Набор инструментов для аудита беспроводных сетей AirCrack

Агафонова Оксана

12 мая 2015 г.

Содержание

1 Взлом WPA2 PSK сети **3**
1.1 Установка 3
1.2 Находим точку доступа 3
1.3 Сбор данных 3
1.4 Словарная атака 4

2 Взлом WEP сети **5**
2.1 Запуск беспроводного интерфейса в режиме мониторинга . 5
2.2 Начало. Сбор хэндшейков 5
2.3 Aircrack-ng - взлом предварительного ключа 6

1 Взлом WPA2 PSK сети

Один из лучших инструментов для мониторинга траффика и взлома ключей WEP/WPA-PSK это набор утилит aircrack-ng.

Будут использованы следующие утилиты:

`airmon-ng` – переводит адаптер в режим мониторинга
`airodump-ng` – для WLAN мониторинга и перехвата пакетов
`aireplay-ng` – генерит дополнительный траффик в беспроводной сети
`aircrack-ng` – используется для восстановления ключа WEP или словарной атаки на WPA-PSK.

1.1 Установка

Чтобы захватывать траффик сети, не ассоциируясь с точкой доступа нужно установить беспроводную сетевую карту в режим мониторинга. Чтобы это сделать, в консоле вводится под рутом:

`iwconfig` - отображение всех беспроводных интерфейсов
`airmon-ng start wlan0` - перевод интерфейса в режим мониторинга

1.2 Находим точку доступа

Этот шаг предполагает, что сетевой интерфейс переведен в режим мониторинга. Следующий шаг – это найти доступные беспроводные сети и выбрать цель:

`airodump-ng mon0` – просматривает все каналы, перечисляя доступные точки доступа.

Лучше выбрать точку с сильным сигналом (колонка PWR), большим количеством траффика (колонки Beacons/Data). Выбрав цель, можно записать его канал и BSSID (мак адрес).

1.3 Сбор данных

Для этого понадобится airodump-ng с некоторыми дополнительными параметрами. Лучше сузить мониторинг до одного канала, чтобы уско-

рить процесс. Предполагая что адаптер называется mon0, мы, к примеру, захватываем пакеты с шестого канала в файл data:

```
airodump-ng -c 6 bssid 00:0F:CC:7D:5A:74 -w data mon0
```

-c 6 – ловятся пакеты с 6 канала,
bssid 00:0F:CC:7D:5A:74 – мак-адрес целевой точки доступа

В качестве выходного файла необходимо использовать именно cap-файл, а не ivs. Поэтому в настройке airodump на вопрос «Only write WEP IVs (y/n)» отвечаем нет.

Также для расшифровки WPA ключа, вам будет нужно захватить процедуру инициализации клиента в сети. Для этого под Линуксом можно провести атаку, которая заставит провести процедуру переинициализации клиентов сети, хотя можно подождать, пока клиент сам это сделает.

Это можно сделать следующей командой:

```
aireplay-ng -deauth 3 -a MAC_IP -c MAC_Client mon0
```

где MAC-IP это мак-адрес точки доступа, MAC-Client- мак адрес клиента, mon0 – беспроводной NIC).

Так как для вычисления секретного ключа используются только пакеты, передаваемые между точкой доступа и клиентом во время инициализации, накапливать пакеты не нужно.

1.4 Словарная атака

Сначала необходимо скачать словарь в директорию с программой aircrack. Словари можно найти по адрес: http://ftp.se.kde.org/pub/security/tools/net/Openwal

Теперь из консоли запускаем aircrack-ng:

```
aircrack-ng -w wordlist capture_file
```

wordlist – словарь, capture-file – файл с данными, с расширением cap

Перебор ключей занимает довольно долгое время, но если пароль простой, он может подобраться за несколько минут.

Таким образом, можно сделать вывод: если вы хотите обезопасить свою беспроводную сеть, выбирайте сложный и длинный пароль. Подбор такого пароля будет очень долгий по времени. Мало у кого на это хватит терпения.

2 Взлом WEP сети

2.1 Запуск беспроводного интерфейса в режиме мониторинга

Цель этого шага в том, чтобы запустить вашу wi-fi карту в так называемом режиме мониторинга. Данный режим позволяет вам «слушать» все пакеты, т. е. Не только те которые адресованы вашей карте.

Теперь введем следующую команду, чтобы переключить беспроводную карту на канал 9 в режиме мониторинга:

```
airmon-ng start wifi0 9
```

2.2 Начало. Сбор хэндшейков

Целью этого шага является сбор т. н. рукопожатий.

Выполняем:

```
airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w psk ath0
```

Где:
-c 9 является каналом для беспроводной сети
- BSSID 00:14:6 C: 7E : 40:80 является MAC адресом точки доступа
-w psk является префиксом имени файла вывода
ath0 является именем нашего интерфейса

Данный шаг может затянуться, и придется ждать пока кто-то из клиентов не подключится к точке доступа. Но это не проблема.

На основании вывода Airodump-ng в предыдущем шаге, удалось определить клиента, который в данный момент подключен. Нам понадобится его MAC-адрес.

Открываем другой сеанс консоли и вводим:

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0
```

Где:

-0 средство деаутентификации
1 число деаутентификаций для отправки (можно отправить несколько)
-a 00:14:6C:7E:40:80 MAC-адрес точки доступа
-c 00:0F:B5:FD:FB:C2 MAC-адрес клиента которого обнаружили
ath0 имя интерфейса

Вот как будет выглядеть результат команды:

```
11:09:28 Sending DeAuth to station -- STMAC: [00:0F:B5:34:30:30]
```

2.3 Aircrack-ng - взлом предварительного ключа

На данном этапе надо взломать предварительный ключ WPA/WPA2. Чтобы сделать это, понадобиться словарь слов в качестве входных данных.

Существует небольшой словарь, который поставляется с aircrack-ng - “password.lst”. Будем использовать его.

Открываем другой сеанс консоли и вводим:

```
aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap
```

Где:
-w password.lst это имя файла словаря
*.cap название группы файлов, содержащих перехваченные пакеты . В данном случае используется специальный символ *, чтобы включить несколько файлов.

Если хэндшейк будет найден, то Aircrack-ng начнет пытаться взломать предварительный ключ.