WEPクラックもWPA-PSK辞書攻撃も思いのまま！

実践1

Aircrack-ngをコマンドラインで使いこなす

文●西方 望

無線LANクラック最強のツール、それがAircrack-ngだ。各種ツール群を駆使すればWEPは完全に制覇できる。でもコマンドラインはちょっと…　という人も多いだろうが、実はそれほど難しいわけではないぞ。ここでは主要ツールの基本的な使い方を解説する。

Aircrack-ngで無線LANの危険性を実感しよう

いちばん危険なパスワード

いま現在、最も現実的な脅威といえるパスワードクラックは何か、と考えると、やはり無線LANのWEPキー・WPA-PSKパスフレーズのクラック、ではないだろうか。Windowsなどのログオンパスワードクラックは、対話型ログオンなら「勝手にマシンに触れる」必要があるし、ネットワークログオンでもLAN上にいなければならない。いずれにせよクラック可能な状況自体がかなり限定される。Webなどのパスワードのオンラインクラックは、足がきわめて付きやすいのでおいそれとできることではない。

だが無線LANは違う。なにせ電波なのだから、傍受可能な範囲にさえ入ればいいのだし、少なくとも受動的な解析を行うぶんには絶対に相手に気づかれない。いったんクラックされればLAN内に侵入されてしまうわけで、ログオンパスワードクラックや保存されたパスワードの解析などがここで現実の脅威となる。ARPスプーフィングなどの手間を掛けずともスニッフィングも楽勝。

もちろん脅威はLAN内だけに留まらず、クラックされたアクセスポイント（AP）を踏み台にして外部サイトへの各種攻撃をされ、濡れ衣を着せられることもあり得る。ひとたびパスワードが破られて侵入されれば、たいへんな事態が待っているかもしれないのだ。

もう口が酸っぱくなってますが

しかるに、全くの無防備状態で無線LANを気軽に使っている人が多すぎる。WEPでは無防備とほとんど変わらない、いや、防備してると思い込んでるぶん余計タチが悪い。今まではたまたまクラックされていなかっただけで、自分がどれだけ薄氷を踏んでいるのか、いい加減みんな知ってほしい。ああ、実はとっくにクラックされて毎日侵入されてるけど、単にそれに気づいてないだけ、ってこともあるかもね。

過去HackerJapan本誌やムックなどで何度も何度も何度も言ってきたが、お願いだからWEPは止めてくれ。まだWEPの危険性が実感できていない人は、ぜひこの機会にAircrack-ngを使ってWEPを解析してみよう（もちろん、自分の管理するAPに限るぞ）。本当にWEPは役に立たないとわかるはずだ。

もちろんWPA-PSKも弱いフレーズなら解析可能。これまた実際にやってみれば、長くて複雑なパスワードの重要性が理解できるだろう。

Aircrack-ngをコマンドラインで使う

ただ、Aircrack-ngはコマンドラインツールのうえオプションが多く、さらに複数のツールを使い分けたり同時に使ったりといったテクニックが必要となるため、なかなか使いこなせない、という人もいるだろう。そういった場合は、Aircrack-ngを使いやすくするGUIフロントエンドを利用するのも1つの手だ。今回もp236よりAircrack-ngをGUIで使うツールを紹介している。

しかし、やはり柔軟に解析を行うにはコマンドラインがいちばんだ。それに、よくよく見ればそれほど複雑なものではないし、ヘルプもある…　ていうか、私もさんざ使ってるけどいまだにしょっちゅうヘルプ見る（笑）。とりあえず、「Aircrack-ng」「Airodump-ng」「Aireplay-ng」の3つをどういう場面で使うか、がわかっていれば、あとはヘルプ頼みでも結構なんとかなるものだ。いやホント。

それでは実際にAircrack-ngを使ってみよう。解析手法などにはいろいろあるが、今回は紙幅も限られているので、以下の3つの概要を解説する。

・通信量が多い状態での受動的 WEP 解析
・通信量が少ない状態での ARPreplay 攻撃
・WPA-PSK 認証パケット取得・辞書攻撃

この他の攻撃や、より詳しい操作などを知りたいのであれば、ぜひ「無線 LAN セキュリティの教科書 2009-2010 年版」を読んでほしい。

どの攻撃にも共通する手順

start-networkはしなくてOK

Aircrack-ng は当然ながら BackTrack4 に含まれているので、今回はこれを使った方法を解説する…といっても別に他のディストリビューションで動かすのと特に変わるわけではないが。Aireplay-ng で使える無線 LAN アダプターについては今回は割愛する。ノートやネットブックなどで BackTrack4 を起動してみて、実際に動くかどうか確かめるのがいちばんの早道だ。

では BackTrack4 を起動… おっと待った、p17 で「start-network しないとネットワークが使えない」という解説があったが、Aircrack-ng を使う上では start-network の必要はない。というかむしろしない方がいい。せっかく無線 LAN アダプターを使う他のプログラムがない状態なのだ、わざわざ動かす必要はあるまい。おそらく BackTrack4 では、こういったネットワークアダプターを直接使うツールのためにネットワークが無効にされているのだろう。ということで、すでにネットワークを有効にしたとか /root/.bash_profile に「start-network」入れたとかいう人は、「stop-network」を実行してネットワークを止めておこう。

メニューからでなくKonsoleで

Aircrack-ng ツール群は、メニューの「Backtrack」→「Radio Network Analysys」→「802.11」→「Cracking」から呼び出せるが、他のコマンドラインツールと同様、何のオプションも付けずに実行されるので、単にヘルプが出るだけ。最初から Konsole（ターミナル）を開いた方がいい。

モニターモードへ移行→収集開始

最初に、無線 LAN アダプターを周りの通信が傍受できる「モニターモード」にする必要がある。これで無線 LAN パケットが収集できるようになるわけだ。モニターモードにすると「mon0」というデバイスが作成されるので、以下はその mon0 デバイスに対してツールから操作を行うことになる。

続いては、当然ながらパケットの収集をする必要がある。そのために使用するのが Airodump-ng だ。

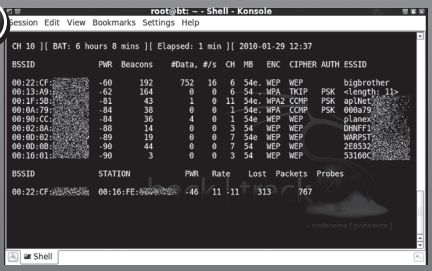
Airmon-ngによるモニターモードへの移行

```
eth0      no wireless extensions.

wmaster0  no wireless extensions.

wlan0     IEEE 802.11bg  ESSID:""
          Mode:Managed  Frequency:2.437 GHz  Access Point: Not-Associated
          Tx-Power=27 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@bt:~# airmon-ng start wlan0

Interface       Chipset         Driver

wlan0           Atheros         ath5k - [phy0]
                                (monitor mode enabled on mon0)

root@bt:~#
```

メニューにはAircrack-ngをはじめ各ツールへのリンクがあるが、選んでもヘルプが出るだけなのであまり意味はない。メニューバーのアイコンをクリックしてKonsoleを開こう。「airmon-ng start wlan0」で無線LANアダプターがモニターモードになる。「wlan0」の部分は無線LANアダプターを示すデバイス名だ。ほとんどの環境ではwlan0だと思うが、あらかじめ「iwconfig」コマンドで確認しておこう。無事モニターモードになると図のように「(monitor mode enabled on mon0)」と表示される。「mon0」というデバイスが作成された、という内容だ

Airodump-ng によるパケット収集の開始

①



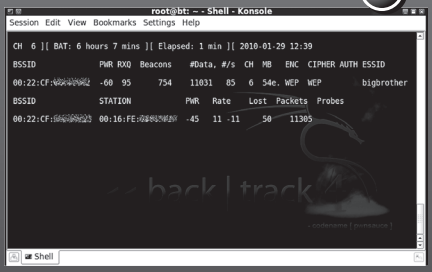
「airodump-ng mon0」と実行すると、この図のように受信範囲にあるAPがすべて表示される。ESSIDなどを見て、解析対象のAPがわかったら[Ctrl]＋[C]でAirodump-ngの動作を停止。「BSSID」の項目に表示されているMACアドレス（コロンで区切られた12桁の数字）は、この後のコマンドで入力する必要があるので、ドラッグして右クリック→「Copy」をしておこう

解析対象とするAPのパケットのみを拾うために、以下のようにチャンネルとBSSIDを指定してAirodump-ngを再実行する

airodump-ng --channel［APのチャンネル］--bssid［APのMACアドレス］-w［ファイル名のプレフィックス］mon0

この図の例では、「test-01.cap」というキャプチャーファイル（ディレクトリに同じファイル名があればtest-02.cap）が作成される

②



受動的WEP解析

相手には気づかれない解析

ここからは受動的なWEP解析、つまりこちらからはいっさいAPに対して手を出さず、飛んでいるパケットを拾うだけでWEPをクラックする手法を解説する。この解析を行うには多量のパケットを集めなければならないので、APにクライアントが接続しており、AP経由である程度の量の通信を行っているという条件が必要だ。

攻撃者の立場からすれば、いちばん安全なこの手でクラックできるのが望ましい。攻撃対象者がAP経由でネットからファイルをダウンロードしてるとか、YouTubeとかニコニコとかで動画見てるとか、今どきは多量のパケットが飛ぶ機会はそう珍しいことではあるまい。しかも単に受信するだけなので、他のことでヘマ（ノートPC持ってうろついてるのを見られるとか）をしないかぎりは相手には絶対気づかれない…だからといって実際に他人のAPに対してやってはいけないぞ、絶対。

つまりこの攻撃が防げないかぎり、無線LANは常に大きな危険にさらされていることになる。まあ、WEP使って通信してるのであればどうしたって防ぎようがないので、a. WEPを止める　b. APを窓から投げ捨てる　以外に選択肢はないんだけどね。

パケット収集しつつAircrack-ngを起動

今回は、PSPから無線LAN AP経由でLocation Freeサーバーにアクセスし、動画を視聴しているところを傍受・クラックしてみた。トラフィックはおおむね180～250KBps程度、つまり2Mbps以下。今どきはごく普通にある通信量だ。

Airodump-ngで「#Data」と表示されている部分が解析に必要なパケットの数だ。だいたい4万あれば50%の確率でWEPキーが解析できるが、4万溜まるのを待つ必要はない。もう1つKonsole

Aircrack-ngでWEPをクラック！

```
                    [00:04:46] Tested 227697 keys (got 45000 IVs)

  KB    depth   byte(vote)
   0    0/  1   69(58112) FF(56064) 59(55040) B7(55040) F1(53760) 15(53248)
   1    0/  3   73(57344) E6(57088) A8(55552) EF(54016) 99(52992) 6C(52480)
   2    0/  1   77(56064) 48(52992) C7(52736) 9A(52480) 41(52224) F1(51968)
   3    0/  1   61(57344) BC(55296) A9(54528) ED(53504) 74(52992) 0C(52736)
   4    0/  1   74(69632) ED(55296) AC(54784) 12(54272) 97(53504) 33(52992)
   5    0/  1   63(58112) 93(54016) F5(52736) 9C(52480) 9B(51968) 5F(51456)
   6    0/  1   68(56064) 49(53760) FD(53760) 9B(52736) 31(52224) 65(52224)
   7    0/  1   69(60672) 89(53248) F4(53248) B9(52992) 04(52480) D9(51712)
   8    0/  2   7D(56064) CA(54272) 35(53760) 74(52480) 76(51968) 8F(51968)
   9    0/  1   67(57088) E0(54784) D7(52736) 4B(52480) 2F(51712) 11(51456)
  10    0/  1   9A(55296) 4B(54528) A4(53760) 05(52992) AD(52992) 4F(52480)
  11    0/  1   89(53504) 26(53248) 9B(53248) FA(53248) 66(52992) 2C(52480)
  12    0/  1   75(58232) BC(53668) 29(52952) 8F(52616) 2D(52028) A9(51692)

    KEY FOUND! [ 69:73:77:61:74:63:68:69:6E:67:79:6F:75 ] (ASCII: iswatchingyou )
        Decrypted correctly: 100%

root@bt:~#
```

Airodump-ngで#Dataが収集できているようなら、Aircrack-ngを立ち上げる。Airodump-ngで指定したプレフィックスに「-01.cap」を付けたファイル名をオプションとして、

aircrack-ng test-01.cap

のように実行しよう。ファイルに複数のAPのパケットが含まれる場合は選択が必要だが、今回は1つのAPからしか採取していないので、すぐに解析に入る。当初はパケット数が不足でも、5000パケットごとに自動的に再解析がはじまり、最終的にはこのようにWEPキーが明らかになってしまう

を開いて、そちらでAircrack-ngを実行しよう。パケットが不足でも溜まったら自動的に再解析を行ってくれる。

パケットさえ集まれば100％解析可能

いかがだろう？　たった2つのツール（Airmon-ng入れれば3つだけど）で、さほど難しいオプションも使わずにWEPクラックができるのだ。今までコマンドラインだからと敬遠していた方でも「自分にもできる！」と思っていただけたのではないだろうか。

ともあれ、単にパケットを受信しているだけでWEPキーがあっさりと判明してしまった。今回の解析に要した時間はわずか7分。この章のタイトルの「10分クラック」はなんとかキープできました（笑）。

というか、受動的解析の所要時間は、単に時間あたりどれだけパケットをキャプチャーできるか、にかかっている。もっとパケットが少なければ数時間とか数日かかることもあるし、多数のパケットが飛んでいれば数十秒ですむこともある。ちなみに筆者の実験環境での最短記録はたしか25秒ほど。別に記録を目指してたわけじゃないんで、正確には覚えてないが。

いずれにせよ、2Mbps程度の通信量で7分（実際にはデータ量よりパケット数が問題だが）。今主流の802.11gやnで、その帯域が活きるほどの通信を行っていれば、せいぜい1分かそこらでクラックされてしまうわけだ。WEPがいかに役に立たないか、ご理解いただけたことと思う。

能動的WEP解析ーARPreplay攻撃

通信量が少ないAPを解析するには

このようにWEPは簡単に解析できるが、上記のようにそのキモは「解析に使えるパケットをどれだけ多く集められるか」だ。ファイル共有ソフトを使っているとか、いつも多量のパケットが飛んでるような相手なら何の苦労もない。しかし、たいていはちょっとWebやメールを見る程度にしか使ってない、というテキだと面倒だ。

もちろん、通信量が少なくても粘ればいつかは必要な数のパケットが集まる（その間WEPキーが変更されなければ）が、自宅で受信できるAPをクラックするならともかく、離れた場所のターゲットを狙う場合、相手の家の周りを毎日うろついてパケットを蓄積するというわけにもいくまい…　いや、もちろん悪意ある攻撃者の立場では、という意味であって、近所だろうと何だろうと実際にクラックしてはダメだが。

APを突いてパケットを出す

そんなときに使う手法の1つがARPreplay攻撃だ。こちらから特定のパケットを多数APに送りつけ、それに対してAPが返答してくるパケットを収集する。だがもちろん、APにちょっかいを出しているわけだから、攻撃相手に気がつかれる可能性はある（自分は使ってないのにAPのランプが激しく明滅するなど）し、APのログにも残る。しかし、これを使えば確実

に短時間でクラックが可能だ。

ただし無条件でできるわけではない。別に通信を行っている必要はないのだが、少なくとも 1 台は AP に接続しているクライアントがいなければならない。全く接続がなく単に AP が起動しているだけ、という状況では、他の攻撃手法を使う必要がある。今回はそちらについては割愛するが、「無線 LAN セキュリティの教科書 2009-2010 年版」では詳しく解説しているので、興味のある方は参照していただきたい。

正規のパケットを傍受して再送

AP にパケットを送って返答パケットを得る、といっても、もちろん AP に送りつけるパケットはなんでもいいわけではない。そんな何にでもホイホイ返事してくれるならこちらも苦労せんわ（笑）。必要なのは「ARP 要求」と呼ばれるパケットだ。

紙幅の都合もあり今回は ARP 要求自体について解説はしない（p206 からの Cain & Abel のところで少し触れられている）が、要は PC が接続先を探す際に発行するパケット。これを何度も再送（replay）するので ARPreplay 攻撃と呼ばれるのだ。これに対する AP からの応答パケットを収集することになる。

しかし再送するためには、そもそもまず ARP 要求パケットを入手しなければならない。そのために、AP に接続しているクライアントが必要となる。正規のクライアントが発行した ARP 要求パケットを傍受すればよい、というわけだ。

APの認証を突破する

ただし、AP にとって見も知らぬ攻撃者 PC が ARP 要求を送ったところで、AP は応答してくれない。そんな誰にでもホイホイ返事してくれるなら（略）

まずは AP との「アソシエーション」を確立しなければならない。アソシエーションというのは、「自分の管轄下にこのステーションが入ったよ」と AP が認識することだ。もちろんこの時点では AP に登録されたというだけの話で、WEP キーを知らなければその後実際に通信を行うことはできない。

アソシエーションを確立するためには、まず AP の「認証」を受ける必要がある。認証の方式には「オープンシステム認証」「共有鍵認証」の 2 種類があるが、今回はオープンシステム認証の場合のみを解説する。共有鍵認証の突破について知りたい方は、先ほども紹介した「無線 LAN セキュリティの教科書」を見ていただきたい。

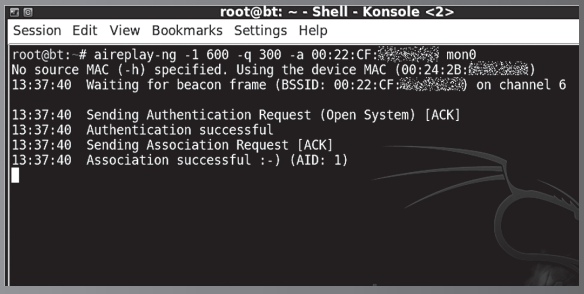
偽装認証の実行

だが、認証といっても実はオープンシステム認証は「誰でも OK」という、「オープンにも程があるだろ」と言いたくなる方式だ（笑）。そのため、コマンド一発でアソシエーションを確立できる。

認証を受ける場合であれ ARPreplay 攻撃の場合であれ、こちらから何かを送り出す、という際に登場するツールが「Aireplay-ng」だ。ではさっそく Aireplay-ng を使って AP の認証を受けてみよう。

おっとその前に、受動的攻撃の時と同様 Airmon-ng でモニターモードにし（まだなっていない場合）、Airodump-ng でパケット収集を開始しておこう。そして別 Konsole を開いて Aireplay-ng を実行だ。

Aireplay-ngで偽装認証を実行



APの認証を受けてアソシエーションを確立するには、

aireplay-ng -1［認証を受ける間隔（秒）］-q［Keep Aliveを送る間隔（秒）］-a［APのMACアドレス］mon0

と実行する。図のように「Association successful:-)」と表示されれば成功だ。失敗する場合の原因としては、無線LANアダプターがインジェクションに対応していない、パラメーターを間違えている、APが共有鍵認証、などが考えられる

ARPパケット待ちぼうけ

アソシエーションの確立に成功すれば準備完了。後は接続している正規のクライアントがARPパケットを送るのを待つだけだ…　といっても、そう都合よくパケットが飛んでくるとは限らない。ターゲットがPC点けっぱなしで風呂にでも入ってるとか、寝落ちしてるとかならいつ飛ぶことやら。まあ、今どきはNTPクライアントやらアンチウイルスやら、勝手にネットに接続するソフトが動いていることが多いので、PCが起動さえしていれば（それがこの攻撃の前提）おそらくそれほど待つ必要はないとは思われる。

だが待つのはヤダ、すぐARPパケット入手したい、というせっかちなアナタ。その方法ももちろんある。だがその手法は次のWPA-PSK攻撃のところで解説するので、しばし待たれよ。え？　待つのヤダ？（笑）

ARP要求さえ来れば終了

ともあれ、ARPreplay攻撃の準備はしておこう。これでARPパケットが飛んでくれば、自動的に再送攻撃が始まる。もちろん受動的解析と同様に、Aircrack-ngも立ち上げておけばこちらも自動的に再解析してくれるので、待つといっても放置しておけばよい。

いったんARPパケットが来たなら、あとは下のカコミのように楽勝だ。今回のテスト環境では、5分かからずにクラックできた。章のタイトルは「5分クラック」にしとけばよかったかなあ（笑）。

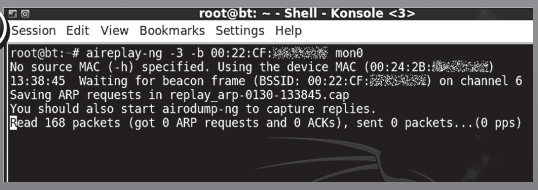
WEPは本当に役に立たない

ということで、WEPの無能っぷりについてはわかっていただけただろうか。この他にAPに誰も接続していない場合の攻撃もあるが、そういった能動的攻撃まで考えずとも、そもそも通信をするために無線LANを導入しているのだから、WEPを使っているかぎりは常に受動的攻撃の脅威があるのだ。

WEPはもう絶対に使わないでほしい。

Aireplay-ngでARPreplay攻撃を開始

①

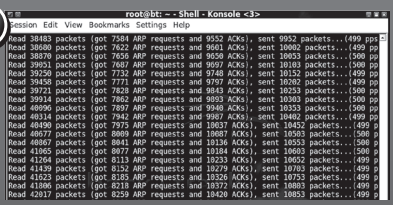


Konsoleをさらにもう1つ立ち上げて、以下のように実行しよう。

aireplay-ng -3 -b［APのMACアドレス］mon0

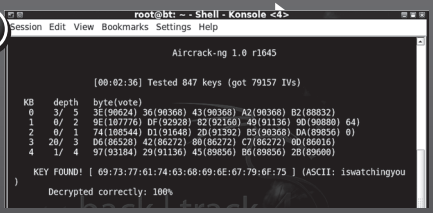
当初はこのように「got 0 ARP request」「sent 0 packets」つまりARPパケットを入手できてないので送り出せない、と表示されるだろう

②



いったん正規クライアントがARPを送信すれば、今度はこのようにパケットを送ったという表示がずらずらと出てくることになる。そしてAirodump-ngの方を見れば#Dataが景気よく増えているはずだ

③



あとは受動的解析の時と同様にもう1つKonsoleを開いて（つまり4枚目）Aircrack-ngを実行しよう。十分な数のパケットが集まれば、ほれこのとおり

WPA-PSKパスフレーズ解析

本当は怖いWPA-PSK

で、だ。「WEPを使うな!」ということになれば、選択肢は当然WPA/WPA2 TKIPかAES以外にない。TKIPはWEPの改良版であるものの、現在でもまだ完全には破られていない。とはいえ危険性をはらんでいるのは間違いないので、できればAESにした方がよい。p227の解説にも書かれているとおり、やむを得ずTKIPを使う場合は、パスフレーズの管理など運用には特に気をつけよう。

もちろん「パスフレーズの管理」はAESの場合でも非常に重要だ。そう、TKIPだろうとAESだろうと、ご家庭レベルで使用するPSK、つまり事前共有鍵方式の場合（ご家庭でもEAPを構築できないことはないが）、短いパスフレーズなら容易に解析されてしまうのだ。

たった4つのパケットで

しかもこの攻撃は、たった4つのパケット（4ウェイハンドシェイク）を傍受するだけでよい。WEPは4万パケットあれば50%の確率でクラックできる、と先ほど書いたが、こちらは4万ちゃいまっせ、「4」でっせ。

これは、p195の解説で触れられている、チャレンジレスポンス認証に対する攻撃と同じことだ。APから送られてきたメッセージとクライアントからのレスポンスが傍受できれば、アルゴリズムはわかっているわけだから、こちらが用意したフレーズに基づきメッセージを計算、同じレスポンスが出現するまでフレーズを変えて試行を繰り返せばよい。つまり辞書攻撃。

さらに、いったんこの4つのパケットさえ入手してしまえば、あとは好きな場所で好きなだけ時間をかけて解析できる。悪意あるクラッカーの立場で言えば、ターゲットに近づく必要があるのは4ウェイハンドシェイクをキャプチャーする時だけで、後は何の危険性もなくクラックに励めるというわけだ。

さらにしんどい待ちぼうけ

ただ、認証パケットさえ手に入れば、と言うのは簡単だが、実際これをどうやって入手するか。要するにクライアントがAPに接続する際に飛ぶパケットだから、その瞬間に傍受していなければならない。これは以外と高いハードルだ。

…いやもちろん皆さんは自分の管理する実験環境で試しているはずだから（だよね？）、他のクライアントを好き自由に接続させればいいのだが、実際の攻撃者を想定した場合、どういう行動を取るのだろう？

ターゲット宅門前の電柱の影で、ひたすら認証パケットが飛ぶのを待つしかないのか？

ARPreplay攻撃の際のARP要求は、接続されているクライアントがいればおそらくそれほど待たずに入手可能だ。だがWPA-PSKの認証は、新しいクライアントが接続するか、接続済みクライアントの再認証が行われるのを待たなければならないので、はっきり言っていつになるかわからない。

誰かが電子レンジでも使って接続済みクライアントが切断されれば、自動再接続機能がある場合再認証が行われる。そうだ、こちらから2.4GHzマイクロ波を照射して切ってやればいいのだ！（笑）…そんな間抜けなことするわけねえだろ。Aircrack-ngはちゃんと考えられてる。角度とか（古い）。

無理矢理再認証させる

そう、Aircrack-ngというかAireplay-ngには、こちらからパケットを送って現在接続しているクライアントを強制的に切断する機能があるのだ。これを使えば、接続済みクライアントがいるかぎり認証パケットの入手は思いのまま。

ただしもちろん、相手に気づかれるリスクもある。ストリーミング動画を視聴していたりする場合、一瞬固まったり、場合によっては切断されてしまう、ということもあるので、できるだけ通信量が少ない時を狙った方が…　いや、悪人の立場ではね。

また、再接続の際にARP要求が出る可能性は高いので、WEP解析のARPreplay攻撃でもこの認証切断攻撃は役に立つ。そう、先ほど言った「すぐARPパケットを入手する方法」というのがこれだ。

話を元に戻して、ではWPA-PSKパスフレーズのクラックを実際にやってみよう。

辞書攻撃によるWPA-PSKパスフレーズ解析

①
```
root@bt:~# aireplay-ng -0 1 -a 00:22:CF:[redacted] -c 00:16:FE:[redacted] mon0
14:57:05  Waiting for beacon frame (BSSID: 00:22:CF:[redacted]) on channel 6
14:57:05  Sending 64 directed DeAuth. STMAC: [00:16:FE:[redacted]] [80|76 ACKs]
root@bt:~#
```

例によってAirodump-ngでパケット収集を開始した後、別Konsoleで以下のように認証切断攻撃を実行。

aireplay-ng -0 1 -a [APのMACアドレス] -c [クライアントのMACアドレス] mon0

これでクライアントがAPから切断される

②
```
7 mins ][ Elapsed: 44 s ][ 2010-01-30 14:57 ][ WPA handshake: 00:22:CF:

 RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

  44      379     4527  114   6  54e. WPA  CCMP   PSK  bigbrother

TION            PWR   Rate    Lost  Packets  Probes
```

Windowsなどが自動再接続したり、ユーザーが切断に気づいて再接続した場合、クライアントとAPの間で認証パケットが飛ぶことになる。これをキャプチャーできていれば、Airodump-ngでこのように「WPA handshake:[APのMACアドレス]」と表示される。こうなったらAirodump-ngは止めてもよい

③
```
[00:00:38] 6728 keys tested (170.74 k/s)

Current passphrase: 0472376796

Master Key     : 2D 6A C9 21 B2 57 15 7C 1C D2 4E 57 81 5E 25 3A
                 C1 5E A8 2C 67 1B BB 1D 63 CC 89 FE FA 05 45 2E

Transient Key  : 18 72 31 7C 1E 29 DA FC D4 1C 28 EB 64 B4 7A D5
                 0C 32 F1 9D 1D 27 D8 5A D0 73 E2 C3 DA EB B7 87
                 71 AE 70 9A AE CD 60 E1 68 E5 8D D7 F0 D3 76 8C
                 20 28 96 CF FD F6 27 ED B2 BE B5 85 BC 3E 07 0B

EAPOL HMAC     : 8C 34 9E 4A C0 E0 D8 3F 40 B4 99 45 63 94 F9 C3
```

あとはAircrack-ngを、キャプチャーファイル名と「-w」オプションで辞書ファイル名を指定して実行するだけだ。他の辞書攻撃同様、辞書の精度が勝負の分かれ目。ひたすら辞書のフレーズを試していく

④
```
[00:51:38] 224460 keys tested (55.01 k/s))

KEY FOUND! [ androphagous ]

Master Key     : F0 28 C6 0C 1A B4 85 D0 0B F7 E0 E3 87 40 6E 9C
                 AC 0E 33 1E DB 0C B8 24 B3 1E 1E 11 A7 C0 20 AA

Transient Key  : F4 3E 97 93 00 BD 43 4B 42 C7 A4 5C 97 82 E0 4B
                 A6 B1 43 F8 CD 8B 58 CC 9E D1 E5 F6 CF 4C B3 51
                 D1 CB 83 68 45 A7 B6 F4 10 D9 0D 6E D1 D8 E1 57
                 58 24 8E 0B E8 0E 8A 22 9B F2 7F 7C 37 05 EC 65

EAPOL HMAC     : AD C8 01 A5 B3 B6 74 16 79 52 96 BF D1 D4 59 93
t@bt:~#
```

辞書にマッチする語が見つかればこのとおり。今回はネットブックでしかもバッテリー駆動のため、20数万語ほどの検索に50分以上もかかっているが、解析には無線LANアダプターなどは無関係なので、高速なデスクトップ機で実行した方がよいだろう

まとめ

このように Aircrack-ng を使えば、WEP は全くお話にならないこと、そして WPA-PSK でも解析辞書に含まれる程度のフレーズでは簡単に破られてしまうことが、きっとおわかりいただけると思う。ぜひ自分で試してみて実感し、周りにまだ WEP を使ってるような人がいれば啓蒙してほしい。

ただし、もう一度念を押すが、許可を受けていない AP のクラックは違法だ。絶対にやってはいけない。