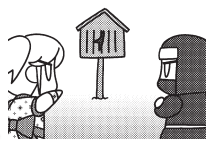
煩雑なWEP・WPA-PSKのクラック手順をGUIでわかりやすく

最強のAircrack-ngフロントエンド・Gerix



Aircrack-ngスイートを駆使できれば、WEPもWPA-PSKもクラック可能だ。でもコマンド多いしオプションも複雑で…　という人は、まずGUIフロントエンドを使ってみてはどうだろうか。

文●西方 望

●やっぱりAPクラックだよね

さて、これでOSが無線LANアダプターを認識してAPも見えるようになった。ネットにつなげるようになってめでたしめでたし…　って、本誌読者の皆さんはむろんそんな普通の使い方をしたいわけじゃないよね。BackTrackのツールを使えば各種の「普通じゃない」ことができるわけだが、なんといってもその代表格は「APのクラック」だろう。

WEPキーやWPAパスフレーズを解読できれば、他人のAPを勝手に使えてネット接続がロハ、お隣さんが見てるサイトやらメールなんかも覗ける、さらに某巨大掲示板で犯行予告をしまくっても足が付かなくてウハウハ…　と言いたいところだが、思いっきり犯罪なので絶対に他人のAPをクラックしてはいけない。実際に捕まったバカもいるし、この後解説されているようなハニーポットの可能性だってないわけじゃない。

正直、リスクに見合うリターンがある行為とは思えないので、本誌読者の皆さんは、あくまでスマートに紳士的に、管理者の許可を得た上でのテストや、自分で用意した実験環境などでの試行にとどめるようにしてほしい。

●Aircrack-ngと愉快な仲間たち

ここ最近のAPクラックツールといえば、Aircrack-ngスイートがほぼワンアンドオンリーだ（ワンといっても複数のツール群だが）。BackTrackにも他のクラックツールが収録されていないわけではないが、古いものばかり。APのクラックに限れば、他のツールにできてAircrack-ngスイートにできない、ということはほぼ皆無なので、実用性の面でも他のツールにあまり意味はない。

ただこのAircrack-ngスイート、単にコマンドラインツールというだけでなく、多くのツールを使い分けなければならない上にオプションも複雑で、少々取っつきにくい。かなり慣れていてもしょっちゅうヘルプを参照する始末だ。

そこで、この操作を楽にするために、解析作業をGUIや番号の選択などだけで簡単にできるようにしたフロントエンドが数多く存在する。Aircrack-ng公式のスクリプトであるAiroscript、中国製某アダプターで有名になったSpoonWep/Wpa、そしてここで紹介するGerixなどなど。

こういったフロントエンドを利用すれば、どこでどのツールを選ぶか、どのオプションを使うかで頭を悩ませたりいちいちヘルプを参照しなくても済むし、MACアドレスをコピペする手間からも解放される。ただ、やはり個々のコマンドを使った方が柔軟なクラックができるので、GUIに慣れたらコマンドラインの方にもトライしてみるといいだろう。

●おばあちゃんにも使えるGUI

Gerix Wifi Cracker NGは、「おばあちゃんでも使える」（その証拠（?）は脚注URLを見よ）がウリのAircrack-ng GUIフロントエンドだ。たしかに、数あるAircrack-ngフロントエンドの中でもインターフェイスのわかりやすさは一頭地を抜いてると言ってもいいだろう。とはいえ、Fake AuthだのARP request replayだのFragmentation attackだのといった用語は説明なく使われているし、具体的にどの順番で何を実行すればいいのかまでは示されていないので、ある程度の基礎知識は必要だ。

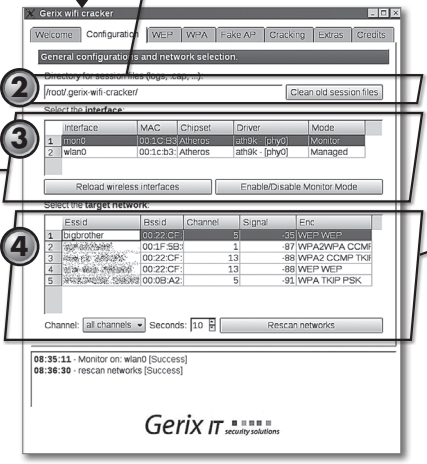
では以下でGerixを使って解析を実行してみる。操作に対応するAircrack-ngスイートのコマンドがある場合は、キャプションの後に付記しているので参考にしていただきたい。

※ http://www.crack-wifi.com/forum/viewtopic.php?id=1277

まずは使用環境を整える

起動は例によってK Menuから「Backtrack」→「Radio Network Analysis」→「80211」→「Cracking」（または「All」）→「Gerix-Wifi-Cracker-NG」だ。ネットブックの縦600の解像度でも使えないことはないのだが、実行ログが半分隠れてしまうのでできれば768は欲しいところ

「Configuration」タブで基本設定を行う。この時点ではまだ関係ないが、キャプチャーしたデータなどのファイルはこのディレクトリに保存される。Gerixで解析を行う場合、ディレクトリ内のすべてのファイルが対象となるので、効率的な解析のためには、新たにキャプチャーを開始する前に「Clean old session files」で削除するか、ファイルを別の場所に移動するか、保存ディレクトリを変更するなどした方がいいだろう



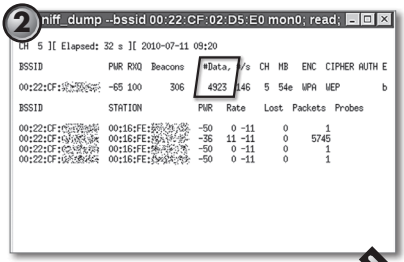
無線LANアダプターをモニターモードにする。すでにBackTrackが認識するアダプターが装着されている場合は「Select the Interface」欄に表示されているはずだ。それを選んで「Enable/Disable Monitor Mode」をクリック。Interfaceが「mon0」、Modeが「Monitor」というインターフェイスが新たに出てくるので、それを選択する（airmon-ng start <インターフェイス名>）

「Select the taget network」で攻撃対象とするAPを選ぶ。最初は何も表示されていないが「Rescan networks」をクリックすれば、周辺のAP情報を収集する。デフォルトだと全チャンネルを10秒間にわたってスキャンするようになっているが、すでにチャンネルがわかっている場合など、必要があれば左欄で変更しよう。ターゲットが表示されたらそれを選択（airodump-ng --channel <チャンネル> mon0）

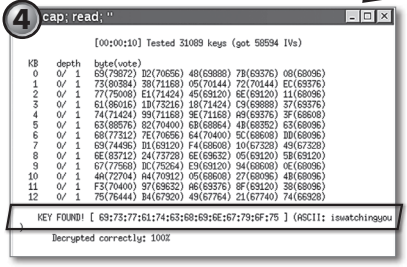
パケットを集めて WEP を解析

ここからがいよいよクラック本番。まずは基本中の基本、APにクライアントが接続していて十分な量の通信を行っているシチュエーションでの受動的解析だ。「WEP」タブに移動して「General functionalities」の項目を開き（デフォルトではこれが開いている）、「Start Sniffing and Logging」をクリックする。エラーが出る場合は、アダプターがモニターモードになっているか、Configurationタブでインターフェイスとターゲットを選んだか確認しよう

（次ページに続く）



①の画面で「#Data」の数字、すなわち解析に必要なパケットの数がある程度増えたら解析を実行する。Gerixの「Cracking」タブで「WEP cracking」の項目を開き（デフォルト）「Aircrack-ng - Decrypt WEP Password」をクリック（aircrack-ng <キャプチャーファイル名>）



すると別窓が開き、Airodump-ngが自動で実行され（Gerixを使っているぶんには、何が実行されているかを意識する必要はないが）パケットのキャプチャーがはじまる。なお、キャプチャーの停止については自動でやってくれるわけではない。解析が終了したら自分でウインドウを閉じよう。忘れるとキャプチャーファイルが際限なく大きくなるぞ（airodump-ng --bssid <APのMACアドレス> --channel <チャンネル> -w <保存ファイル名> mon0）

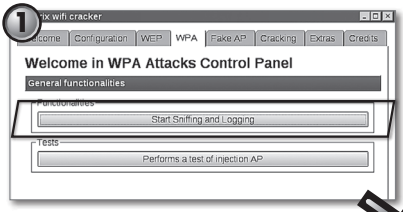
これだけで自動的にWEPの解析がはじまり、十分な「#Data」が集まれば（4万パケットで50%の確率）WEPキーを表示して終了する。なお、筆者環境では#Dataがあまり少ない状態から解析をはじめると、途中で解析の進行が止まってしまうことが何度かあったので、4万パケット程度集まってからはじめた方が無難かもしれない

ARP request replay 攻撃

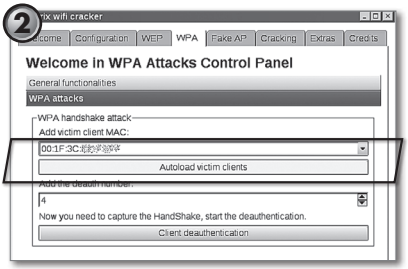
普通に傍受するだけでは十分なパケットが得られない場合に使用する能動的な攻撃も、もちろんGerixから実行可能だ。ここでは解説する紙幅がないのでARP request replay攻撃にだけ簡単に触れよう。まずは先ほどと同様、「WEP」タブの「General functionalities」の項目から「Start Sniffing and Logging」を実行してキャプチャーを開始、続いて「WEP Attacks（with client）」の項目を開く。通常は上の「ARP request replay attack」にある2つのボタンだけで用は足りるはずだ。「Assosiate with AP Using fake auth」をクリックすると、ターゲットAPとのアソシエーションを確立する（aireplay-ng -1 0 -a <APのMACアドレス> mon0）。そして「ARP request replay」をクリックすれば、クライアントのARPリクエスト送信を待って再送攻撃が自動実行される（aireplay-ng -3 -b <APのMACアドレス> mon0）。これで#Dataが増えていけば成功だ。

なお、クライアントが存在しない場合に行うFragmentation攻撃やChop-chop攻撃は、Gerixではうまくいかないことが多かった。おそらく、継続的にFake authできないので、APの認証がタイムアウトしてしまうせいだと思われる。このあたりはまだ改良の余地がありそうだ

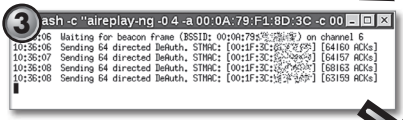
WPA-PSK パスフレーズを辞書攻撃



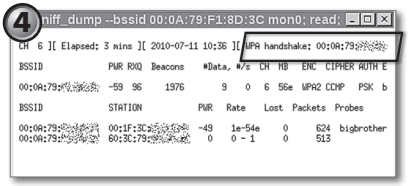
WPA自体はWEPより飛躍的に安全だが、ご家庭で使用するPSK（事前共有鍵）の場合は、認証パケットを入手するだけで、フレーズのリスト（辞書）と照らし合わせての検証ができてしまう。つまり攻撃者の持つ辞書にあるような言葉をパスフレーズとして使用するのは非常に危険といえる。Gerixでは、もちろん「WPA」タブでこの攻撃が可能だ。「General functionalities」の項目はWEPと変わらない。「Start Sniffing and Logging」でキャプチャーを開始しよう



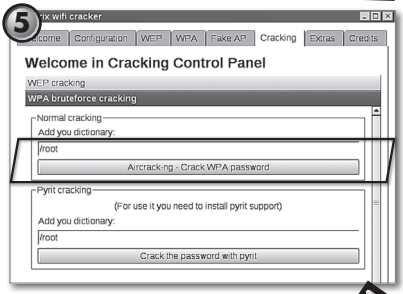
続いて「WPA attacks」の項目を開き、「WPA handshake attack」の「Add victim client MAC」に、接続を切断させるクライアントのMACアドレスを入力する。「Autoload victim clients」をクリックすれば、APと関連付けられているクライアントのMACアドレスが自動的に表示される。これで「Client deauthentication」をクリックすると、そのクライアントをAPから強制切断させる（aireplay-ng -0 4 -a <APのMACアドレス> -c <クライアントのMACアドレス> mon0）



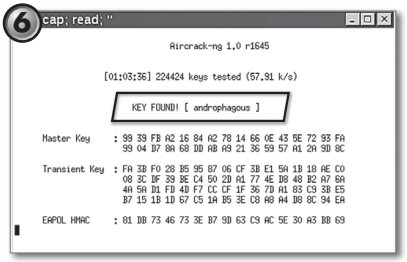
別ウインドウが開いて、強制切断が実行される。このウインドウにはこれだけで用はなくなるのだが、自動的に閉じないので自分でクローズしておこう



切断されたクライアントは、通常はAPに自動再接続をしようとするので、その際に認証パケットが飛ぶことになる。①で実行したキャプチャーウインドウ右上に、このように「WPA handshake: <MACアドレス>」と表示されれば、首尾よくその認証パケットを入手できたということだ。キャプチャーウインドウはこれで閉じてかまわない



「Cracking」タブで、今度は「WPA bruteforce cracking」の項目を開く。「Normal cracking」の「Add you dictionary」にまず辞書ファイル名をフルパスで入力（この欄にドラッグ&ドロップしただけではダメだが「file://」のスキーム部を削れば使える。このあたりも改善の余地あり）し、「Aircrack-ng - Crack WPA password」をクリックする（aircrack-ng <キャプチャーファイル名> -w <辞書ファイル名>）



また別窓で解析がはじまる。辞書の単語を次々と試していき、正解に行き当たれば解析を終了してその語が表示される。この例では1時間ちょっとで正しい語を見つけ出すことができた