Ganas de hacer lo que otros hacen con Linux aircrack, ethereal u similares???

fuente: http://screammy.name/projects/kismacmacbook/

HOWTO: Compile, install, and run KisMAC in passive mode on a MacBook

Why?

The current distribution of KisMAC does not allow you to use the AirPort Extreme card in passive mode, capture packets, etc.
Please keep in mind, this howto uses the latest development version of KisMAC, it may crash without warning.

UPDATE 09/05/2007 -- I've modified this for the SVN location change.

1. Download and install Xcode

a. If you don't have an Apple Developer Connection account, create one here .
b. Download and install Xcode from here . Use the account you just created to access the download.

2. Get subversion

You have a couple options to get subversion.

Option 1 (.dmg pre-built binary):
a. Download the latest .dmg from here .
b. Install it.

Option 2 (darwinports):
a. Download and install darwinports from here . It's the first link, "for Tiger (Universal)".
b. After you install darwinports, open terminal.app and run the following commands, exactly as shown:
NOTE: if you are running PeerGuardian, disable the filters

```
cd; echo 'export PATH=$PATH:/opt/local/bin' >> .profile
source .profile
sudo port selfupdate
sudo port sync
sudo port install subversion
```

Option 3 (fink):

I don't use fink but it will work to get subversion; fink's site is here .

Final (test subversion):
a. Open Terminal.app
b. Type "svn" and hit enter. If you see the output listed next, subversion is installed. Type 'svn help' for usage.

3. Download and compile KisMAC

a. Open Terminal.app
b. Type the following commands, exactly as shown:
NOTE: You should be a local administrator of the mac

```
cd Desktop
mkdir KisMAC.src
cd KisMAC.src
svn co http://kismac-ng.googlecode.com/svn/trunk/
```

NOTE: svn will ask you to accept the SSL cert from the site before it continues, type 't' and hit enter for temporarily. Subversion will now download the source tree.

```
cd trunk
./compile.command image
```

NOTE: this script will compile KisMAC using Xcode.

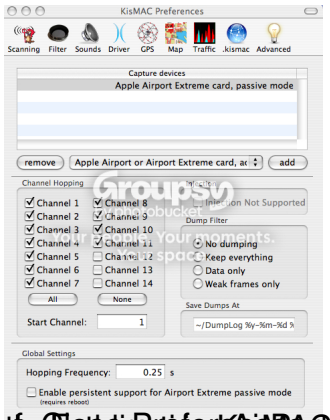
KisMAC will now be compiled in a folder on your desktop, KisMAC.src/trunk/build/Universal/

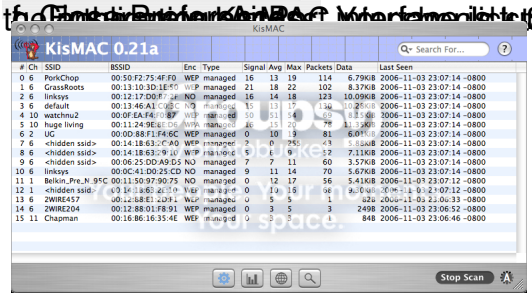
Install KisMAC

NOTE: if you already have KisMAC installed, you must remove it. Drag KisMAC.app from Applications to your trash
a. Open finder and navigate to the newly compiled KisMAC.app, Desktop->KisMAC.src->trunk->build->Universal
b. Drag KisMAC.app to Applications

Configure and use

a. Open KisMAC.app from Applications
b. Click KisMAC->Preferences
c. Click Driver
d. Select the one capture device listed, "Apple Airport or Airport Extreme card, active mode", and click remove
e. Expand the drop down next to "remove", select "Apple Airport Extreme card, passive mdoe", and click "add"
Your preferences should look like this:


KisMAC Preferences
Scanning
Filter
Sounds
Driver
GPS
Map
Traffic
kismac
Advanced
Capture devices
Apple Airport Extreme card, passive mode
remove
Apple Airport or Airport Extreme card, ac
add
Channel Hopping
Channel 1
Channel 2
Channel 3
Channel 4
Channel 5
Channel 6
Channel 7
Channel 8
Channel 9
Channel 10
Channel 11
Channel 12
Channel 13
Channel 14
All
None
Start Channel:
1
Dump Filter
No dumping
Keep everything
Data only
Weak frames only
Save Dumps At
~/DumpLog %y-%m-%d %
Global Settings
Hopping Frequency:
0.25
s
Enable persistent support for Airport Extreme passive mode
(requires reboot)


KisMAC
KisMAC 0.21a
Search For...
Ch SSID BSSID Enc Type Signal Avg Max Packets Data Last Seen
0 6 PorkChop 00:50:F2:75:4F:F0 WEP managed 16 13 19 114 6.79KiB 2006-11-03 23:07:14 -0800
1 6 GrassRoots 00:13:10:3D:1E:50 WEP managed 21 18 22 102 8.37KiB 2006-11-03 23:07:14 -0800
2 6 linksys 00:12:17:D0:F7:4E NO managed 16 14 18 123 10.09KiB 2006-11-03 23:07:14 -0800
3 6 default 00:13:46:A1:C9:BC NO managed 15 13 17 [illegible] [illegible] 2006-11-03 23:07:14 -0800
4 10 watchnu2 00:0F:EA:F4:F0:87 WEP managed 50 51 54 [illegible] [illegible] 2006-11-03 23:07:14 -0800
5 10 huge living 00:11:24:9E:[illegible] WPA managed [illegible] 15 20 78 11.32KiB 2006-11-03 23:07:14 -0800
6 2 UG 00:0D:88:F1:F4:6C WEP managed 0 10 19 81 6.07KiB 2006-11-03 23:07:14 -0800
7 6 <hidden ssid> 00:14:1B:63:C[illegible] WEP managed [illegible] 0 [illegible] [illegible] [illegible] 2006-11-03 23:07:14 -0800
8 6 <hidden ssid> 00:14:1B:63:[illegible] WEP managed 5 [illegible] 9 [illegible] 7.11KiB 2006-11-03 23:07:14 -0800
9 6 <hidden ssid> 00:06:25:DD:A9:D5 NO managed 7 7 11 60 3.57KiB 2006-11-03 23:07:14 -0800
10 6 linksys 00:0C:41:D0:25:CD NO managed 9 11 14 70 5.67KiB 2006-11-03 23:07:14 -0800
11 1 Belkin_Pre_N_95C 00:11:50:97:90:75 NO managed 0 12 17 56 5.41KiB 2006-11-03 23:07:12 -0800
12 1 <hidden ssid> [illegible] managed 0 [illegible] [illegible] [illegible] [illegible] 2006-11-03 23:07:12 -0800
13 6 2WIRE457 00:12:88:E1:[illegible] WEP managed 0 5 5 1 [illegible] 2006-11-03 23:00:33 -0800
14 6 2WIRE204 00:12:88:01:F8:91 WEP managed 0 3 5 3 2498 2006-11-03 23:06:52 -0800
15 11 Chapman 00:16:B6:16:35:4E WEP managed 0 [illegible] [illegible] [illegible] 848 2006-11-03 23:06:46 -0800
Stop Scan