Escrito por Dr. Arroyo Sábado, 22 de Marzo de 2008 09:41 -

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  $\underline{here}$  . 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 <u>here</u>.b. Install it.

#### **Option 2 (darwinports):**

a. Download and install darwinports from <u>here</u>. It's the first link, &quot;for Tiger (Universal)&quot;.

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):** 

Escrito por Dr. Arroyo Sábado, 22 de Marzo de 2008 09:41 -

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.appb. 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:

Escrito por Dr. Arroyo Sábado, 22 de Marzo de 2008 09:41 -

Capture o Apple Airpo	Map Traffic .kismac Advanced evices rt Extreme card, passive mode		
remove Apple Airport or Airp	ort Extreme card, at 🗘 🛛 add		
Channel Hogslov Channel 7 Channel 8 Channel 7 Channel 8 Channel 3 Channel 10 Channel 4 Channel 11 Channel 5 Channel 12 Channel 5 Channel 12 Channel 5 Channel 13 Channel 13 Channel 5 Channel 13 Channel 14 Channel 13 Channel 14 Channel 13 Channel 14 Channel 14 C	bijection Infection Not Supported Dump Filter No dumping Rese everything Uptara only Weak frames only Save Dumps At -/DumpLog %9-%m-%d %		
Clobal Settings Hopping Frequency: 0.25 Enable persistent support for Greaters rebeat	Airport Extreme passive mode	A Whantemanilate	<b>Sated</b> eienithgenletweorkisjlæppearvaihlchpedktetsubteiengticædeutrædgiv
KisMAC 0.21a           # Ch Stol         850           6 Orsking         00367234           7 Ch Stol         00367234           6 Graskost         001317030           7 Ch Brekney         001217001           7 Ch Brekney         001217001           8 default         0013146A14           10 wathug         001714764           2 UC         00076A464           6 default         001217001           7 B defade stals         000762A464           9 defade stals         000742040           9 defade stals         000742047           9 defade stals         000742047           10 Hinkrys         000741000           11 Bekin, PRJC 0011150077407         00141000	Enc         Type         Signal Avg         Max         P           F0         WP         managed         16         13         19           E50         WP         managed         11         18         22           71         NO         managed         16         13         14           72         NO         managed         16         13         14           73         NO         managed         10         15         20           66         WP         managed         2         10         19           45C         WP         managed         2         2         23           905         NO         managed         2         2         395           5CO NO         managed         9         1         14	Qr Search For ?	