 0B | 2005-08-28 11:33:39 -0400 |
| 2 | 11 | Family Apple Netv | 00:11:24:94:F2:64 | NO | managed | 0 | 19 | 19 | 0 | 0B | 2005-08-28 11:22:08 -0400 |
| 3 | 8 | roamer | 00:11:21:E0:98:00 | NO | managed | 0 | 65 | 68 | 0 | 0B | 2005-08-28 11:32:49 -0400 |

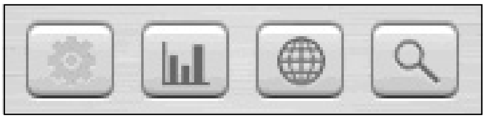
After you have configured the options for your WarDrive, press the **Start Scan** button (located in the bottom right corner of the interface) to begin locating access points. Additionally, there are four buttons across the bottom toolbar that allow you to see specific information about your current drive.

### *The KisMAC Window View Buttons*

KisMAC allows you to see specific information about your current WarDrive by selecting one of four buttons that are located on the bottom toolbar (see Figure 6.17).

The **Show Networks** button is the default setting. To return to the default setting after selecting other options, press this button to see all of the networks that have been discovered.

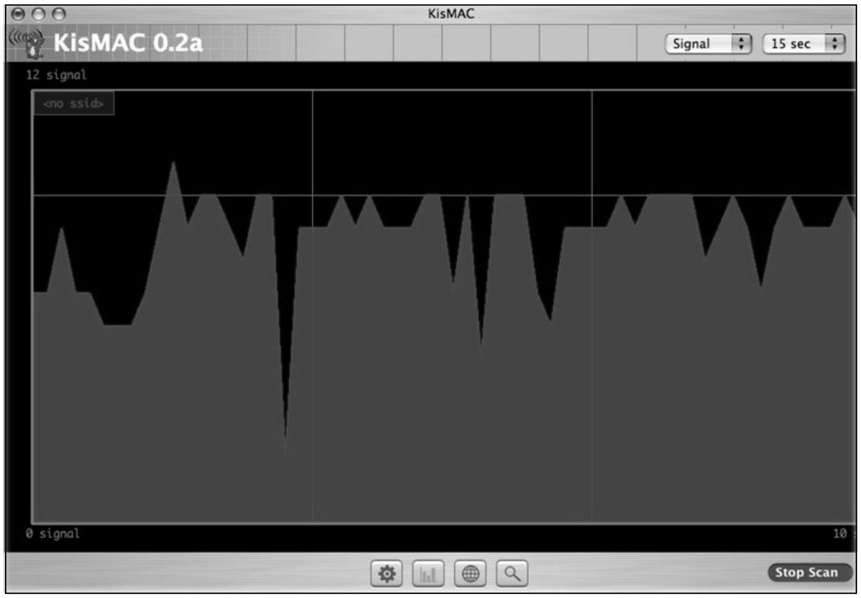
**Figure 6.17** KisMAC Window View Buttons



The **Show Networks** button is the default setting. To return to the default setting after selecting other options, press this button to see all of the networks that have been discovered.

Selecting the **Show Traffic** button 📊 brings up a signal graph of the networks that were discovered during your WarDrive. By default, this view shows a signal strength graph (see Figure 6.18). Each access point is denoted by a unique color, and a key showing which network is assigned to each color is in the upper right-hand corner. The taller lines in the graph indicate a stronger signal.

**Figure 6.18** "Show Traffic" View

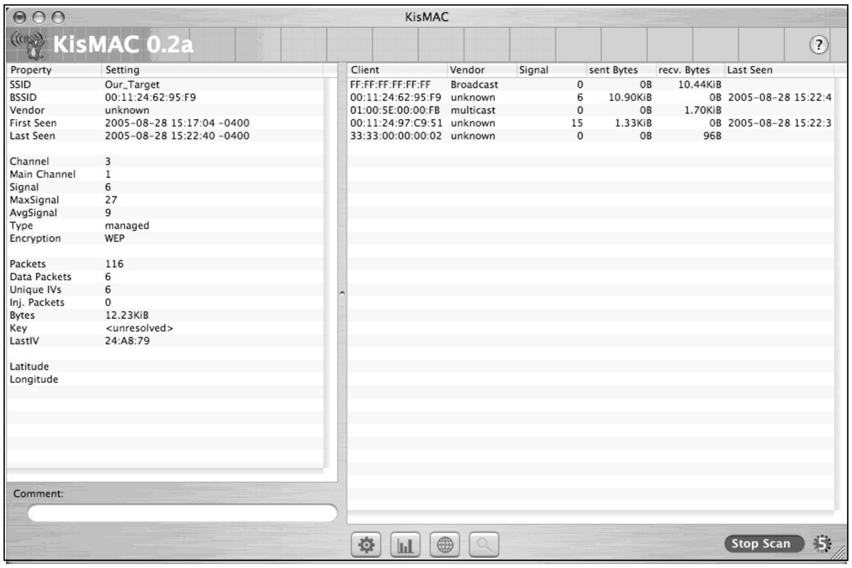


There are two drop-down menus in the upper left-hand corner. One is the interval (15 seconds by default) that is displayed, and the other is a menu that allows you to change the type of information that can be viewed using the "Show Traffic" view. In addition to the signal strength, you can also display the packets per second that are traversing the wireless network, or the total number of bytes that have been sent and received by the access points.

The **Show Map** button allows you to view a live map of your current WarDrive. (For more information on mapping your WarDrive, see "Mapping Your WarDrive" earlier in this chapter.)

The last view is accessed with the **Show Details** button . This view allows you to obtain a significant amount of information about a specific access point (see Figure 6.19).

**Figure 6.19** "Show Details" View



| Property | Setting |
|---|---|
| SSID | Our_Target |
| BSSID | 00:11:24:62:95:F9 |
| Vendor | unknown |
| First Seen | 2005-08-28 15:17:04 -0400 |
| Last Seen | 2005-08-28 15:22:40 -0400 |
| Channel | 3 |
| Main Channel | 1 |
| Signal | 6 |
| MaxSignal | 27 |
| AvgSignal | 9 |
| Type | managed |
| Encryption | WEP |
| Packets | 116 |
| Data Packets | 6 |
| Unique IVs | 6 |
| Inj. Packets | 0 |
| Bytes | 12.23KiB |
| Key | <unresolved> |
| LastIV | 24:A8:79 |
| Latitude | |
| Longitude | |

| Client | Vendor | Signal | sent Bytes | recv. Bytes | Last Seen |
|---|---|---|---|---|---|
| FF:FF:FF:FF:FF:FF | Broadcast | 0 | 0B | 10.44KiB | |
| 00:11:24:62:95:F9 | unknown | 6 | 10.90KiB | 0B | 2005-08-28 15:22:4 |
| 01:00:5E:00:00:FB | multicast | 0 | 0B | 1.70KiB | |
| 00:11:24:97:C9:51 | unknown | 15 | 1.33KiB | 0B | 2005-08-28 15:22:3 |
| 33:33:00:00:00:02 | unknown | 0 | 0B | 96B | |

The information listed in the default view is on the left side of the interface, and the information about clients that are attached to the network is on the right-hand side of the interface. The information available in this view is essential to a penetration tester, and is discussed in detail in the "Penetration Testing with OS X" section later in this chapter.

## *Additional View Options with KisMAC*

In addition to the View buttons, KisMAC provides you with the ability to obtain additional information about specific networks while in "Show Networks" view. Using the OS X menu bar, press **Windows | Show Hierarchy** (see Figure 6.20).

With "Show Hierarchy" displayed (see Figure 6.21), you can gather more information about specific networks; networks utilizing different types of encryption; or all networks transmitting on a specific channel. This information is vital during a penetration test.

**Figure 6.20** OS X Menu Hierarchy

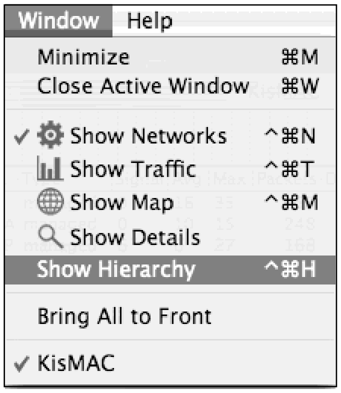
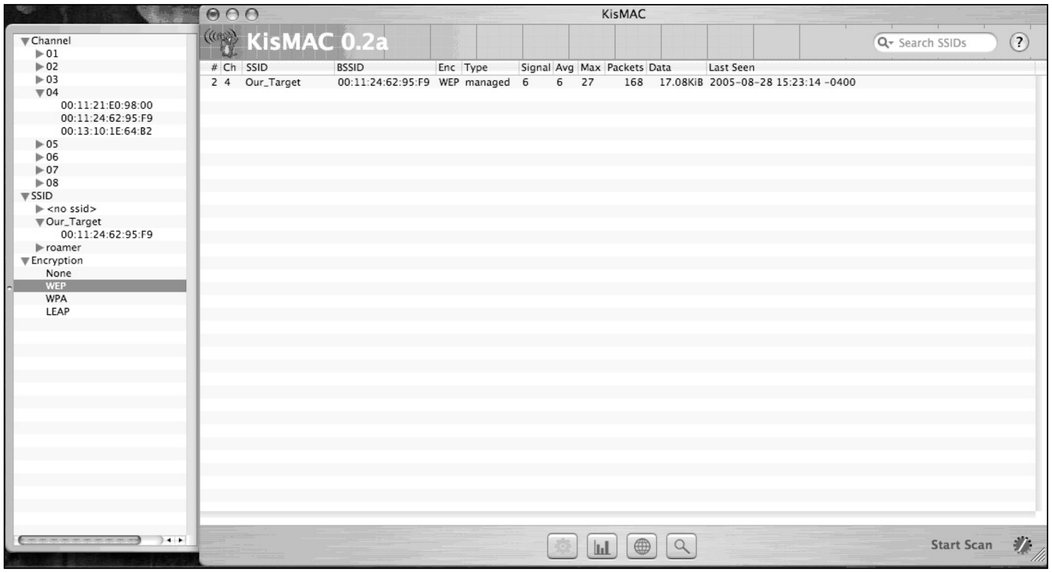


**Figure 6.21** "KisMAC Hierarchy" View



| # | Ch | SSID | BSSID | Enc | Type | Signal | Avg | Max | Packets | Data | Last Seen |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 4 | Our_Target | 00:11:24:62:95:F9 | WEP | managed | 6 | 6 | 27 | 168 | 17.08KiB | 2005-08-28 15:23:14 -0400 |

# Penetration Testing with OS X

In addition to being used as a WarDriving application, KisMAC is the best tool available for wireless network penetration testing. KisMAC has built-in functionality to perform many of the most common WLAN attacks, using an easy "point-and-click" interface. Additionally, KisMAC can import packet capture dumps from other programs to perform many offline attacks against wireless networks. This section walks through many of these attacks on the target network.

The following is a working example: You're contracted to perform a penetration test for a company and need to correctly identify their wireless network. Using the information gathered during your WarDrive of the area surrounding your target, you successfully identified the target network based on the signal strength, map data, and naming convention used on the access point. To successfully penetrate this network, you have to determine what type of encryption is being used.

# Attacking WLAN Encryption with KisMAC

There are several different types of encryption that wireless networks can employ. The most commonly used encryption schemes are WEP and WPA, although there are other, more advanced schemes available. Looking at the KisMAC display, you see that the access point with the SSID *Our_Target* is a WEP-encrypted network.

## Attacking WEP with KisMAC

Since you have determined that WEP is being used on your target wireless network, you now have to decide how you want to crack the key. KisMAC has three primary methods of WEP cracking built in:

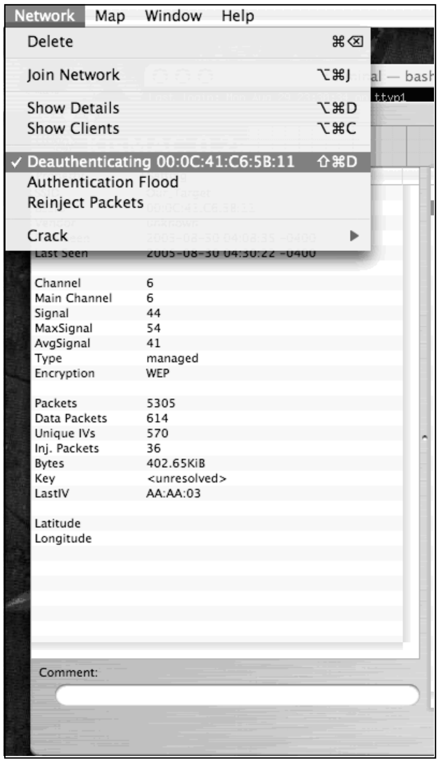
- Wordlist attacks
- Weak scheduling attacks
- Bruteforce attacks

To use one of these attacks, you have to generate enough initialization vectors (IVs) for the attack to work. The easiest way to do this is by reinjecting traffic, which is usually accomplished by capturing an Address Resolution Protocol (ARP) packet, spoofing the sender, and sending it back to the access point. This generates a large amount of traffic that can then be captured and decoded. Unfortunately, you can't always capture an ARP packet under normal circumstances; however, when a client authenticates to the access point, an ARP packet is usually generated. Because of this, if you can deauthenticate the clients that are on the network and cause them to reassociate, you may get your ARP packet.

Looking at the detailed view of *Our_Target*, you can see that there are several clients connected to it. Before continuing with the attack, you need to determine the role that KisMAC will play. Two hosts are required to successfully crack the WEP key: one host is used to inject traffic, and the other host is used to capture the traffic (specifically the IVs). In this case, you will use KisMAC to inject and will have a second host to capture the traffic. While KisMAC and OS X are very powerful attack tools, the actual cracking is often best performed on a Linux host utilizing tools such as Aircrack (*www.cr0.net:8040/code/network*),because KisMAC does not include support for many of the newer WEP attacks, such as chopping. Hopefully, these attacks will be included with future releases of KisMAC.

Deauthenticating clients with KisMAC is simple; however, before you can begin deauthenticating, you must lock KisMAC to the specific channel that your target network is using. From the top menu press **KisMAC ? Preferences ? Driver Preferences**. Highlight the driver you are using and deselect all channels other than the one that the target is using. Also, ensure that **use as primary device** is checked under the "Injection" menu. Close the "Preferences," highlight the access point you want to deauthenticate clients from, and press **Network ? Deauthenticate**. If KisMAC is successful in its attempt to deauthenticate, the dialog changes to note the BSSID of the access point it is deauthenticating (see Figure 22). During the time the deauthentication is occurring, clients cannot use the wireless network.

**Figure 6.22** Deauthenticaion



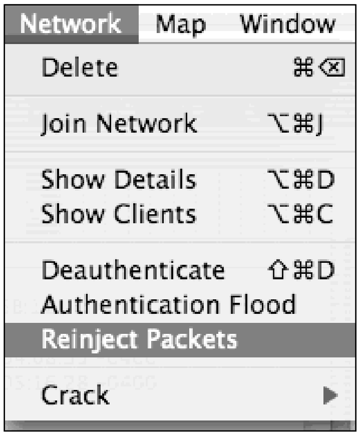
```
Last Seen      2005-08-30 04:30:22 -0400

Channel        6
Main Channel   6
Signal         44
MaxSignal      54
AvgSignal      41
Type           managed
Encryption     WEP

Packets        5305
Data Packets   614
Unique IVs     570
Inj. Packets   36
Bytes          402.65KiB
Key            <unresolved>
LastIV         AA:AA:03

Latitude
Longitude
```

During deauthentication, the number of Inj. Packets should increase (see Figure 6.22). After several of these have been captured, stop the deauthentication.

## Reinjection

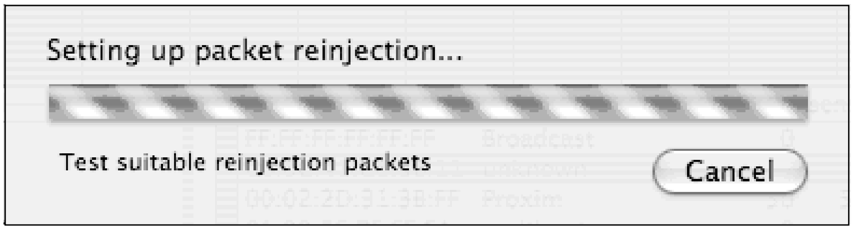
Once several potentially reinjectable packets have been captured (noted in the "Show Details" view of KisMAC), it is time to attempt reinjection. Press **Network | Reinject Packets** (see Figure 6.23).

**Figure 6.23** Preparing to Reinject Packets



This opens a dialog box (see Figure 6.24) indicating that KisMAC is testing each packet to determine if it can be successfully reinjected into the network.

**Figure 6.24** Testing the Packets



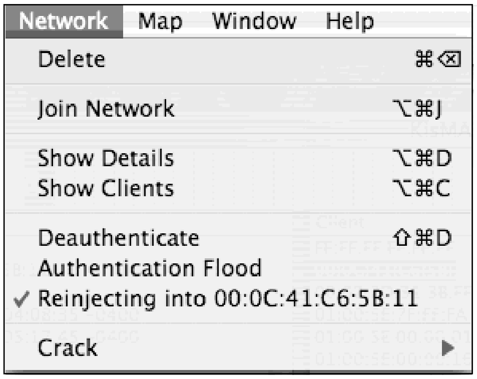
Setting up packet reinjection...

Test suitable reinjection packets

Once KisMAC finds a suitable packet, the dialog box closes and KisMAC begins injection. This can be verified by viewing the "Network" options (see Figure 6.25).

Now the traffic has to be captured with a second card (usually on a second machine) in order to capture enough IVs to attempt to crack the key. KisMAC can be used to perform weak scheduling attacks after enough weak IVs have been captured; however, it is probably more efficient to use KisMAC to inject packets, and to use a tool such as Aircrack to perform the actual WEP crack.

**Figure 6.25** Reinjection



# Attacking WPA with KisMAC

Unlike WEP, which requires a large amount of traffic be generated in order to crack the key, cracking WPA only requires that you capture the four-way Extensible Authentication Protocol Over Local Area Network (EAPOL) handshake at authentication. Also, unlike cracking WEP, the WPA attack is an offline dictionary attack, which means that when you use KisMAC to crack a WPA pre-shared key (or passphrase), you only need to capture a small amount of traffic; the actual attack can be carried out later, even when you are out of range of the access point.

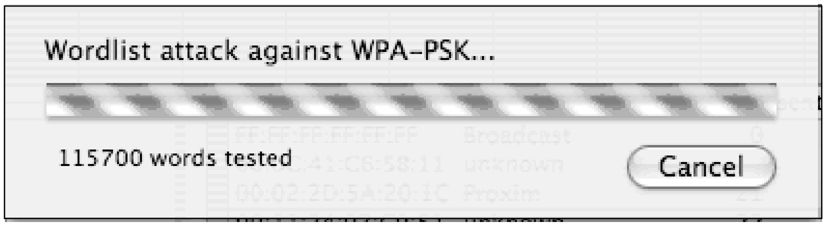
WPA is only vulnerable when a short passphrase is used. Even then, it must be a dictionary word or one that is in your wordlist. An extensive wordlist with many combinations of letters, numbers, and special characters can help increase the odds of successfully cracking WPA.

To attempt a dictionary attack against KisMAC, you may need to deauthenticate clients (detailed in the "Attacking WEP with KisMAC" section). However, when attempting dictionary attacks against WPA, everything can be done from one host, which will cause the client to disassociate from the network and force them to reconnect. This requires the four-way EAPOL handshake to be transmitted again.

Once you have captured an association between a client and the WPA network, press **Network | Crack | Wordlist Attack | Wordlist against WPA-PSK Key**. You will be prompted for the location of the wordlist or dictionary file that you want to use. After you have selected your dictionary file, KisMAC begins testing each word in that file against the WPA Pre-Shared Key (PSK)(see Figure 6.26).

When KisMAC has successfully determined the key, it is displayed in the "Show Details" view.

**Figure 6.26** WPA Cracking



Wordlist attack against WPA-PSK...

115700 words tested

# Other Attacks

KisMAC also offers the ability to perform attacks against other forms of encryption and authentication. Because these other methods have known vulnerabilities and are rarely used by clients, they are not discussed in detail, but are included for completeness.

## Bruteforce Attacks Against 40-bit WEP

KisMAC includes functionality to perform Bruteforce attacks against 40-bit WEP keys. There are four ways KisMAC can accomplish this:

- All possible characters
- Alphanumeric characters only
- Lowercase letters only
- Newshams 21-bit attack

Each of these attacks is very effective, but also very time- and processor-intensive.

## Wordlist Attacks

KisMAC provides the functionality to perform many types of wordlist attacks in addition to WPA attacks. Cisco developed the Lightweight Extensible Authentication Protocol (LEAP) to help organizations concerned about vulnerabilities in WEP. Unfortunately, LEAP is also vulnerable to wordlist attacks similar to WPA. KisMAC includes the functionality to perform wordlist attacks against LEAP by following the same procedure used when cracking WPA. Select the **against LEAP Key** button to begin the attack.

Additionally, wordlist attacks can be launched against 40- and 104-bit Apple keys or 104-bit Message Digest 5 (MD5) keys in the same manner. As with any dictionary attack, these attacks are only effective if a comprehensive dictionary file is used when performing the attack (see *www.securitytribe.com/~roamer/words.txt*).

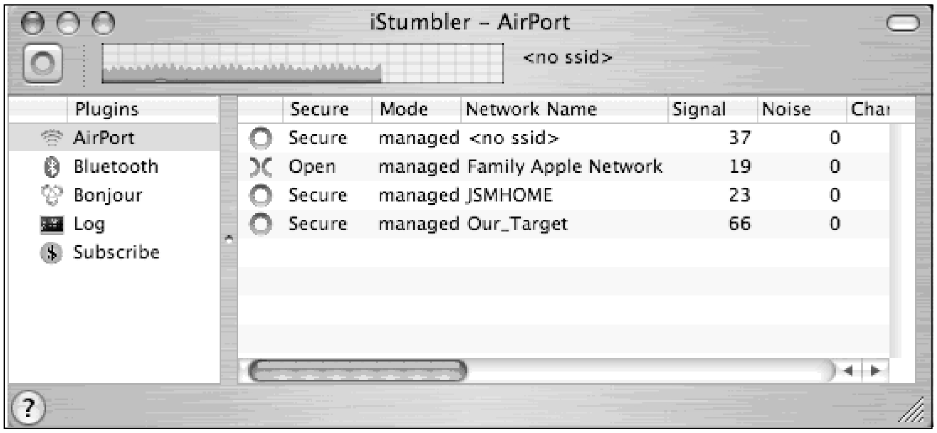
# Other OS X Tools for WarDriving and WLAN Testing

KisMAC has been the focus of the bulk of this chapter; however, there are several other wireless tools that can keep an OS X hacker busy for hours.

EtherPEG (*www.etherpeg.org*) is a program that captures and displays all of the Joint Photographic Experts Group (JPEG) and Graphic Interchange Format (GIF) images that are being transferred across the network (including WLANs). In order to use EtherPEG against a wireless network, encryption must not be in use, or you must be connected to the network.

iStumbler (*http://istumbler.net/)*, as shown in figure 6.27, is an active WLAN discovery tool for OS X that works with the built-in Airport Express card. In addition to WLAN discovery, iStumbler can also detect Bluetooth devices using the built-in Bluetooth adapter. There is no setup required with iStumbler; simply unpack the archive and press the **iStumbler** icon to begin.

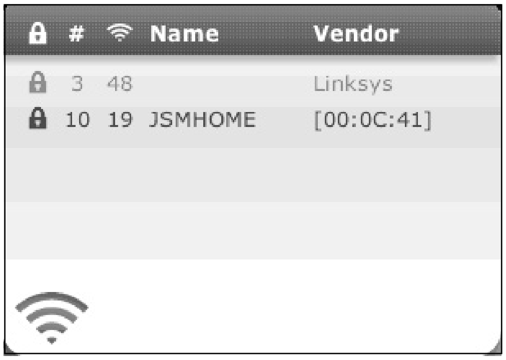
**Figure 6.27** iStumbler



| | Secure | Mode | Network Name | Signal | Noise | Cha |
|---|---|---|---|---|---|---|
| ○ | Secure | managed | <no ssid> | 37 | 0 | |
| )( | Open | managed | Family Apple Network | 19 | 0 | |
| ○ | Secure | managed | JSMHOME | 23 | 0 | |
| ○ | Secure | managed | Our_Target | 66 | 0 | |

With the release of OS X Tiger, there have been several dashboard widgets developed and released that perform active scanning with the Airport and Airport Express cards (e.g., Air Traffic Control) (see Figure 6.28).

**Figure 6.28** Air Traffic Control



| 🔒 | # | 📶 | Name | Vendor |
|---|---|---|---|---|
| 🔒 | 3 | 48 | | Linksys |
| 🔒 | 10 | 19 | JSMHOME | [00:0C:41] |

Dashboard widgets are updated regularly and new ones are released nearly every day. Check out the latest wireless discovery widgets at *www.apple.com/downloads/dashboard* and select the "Networking and Security" option from the "Widget Navigation" menu.

Tcpdump is a network traffic analyzer (sniffer) that ships with OS X. Tcpdump can be configured to listen on a wireless interface to capture traffic coming across the WLAN with the following command:

```
crapple:~ roamer$ sudo tcpdump -i en1
```

Tcpdump can be used to capture usernames and passwords that are sent in clear text (e-mail, Network Basic Input/Output System [NetBIOS], and so forth).

And finally, another useful packet sniffer is Ethereal (*www.ethereal.org*). Information on installing and using Ethereal is presented in Chapter X.

# Summary

When people think of WarDriving and attacking wireless networks, Linux is usually the first OS that comes to mind. While there are fantastic tools available for Linux, there are also several outstanding tools for the wireless hacker available for OS X.

KisMAC is the most popular WarDriving application for OS X. Because it offers the option of both active and passive scanning and a large number of supported chipsets, it is perfect for WarDriving. Add to that the ease of setup and configuration and KisMAC stands out as one of, if not the top WarDriving application available.

In addition to its power as a WarDriving application, KisMAC is also a very powerful tool for WLAN penetration testing. It provides many of the most popular attacks (the new chopping attacks against WEP being the only omission) and offers penetration testers easy, point-and-click options for some attacks that are traditionally more difficult on other OSes (e.g., deauthentication and traffic reinjection). The tools available for these type of attacks on other OSes are either difficult to use or are so restricted that working with KisMAC's point-and-click attack method is a welcome change.

While KisMAC is outstanding, it isn't the only WLAN discovery tool available for OS X. iStumbler has a far smaller feature set than KisMAC, but is extremely easy to use and also includes Bluetooth functionality. There are also several dashboard widgets that can be downloaded from the Apple Web site that work in conjunction with the Airport and Airport Express cards to perform active WLAN discovery.

Wireless hackers are going to be hard pressed to find an OS other than OS X that combines power, functionality, and ease of use with a more robust set of available free tools.

# Solutions Fast Track

## WarDriving with Kismac

☑ Kismac is one of the most versatile tools available for WarDriving

☑ Kismac can operate in both active and passive modes.

☑ Kismac has built in capability to allow WarDrivers to map their drives

## Penetration Testing with OS X

☑ Kismac provides the capability to perform many wireless penetration testing tasks

☑ Kismac has the ability to deauthenticate clients built in

☑ Kismac contains routines for injecting traffic into a wireless network

☑ Kismac has built in tools to crack WEP

☑ Kismac has built in tools to crack WPA Passphrases

## Other OS X Tools for WarDriving and WLAN Testing

☑ iStumbler is a tool that can detect not only 802.11 b/g wireless networks, but also Bluetooth devices

☑ As of OS X 10.4 Tiger, there are many dashboard widgets available that can detect wireless networks.

☑ A packet analyzer, or sniffer, such as TCPDump or Ethereal is a valuable tool for a wireless penetration tester.

# Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

**Q.** Why do some attacks require weak IVs and some only require unique IVs?

**A.** The traditional attacks against WEP were originally detailed by Scott Fluhrer, Itsik Mantin, and Adi Shamir in their paper, "Weaknesses in the Key Scheduling Algorithm of RC4." (www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf). These attacks are known as FMS attacks. This paper details that a small subset of the total IVs were weak and, if enough were collected, could be used to determine the WEP key. The problem with this method was that it was very time consuming due to the number of packets required to capture enough weak IVs to crack the key.

In February 2002, H1kari detailed a new method for attacking WEP (www.dachb0den.com/projects/bsd-airtools/wepexp.txt), dubbed "chopping," where weak IVs were no longer required. Instead, approximately 500,000 unique IVs needed to be gathered in order to successfully crack the WEP key. This, coupled with the ability to reinject ARP packets into the network, greatly reduced the amount of time required to crack WEP. Using the FMS method of WEP cracking, it could take weeks or months to successfully crack the WEP key. The chopping method has reduced this to a matter of hours (and sometimes less). This attack took a theoretical threat and turned it into a significant vulnerability for wireless networks utilizing WEP.

More information on WEP cracking and the tools available for cracking can be found in Chris Hurley's paper, "Aircrack and WEPlab: Should You Believe the Hype," available for download at www.securityhorizon.com/journal/fall2004.pdf.

**Q.** I remember a tool call MacStumbler. Why isn't it mentioned in this chapter?

**A.** MacStumbler (www.macstumbler.com) was one of the first WLAN discovery tools available for OS X. Unfortunately, it only operated in active mode, and development and maintenance ceased in July 2003. Many tools, such as KisMAC, have taken WLAN discovery for OS X to the next level and essentially rendered MacStumbler obsolete. However, it is still available for download and is compatible with both Airport Express cards and OS X Tiger.

**Q.** Can KisMAC logs be imported into other applications?

**A.** Yes. You can export KisMAC to NetStumbler and MacStumbler readable formats.

**Q.** Why would I want to export to NetStumbler format?

**A.** There are a couple of good reasons to export to NetStumbler format. First, it allows you to map your drives after completion using the assorted mapping tools available. Second, NetStumbler has excellent support for exporting WarDrive data to different formats. Once you have imported your KisMAC data into NetStumbler, you have the ability to export to any of these formats.