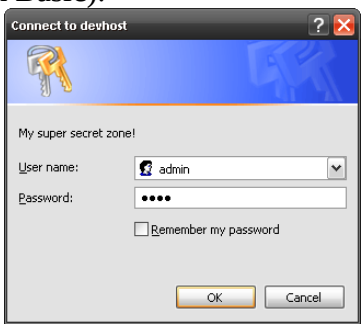
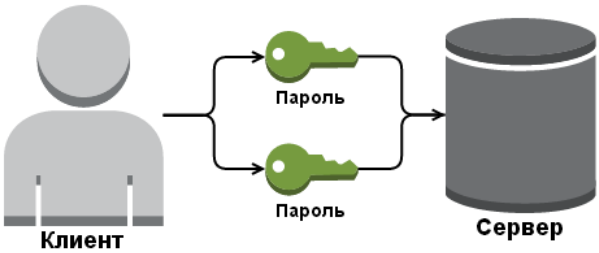
ЛЕКЦИЯ 3. УЯЗВИМОСТИ WI-FI. УСИЛИТЕЛИ И ГЛУШИТЕЛИ WI-FI. СЕТЕВЫЕ АППАРАТНЫЕ ШПИОНЫ

3.1. УЯЗВИМОСТИ WI-FI

Представьте, что вы — устройство, которое принимает инструкции. К вам может подключиться каждый желающий и отдать любую команду. Всё хорошо, но на каком-то этапе потребовалось фильтровать личностей, которые могут вами управлять. Вот здесь и начинается самое интересное.

Как понять, кто может отдать команду, а кто нет? Первое, что приходит в голову — по паролю. Пусть каждый клиент перед тем, как передать новую команду, передаст некий пароль. Таким образом, вы будете выполнять только команды, которые сопровождались корректным паролем. Остальные — в игнор. Именно так работает базовая авторизация HTTP (Auth Basic):



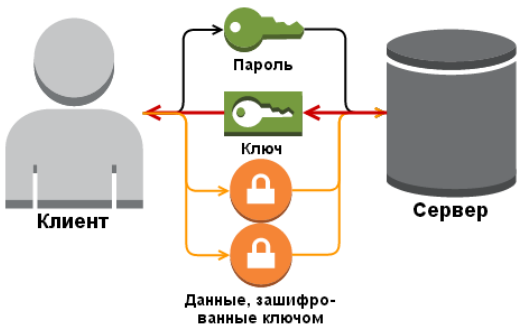


После успешной авторизации браузер просто-напросто будет передавать определённый заголовок при каждом запросе в закрытую зону, соответствующий логину и паролю.

У данного подхода есть один большой недостаток — так как пароль (или логин-пароль, что по сути просто две части того же пароля) передаётся по каналу «как есть» — кто угодно может встрять между вами и клиентом и получить ваш пароль на блюдечке. А затем использовать его и распоряжаться вами, как угодно!

Для предотвращения подобного взлома можно прибегнуть к хитрости: использовать какой-либо двухсторонний алгоритм шифрования, где закрытым ключом будет как раз наш пароль, и явно его никогда не передавать. Однако проблемы это не решит — достаточно один раз узнать пароль и можно будет расшифровать любые данные, переданные в прошлом и будущем, плюс шифровать собственные и успешно маскироваться под клиента.

Что делать? А поступим так, как поступают настоящие конспираторы: при первом контакте придумаем длинную случайную строку (достаточно длинную, чтобы её нельзя было подобрать, пока светит это солнце), запомним её и все дальнейшие передаваемые данные будем шифровать с использованием этого «псевдонима» для настоящего пароля. А ещё периодически менять эту строку — тогда джедаи вообще не пройдут.



Первые две передачи (зелёные иконки на рисунке выше) — это фаза с «пожатием рук» (handshake), когда сначала мы говорим серверу о нашей легитимности, показывая правильный пароль, на что сервер нам отвечает случайной строкой, которую мы затем используем для шифрования и передачи любых данных.

Итак, для подбора ключа хакеру нужно будет либо найти уязвимость в алгоритме его генерации (как в случае с Dual_EC_DRBG), либо арендовать несколько тысяч ATI-ферм для решения этой задачи. Всё это благодаря тому, что случайный ключ может быть любой длины и содержать любые коды из доступных 256, потому что пользователю-человеку никогда не придётся с ним работать.

Именно такая схема с временным ключом (сеансовый ключ, session key или ticket) в разных вариациях и используется сегодня во многих системах — в том числе SSL/TLS и стандартах защиты беспроводных сетей.

3.1.1. OPEN

OPEN — это отсутствие всякой защиты. Точка доступа и клиент никак не маскируют передачу данных. Почти любой беспроводной адаптер в любом ноутбуке с Linux может быть установлен в режим прослушки, когда вместо отбрасывания пакетов, предназначенных не ему, он будет их фиксировать и передавать в ОС, где их можно спокойно просматривать.

Именно по такому принципу работают проводные сети — в них нет встроенной защиты и «врезавшись» в неё или просто подключившись к хабу/свичу сетевой адаптер будет получать пакеты всех находящихся в этом сегменте сети устройств в открытом виде. Однако с беспроводной сетью «врезаться» можно из любого места — 10-20-50 метров и больше, причём расстояние зависит не только от мощности вашего передатчика, но и от длины антенны хакера. Поэтому открытая передача данных по беспроводной сети гораздо более опасна.

Если вам нужно пользоваться открытой сетью в кафе или аэропорту — используйте VPN (избегая PPTP) и SSL (https://, но при этом поставьте HTTPS Everywhere, или параноидально следите, чтобы из адресной строки «внезапно» не исчез замок, если кто включит sslstrip — что, впрочем, переданных паролей уже не спасёт), и даже всё вместе.

3.1.2. WEP

WEP — первый стандарт защиты Wi-Fi. Расшифровывается как Wired Equivalent Privacy («эквивалент защиты проводных сетей»), но на деле он даёт намного меньше защиты, чем эти самые проводные сети, так как имеет множество огрехов и взламывается множеством разных способов, что из-за расстояния, покрываемого передатчиком, делает данные более уязвимыми. Его нужно избегать почти так же, как и открытых сетей — безопасность он обеспечивает только на короткое время, спустя которое любую передачу можно полностью раскрыть вне зависимости от сложности пароля. Ситуация усугубляется тем, что пароли в WEP — это либо 40, либо 104 бита, что есть крайне короткая комбинация и подобрать её можно за секунды (это без учёта ошибок в самом шифровании).

WEP был придуман в конце 90-х, что его оправдывает, а вот тех, кто им до сих пор пользуется — нет. Основная проблема WEP — в фундаментальной ошибке проектирования. Как было проиллюстрировано в начале — шифрование потока делается с помощью временного ключа. WEP фактически передаёт несколько байт этого самого ключа вместе с каждым пакетом данных. Таким образом, вне зависимости от сложности

ключа раскрыть любую передачу можно просто имея достаточное число перехваченных пакетов (несколько десятков тысяч, что довольно мало для активно использующейся сети).

В 2004 IEEE объявили WEP устаревшим из-за того, что стандарт «не выполнил поставленные перед собой цели [обеспечения безопасности беспроводных сетей]».

3.1.3. WPA и WPA2

WPA — второе поколение, пришедшее на смену WEP. Расшифровывается как Wi-Fi Protected Access. Качественно иной уровень защиты благодаря принятию во внимание ошибок WEP. Длина пароля — произвольная, от 8 до 63 байт, что сильно затрудняет его подбор (сравните с 3, 6 и 15 байтами в WEP).

WPA отличается от WEP и тем, что шифрует данные каждого клиента по отдельности. После рукопожатия генерируется временный ключ — PTK — который используется для кодирования передачи этого клиента, но никакого другого. Поэтому даже если вы проникли в сеть, то прочитать пакеты других клиентов вы сможете только, когда перехватите их рукопожатия — каждого по отдельности.

Кроме разных алгоритмов шифрования, WPA(2) поддерживают два разных режима начальной аутентификации (проверки пароля для доступа клиента к сети) — PSK и Enterprise. PSK (иногда его называют WPA Personal) — вход по единому паролю, который вводит клиент при подключении. Это просто и удобно, но в случае больших компаний может быть проблемой — допустим, у вас ушёл сотрудник и чтобы он не мог больше получить доступ к сети приходится применять способ из «Людей в чёрном» менять пароль для всей сети и уведомлять об этом других сотрудников. Enterprise снимает эту проблему благодаря наличию множества ключей, хранящихся на отдельном сервере — RADIUS. Кроме того, Enterprise стандартизирует сам процесс аутентификации в протоколе EAP (Extensible Authentication Protocol), что позволяет написать собственный велосипед алгоритм. Короче, одни плюшки для больших дядей.

3.1.4. WPS/QSS

WPS, он же Qikk aSS QSS — интересная технология, которая позволяет нам вообще не думать о пароле, а просто нажать на кнопку и тут же подключиться к сети. По сути это «легальный» метод обхода защиты по паролю вообще, но удивительно то, что он получил широкое распространение при очень серьёзном просчёте в самой системе допуска — это спустя годы после печального опыта с WEP.

WPS позволяет клиенту подключиться к точке доступа по 8-символьному коду, состоящему из цифр (PIN). Однако из-за ошибки в стандарте нужно угадать лишь 4 из них. Таким образом, достаточно всего-навсего 10000 попыток подбора и вне зависимости от сложности пароля для доступа к беспроводной сети вы автоматически получаете этот доступ, а с ним в придачу — и этот самый пароль как он есть.

Учитывая, что это взаимодействие происходит до любых проверок безопасности, в секунду можно отправлять по 10-50 запросов на вход через WPS, и через 3-15 часов (иногда больше, иногда меньше) вы получите ключи от рая.

Когда данная уязвимость была раскрыта производители стали внедрять ограничение на число попыток входа (rate limit), после превышения которого точка доступа автоматически на какое-то время отключает WPS — однако до сих пор таких устройств не больше половины от уже выпущенных без этой защиты. Даже больше — временное отключение кардинально ничего не меняет, так как при одной попытке входа в минуту нам понадобится всего 10000/60/24 = 6,94 дней. А PIN обычно отыскивается раньше, чем

проходится весь цикл.

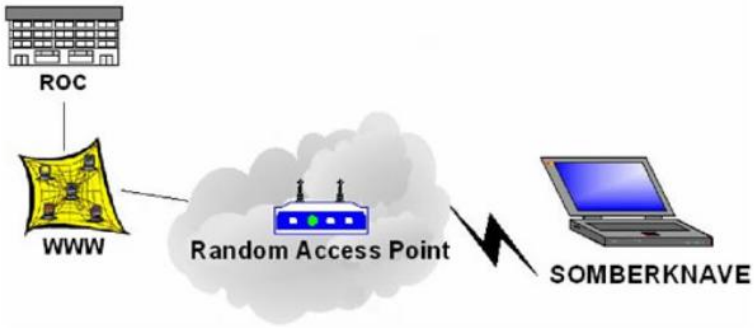
При включенном WPS пароль будет неминуемо раскрыт вне зависимости от своей сложности. Поэтому если нужен WPS — включайте его только когда производится подключение к сети, а в остальное время держите этот бекдор выключенным.

Выводы:

Используйте WPA2-PSK-CCMP с паролем от 12 символов a-z (2000+ лет перебора на ATI-кластере). Измените имя сети по умолчанию на нечто уникальное (защита от rainbow-таблиц). Отключите WPS (достаточно перебрать 10000 комбинаций PIN). Не полагайтесь на MAC-фильтрацию и скрытие SSID.

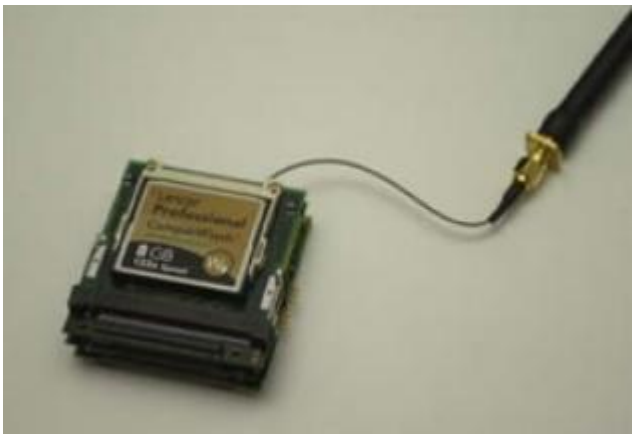
3.1.5. ШПИОНСКИЕ ЗАКЛАДКИ WI-FI

SOMBERKNAVE программная закладка работающая под Windows XP предоставляющая удаленный доступ к целевому компьютеру. Использует незадействованные Wi-Fi адаптеры, в случае, когда пользователь задействовал адаптер SOMBERKNAVE прекращает передачу данных.



NIGHTSTAND мобильный комплекс для проведения активных атак на Wi-Fi сети, целями являются машины под управлением Windows (от Win2k до WinXP SP2). Обычно используется в операциях, в которых доступ к цели невозможен. Комплекс реализован на базе ноутбука под управлением Linux и радиооборудования. Вместе с внешними усилителями и антеннами дальность действия может достигать 13 км.

SPARROW II встраиваемая компьютерная система под управлением Linux. Это полностью функциональная система для сбора данных о беспроводных сетях. Для расширения функционала имеет четыре встроенных Mini PCI слота позволяющие подключить GPS-модуль и дополнительные беспроводные сетевые карты.



3.2. УСИЛИТЕЛИ WI-FI

3.2.1. Усилитель Wi-Fi сигнала RE650

- Улучшенное вещание Wi-Fi – 4 внешние антенны для расширения покрытия до 1300 м2;
- 4 потоковый AC2600 двухдиапазонный Wi-Fi – скорость до 800 Мбит/с на 2,4 ГГц + до 1733 Мбит/с на 5 ГГц;
- 4×4 MU-MIMO – одновременная передача данных нескольким устройствам повышает производительность в 4 раза;
- Beamforming – вещание направленного Wi-Fi сигнала устройствам для более надёжных соединений;
- Гигабитный порт Ethernet – более быстрое проводное подключение для Smart TV, компьютеров и игровых консолей;
- Умный индикатор сигнала – позволит лучше установить устройство, отображая силу сигнала Wi-Fi в текущем месте;
- Режим точки доступа – создайте новую точку доступа Wi-Fi в дополнение к вашей проводной сети;
- Поддержка TP-Link Tether – простой доступ и управление вашей сетью с любого устройства на iOS или Android;
- Совместимость с любым Wi-Fi роутером или точкой доступа.

3.2.2. Усилитель Wi-Fi сигнала со встроенной розеткой RE360

- Расширение домашней сети Wi-Fi обеспечит общую скорость до 1,2 Гбит/с в двух диапазонах;
- Встроенная электрическая розетка;
- Умный индикатор сигнала позволит лучше установить устройство, отображая силу сигнала Wi-Fi;
- Работа с любым Wi-Fi роутером или Wi-Fi точкой доступа;
- Оригинальный дизайн для современного интерьера.

3.2.3. Усилитель Wi-Fi сигнала RE200

- Усиливает Wi-Fi в недоступных ранее местах, где невозможна прокладка кабеля;
- Совместим с беспроводными устройствами стандартов 802.11b/g/n и 802.11ac;
- Скорость беспроводной передачи данных в двух частотных диапазонах до 750 Мбит/с;
- Компактный размер и подключение к настенной розетке делают устройство удобным для установки и перемещения;
- Порт Ethernet позволяет усилителю функционировать в качестве двухдиапазонного беспроводного адаптера для подключения проводных устройств.

3.3. ПОДАВИТЕЛИ WI-FI

Технологии беспроводного Интернета Wi-Fi, а также частоты Bluetooth активно используются в технических средствах несанкционированного сбора информации. Множество камер, жучков, прослушивающих устройств используют данные стандарты беспроводной связи для передачи фиксируемого материала. Именно поэтому возникает необходимость в блокировке всех возможных сетей для предотвращения утечки важной личной или коммерческий информации.

3.3.1. Мобильный мультичастотный подавитель "Терминатор-15С (Интернет)

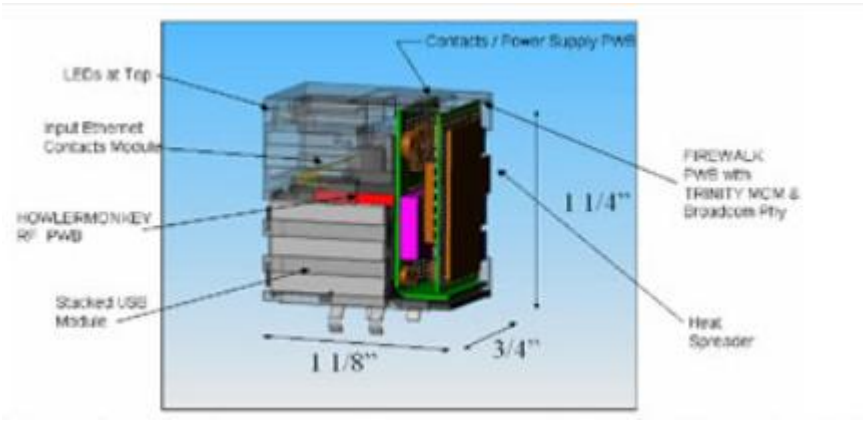
15-частотный автономный подавитель связи «Терминатор-15С (Интернет)» предназначен для блокировки сотовой связи в диапазонах GSM 900/1800, CDMA, 2G, 3G и 4G Mobile, мобильного интернета в диапазонах 2G GPRS и EDGE, 3G и 4G/LTE, а также беспроводных компьютерных сетей Wi-Fi и Bluetooth. Радиус эффективной работы подавителя составляет до 15 метров и может изменяться в зависимости от близости и мощности передатчиков мобильной связи и интернета.

Особенности:

- Блокировка всего мобильного интернета и сотовой связи;
- Подавитель способен создавать радиопомехи на 15 частотах 2G, 3G, 4G сетей, что предотвращает любую передачу данных через сотовую связь и мобильный интернет;
- Выбор частот подавления. Для настройки прибора под нужные задачи, кнопками на корпусе можно включать или отключать необходимые диапазоны частот блокировки, также можно одновременно включить все радиочастотные помехи;
- Автономная работа. Подавитель оснащен сменным аккумулятором 7,4В, 4700 мАч который позволяет использовать устройство без внешнего питания до 120 минут. Зарядка батарее осуществляется от адаптера или от прикуривателя;
- Активное охлаждение. Блокиратор оснащен двумя вентиляторами, которые охлаждают внутренние элементы устройства, что позволяет работать ему стабильно и более эффективно. Автомобильная зарядка. В комплекте к подавителю идет адаптер зарядки от автомобильного прикуривателя, что позволяет подзаряжать устройство в машине, там где нет доступа к сети 220В;
- Универсальный чехол. Позволяет его удобно носить на предплечье, что дает больше свободы в движении.

3.4. СЕТЕВЫЕ АППАРАТНЫЕ ЗАКЛАДКИ И ШПИОНЫ

FIREWALK аппаратная сетевая закладка, способная пассивно собирать трафик сети Gigabit Ethernet, а также осуществлять активные инъекции в Ethernet пакеты целевой сети. Позволяет создавать VPN туннель между целевой сетью и центром. Возможно установление беспроводной коммуникации с другими HOWLERMONKEY-совместимыми устройствами. Исполнение данной закладки аналогично COTTONMOUTH-III, такой же блок разъемов(RJ45 и два USB) на шасси. В основе лежит элементная база TRINITY, в качестве радиопередатчика используется HOWLERMONKEY.



LAN Turtle - это тайное средство администрирования систем и тестирования проницаемости, обеспечивающее скрытый удаленный доступ, сбор данных по сети и возможности мониторинга « человек-в-середине».

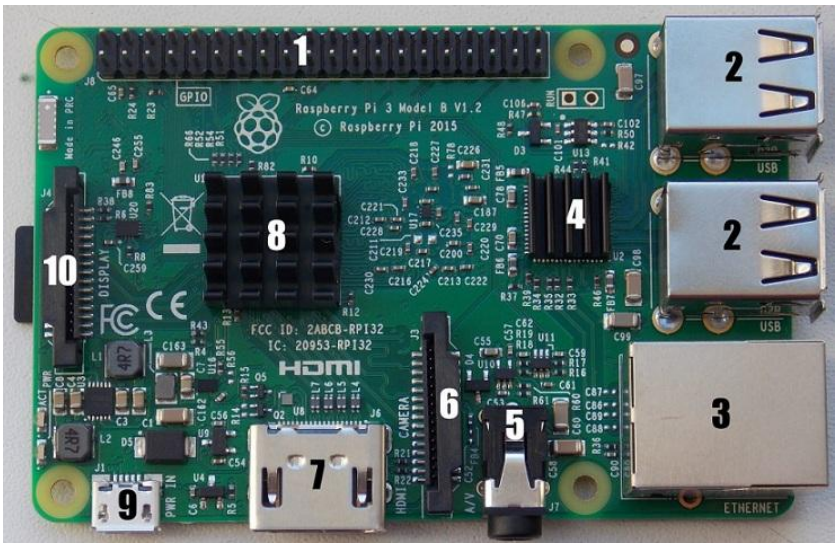
Размещенный в общем случае «USB-адаптер Ethernet», скрытый внешний вид LAN Turtle позволяет ему встраиваться во многие ИТ-среды.

3.5. УСТРОЙСТВА ДЛЯ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ WI-FI СЕТИ (RS WI-FI PENTESTER)

В настоящее время для аудита безопасности сетей Wi-Fi широко применяется ОС Kali Linux, содержащая готовые наборы программ для тестирования и поиска различных уязвимостей в сетях. С их помощью можно обнаруживать уязвимость Pixie Dust, слабые пароли WPA/WPA2, тестировать роутеры на отказоустойчивость. Но это достаточно трудоемкий процесс, требующий от пользователя определённого уровня знаний в операционной системе Linux. Кроме того, такая система будет стационарна, её достаточно проблематично перемещать с места на место.

Для решения этих проблем и было разработано устройство RS Wi-Fi Pentester. В его основе лежит концепция автоматизации и мобильности. Теперь от пользователя не требуется вводить длинные команды и уметь работать в Linux. Достаточно нажатия нескольких кнопок на смартфоне, и Вы получите всю информацию о уязвимостях в Вашей Wi-Fi сети.

Основой устройства RS Wi-Fi Pentester является одноплатный компьютер Raspberry Pi 3B. Он обладает рядом улучшений по сравнению с предыдущей моделью. В частности в нём стоит более мощный процессор ARM Cortex-A53 x64 с тактовой частотой 1,2 ГГц. Но ключевым отличием от прошлых версий является наличие беспроводных интерфейсов Wi-Fi и Bluetooth.



Более подробные характеристики Raspberry Pi 3B можно посмотреть в таблице ниже.

Характеристика	Значение
Процессор	ARM Cortex-A53 x64
Тактовая частота	1,2 ГГц
Количество ядер	4
ОЗУ	1 Гб
Проводные интерфейсы	• 40 портов GPIO (разъём PLD-40) • 4 порта USB 2.0 • Ethernet 10/100 Мб • Full HDMI • Аудио разъем 3,5 мм • Разъем для подключения CSI камеры • Разъем для подключения LCD дисплея
Беспроводные интерфейсы	• Wi-Fi 802.11n • Bluetooth 4.1
Напряжение питания	5 В через разъём microUSB

SD-карта – это очень важный компонент, т.к. именно на неё устанавливается операционная система, под управлением которой работает Raspberry Pi. От её быстродействия зависит скорость работы всей системы. Если SD-карта имеет слишком низкие значения скорости чтения/записи данных, то ОС может вообще не установится.

Адаптер беспроводной сети Wi-Fi является главным элементом любой системы. По большому счёту, важна не марка самого адаптера, а микросхема, на которой он основан. Бывают случаи, когда даже в адаптерах одного производителя и одной модели могут стоять разные микросхемы, следовательно, они могут работать по-разному. Одним из требований к микросхеме является возможность перевода адаптера в режим монитора для того, чтобы можно было проводить тестирование уязвимостей.

Одними из лучших адаптеров для пентестинга считаются адаптеры на микросхеме Ralink RT3070. Но во многих современных адаптерах стоит более дешёвая и урезанная версия этой микросхемы под названием Ralink RT3070L. Она показывает нестабильную работу, что выражается в плохой ассоциации с точкой доступа.

Лучшими адаптерами для пентестинга, основанными на этих микросхемах, считаются адаптеры Alfa Network AWUS 036H (на микросхеме Realtek rtl8187l) и Alfa Network AWUS 036NHA (на микросхеме Atheros AR9271). На рисунке ниже -- левый и правый соответственно. Последний отличается тем, что в нём добавлена поддержка сетей Wi-Fi 802.11n.

RS Wi-Fi Pentester работает под управлением ОС Kali Linux. Эта операционная система была изначально разработана для проведения тестов на безопасность различных сетей и систем и предоставляет готовый набор программ для этого. Мы выбрали версию Kali Linux 2016.2, т.к. она показывает стабильную работу на Raspberry Pi.

3.5.1. Приложение на Android