Министерство образования и науки Российской Федерации
ФГАОУ ВО «Северо-Восточный федеральный университет
им. М.К. Аммосова»
Физико-технический институт
Кафедра радиофизики и электронных систем

Отчет по лабораторным работам
по дисциплине «Защита информации в беспроводных сетях»
11.04.01 Радиотехника
Профиль: Радиотехнические средства обработки и защиты информации в каналах связи

Выполнил студент: гр. М-РТ-21
Дмитриева А.Н.
Проверил: Леонтьев Н.А.

Якутск
2022 г.

Лабораторная работа №1

Изучение операционной системы Linux Kali

Цель работы: изучить основные команды Kali Linux, установить ОС.

Kali Linux – это дистрибутив Linux, созданный на основе Debian, предназначенный для цифровой криминалистики и тестирования на проникновение.

Основные команды:

- Для отображения текущего рабочего каталога: pwd

Эта команда отображает текущий каталог.

- Перечислить каталоги и файлы в текущем каталоге: ls

Эта команда отображает список файлов и каталогов в текущем каталоге.

- Чтобы изменить текущий рабочий каталог: cd

Эта команда изменяет каталог, над которым сейчас работаете.

- Чтобы найти слово в файле: grep keyword filename

Эта команда выведет список всех строк, содержащих ключевое слово в них.

- Для создания нового каталога: mkdir directory_name

Эта команда создаст новый каталог в текущей папке с именем directory_name**.**

- Чтобы удалить каталог: rmdir directory_name

Эта команда удалит каталог с именем directory_name из текущего каталога.

- Для перемещения файла: mv source destination

Эта команда используется для перемещения файла из одного места в другое.

- Для копирования файла: cp source destination

Эта команда скопирует файл из источника в место назначения.

- Для создания нового файла: touch filename

Эта команда создаст новый файл с именем “filename”

- Для отображения руководства по команде: man ls

Эта команда отобразит руководство или руководство пользователя для команды.

- Чтобы проверить подключение к Интернету или проверить, активен ли хост или нет: ping google.com

Эта команда отправит некоторые пакеты на указанный хост и предоставит нам информацию о том, каков статус пакета. Эта команда может использоваться для проверки подключения к Интернету.

- Для отображения сведений о сетевом интерфейсе: ifconfig

Эта команда используется для отображения сведений о сетевых интерфейсах, подключенных к системе.

- Для загрузки файла: wget link_to_file

Эта команда загрузит файл по ссылке, введенной в команде.

- Для установки пакета: sudo apt install package_name

Эта команда используется для установки указанного пакета в системе.

- Чтобы удалить пакет: sudo apt remove package_namme

Эта команда удалит упомянутый пакет из системы.

- Для обновления пакетов в системе: sudo apt upgrade

Эта команда обновит все пакеты в системе.

- Для получения обновлений пакетов: sudo apt update

Эта команда проверит наличие обновлений во всех пакетах и добавит обновления в список для обновления.

- Чтобы получить текущее имя пользователя: whoami

Эта команда используется для печати имени пользователя текущего пользователя.

- Чтобы изменить текущего пользователя на суперпользователя или root: sudo su

Эта команда запросит пароль и изменит текущего пользователя на root.

- Для печати в терминале: echo " To print something on terminal"

Команда напечатает указанный текст на терминале.

Создали LIVE систему на флешке с Kali Linux с помощью видео https://www.youtube.com/watch?v=jMbppmRk-I8,
Вывод: изучили основные команды Kali Linux.

Лабораторная работа №2
Изучение сетевых протоколов Wi-Fi

Из современных технологий беспроводной передачи информации наибольшее распространение получили Wi-Fi. Технология Wi-Fi применяется для организации локальных сетей внутри предприятия, объединения территориально распределенных подсетей в одну сеть Ethernet, а также для передачи информации между разными устройствами (например, камерой видеонаблюдения и регистратором).

Протоколы Wi-Fi

802.11. Скорость передачи Wi-Fi по нему равна 1-2 Мбит/с.

802.11a. Теоретическая скорость передачи Wi-Fi по этому протоколу может достигать 54 Мбит/с.Реальная скорость обычно располагается в пределах 22-26 Мбит/с. Wi-Fi частота данного протокола равна 5 ГГц. Передача данных осуществляется с помощью метода OFDM (мультиплексирование с ортогональным делением частот). В помещении скорость передачи Wi-Fi равна 54 Мбит/с. При этом расстояние между устройствами сети должно быть не больше 12-15 м. Если удалить их друг от друга на 50-90 м, то скорость упадет до 6 Мбит/с. На открытом пространстве дальнобойность растет: 54 Мбит/с на 30-40 м, а 6 Мбит/с - 250-350 м.

802.11b. Теоретическая скорость передачи Wi-Fi до 11 Мбит/с.

Реальная - 5-7 Мбит/с. Wi-Fi частота - 2.4 ГГц. Передача данных осуществляется методом DSSS (прямая последовательность с разнесением сигнала по широкому диапазону). В замкнутом пространстве максимальная скорость передачи WiFi может дойти до 11 Мбит/с, расстояние между устройствами 30-40 м, или 1 Мбит/с на 80-100 м. На открытом пространствескорость передачи Wi-Fi составляет 11 Мбит/с, расстояние от 200-300 м и 1 Мбит/с на 500-600 м.

802.11g. Наиболее распространенный протокол.

Теоретическая скорость передачи Wi-Fi до 54 Мбит/с.Реальная скорость составляет примерно 50% от теоретической, т.е. около 25 Мбит/с. Для передачи данных использованы методы OFDM и FSSS. Wi-Fi частота 802.11g 2.4 ГГц. В закрытом пространстве скорость передачи Wi-Fi достигает 54 Мбит/с, расстояние 30-40 м, и 1 Мбит/с на 80-100 м. На улице дистанция увеличивается до 150-200 м и 400-500 м соответственно. Обратно совместим с протоколом 802.11b.

802.11i. Набирающий обороты протокол. Максимальная теоретическая скорость передачи Wi-Fi достигает 480 Мбит/с. Wi-Fi частота 802.11i 2.4 — 2.5 или 5.0 ГГц.

Устройства, поддерживающие протокол 802.11i, способны работать в трех режимах:

- Legacy (наследуемый). Обеспечивается совместимость с 802.11b/g и 802.11a устройствами.
- Mixed (смешанный). К этому списку добавляются 802.11i устройства.
- «Чистый» режим. Возможно соединение только с 802.11i устройствами.

Таблица 1

Поколения Wi-Fi

Поколение	Стандарт IEEE	Максимальная скорость соединения (Мбит/с)	Принято	Радиочастота (ГГц)
Wi-Fi 7	802.11be	С 1376 по 46120	(2024)	2.4/5/6
Wi-Fi 6E	802.11ax	С 574 по 9608	2020	2.4/5/6
Wi-Fi 6			2019	2.4/5
Wi-Fi 5	802.11ac	с 433 по 6933	2014	5[41]
Wi-Fi 4	802.11n	от 72 до 600	2008	2.4/5
(Wi-Fi 3)*	802.11g	от 6 до 54	2003	2.4
(Wi-Fi 2)*	802.11a	от 6 до 54	1999	5
(Wi-Fi 1)*	802.11b	с 1 по 11	1999	2.4
(Wi-Fi 0)*	802.11	от 1 до 2	1997	2.4

Оборудование часто поддерживает несколько версий Wi-Fi. Для связи устройства должны использовать общую версию Wi-Fi. Версии отличаются диапазонами радиоволн, в которых они работают, занимаемой полосой пропускания, максимальной скоростью передачи данных, которую они могут поддерживать, и другими деталями. Некоторые версии допускают использование нескольких антенн, что позволяет увеличить скорость, а также уменьшить помехи.

Исторически сложилось так, что оборудование просто перечисляло версии Wi-Fi, используя название стандарта IEEE, который оно поддерживает. В 2018 году Wi-Fi Alliance ввел упрощенную нумерацию поколений Wi-Fi для обозначения оборудования, поддерживающего Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac) и Wi-Fi 6 (802.11ax). Эти поколения имеют высокую степень обратной совместимости с предыдущими

версиями. Альянс заявил, что уровень поколения 4, 5 или 6 может быть указан в пользовательском интерфейсе при подключении вместе с уровнем сигнала.

Список наиболее важных версий Wi-Fi: 802.11a, 802.11b, 802.11g, 802.11n (Wi-Fi 4), 802.11h, 802.11i, 802.11-2007, 802.11-2012, 802.11 переменный ток (Wi-Fi 5), 802.11ad, 802.11af, 802.11-2016, 802.11ah, 802.11ai, 802.11aj, 802.11aq, 802.11ax (Wi-Fi 6), 802.11ay.

Лабораторная работа №3
Изучение протоколов безопасности WEP, WPA, WPA2, WPA3

WPA (Wi-Fi Protected Access) – это стандарт безопасности для вычислительных устройств с беспроводным подключением к интернету. Он был разработан объединением Wi-Fi Alliance для обеспечения лучшего шифрования данных и аутентификации пользователей, чем было возможно в рамках стандарта WEP (Wired Equivalent Privacy), являющегося исходным стандартом безопасности Wi-Fi.

Беспроводные сети передают данные посредством радиоволн, поэтому, если не приняты меры безопасности, данные могут быть с легкостью перехвачены. Представленная в 1997 году технология WEP является первой попыткой защиты беспроводных сетей. Ее целью было повышение безопасности беспроводных сетей за счет шифрования данных. Даже в случае перехвата данных, передаваемых в беспроводной сети, их невозможно было прочитать, поскольку они были зашифрованы. Однако системы, авторизованные в сети, могут распознавать и расшифровывать данные, благодаря тому, что все устройства в сети используют один и тот же алгоритм шифрования.

WEP шифрует трафик с использованием 64 или 128-битного ключа в шестнадцатеричном формате. Это статический ключ, поэтому весь трафик, независимо от устройства, шифруется с помощью одного ключа. Ключ WEP позволяет компьютерам внутри сети обмениваться зашифрованными сообщениями, однако содержимое сообщений скрыто от злоумышленников. Этот ключ используется для подключения к беспроводной сети с включенной безопасностью.

Одна из основных задач технологии WEP – предотвращение атак типа «человек посередине», с которой она успешно справлялась в течение определенного времени. Однако, несмотря на изменения протокола и увеличение размера ключа, со временем в стандарте WEP были обнаружены различные недостатки. По мере роста вычислительных мощностей злоумышленникам стало проще использовать эти недостатки. Объединение Wi-Fi Alliance официально отказалось от использования технологии WEP в 2004 году из-за ее уязвимостей. В настоящее время технология безопасности WEP считается устаревшей, хотя иногда она все еще используется либо из-за того, что администраторы сети не изменили настроенные умолчанию протоколы безопасности беспроводных роутеров, либо из-за того, что устройства устарели и не способны поддерживать новые методы шифрования, такие как WPA.

WPA (Wi-Fi Protected Access) – это появившийся в 2003 году протокол, которым объединение Wi-Fi Alliance заменило протокол WEP. WPA похож на WEP, однако в нем усовершенствована обработка ключей безопасности и авторизации пользователей. WEP предоставляет всем авторизованным системам один ключ, а WPA использует протокол целостности временного ключа (Temporal Key Integrity Protocol, TKIP),

динамически изменяющий ключ, используемый системами. Это не позволяет злоумышленникам создать собственный ключ шифрования, соответствующий используемому в защищенной сети. Стандарт шифрования TKIP впоследствии был заменен расширенным стандартом шифрования (Advanced Encryption Standard, AES).

Кроме того, протокол WPA включает проверку целостности сообщений, чтобы определить, имел ли место захват или изменение пакетов данных злоумышленником. Протокол WPA использует 256-битные ключи, что значительно надежнее 64 и 128-битных ключей, используемых протоколом WEP. Однако, несмотря на эти улучшения, в протоколе WPA также были обнаружены уязвимости, что привело к созданию протокола WPA2.

Иногда используется термин «ключ WPA» – это пароль для подключения к беспроводной сети. Пароль WPA можно получить от администратора сети. В ряде случаев установленный по умолчанию пароль WPA может быть напечатан на беспроводном роутере. Если не удается определить пароль роутера, возможно, его можно сбросить.

Протокол WPA2 появился в 2004 году. Он является обновленной версией WPA. WPA2 основан на механизме сети высокой безопасности (RSN) и работает в двух режимах:

Персональный режим или общий ключ (WPA2-PSK) – использует общий пароль доступа и обычно применяется в домашних сетях.

Корпоративный режим (WPA2-EAP) – больше подходит для сетей организаций и коммерческого использования.

В обоих режимах используется протокол CCMP, основанный на алгоритме расширенного стандарта шифрования (AES), обеспечивающего проверку подлинности и целостности сообщения. Протокол CCMP является более надежным, чем исходно используемый в WPA протокол TKIP, поэтому его использование затрудняет атаки злоумышленников.

Однако у протокола WPA2 также есть недостатки. Например, он уязвим для атак с переустановкой ключа (KRACK). Атаки с переустановкой ключа используют уязвимость WPA2, позволяющую имитировать реальную сеть и вынуждать пользователей подключаться к вредоносной сети вместо настоящей. Это позволяет злоумышленникам расшифровывать небольшие фрагменты данных, объединение которых позволит взломать ключ шифрования. Однако на устройства могут быть установлены исправления, поэтому WPA2 считается более надежным, чем WEP и WPA.

WPA3 – это третья версия протокола защищенного доступа Wi-Fi. Объединение Wi-Fi Alliance выпустило WPA3 в 2018 году. В протоколе WPA3 реализованы следующие новые функции для личного и для корпоративного использования:

Индивидуальное шифрование данных. При входе в публичную сеть WPA3 регистрирует новое устройство способом, не подразумевающим использование общего пароля. В WPA3 используется протокол DPP (Device Provisioning Protocol) для сетей Wi-Fi, позволяющий пользователям

использовать теги NFC или QR-коды для подключения устройств к сети. Кроме того, для обеспечения безопасности WPA3 используется шифрование GCMP-256 вместо применявшегося ранее 128-битного шифрования.

Протокол SAE (одновременная аутентификация равных). Этот протокол используется для создания безопасного «рукопожатия», при котором сетевое устройство подключается к беспроводной точке доступа, и оба устройства обмениваются данными для проверки аутентификации и подключения. Даже если пароль пользователя недостаточно надежный, WPA3 обеспечивает более безопасное взаимодействие по протоколу DPP для сетей Wi-Fi.

Усиленная защита от атак методом подбора пароля. Протокол WPA3 защищает от подбора пароля в автономном режиме. Пользователю позволяется выполнить только одну попытку ввода пароля. Кроме того, необходимо взаимодействовать напрямую с устройством Wi-Fi: при каждой попытке ввода пароля требуется физическое присутствие. В протоколе WPA2 отсутствует встроенное шифрование и защита данных в публичных открытых сетях, что делает атаки методом подбора пароля серьезной угрозой.

Устройства, работающие по протоколу WPA3, стали широко доступны в 2019 году. Они поддерживают обратную совместимость с устройствами, работающими по протоколу WPA2.

Для обеспечения надлежащего уровня безопасности сети Wi-Fi важно знать, какой тип шифрования в ней используется. Устаревшие протоколы являются более уязвимыми, чем новые, поэтому вероятность их взлома выше. Устаревшие протоколы были разработаны до того, как стало полностью понятно, каким способом злоумышленники осуществляют атаки на роутеры. В новых протоколах эти уязвимости устранены, поэтому считается, что они обеспечивают лучшую безопасность сетей Wi-Fi.

В настоящее время WEP считается устаревшим стандартом шифрования Wi-Fi, и по возможности следует использовать более современные протоколы.

Лабораторная работа №4
Изучение протоколов безопасности WPA2 Enterprise

Корпоративные сети с шифрованием WPA2-Enterprise строятся на аутентификации по протоколу 802.1x через RADIUS-сервер. Протокол 802.1x (EAPOL) определяет методы отправки и приема запроса данных аутентификации и обычно встроен в операционные системы и специальные программные пакеты.

802.1x предполагает три роли в сети:

- клиент (supplicant) - клиентское устройство, которому нужен доступ в сеть;
- сервер аутентификации (обычно RADIUS);
- аутентификатор — роутер/коммутатор, который соединяет множество клиентских устройств с сервером аутентификации и отключает/подключает клиенсткие устройства.

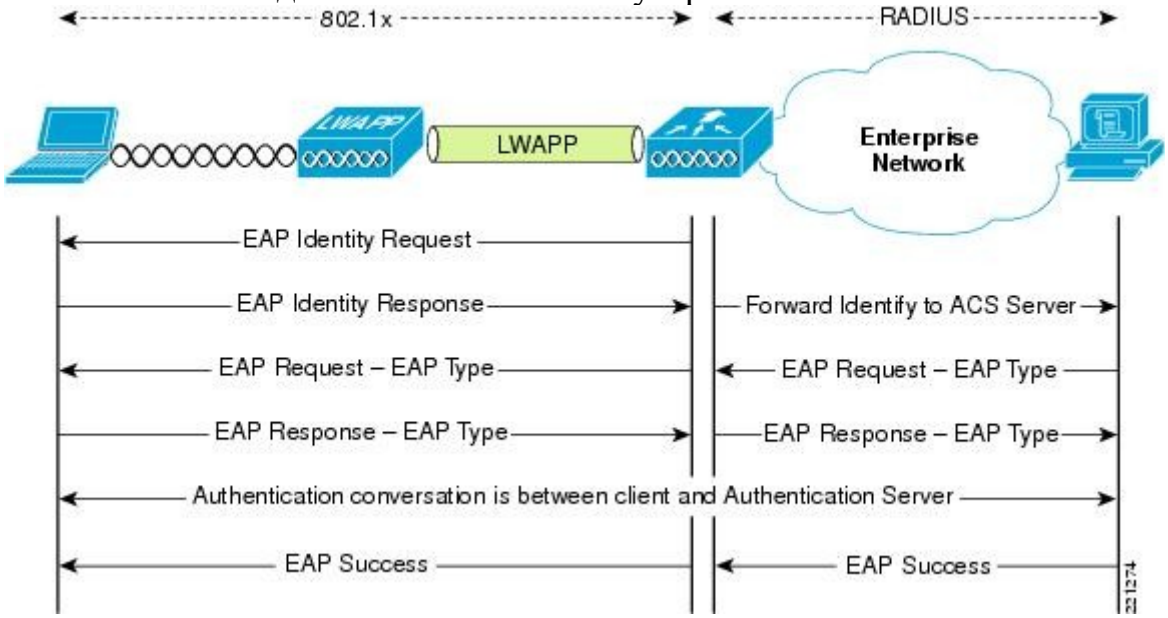


Рис.1 - Схема работы WPA2-Enterprise 802.1x

Есть несколько режимов работы 802.1x, но самый распространенный и надежный следующий:

- Аутентификатор передает EAP-запрос на клиентское устройство, как только обнаруживает активное соединение.
- Клиент отправляет EAP-ответ — пакет идентификации. Аутентификатор пересылает этот пакет на сервер аутентификации (RADIUS).
- RADIUS проверяет пакет и право доступа клиентского устройства по базе данных пользователя или другим признакам и затем отправляет на аутентификатор разрешение или запрет на подключение.

Соответственно, аутентификатор разрешает или запрещает доступ в сеть.

Использование сервера RADIUS позволяет отказаться от PSK и генерировать индивидуальные ключи, валидные только для конкретной сессии подключения. Проще говоря, ключи шифрования невозможно извлечь из клиентского устройства. Защита от перехвата пакетов обеспечивается с помощью шифрования по разным внутренним протоколам EAP, каждый из которых имеет свои особенности. Так, протокол EAP-FAST позволяет авторизоваться по логину и паролю, а PEAP-GTC — по специальному токену (карта доступа, карточки с одноразовыми паролями, флешки и т. п.). Протоколы PEAP-MSCHAPv2 и EAP-TLS проводят авторизацию по клиентским сертификатам.

Максимальную защиту сети Wi-Fi обеспечивает только WPA2-Enterprise и цифровые сертификаты безопасности в сочетании с протоколом EAP-TLS или EAP-TTLS. Сертификат — это заранее сгенерированные файлы на сервере RADIUS и клиентском устройстве. Клиент и сервер аутентификации взаимно проверяют эти файлы, тем самым гарантируется защита от несанкционированных подключений с чужих устройств и ложных точек доступа. Протоколы EAP-TTL/TTLS входят в стандарт 802.1X и используют для обмена данными между клиентом и RADIUS инфраструктуру открытых ключей (PKI). PKI для авторизации использует секретный ключ (знает пользователь) и открытый ключ (хранится в сертификате, потенциально известен всем). Сочетание этих ключей обеспечивает надежную аутентификацию.

Цифровые сертификаты нужно делать для каждого беспроводного устройства. Это трудоемкий процесс, поэтому сертификаты обычно используются только в Wi-Fi-сетях, требующих максимальной защиты. В то же время можно легко отозвать сертификат и заблокировать клиента.

Сегодня WPA2-Enterprise в сочетании с сертификатами безопасности обеспечивает надежную защиту корпоративных Wi-Fi-сетей. При правильной настройке и использовании взломать такую защиту практически невозможно "с улицы", то есть без физического доступа к авторизованным клиентским устройствам. Тем не менее, администраторы сетей иногда допускают ошибки, которые оставляют злоумышленниками "лазейки" для проникновения в сеть. Проблема осложняется доступностью софта для взлома и пошаговых инструкций.

Лабораторная работа №5
Изучение протокола Bluetooth

При работе устройств Bluetooth используются специфические протоколы для Bluetooth и общие, которые используются в различных телекоммуникационных системах. Все они образуют стек протоколов Bluetooth.

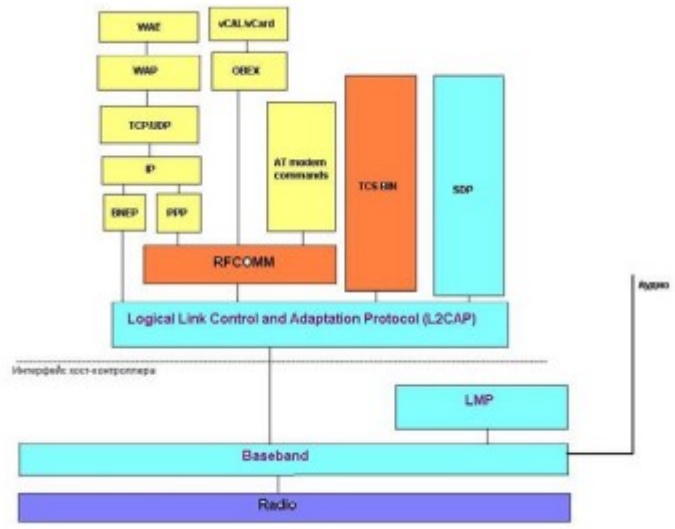


Рис.1 – Стек протоколов Bluetooth

Все эти протоколы можно разделить на 4 слоя:
1. Корневые протоколы.
2. Протокол замены кабеля
3. Протокол управления телефонией
4. Заимствованные протоколы

Помимо этих протокольных слоев спецификация Bluetooth определяет также интерфейс хост-контроллера (HCI — Host Controller Interface), который дает командный интерфейс к baseband-контроллеру, диспетчеру соединений (Link Manager), и доступ к аппаратным регистрам статуса и управления.

Три (нижних) слоя — слой замены кабеля, слой управления телефонией и слой заимствованных протоколов — совместно определяют совокупность протоколов, которые ориентированны на приложения, которые позволяют прикладным задачам выполняться над корневыми протоколами Bluetooth.

Спецификация Bluetooth является открытой и дополнительные протоколы (например, HTTP, FTP и т.д.) могут быть подключены поверх специфических транспортных протоколов Bluetooth или поверх протоколов, ориентированных на приложения. Корневые протоколы Bluetooth требуются для большинства устройств, тогда как остальные протоколы используются только там, где они нужны.

Радио

Определяет детали поверхности воздуха. Использует не имеющий разрешения ISM – диапазон около 2.45 ГГц.

Расширение спектра посредством частотных скачков

• частотные скачки зафиксированы на f=2402+k МГц, где k= 0,1,...,78 (число каналов)

• количество скачков до 1600 в секунду

• передача данных основывается на разделении времени (TDD)

• каждое устройство подразделяется на классы мощности – 1, 2 и 3

Корневые протоколы Bluetooth

Baseband (Link Controller) и протокол управления связью (LMP – Link Manager Protocol) обеспечивают физическую радиочастотную связь между устройствами Bluetooth, образующими пикосеть. Этот уровень предоставляет два различных способа физического подключения с соответствующими пакетами базовой полосы:

1. Синхронным, ориентированным на соединение (SCO – Synchronous Connection Oriented)

2. Асинхронным без установления соединения (ACL – Asynchronous Connection Less). Также здесь определяется формат пакетов, адресация устройств, процедуры вызова и запроса, физические и логические каналы.

Протокол управления связью (LMP — Link Manager Protocol) отвечает за установление подключений между устройствами Bluetooth. Также сюда относятся и вопросы безопасности, такие как идентификация и шифрования, связанные генерированием ключей шифрования и подключения, а также с обменом ключами и их проверкой. LMP имеет более высокий приоритет чем остальные протоколы (например, L2CAP). Если, например, получается, что канал занят чем-либо другим, то при необходимости передать LMP сообщение он немедленно освобождается.

Протокол управления логическим подключением и адаптацией (L2CAP — Logical Link Control and Adaptation Protocol) адаптирует протоколы верхнего уровня над Baseband.

L2CAP является базовым протоколом передачи данных для Bluetooth. Протокол Baseband позволяет устанавливать SCO и ACL соединения. L2CAP работает только с ACL соединениями. Многие протоколы и службы более высокого уровня используют L2CAP как транспортный протокол.

Протокол обнаружения услуг (Service Discovery Protocol – SDP) является одним из важнейших протоколов Bluetooth, который использует L2CAP в качестве транспортного протокола. Используя протокол SDP можно запросить информацию о самом устройстве, о его услугах и о характеристиках этих услуг, а после этого может быть установлено соединение между двумя или несколькими устройствами Bluetooth.

Ещё одним из протоколов, которые использует L2CAP в качестве транспортного, является **RFCOMM** (Radio Frequency Comm.). Этот

протокол эмулирует соединение PPP (point-to-point) по последовательному порту (RS-232 или EIATIA-232-E, более известным как COM-порты). Также он обеспечивает транспортировку при выполнении услуг верхнего уровня, которые используют последовательную линию как транспортный механизм. Через него работают такие службы как доступ к локальной сети (LAN). Эта служба может работать как эмуляция прямого кабельного соединения, когда надо обеспечить связь между двумя персональными компьютерами, так и использоваться для полноценного входа в уже существующую локальную сеть. Во втором случае используется точка доступа к локальной сети, через которую компьютер Bluetooth оказывается подключен к LAN так, как он мог бы подключиться через dial-up соединение.

Двоичный протокол управления телефонией (TCS Binary (Telephony Control Protocol Specification- Binary) или TCS BIN) является бит- ориентированным протоколом. Он определяет контроль сигнализации вызова для установления речевого вызова или вызова данных между устройствами Bluetooth. Кроме того, он определяет процедуры управления мобильностью при манипулировании с группами TCS-приборов Bluetooth.

Bluetooth SIG определила набор **АТ-команд** (Attention Sequence), с помощью которых можно управлять мобильным телефоном или модемом в режиме моделей мультииспользования. Команды, используемые при FAX-услугах, специфицируются реализацией. Это могут быть FAX-услуги класса 1.0 и класса 2.0.

Voice или Bluetooth audio одна из служб Bluetooth которая использует синхронное соединение. Одновременно может передаваться до 3 аудиоканалов. Характеристики звуковых потоков могут различаться, и во многом определяются используемым приложением. Максимально звуковой поток может передаваться с точностью в 16 бит при частоте дискретизации 48 кГц.

В технологии Bluetooth **протокол «точка-точка»** (Point-to-Point Protocol — PPP) должен работать «поверх» RFCOMM. Соединения PPP служат средством, позволяющим перемещать IP-пакеты с уровня PPP на уровень локальных сетей.

В настоящее время семейство **протоколов TCP/IP** используется наиболее широко во всем мире. Стеки TCP/IP установлены на самых разных устройствах. Встраивание этих стандартов в приборы Bluetooth позволяет осуществлять связь с любым другим устройством, подключенным к Internet. Такой прибор Bluetooth используется затем как «мост» к Internet.

Протокол IrOBEX (Infrared Object Exchange Protocol) или, сокращенно, OBEX, является сеансовым протоколом, разработанным ассоциацией IrDA для простого, поэтапного обмена объектами. OBEX, обеспечивающий функциональность, сходную с HTTP, использует модель клиента-сервера, не зависит ни от транспортного механизма, ни от транспортного API-интерфейса (Application Programming Interface). Наряду с самим протоколом — «грамматикой» для OBEX-переговоров между устройствами — OBEX дает также модель для представления объектов и

операций. Вдобавок OBEX определяет оглавление папок, которое используется для просмотра содержимого папок, находящихся на удаленных устройствах.

Форматы vCard (обмен электронными визитными карточками) и vCalendar (обмен электронными календарными данными) являются открытыми спецификациями, которые были разработаны консорциумом Versit и контролируются сегодня консорциумом Internet Mail. Сами по себе vCard и 5 0 TD0 TvCalendar не определяют никакого транспортного механизма. Они определяют только форматы данных, которые должны транспортироваться.

Два других формата содержимого, которые передаются протоколом OBEX, — это форматы vMessage («сообщение») и vNote («заметка»). Они также являются открытыми стандартами и используются для обмена сообщениями и замечаниями. Они определены в спецификации Инфракрасных мобильных коммуникаций (IrMC — Infrared Mobile Communications). Там же определен формат журнальных файлов, который необходим для синхронизации данных между отдельными приборами.

Протокол беспроводных приложений (WAP — Wireless Application Protocol), разработанный Форумом WAP, должен работать в самых разнообразных беспроводных сетях.

Цель состоит в том, чтобы распространить содержимое сети Internet на устройства BT.

Идея, стоящая за разработкой WAP, — повторно использовать приложения верхнего уровня, разработанные для среды WAE (WAP Application Environment).

К таким приложениям относятся браузеры WML и WTA, способные взаимодействовать с приложениями на компьютере. Построение шлюзов для приложений, обеспечивающих связь между WAP-серверами и приложениями на компьютере позволяет реализовать различные виды «скрытой» функциональности, такие как дистанционное управление, передача данных с компьютера на телефон и т.д.

Протокол BNEP (Bluetooth Network Encapsulation Protocol)

Протокол инкапсулирует Ethernet пакеты в BNEP пакеты.

Сетевой протокол инкапсуляции Bluetooth предоставляет инкапсуляцию, заменив заголовок сетей, таких как Ethernet заголовок, на BNEP заголовки. То есть предоставляет Ethernet-подобный интерфейс на каждом конце Bluetooth-соединения.

Лабораторная работа №6
Применение программ для анализа сетей Wi-Fi.
Пример программы Aircrack.

Анализатор WiFi – это отдельный инструмент, который диагностирует проблемы сети WiFi, а затем решает их для ее оптимизации. Таким образом, он может повысить скорость интернета и возможность подключения маршрутизатора к сети. Этот инструмент обнаруживает все ближайшие беспроводные сети, оценивает их для сбора информации, выбирает вашу сеть среди них и затем работает с ней.

В Интернете доступны различные типы анализаторов WiFi. Некоторые из них являются базовыми, что означает, что они будут информировать только о проблеме и способах ее устранения, а некоторые являются расширенными и имеют такие функции, как тепловая карта, автоматическая оптимизация и т. д. Тем не менее ожидается, что анализатор WiFi будет служить основной цели - анализу вашей сети WiFi.

Программное обеспечение для анализа Wi-Fi может обнаружить проблемы, вызывающие низкую производительность, и устранить их, чтобы обеспечить максимальную производительность сети.

1. Анализатор WiFi

Программное обеспечение WiFi Analyzer это первая рекомендация по сканированию сети Wi-Fi, обнаружению проблем и их. Этот инструмент позволяет подключиться к сети одним касанием, а затем показывает важные детали на экране. Он может блокировать функцию тайм-аута экрана и предлагает поддержку живых плиток.

2. INSSID

INSSID - это хорошо известный инструмент анализа WiFi, который визуально представляет сеть WiFi на экране. Оттуда он обнаруживает и объясняет проблемы с сетью. Он информирует о том, что можно сделать, чтобы устранить проблемы и получить максимальную производительность от сети.

InSSIDer поставляется в трех различных версиях, которые подходят как для домашних, так и для профессиональных пользователей.

3. NetSpot

Этот инструмент предлагает два типа сканирования сети. Один из них – это режим обнаружения, который отображает скорость перемещения данных от пользователя в Интернет. Другой - режим Survey, который создает тепловые карты мощности Wi-Fi, которые помогают анализировать области сети.

Пользовательский интерфейс богатый, стильный и в то же время такой простой.

4. Акриловый домашний сканер WiFi

Акриловый домашний сканер WiFi имеет две отдельные версии, предназначенные для домашних пользователей и для предприятий или предприятий.

Он может сканировать сеть, отображать различные области, обнаруживать проблемы, а также предлагать лучшие сетевые каналы в соответствии с маршрутизатором.

5. Ekahau Heat Mapper бесплатно

Ekahau Heat Mapper бесплатно - еще один отличный инструмент, который можно использовать дома для анализа сети Wi-Fi. Можно увидеть тепловую карту сети. По тепловой карте можно определить области сильного и слабого сигнала, узнать, не мешают ли стены работе сети.

Этот инструмент также предлагает вам лучшее место для размещения маршрутизатора, чтобы могли получить максимальную производительность сети Wi-Fi. Он также порекомендует, какой канал следует использовать в зависимости от должности.

6. WireShark

WireShark - это продвинутое программное обеспечение для анализа Wi-Fi, которое может устранять неполадки различных протоколов связи. Этот бесплатный инструмент с открытым исходным кодом рекомендуется многими профессиональными сетевыми администраторами.

7. GlassWire

GlassWire - еще один инструмент, который настоятельно рекомендуется домашним пользователям. Он имеет простой и быстрый пользовательский интерфейс. Каждый может легко понять и работать с этим. Он собирает сведения о связи между вашей системой и другими IP-адресами и отображает их на экране.

8. Анализатор и сканер WiFi

Анализатор и сканер WiFi это простой, бесплатный и очень полезный инструмент для анализа сети Wi-Fi в вашем доме, поиска проблем с ней и их эффективного устранения.

Это приложение также поможет вам найти лучшее место для размещения вашего WiFi-роутера. Таким образом, можно получить лучший диапазон и скорость сети.

Выводы

Анализатор Wi-Fi необходим, когда вам нужно обеспечить максимальную производительность вашей сети Wi-Fi, а также избежать каких-либо проблем с сетью.

Пример программы Aircrack

- «Aircrack-ng» позволяет взламывать ключи WEP и WPA путём перебора паролей в файле-словаре;
- «Airodump-ng» являет собой анализатор трафика, может помещать трафик в файлы IVS или PCAP, показывает информацию о сетях;
- «Airdecap-ng» поможет в расшифровке перехваченного трафика при заранее известном ключе;
- «WZCook» поможет в восстановлении ключей WEP, отображает PMK (Pairwise Master Key) и так далее.
- «About» расскажет о текущей версии приложения и специфике улучшений программы.

Пример алгоритма взлома пароля Wi-Fi сети, которая зашифрована протоколом WPA используя Aircrack-ng.

Запустите программу, перейдите в первую вкладку «Aircrack-ng»;

- В строке «Filenames» указываем путь к файлу дампа с перехваченными пакетами (данный файл можно получить, использовав, к примеру, программу «CommView for WiFi»);
- В «Encryption» (шифрование) выбираем «WPA»;
- В строке «Wordlist» указываем путь к файлу, содержащему огромную базу вариантов паролей (его можно поискать в сети);
- Ставим галочку в «Advanced option» (Дополнительные опции);
- Ставим галочку в «Specify ESSID» и указываем там имя взламываемой нами Wi-Fi сети;
- Теперь ставим галочку в «Specify BSSID», и в открывшейся строке указываем MAC-адрес сети (с ним поможет та же «CommView for WiFi», во вкладке «Узлы» которой необходимо кликнуть правой клавишей мыши на нужной нам сети и выбрать в появившемся меню «Копировать MAC-адрес»);
- Затем кликаем на кнопку «Launch» (запуск) внизу и ждём нахождения правильного пароля. В зависимости от сложности пароля время поиска может занять от нескольких минут до 5-10 часов (а то и более).

Лабораторная работа №7

Применение учебной атаки на протокол WPS

Программа Reaver

В декабре 2011 Стефан Фибёк (англ. Stefan Viehböck) и Крейг Хеффнер (англ. Craig Heffner) рассказали о серьёзных прорехах в протоколе WPS. Оказалось, что если в точке доступа активирован WPS с PIN (который по умолчанию включен в большинстве роутеров), то подобрать PIN-код для подключения можно за считанные часы.

PIN-код состоит из восьми цифр — следовательно, существует 108 (100 000 000) вариантов PIN-кода для подбора. Однако количество вариантов можно существенно сократить. Дело в том, что последняя цифра PIN-кода представляет собой контрольную сумму, которая можно вычислить на основании первых семи цифр. Таким образом количество вариантов уже сокращается до 107 (10 000 000).

Авторизация по WPS предполагает отправку клиентом последовательности цифр PIN-кода и пакетов M4 или M6 и ответы на них от базовой станции. Если первые 4 цифры PIN-кода некорректны то получив их точка доступа отправит EAP-NACK сразу после получения M4, а если была ошибка в последних 3 цифрах правой части (8-ое число не считаем так как оно легко генерируется атакующим по формуле) — то после получения M6. Таким образом, недостаток протокола позволяет разделить PIN-код на две части, 4 начальные цифры и 3 последующие и проверять каждую часть на корректность отдельно используя базовую станцию как оракула, который подсказывает правильная ли последовательность цифр была отправлена.

Если PIN-код разбить на две части: Следовательно, получается 10^4 (10 000) вариантов для первой половины и 10^3 (1000) для второй. В итоге это составляет всего лишь 11 000 вариантов для полного перебора, что в более 9000 раз меньше исходного числа вариантов 10^8.

Таким образом вместо одного большого пространства значений 10^7 мы получаем два по 10^4 и 10^3, и, понятно, что $10^7 <> 10^4+10^3$. В итоге достаточно протестировать 11 000 комбинаций (больше 4-х цифр на тысячу) вместо 10 000 000.

Также были обнаружены уязвимости в генераторе случайных чисел маршрутизаторов некоторых производителей. Уязвимость получила название **pixie dust**. Для уязвимых роутеров можно получить pin после первой попытки и оффлайн-брутфорса.

Защита от взлома WPS

Защититься от атаки можно пока одним способом — отключить WPS с пином в настройках роутера. Правда, сделать это возможно далеко не

всегда, иногда WPS отключается только полностью. Самое большее, что могут сделать производители — выпустить прошивку, позволяющую вводить таймаут на блокировку функции, например, после 5 неудачных попыток ввода PIN-кода, что усложнит брутфорс и увеличит время подбора идентификатора злоумышленником.

Алгоритм атаки на WPS

1. Переводим беспроводной интерфейс в режим монитора
2. Ищем цели для атаки
3. Проверяем на подверженность Pixie Dust
4. Пробуем, подойдут ли ПИНы из базы данных известных ПИНов и сгеренированные по определённым алгоритмам.
5. Запускаем полный перебор, если предыдущие шаги не дали результата.
6. Если получен ПИН, но не показан WPA пароль, то запускаем команды для получения пароля от Wi-Fi.

Перевод беспроводной карты в режим монитора

Для поиска сетей с WPS, а также для атаки на них нам понадобиться перевести Wi-Fi карту в режим монитора.

Закрываем программы, которые могут помешать нашей атаке:

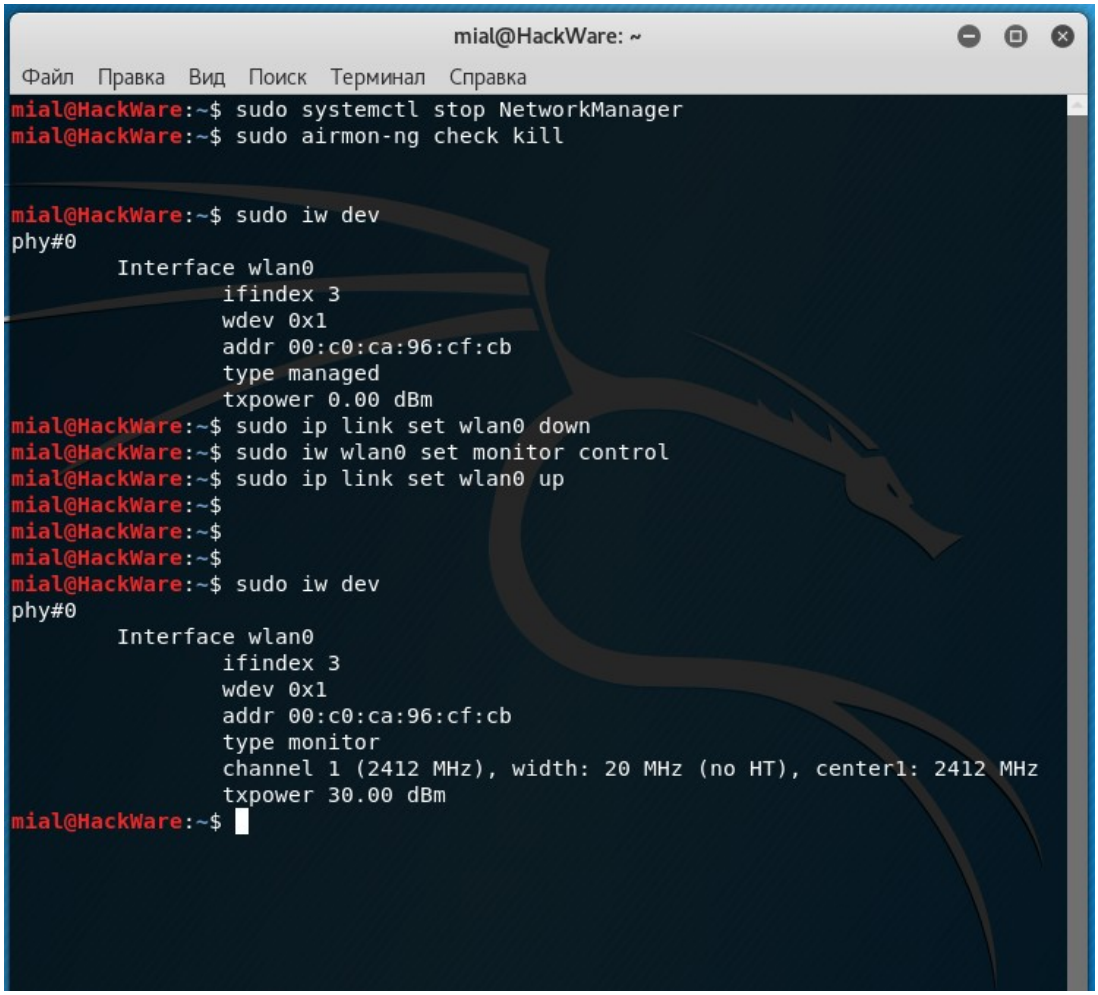
```
1 sudo systemctl stop NetworkManager
2 sudo airmon-ng check kill
```

Узнаём имя беспроводного интерфейса:

```
1 sudo iw dev
```

И переводим его в режим монитора (замените **wlan0** на имя вашего интерфейса, если оно отличается):

```
1 sudo ip link set wlan0 down
2 sudo iw wlan0 set monitor control
3 sudo ip link set wlan0 up
```



Новый сетевой интерфейс в режиме монитора также называется **wlan0**.

Если у вас другое имя беспроводного сетевого интерфейса, то во всех последующих командах вставляйте его вместо **wlan0**.

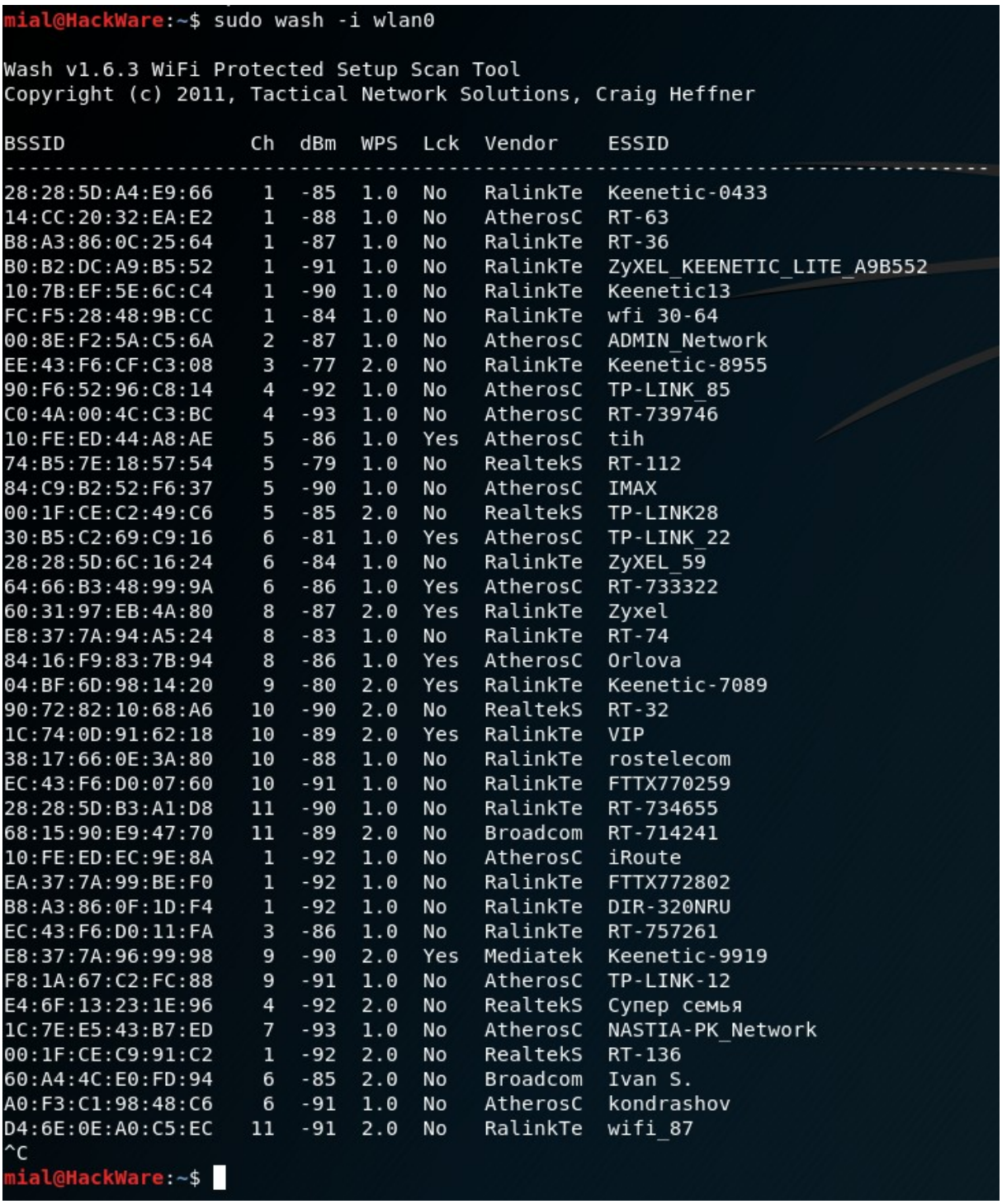
Поиск точек доступа с включённым WPS

Очень многие ТД имеют функционал по работе с WPS. Но у многих эта функция отключена, а у тех, у которых включена, может быть заблокирована (например, из-за нескольких неудачных попыток подбора ПИНа).

Чтобы собрать информацию о точках доступа мы воспользуемся программой Wash, которая поставляется вместе с Reaver и именно для этого и предназначена.

1 sudo wash -i wlan0

Через несколько минут работы программы будет выведен похожий список:



Для завершения работы программы **CTRL+c**.

Wash – это утилита для выявления точек доступа с включённым WPS. Выше показан пример исследования на live («живом») интерфейсе, также она может сканировать pcap файлы (несколько за один раз).

Wash показывает следующую информацию об обнаруженных точках доступа:

1 BSSID BSSID Точки Доступа (т.е. MAC-адрес)
2 Ch Канал ТД
3 dBm Уровень сигнала ТД
4 WPS Версию WPS, поддерживаемую ТД

5 Lck Статус блокировки WPS

6 Vendor Производитель ТД

7 ESSID ESSID (т.е. имя) Точки Доступа

Для атаки подходят только точки доступа, у которых в колонке **Lck** стоит **No**, т.е. у которых не заблокирован WPS.

По умолчанию wash выполняет пассивное исследование. Т.е. программа не отправляет какие-либо пакеты и остаётся абсолютно незаметной для возможных систем мониторинга беспроводной активности. Тем не менее, можно указать опцию **-s** и тогда wash будет отправлять probe requests (зондирующие запросы) к каждой ТД, это позволит получить больше информации о ТД.

Для того, чтобы проводить поиск на 5GHz 802.11 каналах используется опция **-5**.

Проверка на уязвимость Pixie Dust в Reaver

Атака Pixie Dust позволяет очень быстро получить ПИН. Но не все Точки Доступа подвержены этой уязвимости.

Для проверки конкретной ТД на эту уязвимость с помощью Reaver используется опция **-K**. Т.е. команда имеет следующий вид:

```
1 sudo reaver -i интерфейс -b MAC_адрес_ТД -K
```

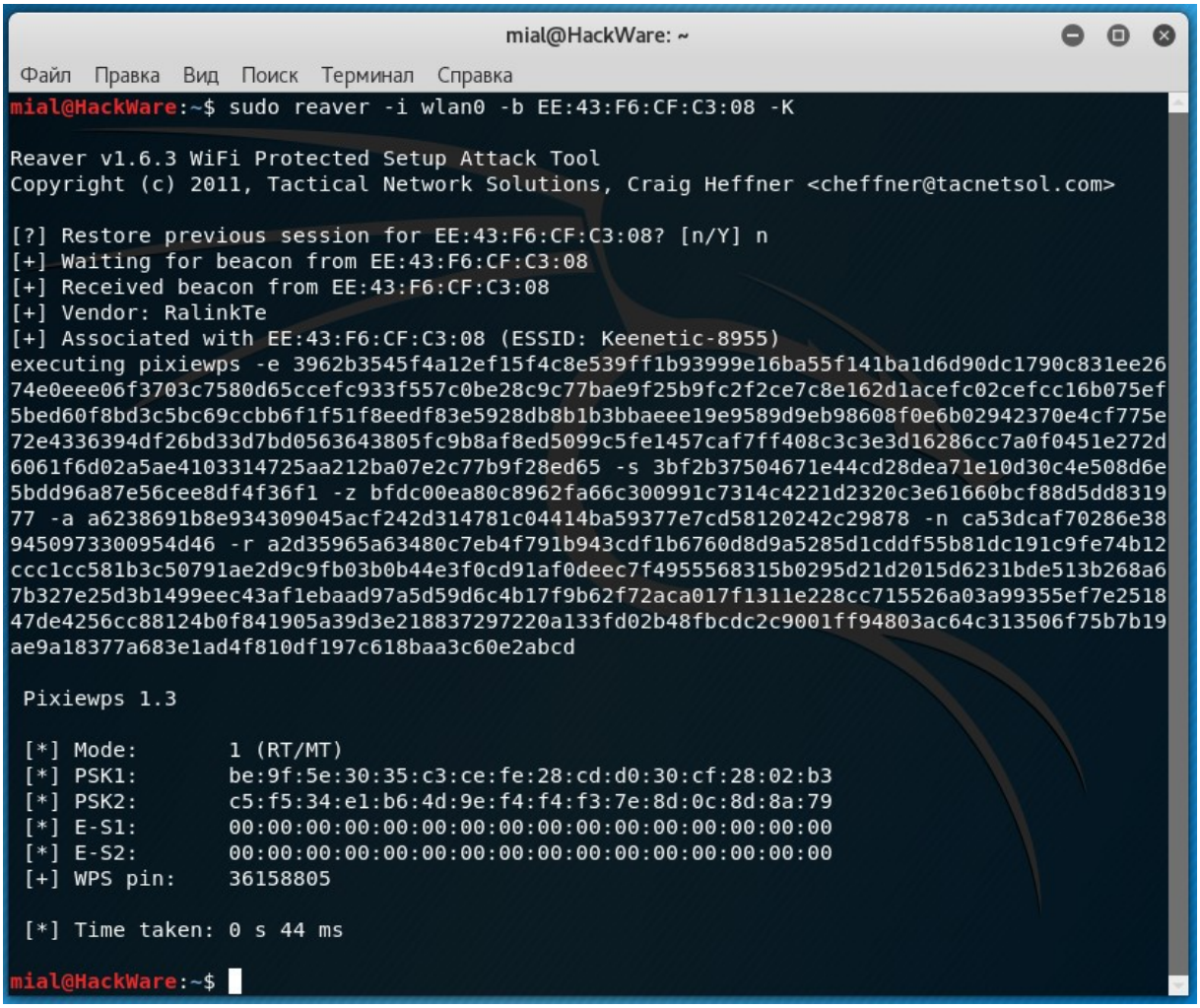
MAC адрес Точки Доступа можно взять из столбца BSSID полученного в Wash вывода.

К примеру, меня заинтересовала следующая точка доступа:

```
1 BSSID Ch dBm WPS Lck Vendor ESSID
2 ----------------------------------------------------------------------------
3 EE:43:F6:CF:C3:08 3 -81 2.0 No RalinkTe Keenetic-8955
```

Тогда команда для атаки будет выглядеть так:

```
1 sudo reaver -i wlan0 -b EE:43:F6:CF:C3:08 –K
```



Как можно увидеть на скриншоте, ТД оказалась уязвимой, и получен её WPS пин:

1 WPS pin: 36158805

При выполнении атаки Pixie Dust не происходит получение WPA пароля (пароля от Wi-Fi сети), как его узнать будет показано ниже.

Если точка доступа неуязвима к Pixie Dust, то прежде чем перейти к полному перебору рекомендуется попробовать наиболее вероятные варианты для атакуемой Точки Доступа.

Полный перебор WPS пинов с Reaver

Команда для запуска перебора похожа на предыдущую, но отсутствует опция, запускающая атаку Pixie Dust:

1 sudo reaver -i интерфейс -b MAC_адрес_ТД

Перебор WPS пинов может идти неудачно по многим причинам, поэтому для более подробного вывода, чтобы определить, в чём проблема, используются опции **-v**, **-vv** или **-vvv**. Как можно догадаться, чем больше букв **v**, тем больше будет выведено подробной информации.

Получение пароля Wi-Fi при известном WPS пине в Reaver

Если атака Pixie Dust прошла успешно, то показывается только ПИН. При полном переборе показывается и пин и WPA пароль. Если уже есть

пин, то для получения пароля Wi-Fi сети вам нужно в Reaver использовать опцию **-p**, после которой указать известный ПИН.

Лабораторная работа №8

Методы атак на сети Wi-Fi

Wireshark – для анализа сетей Wi-Fi. Wifite –захват рукопожатий, автоматическая деаутентификация клиентов, подмена MAC-адресов, перебор паролей.

- Взлом WPA / WPA2 паролей
- Атака на WEP
- Взлом WPS пина
- Понижение WPA
- Замена истинной точки доступа фальшивой
- Мошенническая точка доступа
- Атака на Wi-Fi точки доступа из глобальной и локальной сетей
- Атаки вида «отказ в обслуживании» (DoS Wi-Fi)
- Атаки на специфические сервисы и функции роутеров

Взлом WPA / WPA2 паролей

Это самая универсальная атака на Wi-Fi. Её плюсом является то, что она применима ко всем точкам доступа, которые используют WPA / WPA2 (таких большинство).

Есть и минусы, которые вытекают из силы (надёжности) WPA / WPA2. Они заключаются в том, что:

- для реализации атаки у ТД должны быть подключённые клиенты;
- расшифровка паролей ведётся брутфорсингом (методом перебора).

Т.е. при надёжном пароле взломать Wi-Fi за приемлемое время не получится.

Атака на WEP

В эту группу атак входят не только расшифровка пароля в виде простого текста. Для WEP открыт и реализован ряд разнообразных атак, которые позволяют получить желаемый результат даже без расшифровки парольной фразы.

К сожалению, сейчас взлом WEP уходит на второй план, поскольку постоянно уменьшается количество ТД, которые его исопльзуют.

Взлом WPS пина

Ситуация похожа на WEP. Хорошо поддаётся взлому, буквально недавно (меньше года назад) была выявлена новая прореха, которая вместо обычных часов на взлом WPS, требует несколько секунд.

И точно такая же беда как и у WEP — отсутствие универсальности. Всё меньше количество ТД, в которых WPS включён.

Понижение WPA

Чуть выше уже сказано, что WPA / WPA2 обеспечивает достаточно надёжную защиту, если пользователь не выбрал простой пароль. Поскольку с технической точки зрения новые методы не предложены до сих пор, было реализовано несколько методов социальной инженерии.

Производится постоянная деаутентификация Станций и ТД отправкой шифрованных пакетов WPA. Цель — убедить пользователь в неисправности протокола WPA и принудить его перейти на WEP или отключить шифрование. Эта атака реализована в mdk3. mdk3 разрешит клиентам работать с WEP или без шифрования, поэтому есть шанс, что системный администратор просто подумает «WPA сломалась» (что может произойти с некомпетентными сотрудниками). Это можно/нужно комбинировать с социальной инженерией.

Замена истинной точки доступа фальшивой

Суть в том, что точка доступа подавляется бесконечной отправкой пакетов деаутентифекации. При этом злоумышленник «поднимает» свою ТД со схожими характеристиками и ждёт пока пользователи подключаться к ней.

Далее под разными предлогами выманиваются пароли WPA/WPA2.

Наиболее закончено эту атаку может реализовать, например, wifiphisher.

Мошенническая точка доступа

Это не совсем атака на Wi-Fi. Скорее, это атака с использованием Wi-Fi.

Суть в том, что злоумышленник настраивает открытую точку доступа к Интернету. Ничего не подозревающие любители халявы к ней подключаются. А злоумышленник в это время реализует всевозможные атаки для перехвата паролей, сессий, кукиз или перенаправляет на мошеннические сайты.

Атака на Wi-Fi точки доступа из глобальной и локальной сетей

Это достаточно недооценённая проблема. Огромное количество людей имеют беспроводной роутер или модем дома. Как правило, дальше настройки Интернета и Wi-Fi мало кто доходит. Мало кто заботится о том, чтобы сменить пароль администратора, и уже совсем единицы вовремя обновляют прошивку устройств.

И всё это множество устройств с учётными данными admin:password прекрасны видны для сканеров в локальной или глобальной сети.

И уже есть реализации массовой атаки на дефолтные учётные данные и на известные уязвимости роутеров: Router Scan by Stas’M.

И с каждым годом количество и виды устройств, которые подключены к сети, только увеличивается. Естественным следствием этого является рост количества устройств, которые не настраивались вообще ни кем. К этим устройствам добавляются веб-камеры, файловые сервера, телевизоры с Wi-Fi (и с встроенными видеокамерами, между прочим), а также разные другие элементы интерьера «умного дома»,

Атаки вида «отказ в обслуживании» (DoS Wi-Fi)

Атака достаточно проста и весьма эффективна. Её смысл заключается в бесконечной отправки пакетов деаутентификации.

Защититься от такой атаки можно только подключившись к роутеру по проводу. Как и при всех других DoS атаках, утечка данных не

происходит. Только нарушается нормальная работа. Аналогично другим DoS атакам, после её прекращения всё само начинает работать в обычном режиме.

Атаки на специфические сервисы и функции роутеров

Современные продвинутые роутеры имеют USB порты, к которым можно подключить флешки, жёсткие диски, 3G модемы и прочую переферию. Роутеры, кроме своих обычных функций, могут быть файловыми серверами, веб-серверами, торрент-клиентами и т. д.

Здесь кроется две опасности: уязвимость какой-либо второстепенной службы, либо неправильная настройка (например, заводские пароли), которая позволит злоумышленнику перехватить контроль.

Расшифровка WPA трафика в Wireshark

При передаче по Wi-Fi трафик шифруется с использованием PTK (Pairwise transient key — можно перевести как Парный переходной ключ). При этом PTK является динамичным, то есть создаётся заново для каждого нового соединения. Таким образом получается, что Wi-Fi трафик для каждого соединения в одной и той же Точке Доступа зашифрован разными PTK, причём даже для одного Клиента после переподключения PTK меняется. Для вычисления PTK необходимы данные из четырёх этапного рукопожатия, а также пароль от Wi-Fi сети (на самом деле нужна ещё и другая информация, например имя (SSID) сети, но получение этих данных не является проблемой).

Главное, что нужно понять: для расшифровки Wi-Fi трафика необходимо четырёх этапное рукопожатие. Причём не любое, а именно то, которое произошло для передачи того трафика, который нужно расшифровать. Но для использования захваченного рукопожатия необходим пароль от Wi-Fi сети.

Итак, чтобы расшифровать Wi-Fi трафик нужны:

1) рукопожатие, произошедшее между Клиентом и Точкой доступа непосредственно перед обменом расшифровываемой информацией

2) пароль для подключения к Точке Доступа

Далее будет показано два примера захвата Wi-Fi трафика и его расшифровки. Первый захват данных выполнен с помощью Airodump-ng, а затем беспроводной трафик будет расшифрован в Wireshark. Во втором примере данные будут захвачены и расшифрованы с использованием только Wireshark.

Захват Wi-Fi трафика в Airodump-ng

Чтобы данные были пригодны для расшифровки, нужно чтобы Wi-Fi карта не переключала каналы, а выполняла захват информации на одном канале, на котором работает целевая Точка Доступа.

Смотрим имена беспроводных интерфейсов:

```
1          iw dev
```

Переводим ИНТЕРФЕЙС в режим монитора командами вида:

```
1	sudo ip link set ИНТЕРФЕЙС down
2	sudo iw ИНТЕРФЕЙС set monitor control
3	sudo ip link set ИНТЕРФЕЙС up
```

Запускаем airodump-ng командой вида:

```
1	sudo airodump-ng ИНТЕРФЕЙС
```

Тогда нужно перезапустить airodump-ng командой вида:

```
1	sudo airodump-ng ИНТЕРФЕЙС --channel КАНАЛ --write ИМЯ_ФАЙЛА
```

Надпись WPA handshake говорит о том, что было захвачено четырёх этапное рукопожатие. Это означает что:

- теперь мы сможем расшифровать Wi-Fi данные (если у нас есть ключ от Wi-Fi сети)
- мы сможем расшифровать данные только для конкретного клиента (с которым было совершено рукопожатие)
- мы сможем расшифровать данные, которые были отправлены только после этого захваченного рукопожатия

Расшифровка Wi-Fi трафика в Wireshark

Открываем файл захвата в Wireshark. В исходном виде трафик выглядит примерно так:

То есть без расшифровки мы видим только MAC-адреса участников передачи данных, пакеты некоторых видов, а также пакеты с данными — полезная нагрузка в которых зашифрована.

Перед расшифровкой убедимся, что имеется хендшейк, иначе продолжать нет смысла:

```
1	eapol
```

Перед расшифровкой нам нужно сделать некоторые изменения в настройках протокола IEEE 802.11.

Edit → Preferences, раскройте секцию protocol и выберите IEEE 802.11.

Нажмите кнопку Создать. В открывшемся окне в поле Key type выберите wpa-pwd, введите пароль от Wi-Fi сети, а через двоеточие имя (SSID) сети и нажмите ОК.

Например, в моём случае пароль 00001777, а имя сети Paangoon_2G, тогда я ввожу:

```
1	00001777:Paangoon_2G
```

Нажмите кнопку **Применить**:

Теперь там видны DNS, HTTP запросы и ответы, а также другие сетевые пакеты.

Если захвачен трафик не только для данной сети, но и для других сетей, работающих на этом же канале, либо для данной сети но других клиентов, для которых не захвачены рукопожатия, то этот трафик не будет расшифрован.

Захват Wi-Fi в Wireshark

Трафик Wi-Fi можно захватить непосредственно в Wireshark. Но нам предварительно нужно переключить Wi-Fi карту на тот же канал, на котором работает целевая Точка Доступа. Это делается командами вида:

```
1    sudo ip link set ИНТЕРФЕЙС down
2    sudo iw ИНТЕРФЕЙС set monitor control
3    sudo ip link set ИНТЕРФЕЙС up
4    sudo iw dev ИНТЕРФЕЙС set channel КАНАЛ
```

В этих командах нужно слова **ИНТЕРФЕЙС** и **КАНАЛ** заменить на действительные данные.

Когда интерфейс переключён на нужный канал, в Wireshark найдите этот интерфейс, в его свойствах поставьте галочку **Capture packets in monitor mode**.

Вывод

Для расшифровки WEP Wi-Fi трафика достаточно знать только пароль. Но ТД с WEP уже практически не встречаются.

WiFite — это скрипт, который эмулирует действия пентестера. Wifite зама в нужном порядке запускает необходимые программы и сама передаёт необходимые данные из одной в другую.

При типичном запуске Wifite только один раз задаст вопрос пользователю: какие точки доступа атаковать?

Можно запустить Wifite так, что она даже это не будет спрашивать — будет атаковать каждую ТД. Можно указать файл словаря — и программа совершенно автономно будет отправлять пакеты деаутентификации, захватывать рукопожатия, перебирать пароли, перебирать пины WPS и пытаться использовать WPS PixieDust, проводить разнообразные атаки на WEP. Причём, программа будет начинать атаку на самые слабые технологии и, в случае неудачи, переходить к более защищённым.

В зависимости от успеха, результатом работы программы может стать получение пароля в открытом виде, либо захваченных файлов рукопожатий — которые нужно брутфорсить для получения пароля в открытом виде.

Как запустить WiFite

Начать нужно с перевода беспроводной карты в режим монитора. Как это сделать рассказано в соответствующей статье «Как перевести беспроводную карту в режим монитора (контроля) в Kali Linux». В моём случае команда следующая:

```
1 ifconfig wlan0 down && iwconfig wlan0 mode monitor && ifconfi
wlan0 up
```

Нам в любом случае нужен файл словаря. Следующими командами мы его копируем в текущую рабочую директорию, распаковываем и чистим (чтобы все кандидаты в пароли удовлетворяли требованиям WPA паролей).

```
1 cp /usr/share/wordlists/rockyou.txt.gz .
2 gunzip rockyou.txt.gz
3 cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt
```

Ещё немного теории. WiFite это программа «полного цикла» по взлому Wi-Fi точек доступа. Она всё делает хорошо, но такой этап как перебор паролей можно делать не только хорошо — его можно делать на отлично. Процесс перебора паролей можно значительно ускорить, если использовать Pyrit, но уже требует определённых навыков.

Давайте начнём с совсем простого — пусть WiFite всё делает сама.

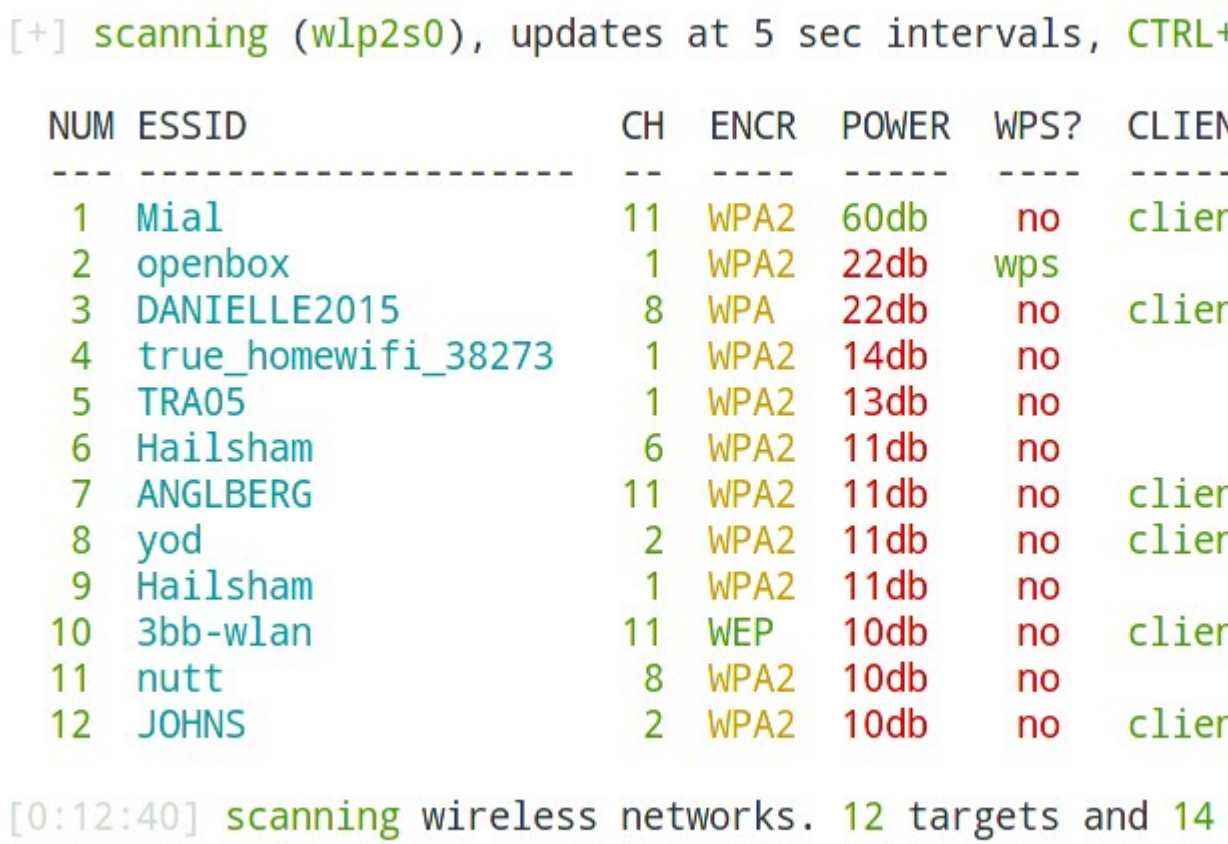
Автоматизированный взлом Wi-Fi в WiFite

Для этого программу WiFite нужно запустить с двумя дополнительными опциями:

- **--crack** говорит о том, что нужно производить взлом по словарю
- **--dict ~/newrockyou.txt** указывает, какой словарь использовать

1 sudo wifite --crack --dict ~/newrockyou.txt

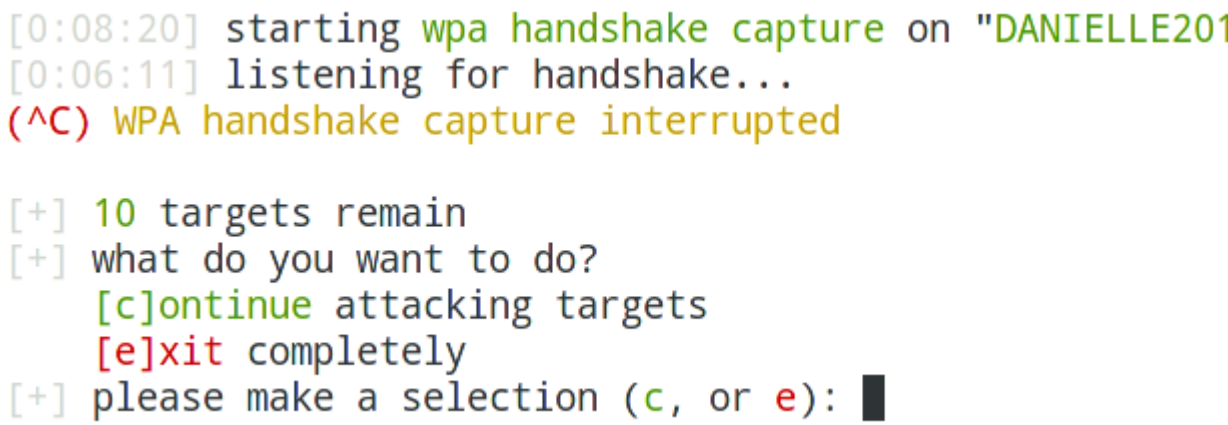
После запуска подождите несколько минут, пока программа соберёт информация о доступных точках доступа:



Когда информации достаточно, нажмите **CTRL+C**.

Нас попросят ввести номера точек доступа, которые мы хотим взломать. Можно выбрать все (нужно ввести all), можно выбрать отдельные ТД, перечислив их через запятую, можно выбрать диапазоны, перечислив их через дефис:

Дальше программа всё будет делать сама. Если вам показалось, что программа на слишком уж долго застряла на какой-либо точке доступа или на какой-либо атаке, то нажмите один раз CTRL+C для перехода к следующему действию. У нас спросят — мы хотим немедленно выйти или продолжить:



Наберите **c**, чтобы продолжить.

Полуавтоматический взлом с WiFite

Единственное отличие этой методики заключается в том, что для подбора пароля к захваченным рукопожатиям мы используем Pyrit. В этом случае мы запускаем wifite без ключей:

```
1 sudo wifite
```

В случае захвата рукопожатий, они будут только сохранены, перебор осуществляться не будет.

Для дальнейшей ускоренной расшифровки можно применять следующие инструкции:

- Взлом рукопожатий в Pyrit — самый быстрый способ с использованием графических процессоров и предварительного расчёта хешей
- Базовое и продвинутое использование oclHashcat (Hashcat) для взлома WPA/WPA2 паролей из хендшейков
- Взлом рукопожатий (handshake) с использованием графического процессора в Windows
- Массовый взлом рукопожатий в BlackArch с помощью Pyrit

Атака на все точки доступа с WiFite

Хотя WiFite и осуществляет автоматический взлом, тем не менее, вмешательство пользователя требуется как минимум один раз. - когда нам нужно выбрать точки доступа для атаки. С помощью ключа **--all** можно дать указание wifite атаковать вообще все точки доступа, в этом случае обойдётся какие-либо действия со стороны пользователя вообще не требуются.

```
1 sudo wifite --crack --dict ~/newrockyou.txt --all
```

Вывод по WiFite

WiFite — пожалуй, лучшая программа для новичков. Свои первые беспроводные точки доступа с ней можно взломать ничего не зная про рукопожатия, деаутентификацию, виды шифрования Wi-Fi и такие технологии как WEP, WPS.

По соотношению «затраченные усилия / полученный результат» для wifite нет равных. И тем не менее, развиваясь в вопросах пентестинга беспроводных сетей Wi-Fi, работая своими руками и головой можно добиться большего результата. Пентестеру с опытом достаточно быстрого взгляда, чтобы увидеть малоперспективные точки доступа (очень слабый сигнал или ни одного клиента), если пентестер обнаружит WPS, он не застрянет на нём на часы, остановив другую работу (wifite застрянет, это, в принципе, правильно, поскольку WPS является часто взламываемым). Пентестер попытался бы захватить все возможные рукопожатия, а потом, пока перебираются хеши, запустить атаки на WPS и WEP.

Возможно, это сильно зависит от условий, но при надлежащей сноровке у меня получает легче получить рукопожатия используя airodump-ng + aireplay-ng, чем используя wifite.

Кстати, для автоматизации захвата рукопожатий рекомендуется ознакомиться со статьёй по использованию нового инструмента zizzania: «Массовый автоматизированный захват рукопожатий в BlackArch с помощью zizzania».

Программа WiFite содержит множество опций, познакомиться с ними вы можете на странице документации в Энциклопедии инструментов для пентестинга.