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, "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):

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

000	KisMAC Prefe	rences		\bigcirc																				
Scanning Filter Sound	s Driver GPS M	ap Traffic .kism	Advanced																					
	Capture devi Apple Airport	ces Extreme card, p	oassive mode																					
(remove) Apple	e Airport or Airport	Extreme card,	a(‡) (add																					
Channel Hopping		Injection		_																				
Channel 1	Channel 8 Channel 9	Dump Filter																						
Channel 3 Channel 4 Channel 5	Channel 10 Channel 11 Channel 12	No dumping Keep everything																						
Channel 6	Channel 13 Channel 14	O Data onl	ly for less ames only																					
All Start Channel:	1	Save Dumps At																						
Global Settings																								
Hopping Frequen	ncy: 0.25 s																							
Enable persist (requires reboot)	tent support for Ai	port Extreme p	assive mode																					
that the	t chiv Duti	strendes/	KisMAC		Man	ishm aniki	hte të	ated	teenit	thger	letw	eorkię	s latp	pea	rvæit	ldhp	adl	ktet	ab	terien	gtic	ande u	tæd	jive
🧤 KisMA	C 0.21a				(Q▼ Search For	?			-				-		-					-	-	_	
0 e PorkChop 1 e GrassRoots 2 e linkxys 3 e default 4 10 watchnu2 5 10 huge living 6 2 UC 5 e <hidden sido-<br="">9 e <hidden sido-<br="">9 e <hidden sido-<br="">9 e <hidden sido-<br="">13 e 2witt#204 13 e 2witt#204 14 e 2witt#204 15 11 Chapman</hidden></hidden></hidden></hidden>	00.507275.447 00.1310.301.147 00.1310.301.147 00.1310.301.147 00.1310.301.147 00.13147.401.801 00.0124.146.302 00.0124.146.302 00.0124.146.302 00.0241.002357 00.141.165.322 00.128.801.147 00.128.801.147 00.128.801.148 00.168.16.354	WEP managed 0 WEP managed 0 WEP managed C NO managed C NO managed 6 WPA managed 0 WEP managed 0 WEP managed 10 WEP managed 1 WEP managed 1 WEP managed	16 13 19 16 13 19 21 18 22 16 14 18 15 13 17 50 51 54 16 15 20 0 10 19 2 0 25 5 5 7 9 11 14 0 12 17 0 10 12 17 0 3 3	114 102 123 123 130 69 78 81 5 43 52 60 70 070 56 68 1 1 3 1 1 1 1 1 1 1 1 1 1 1 1 1	6.79Ki8 2006- 8.37Ki8 2006- 8.37Ki8 2006- 0.28Ki8 2006- 6.15Ki8 2006- 6.11Ki8 2006- 5.85Ki8 2006- 5.85Ki8 2006- 5.67Ki8 2006- 5.67Ki8 2006- 8.28 2006- 8.48 2006- 8.48 2006-	11-02 2307;14-080 11-02 2307;12-080 11-02 2307;12-080 11-02 2307;12-080 11-02 2307;12-080 11-03 2306;52-080 11-03 2306;52-080 11-03 2306;52-080																		
		٥	LL (٩		Stop Scan																		