Л13. Тестирование беспроводных сетей на проникновение в Kali Linux

Беспроводные сети вездесущи. Они могут быть развернуты и работать в различных средах: коммерческих, правительственных, образовательных, а также в обычных жилых домах. В результате испытатели на проникновение должны гарантировать, что эти сети имеют необходимое количество элементов управления безопасностью и в их конфигурации отсутствуют ошибки.

В этой главе мы обсудим следующие темы.

- **Беспроводная сеть.** Разберем базовые протоколы и конфигурацию, определяющие, как клиенты (ноутбуки и планшеты) аутентифицируются и взаимодействуют с точками доступа беспроводной сети.
- **Разведка.** Как и для тестирования на проникновение проводного соединения, в Kali Linux вы найдете множество инструментов, которые можно использовать для определения потенциальных целевых сетей, а также для сбора разных сведений о конфигурации, которые можно использовать во время атаки.
- **Атака на аутентификацию.** В отличие от попыток скомпрометировать удаленный сервер атаки, которые мы будем обсуждать, предназначены для аутентифицированного доступа к беспроводной сети. После проверки подлинности мы можем подключить, а затем привести в действие инструменты, которые рассмотрели ранее.
- **Действия после аутентификации.** Здесь мы обсудим действия, которые могут быть предприняты после взлома механизма защиты от несанкционированного доступа. К ним относятся атаки на точки доступа и способы обхода общего контроля безопасности, реализованного в беспроводных сетях. Кроме того, рассматриваются перехват и анализ («обнюхивание») трафика беспроводной сети, которые позволяют предоставить доступ к учетным данным или другой информации.

Испытателю необходимо иметь четкое понимание механизма тестирования на проникновение в беспроводную сеть. Технология беспроводной передачи сигнала быстро принимает концепцию Интернета вещей (Internet of Things, IoT), на которую переходят все больше и больше устройств, повышающих наш комфорт пребывания в Интернете. Удобству использования и комфорту особенно способствуют беспроводные сети.

В результате количество беспроводных сетей, как и количество объектов для атак будет только увеличиваться. Клиенты и организации должны понимать все риски использования беспроводных сетей и знать, как злоумышленники атакуют эти системы.

Технические требования

В этой главе нам потребуются два разных USB-устройства. Первое — это USB-адаптер TP-LINK TL-WN722N Wireless N150 с большим коэффициентом усиления, а второе — USB-адаптер Alfa AWUSO36NH с большим коэффициентом усиления. Оба устройства доступны в продаже. Дополнительные сведения вы можете найти в Интернете, перейдя по адресу http://aircrack-ng.org/.

Беспроводная сеть

Беспроводная сеть управляется протоколами и конфигурациями так же, как и проводная. Беспроводные сети для передачи данных между точкой доступа и подключенными сетями используют радиочастотный спектр. Испытателю на проникновение *беспроводные локальные сети (WLAN)* напоминают стандартные *локальные сети (LAN)*. Основное внимание специалистов сосредоточено на идентификации целевой сети и получении доступа.

Обзор стандарта IEEE 802.11

Переопределяющим стандартом, регулирующим беспроводную сеть, является IEEE 802.11. Этот набор правил был впервые разработан для удобства использования и возможности быстрого подключения устройств. В первоначальных стандартах, опубликованных в 1997 году, вопросы безопасности не рассматривались. С тех пор в стандарты были внесены поправки, первая из которых оказала значительное влияние на беспроводную сеть стандарта 802.11b. Это наиболее распространенный стандарт, который был внедрен в 1999 году.

Поскольку стандарт 802.11 использует радиосигналы, в определенных регионах предусмотрены различные законы и правила, касающиеся работы беспроводных сетей. В целом, однако, есть только несколько типов элементов управления безопасностью, встроенных в стандарт 802.11, и связанные с ним поправки.

Протокол безопасности беспроводных локальных сетей

Протокол безопасности беспроводных локальных сетей (WEP) был первым стандартом безопасности, разработанным в сочетании со стандартами 802.11. Впервые внедренный в 1999 году наряду с первой широко принятой итерацией 802.11, WEP был разработан, чтобы обеспечить уровень безопасности, характерный для проводных сетей. Это было сделано с использованием комбинации шифров RC4 для обеспечения конфиденциальности и шифров CRC32 для обеспечения целостности.

Аутентификация в сети WEP выполняется с помощью 64- или 128-битного ключа. 64-разрядный ключ представляет собой четыре последовательности из десяти шестнадцатеричных символов. Затем эти начальные 40 бит объединяются с 24-битным *вектором инициализации (IV)*, который формирует ключ шифрования RC4. Для 128-битного ключа 104-битный ключ или 26 шестнадцатеричных символов объединяются с 24-битным IV для создания ключа RC4.

Аутентификация в беспроводной сети WEP производится в четыре этапа.

1. Клиент отправляет запрос точке доступа WEP для проверки подлинности.
2. Точка доступа WEP отправляет клиенту текстовое сообщение.
3. Клиент берет введенный ключ WEP, шифрует переданное точкой доступа текстовое сообщение, после чего отправляет его на точку доступа.
4. Точка доступа расшифровывает отправленное ей сообщение, зашифрованное клиентом с помощью собственного ключа WEP. Если сообщение расшифровано правильно, клиенту разрешено подключиться.

Как рассказывалось ранее, при разработке WEP задача конфиденциальности и целостности сообщений не была основной. В результате WEP получил две ключевые уязвимости. Во-первых, главная цель алгоритма CRC32 — контрольная сумма, позволяющая избежать ошибок, а не шифрование как таковое. Во-вторых, RC4 восприимчив к тому, что называют векторной атакой инициализации. Атака IV возможна из-за того, что шифр RC4 предназначен для шифрования потока и, как следствие, один и тот же ключ нельзя использовать дважды; 24-битный ключ слишком короток для загруженной беспроводной сети. Примерно в 50 % случаев тот же IV будет использоваться в беспроводном канале связи в пределах 5000 вариаций. Это приведет к коллизии, в результате которой IV и весь ключ WEP могут быть отменены.

Из-за уязвимостей безопасности WEP в 2003 году начал постепенно сворачиваться в пользу более безопасных беспроводных реализаций. В результате вы, скорее всего, не столкнетесь с точками доступа, работающими на базе протокола WEP. Но вы можете обнаружить устаревшую сеть, в которой еще используется этот неактуальный протокол.

Защищенный доступ Wi-Fi (WPA)

При реализации беспроводной сети WEP стандарты безопасности 802.11 были обновлены с учетом новых уязвимостей. Такое обновление обеспечило большую степень конфиденциальности и целостности беспроводных сетей. Это было сделано в соответствии со стандартом Wi-Fi Protected Access (WPA), который был впервые реализован в 2003 году в стандарте 802.11i. WPA был дополнительно обновлен до WPA2 в 2006 году, тем самым став стандартом для сетей защищенного доступа Wi-Fi. WPA2 разработан в трех разных версиях, каждая из которых предусматривает свои собственные механизмы аутентификации.

- **WPA-Personal.** Подключение к беспроводной сети типа WPA2 часто встречается в жилых помещениях или небольших офисах. WPA2 использует предварительный общий ключ, который является производным от комбинации кода доступа и *идентификатора (SSID, Service Set Identifier)* беспроводной сети. Этот код настраивается пользователем, и длина его может составлять от 8 до 63 символов. Затем этот код доступа вместе с 4096 взаимосвязями алгоритма хеширования SHA1 добавляется к SSID.
- **WPA-Enterprise.** В корпоративной версии WPA/WPA2 используется сервер проверки подлинности RADIUS. Это позволяет аутентифицировать пользователя и устройство, что значительно уменьшает возможность предварительного подбора ключей с помощью грубой силы.
- **Wi-Fi Protected Setup (WPS).** Сеть такого типа предоставляет упрощенный вариант аутентификации, при котором вместо пароля или секретной фразы используется PIN-код. Поначалу этот вариант разрабатывался как наиболее простой способ подключения устройств к беспроводным сетям. Но в процессе эксплуатации стало ясно, что защита такого рода ненадежна. Злоумышленник может получить как PIN-код, так и код доступа, используемый устройством для подключения к беспроводной сети.

Для наших целей мы сосредоточимся на тестировании версий подключения WPA-Personal и WPS. При использовании WPA-Personal аутентификация и шифрование обрабатываются с помощью четырехстороннего рукопожатия (рис. 11.1).

1. Точка доступа передает клиенту случайное число, называемое *ANonce*.
2. Клиент создает другое случайное число, называемое *SNonce*. SNonce, ANonce и введенный пользователем код доступа объединяются для создания так называемой *проверки целостности сообщений (MIC)*. MIC и SNonce отправляются обратно точке доступа.
3. Точка доступа хеширует ключ ANonce, SNonce и предварительный общедоступный ключ и, если они совпадают, аутентифицирует клиента. Затем она отправляет ключ шифрования клиенту.
4. Клиент подтверждает ключ шифрования.

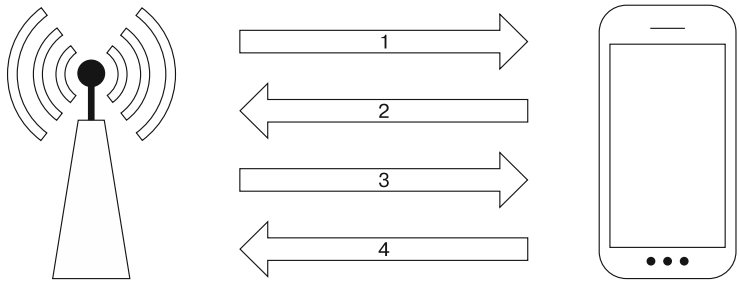

Рис. 11.1. Четырехстороннее рукопожатие

В подключении типа WPA-Personal есть две ключевые уязвимости, которые мы сейчас и рассмотрим.

- **Слабый общий ключ.** При подключении WPA-Personal пользователь должен настроить параметры точки доступа. Часто пользователи для этого используют короткий, простой и хорошо запоминающийся пароль. Как было показано ранее, есть возможность «обнюхать» трафик между точкой доступа и клиентом. Если мы сможем перехватить четырехстороннее рукопожатие, у нас будет вся информация, необходимая для перехвата пароля и аутентификации в сети.
- **WPS.** Wi-Fi Protected Setup (защищенная установка Wi-Fi) — это удобный для конечных пользователей способ подключения устройств к беспроводной сети, при котором для подключения применяется PIN-код. Такую технологию часто используют в принтерах или игровых устройствах. Пользователь должен лишь нажать кнопку на точке доступа с поддержкой WPS, а затем на устройстве, поддерживающем WPS, — и соединение будет установлено. Недостатком такого метода подключения является то, что аутентификация выполняется с помощью PIN-кода. При атаке этот PIN-код может открыть не только PIN-код WPS, но и код доступа к беспроводному устройству.

Разведка в беспроводной сети

Как и при тестировании на проникновение через Интернет, для идентификации целевой беспроводной сети сначала необходимо провести рекогносцировку. В отличие от сетевого подключения, здесь мы также должны гарантировать, что не будем трогать сеть, которую не имеем права тестировать. При тестировании беспроводного соединения это становится очень важной проблемой. Дело в том, что существуют беспроводные сети, пересекающиеся с целевой. Эта проблема особенно актуальна в тех случаях, когда целевая организация и связанные с ней сети расположены в офисном здании.

Антенны

Перед тестированием беспроводного проникновения в первую очередь нужно выбрать антенны. Часто виртуальные машины и ноутбуки не оснащены беспроводными картами и антеннами, позволяющими провести тест на проникновение. В таком случае вам придется приобрести внешнюю антенну, которая поддерживается вашим оборудованием. Большинство таких антенн можно легко купить в Интернете по умеренной цене.

Iwlist

В Kali Linux встроены несколько инструментов, которые можно использовать для идентификации беспроводных сетей. Одним из популярных является инструмент `iwlist` Linux. Эта команда перечисляет беспроводные сети, доступные в пределах диапазона беспроводной карты. Запустите терминал и введите в командную строку следующее:

```
# iwlist wlan0 scan
```

На экране вы увидите такой ответ (рис. 11.2).

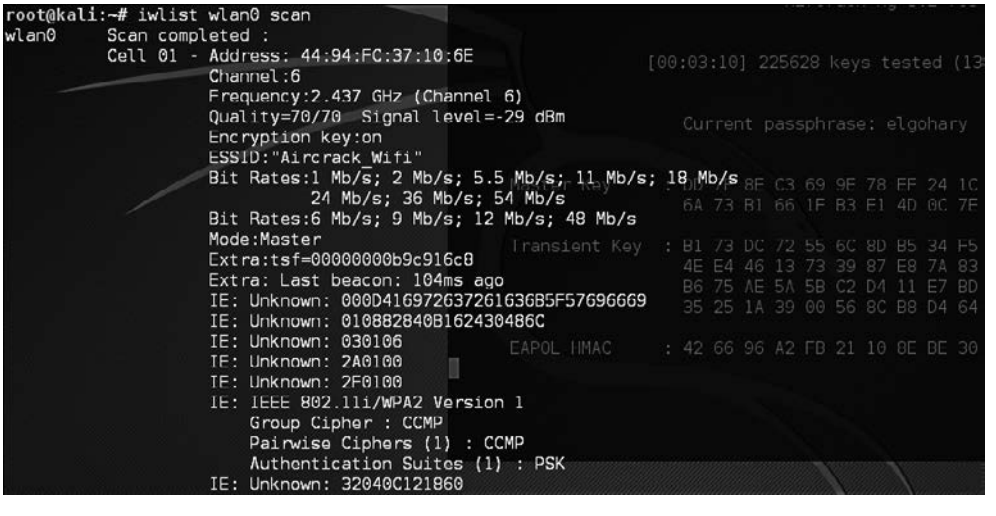

Рис. 11.2. Ответ на команду iwlist wlan0 scan

Хотя это простой инструмент, он предоставляет нужную и полезную информацию, например идентификатор набора базовых услуг (BSSID) или MAC-адрес беспроводной точки доступа (MAC-адрес нам понадобится позже), тип аутентификации и шифрования, а также другую важную информацию.

Kismet

Kismet также установлен в Kali Linux 2 по умолчанию и представляет собой смесь беспроводного сканера, IDS/IPS и пакетного анализатора трафика. Написанный на C++, Kismet предлагает дополнительные функции, которые обычно не встречаются в инструментах, запускаемых из командной строки. Чтобы запустить Kismet, выберите команду основного меню Applications ▸ Wireless Attacks ▸ Kismet (Приложения ▸ Беспроводные атаки ▸ Kismet) или введите в командную строку терминала следующую команду:

```
# kismet
```

После ее выполнения на экране появится окно Kismet (рис. 11.3). Для этого окна предусмотрены различные цветовые схемы. Сообщение об этом вы увидите в терминале.

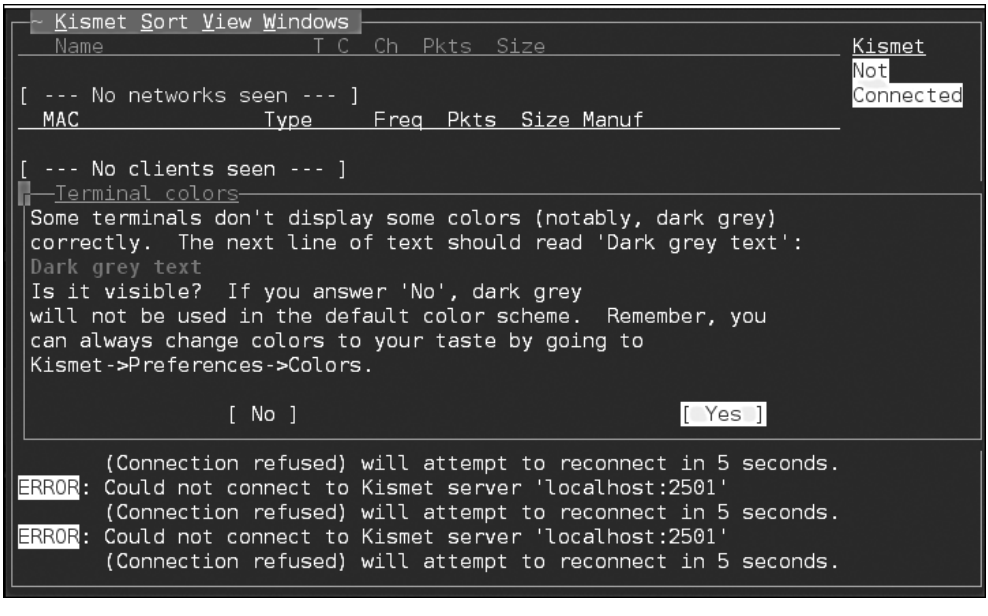

Рис. 11.3. Окно Kismet

Если вы видите терминал без помех и искажений, выберите вариант Yes.

Чтобы Kismet смог провести анализ, ему нужно указать источник. Это будет беспроводной интерфейс вашей Kali Linux. Чтобы найти этот интерфейс, введите в командную строку команду `ifconfig`. Интерфейс, начинающийся с `WLAN`, является беспроводным (рис. 11.4).

Чтобы можно было выбрать вариант Yes, нажмите клавишу Enter. На экране появится следующий диалог, в котором вводится интерфейс для сканирования. Поскольку наш интерфейс называется `wlan0`, вводим его имя, как показано на рис. 11.5.

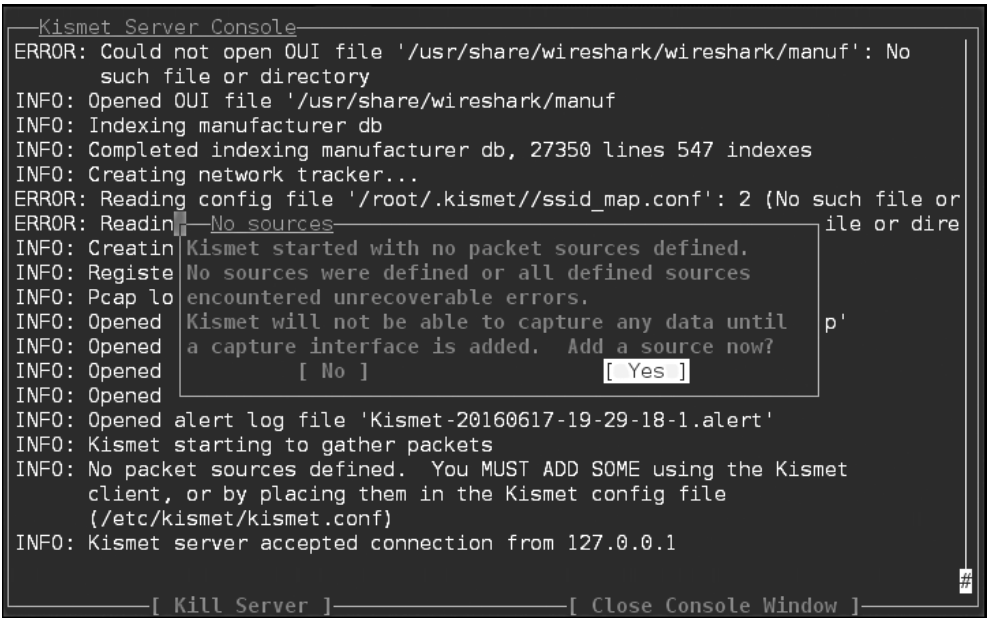

Рис. 11.4. Поиск интерфейса WLAN

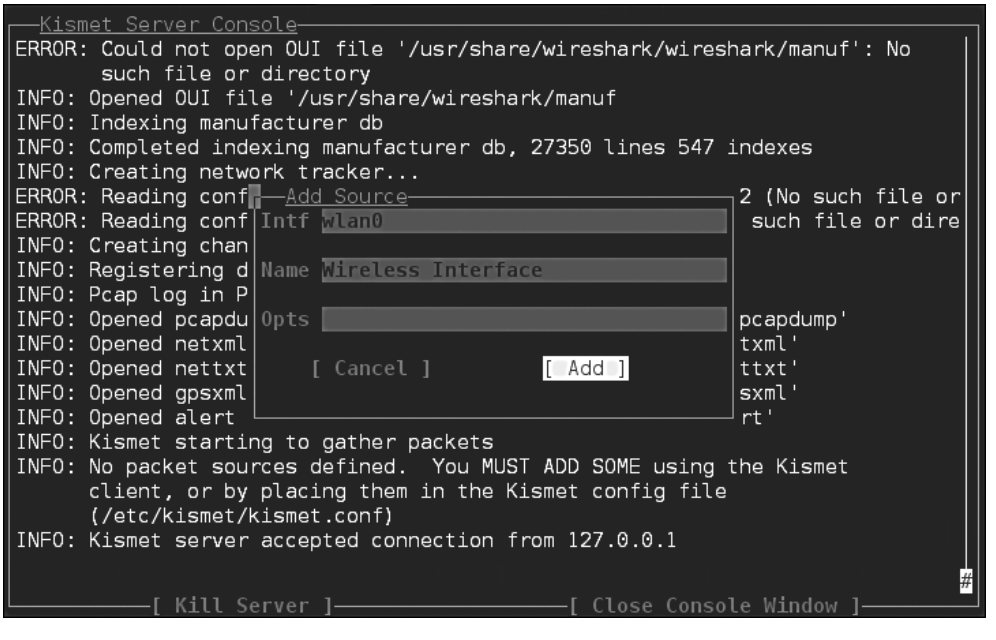

Рис. 11.5. Вводим имя интерфейса беспроводной сети

Чтобы добавить интерфейс, нажмите клавишу Enter. На этом этапе Kismet начнет собирать точки беспроводного доступа. Будут собраны BSSID и каналы, которые использует каждая точка доступа (рис. 11.6).

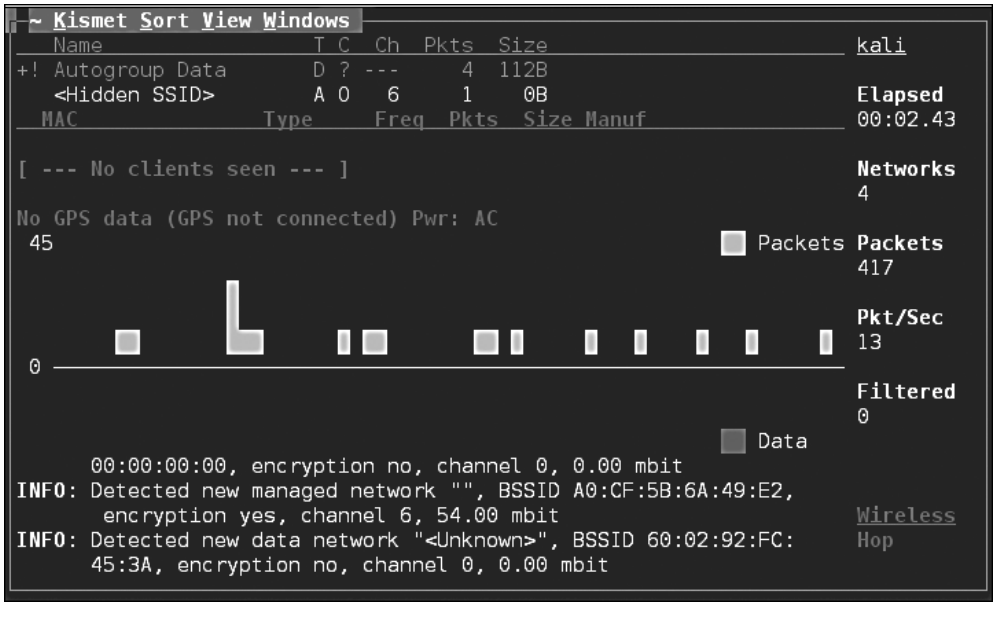

Рис. 11.6. BSSID собирает информацию о каждой точке доступа

Просмотрев ответ Kismet, вы сможете понять, какие беспроводные сети видны вашей системе. Теперь потребуется определить те беспроводные точки доступа, которые являются частью теста на проникновение.

WAIDPS

Другим инструментом командной строки, который мы можем использовать при тестировании на проникновение, является WAIDPS. Несмотря на то что этот сценарий Python представляет собой платформу обнаружения вторжений для беспроводных сетей, он удобен и для сбора информации о беспроводных сетях и клиентах. Чтобы использовать WAIDPS, просто скачайте сценарий Python `WAIDPS.py` с сайта https://github.com/SYWorks/waidps.

После загрузки поместите сценарий в любой каталог, а затем запустите его с помощью следующей команды:

```
# python waidps.py
```

После выполнения команды на экране появится окно выполнения сценария конфигурации (рис. 11.7).

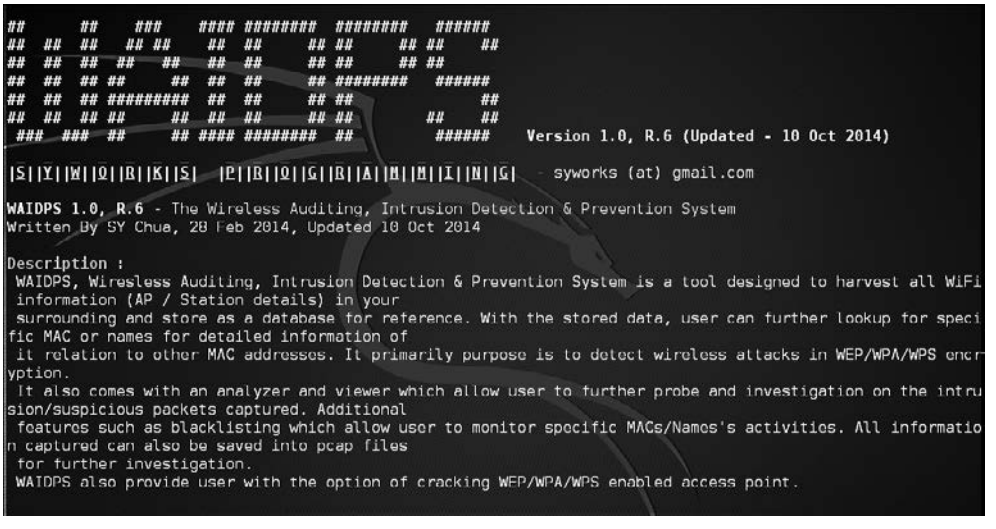

Рис. 11.7. Окно конфигурации WAIDPS

WAIDPS имеет дополнительную функцию, которая сравнивает MAC-адреса точек беспроводного доступа с адресами точек доступа известных производителей. Эта функция полезна, если вы знаете, что конкретная цель использует точки доступа определенного производителя (рис. 11.8).

Рис. 11.8. Определение производителя точек доступа

После запуска начальной конфигурации WAIDPS предоставит список всех видимых им точек доступа и беспроводных сетей. Кроме того, вы увидите индикатор PWR, с помощью которого можно определить уровень сигнала, передаваемого конкретной точкой доступа. Чем ближе данное значение к нулю, тем сильнее сигнал. Эти сведения могут быть полезны, если вас интересует конкретная точка доступа. Если сигнал слабый, значит, вам потребуется приблизиться к нужной точке доступа (рис. 11.9).

Помимо идентификации точек беспроводного доступа, WAIDPS умеет сканировать клиенты, у которых может быть беспроводная связь, но которые не связаны с точкой доступа. Эта информация может быть полезна, если вам нужно подделать MAC-адрес, исходящий, как может показаться, от законного клиента (рис. 11.10).

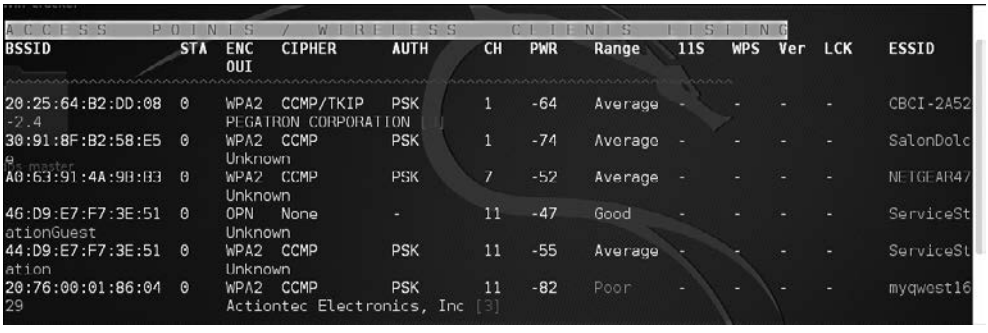

Рис. 11.9. Индикаторы PWR показывают значение уровня сигнала, излучаемого точками доступа

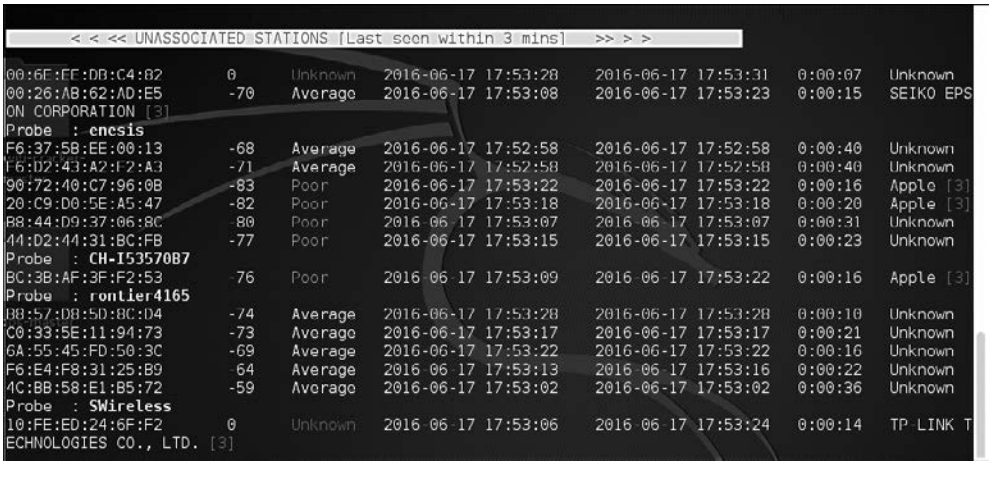

Рис. 11.10. Информация о точках доступа и беспроводной связи