Применение программного комплекса “Kismet” для тестирования технологии Wi-Fi в сетях IoT

Установка и обзор программного комплекса Kismet

Kismet - это детектор беспроводной сети и устройств, сниффер, инструмент Wardriving и WIDS (беспроводная система обнаружения вторжений). Kismet идентифицирует сети пассивным сбором пакетом и выявляет сети, что позволяет ему находить (с учётом времени, раскрывая имена) скрытые сети и присутствие не-маячковых сетей через трафик данных. Работает с интерфейсами Wi-Fi (802.11b, 802.11a, 802.11g, 802.11n, 802.11ac), интерфейсами Bluetooth, некоторыми аппаратными средствами SDR (с программным обеспечением), такими как RTLSDR, и другим специализированным оборудованием для захвата. Kismet работает на Linux, OSX. В Linux он работает с большинством карт Wi-Fi, интерфейсами Bluetooth и другими аппаратными устройствами. В OSX он работает со встроенными интерфейсами Wi-Fi.Условно, задачи, решаемые с помощью Kismet можно разделить на две сферы: аналитика и защита. В первом случае накопленные сведения должны обрабатываться сторонними приложениями, а во втором Kismet работает в качестве детектора различного рода сетевых атак. Рассматривать оба профиля лучше на конкретных примерах. [14]

Установка

Перед началом установки Kismetнужно проверить поддерживает ли ваша Wi-Fiкарта режим мониторинга сетей RFMON. Эта функция позволяет переключить ваш адаптер в режим наблюдения, с помощью которого он производит захват всех пакетов, проходящих в эфире. Для каждой карты свой сценарий, некоторые поддерживают мониторинг из коробки, какие-то требуют сторонний драйвер, а отдельные адаптеры и вовсе не поддерживают RFMON.

Определение совместимости адаптера

У беспроводных карт есть два производителя. Первый - это бренд самой карты. Примерами производителей карт являются Netgear, Ubiquiti, Linksys и D-Link. Второй производитель – это тот, кто изготавливает беспроводной чипсет внутри карты. Знание производителя беспроводного чипсета позволяет определить, какие операционные системы поддерживаются, какие драйверы нужны и какие ограничения связаны с ними.

Определить производителя чипсета можно одним или несколькими из этих методов:

1) Поискать в интернете «чипсет <модель карты>» или «linux модель вашей карты». Довольно часто можно найти ссылки на то, какой набор микросхем использует ваша карта и / или опыт других людей. Это, безусловно, самый простой и успешный способ определения чипсета.

2) Можно взглянуть на имена файлов драйвера Windows, довольно часто оно совпадает с именем чипсета.

4) Проверьте страницу производителей карт, иногда они указывают, какой чипсет используется.

5) На некоторых картах, таких как PCI, вы можете физически видеть беспроводной чип, на них должна быть маркировка, по которой можно определить чипсет.

6) Все беспроводные устройства, продаваемые в США, должны быть одобрены Федеральной комиссией связи (FCC). Эти же устройства обычно продаются по всему миру. Каждое устройство должно иметь идентификационный номер (ID) FCC на самой плате. Если у вас есть этот идентификатор, то вы можете использовать Поиск идентификатора FCC для поиска подробной информации об устройстве. Это даст вам производителя, модель и, как правило, чипсет.

Производители карт добавляют путаницу, сохраняя тот же номер модели карты, но меняя чипсет внутри себя. Здесь вы услышите термин «cardrevision»(ревизия карты) или «cardversion»(версия карты). Поэтому сначала определите, относится ли информация о чипсете к вашей карте. Версия, как правило, указывается на карте и располагается рядом с серийным номером или MAC-адресом.

7)При использовании Linux существует множество способов получения информации о карте и, возможно, определения набора микросхем. Команда «dmesg» довольно часто может содержать подробные сообщения, указывающие, какая карта была обнаружена и чипсет.

Если карта является картой ISAbus(IndustryStandartArchitecture, Шина Архитектуры Промышленного стандарта), то информацию о карте получить не получится.

Если карта является картой PCI(Peripheralcomponentinterconnect, взаимосвязь периферийных компонентов), вам необходимо использовать команду «lspci -nn» для отображения строк идентификации карты. В некоторых случаях, например, на картах с чипсетами Broadcom, только это может раскрыть чипсет. «-Nn» должно вызвать отображение PCI ID. Примером того, как выглядит PCI ID, является «168c: 0013» для карты чипсета Atheros. Как только у вас есть PCI ID, то можно поискать информацию на интернет-сайтах, которые ищут по ним. Также отображаются требуемые и используемые модули ядра. Это может быть очень полезно при идентификации чипсета.

Если аппаратное обеспечение является USB-ключом, вам нужно использовать команду «lsusb» для отображения строк идентификации ключа. В некоторых случаях «lsusb» не работает (например, если usbfs не смонтирован), и вы можете получить идентификационные строки из журнала ядра, используя «dmesg» (или в / var / log / messages).

Команда «lsmod» может использоваться для просмотра загруженных модулей. Если беспроводная карта была обнаружена автоматически, можно

иногда работать в обратном направлении, основываясь на загруженных модулях, чтобы определить набор микросхем. [15]

Установка программы

Для данной работы была выбрана операционная система Ubuntu 18.04.2 LTS. Актуальная версия Kismetдля этой системы 2019-04-R1.

Ход установки программы

1) Для начала нужно проверить систему на наличие старых версий программы и удалить таковые, если они имеются.Для этого нужно ввести команду:

```
sudoaptremovekismet.
```

2) Установить дополнительные библиотеки, которые требуются для работы Kismet, они доступны почти для всех дистрибутивов. Для систем Ubuntu/Debian/Kali/Mintэто делается командой:

```
sudoaptinstallbuild-essentialgitlibmicrohttpd-devpkg-config zlib1g-dev libnl-3-dev libnl-genl-3-dev libcap-devlibpcap-devlibnm-devlibdw-dev libsqlite3-dev libprotobuf-devlibprotobuf-c-devprotobuf-compilerprotobuf-c-compiler libsensors4-dev.
```

(В некоторых старых версиях libprotobuf-c-dev может называться libprotobuf-c0-dev.)

3) Скопируйте Kismetиз git, если не сделали этого ранее:

```
git clone https://www.kismetwireless.net/git/kismet.git
```

Если же у вас имеется репозиторийKismet, то выполните:

```
cdkismet
gitpull
```

4) Запустите настройку. Это позволит узнать все особенности вашей системы и подготовить Kismet к компиляции. Если у вас есть какие-либо отсутствующие зависимости или несовместимые версии библиотеки, они будут отображены здесь.

```
cdkismet
```

```
./configure
```

Обратите внимание на резюме в конце и следите за любыми предупреждениями! Сводка покажет основные функции и выдаст предупреждения о пропущенных зависимостях, которые сильно повлияют на скомпилированный Kismet.

5) Скомпилируйте Kismet:

```
make
```

6) Установите Кисмет. Как правило, вам нужно установить Kismet как suid-root; Kismet автоматически добавит группу и соответственно установит двоичные файлы захвата.

После установки suid-rootKismet запускает двоичные файлы, которые управляют каналами и интерфейсами с необходимыми привилегиями, но будет поддерживать декодирование пакетов и веб-интерфейс без полномочий root:

```
sudomakesuidinstall.
```

1) Добавьте своего пользователя в группу kismet.

`sudousermod -aGkismet$` (имяпользователя)

Это добавит вашего текущего зарегистрированного пользователя в группу kismet.

2) Выйдите из системы и авторизируйтесь снова. Linux не обновляет группы, пока вы не войдете в систему. Если вы только что добавили себя в группу Kismet, вам придется заново войти в систему.

3) Убедитесь, что вы находитесь в группе Kismet с:

```
groups
```

Если вы не в группе Kismet, вы должны полностью выйти из системы или перезагрузиться.

4) Теперь все готово, чтобы запустить Kismet. Направьте его на свой сетевой интерфейс. Ваш интерфейс может быть wlan0 или wlan1, или он может называться наподобиеwlp3s0(в нашем случае), или он может быть

назван с использованием MAC-адреса карты и выглядеть как wlx00c0ca8d7f2e.

Теперь можно запустить Kismet командой:

`kismet -c` (ваше устройство)

или вы можете просто запустить Kismet, а затем с помощью интерфейса выбрать карту, которую хотите использовать, запустив с помощью всего лишь:

`kismet`. [16]

Подготовка к работе

В первый раз, когда вы запускаете Kismet, нужно перейти в веб-интерфейс Kismet и в первый раз, когда вы запускаете Kismet, нужно перейти в веб-интерфейс Kismet и установить свой логин и пароль(как показано на рисунке 6).Этот логин будет сохранен в файле конфигурации:~ / .kismet / kismet_httpd.conf, который находится в домашнем каталоге пользователя, запускающего Kismet.Если вы запускаете Kismet как или с помощью sudo (или с помощью сценария запуска системы, где он запускается с правами root), это будет в корневом каталоге root: /root/.kismet/kismet_httpd.conf.

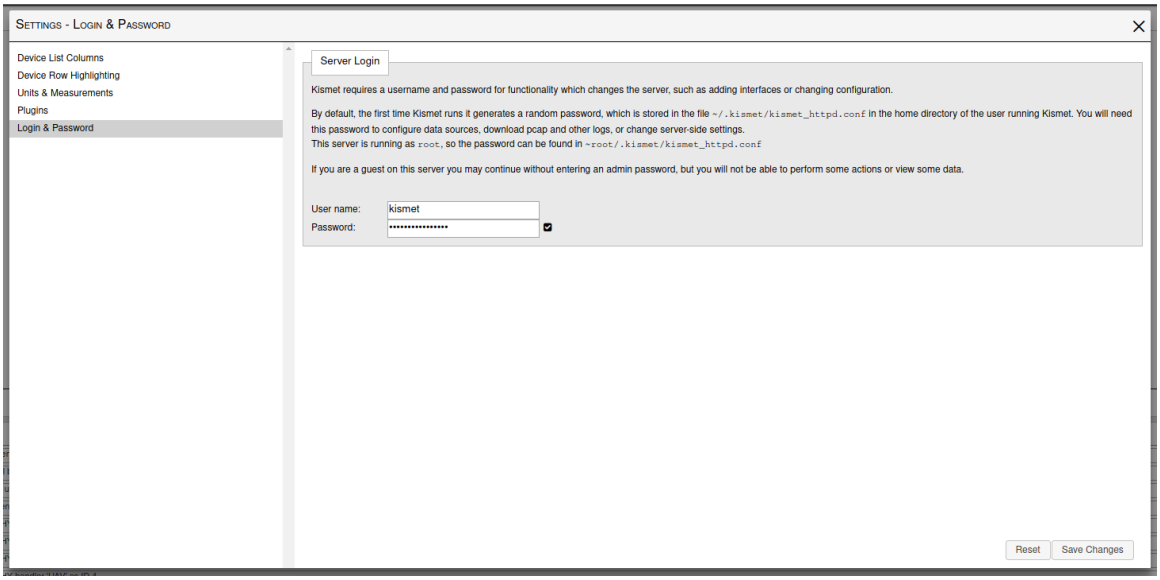

Рисунок 6 – настройка логина и пароля

Этот пароль понадобится вам для управления Kismet с веб-страницы - без него вы все равно сможете просматривать информацию об устройствах, просматривать распределение каналов и большинство других действий, но вы не сможете контролировать источники данных Kismet, просматривать pcaps или выполнять другие действия. Перейдите по ссылке http://localhost:2501, там будет предложено выполнить базовую настройку - Kismet имеет множество опций в веб-интерфейсе, которые можно настроить.[17]

Обзор программы

После того, как вы настроите данные для входа, вы найдете относительно пустой интерфейс, если вы не предоставили источник данных в командной строке или в файлах конфигурации.

Для того чтобы добавить источник, нужно зайти во вкладку DataSources, выбрать нужное устройство и нажать Enable (как показано на рисунке 7). Работающий источник данных показывает тип, интерфейс, каналы, параметры переключения и т. Д. Их можно настроить в веб-интерфейсе.

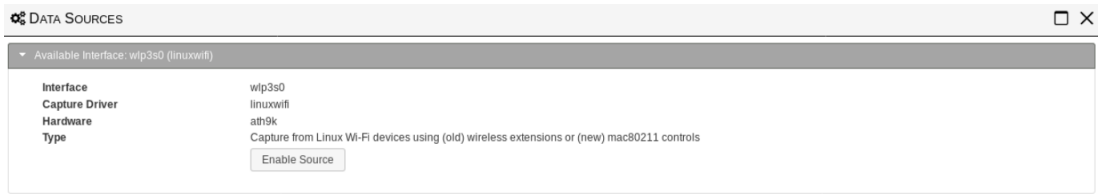

Рисунок 7 – окноDataSources

Для Wi-Fiустройств доступны разные настройки. В первой строке можно поставить мониторинг с помощью этого устройства на паузу (**Paused**) или возобновить его (**Running**). Во второй строке можно выбрать прослушивать один канал (**Lock**) или автоматическое переключение по каналам (**Hop**). На следующей строке можно выбрать каналы, которые вы

хотите прослушивать. Пример захватываемой информации можно увидеть на рисунке8.

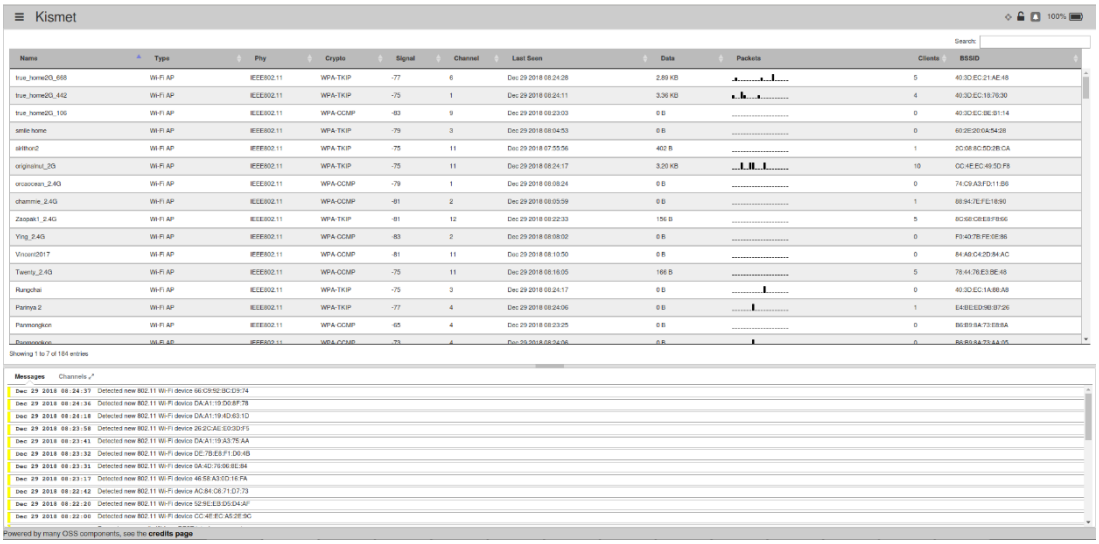

Рисунок8 – пример захватываемой информации

Теперь, когда источник данных работает, основной интерфейс начнет показывать устройства, сообщения, оповещения и другое. Собранная информация будет доступна в веб-интерфейсе, в консоль выводятся важные сообщения, в том числе сообщения об ошибках и подсказки, как показано на рисунке 9.

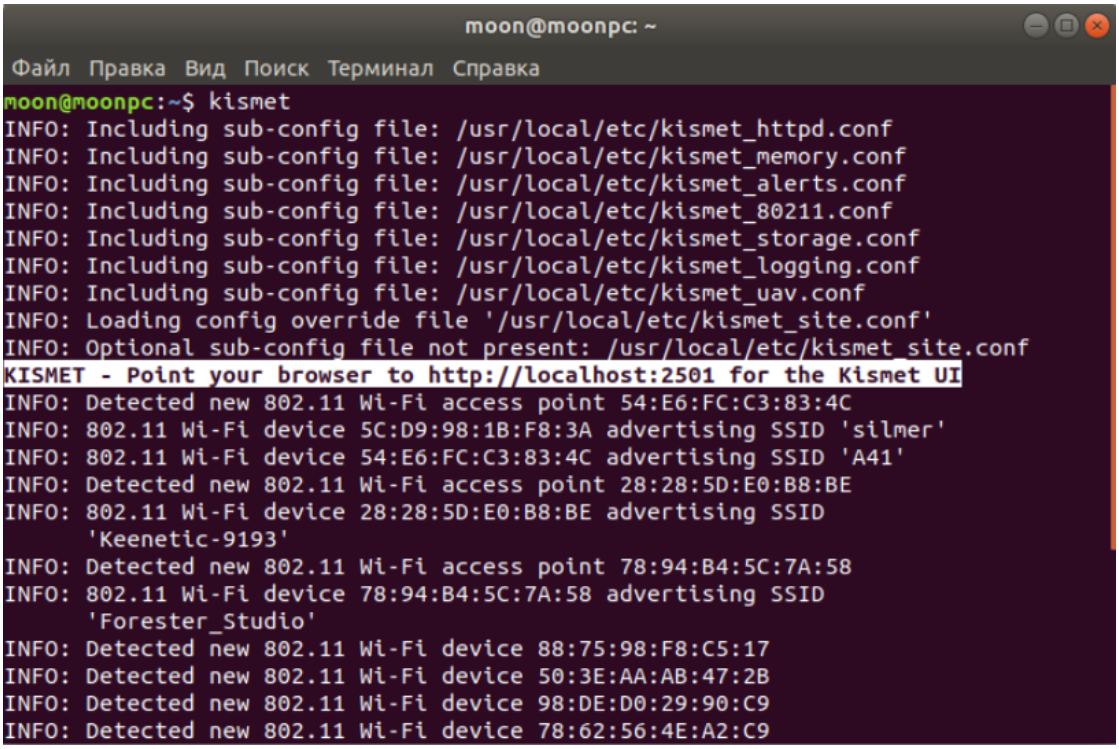

Рисунок 9 – логипрограммы в терминале

По этой информации можно произвести поиск, сортировку по различным признакам, можно кликнуть на нужное устройство и посмотреть подробную информацию о нем, пример показан на рисунке 10.

Для просмотра клиентов точки доступа нужно нажать на нее и открыть вкладку Wi-Fi (802.11), там можно будет увидеть MACадреса всех ассоциированных клиентов, как показано на рисунке 11.

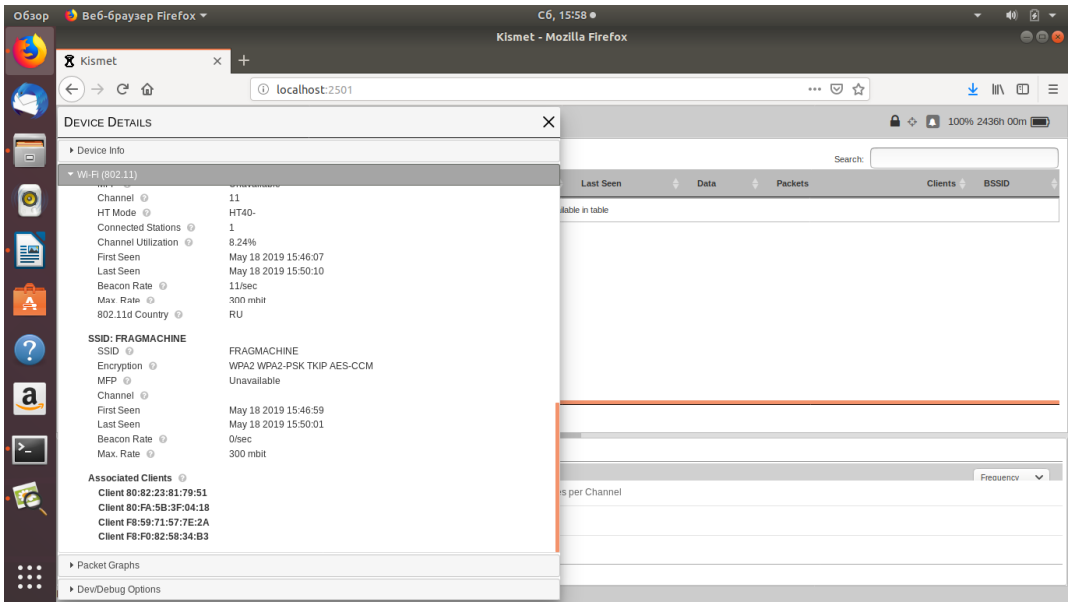

Рисунок 10 – ассоциированные клиенты сети Wi-Fi

Рисунок 11 – подробная информация об устройстве

В правом верхнем углу основного интерфейса находятся значки состояния.Строка состояния может быть расширена с помощью плагинов, а по умолчанию включает статус входа в систему (заблокирован или разблокирован), статус GPS, активные оповещения, а также состояние аккумулятора или питания.При нажатии на оповещения откроется подпанель с перечнем оповещений.

Веб-интерфейс имеет полную систему управления настройками. Столбцы в списке устройств можно перемещать и добавлять дополнительные столбцы (или удалять исходные столбцы).Подсветка строк также может быть настроена.

С помощью вкладки ‘Memorymonitor’ можно просмотреть использование памятипрограммой, пример на рисунке 12.

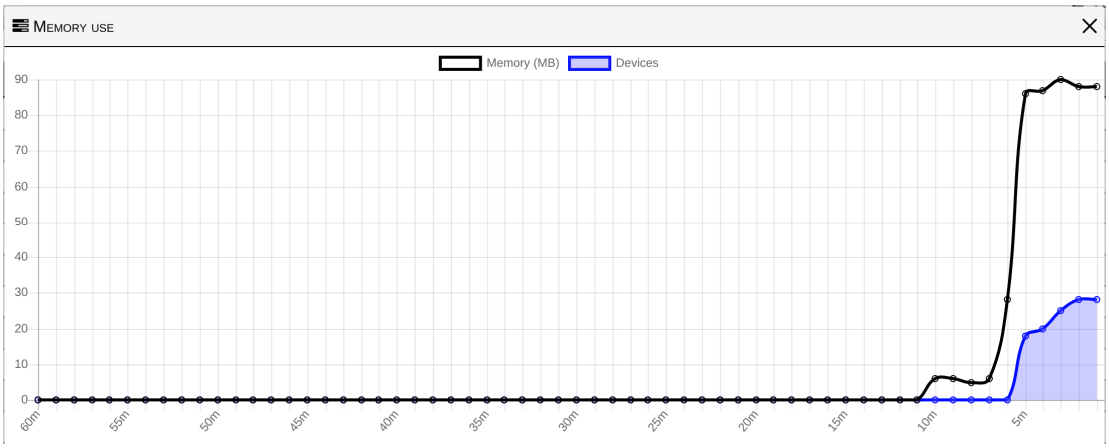

Рисунок 12 – окно использования памяти программой

Kismet также имеет встроенные дисплеи для покрытия канала несколькими источниками данных, а также оценочную схему переключения каналов (переключение каналов обычно происходит слишком быстро, чтобы отобразить реальное представление канала, на котором находится каждый источник данных). [17]

Пример использования программы

Ситуация: имеется Точка Доступа к которой я могу подключиться, но которая находится довольно далеко и из-за этого связь иногда разрывается.

Цель: определить направление, в котором находится целевая ТД, чтобы верно повернуть направленную антенну.

Вместо направленной антенны, например, можно использовать Wi-Fi адаптер с обычной антенной, но переставлять его в разные места комнаты/квартиры, для определения места с наилучшим сигналом связи.

Итак, целевая точка доступа Paangoon_2G, рассмотрим её характеристики на рисунке 13.

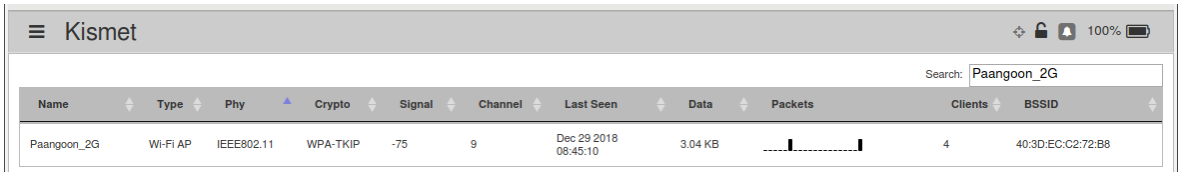

Рисунок 13 – характеристики точки доступа

Точка Доступа работает на 9 канале, уровень сигнала с обычной антенной -75 dbm. Ставим на паузу все ненужные источники данных, включаем адаптер с направленной антенной и настраиваем его прослушивать только 9 канал.Переходим в настройке выбора подсвечиваемых данных и ставим галочку напротив Active. Это включит подсветкуцветом активных точек доступа. Активными считаются те, от которых получены какие-либо данные в течение последних 10 секунд. Дело в том, что если Точка Доступа больше не видна, то она не пропадает из списка и в качестве уровня сигнала показывает последнее значение. Поэтому иногда не сразу можно понять, что ТД уже давно не видна.Пробуем повернуть антенну или перенести Wi-Fi адаптер в разных направлениях. Также можно попробовать разные антенны.

Чем больше значение поля Signal (отрицательные величины чем ближе к нулю, тем они больше) — тем лучше сигнал. В некоторых направлениях сигнал будет ухудшаться, а если цвет выделения строки с ТД сменился с голубого на белый, то ТД больше не видно. Данные могут изменяться просто от невидимых нам причин. Не нужно торопиться с перемещением антенны или адаптера, так как данные обновляются не сразу.[18]

Сбор GPSинформации

Создать собственную машину StreetView, которая будет заниматься т.н. вардрайвингом не так сложно, как кажется на первый взгляд. Из дополнительного оборудования потребуется лишь GPS-приемник для привязки данных к географическому расположению.

Для начала сбора информации устройство GPS должно быть подключено и настроено для работы через демон GPSD. Нужно отметить, что Kismet работает с форматом JSON и поэтому использовать для тестов эмуляторы GPS не получится, разве только входящую в комплект GPSD утилиту gpsfake, которая может проигрывать существующие логи навигаторов. Впрочем, настройка GPS выходит за рамки обсуждения Kismet.

В этот раз сервер необходимо запустить в режиме протоколирования чтобы начать сбор информации. По умолчанию будет доступно 5 видов логов: тревожный протокол, географический XML-лог, текстовой список обнаруженных сетей, сетевой XML-лог и дамп пакетов в формате Pcap.

Если всё сделано правильно, то теперь в главном окне будут отображаются данные о текущем географическом положении. Вопреки распространенному мнению, Kismet не знает координат Wi-Fi точки, а географические данные — не более чем координаты GPS-приемника. И хотя при наличии большого количества информации запеленговать точку вполне реально, программа не ставит себе такую задачу — это дело сторонних продуктов.В процессе движения логи будут быстро расти, поэтому следует подумать о свободном объеме памяти.

Данные, полученные программой сохраняются в простом понятном формате. Так, например, интересующий нас, географический XML-лог состоит измножеставатакихэлементов:

```
<gps-point bssid="00:0C:42:2C:DA:C6" source="00:0C:42:2C:DA:C6" time-
sec="1280155487" time-
usec="724329" lat="47.133453" lon="28.504967" spd="0.000000" heading="0.200000" f
ix="3"alt="1225.000000" signal_dbm="-61" noise_dbm="0"/>
```

Все атрибуты интуитивно понятны и разобраться с данными не составит труда любому программисту. Как использовать эти данные —

решение разработчика. Можно построить карту Wi-Fi точек доступа в своем районе, можно разработать систему пеленгации. В Google заявили о сборе этих данные для псевдо-GPS навигации, когда в качестве ориентира используются не спутники, а базовые станции. Комбинируя данные из различных логов можно собирать статистику, анализировать, составлять карты и графики — всё ограничивается лишь фантазией. Любой может построить в своем автомобиле часть GoogleStreetView и заняться какой-нибудь полезной исследовательской деятельностью. [19]

Обнаружение вторжений

У Kismet есть и более серьезная, хоть и менее востребованная функциональность. Не секрет, что многие предприятия используют Wi-Fi для внутренней связи. Информация в таких сетях зачастую не предназначена для широкой общественности. Защита беспроводного эфира — не менее важная мера, чем любая другая, направленная на поддержание уровня внутренней безопасности. Kismet может обнаруживать большой список сетевых атак на канальном и сетевом уровне. Для этого в программе реализован механизм тревожного оповещения, или попросту говоря — алерты.

Правила тревоги для конкретного случая указываются в конфигурационном файле. Рассмотрим работу системы обнаружения вторжений на примере правила APSPOOF. Этот, пожалуй, один из самых простых методов — он позволяет распознать атаку, в ходе которой злоумышленник выступает в роли поддельной точки доступа. Конфигурация этого правила выглядит так:

```
apsproof=Rule1:ssid="Politia",validmacs="70:3A:02:01:CE:AF"
```

Validmacs — допустимые значения MAC адреса для точки доступа с именем «Politia», которую необходимо защитить. Спровоцированную с помощью

любой программы атаку, Kismet обнаруживает мгновенно, о чем и сообщает в окне Alerts и логе. Точно таким же образом настраиваются и другие правила тревоги. Использовать Kismet для защиты беспроводных сетей не сложнее чем захватывать пакеты, а в совокупности с другими мерами общий уровень защищенности становится значительно выше. [19]

Перехват трафика с анализом пакетов для открытых и закрытых сетей

Для просмотра перехваченного трафика можно использовать программы-анализаторы трафика, например, WireShark.

Wireshark — программа-анализатор трафика для компьютерныхсетей Ethernet и некоторых других. Функциональность, которую предоставляет Wireshark, очень схожа с возможностями программы tcpdump, однако Wireshark имеет графический пользовательский интерфейс и гораздо больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим.

В открытой сети трафик шифроваться не будет, соответственно, для просмотра нужно просто открыть его в программе WireShark. Для дешифрования трафика закрытой сети нужно зайти в настройки 802.11 и мы увидим окно (Рисунок 14), где можно ввести полученные ключи, которые можно перехватить либо ARPспуфингом либо перехваченным рукопожатием.[20]

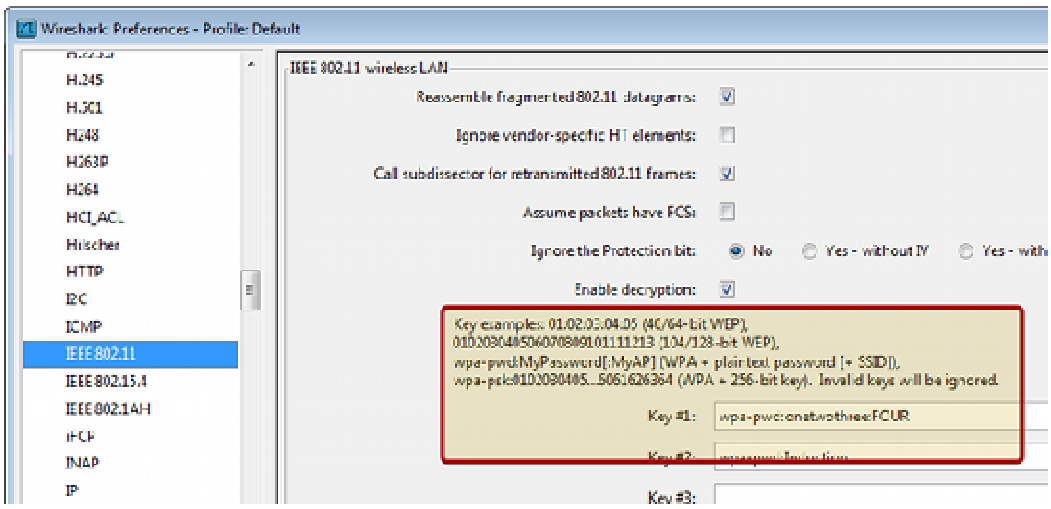

Рисунок 14 – окно настроек 802.11 WireShark

Поиск скрытых сетей

Для примера была взята сеть FRAGMACHINE. Переводим сеть в скрытый режим(показано на рисунке 15).

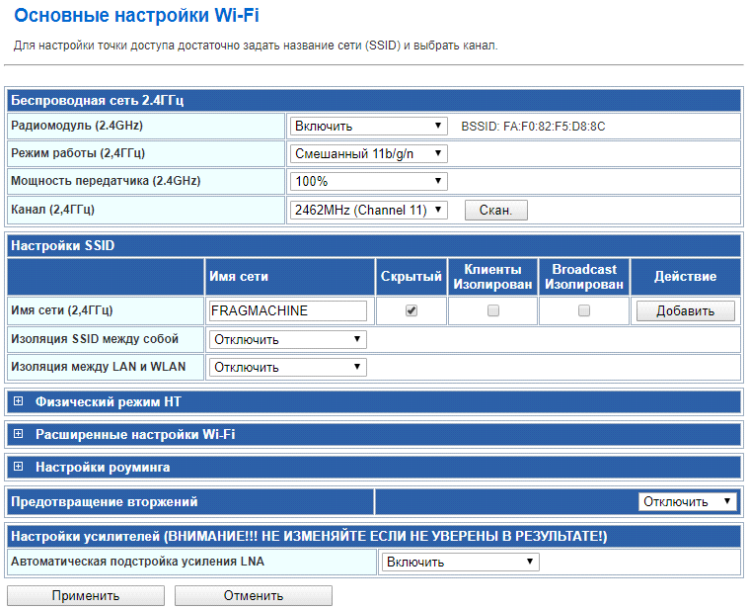

Рисунок 15 – настройки сети FRAGMACHINE

Теперь сеть является скрытой, но Kismetвсе равно обнаружил её, показано на рисунке 16.

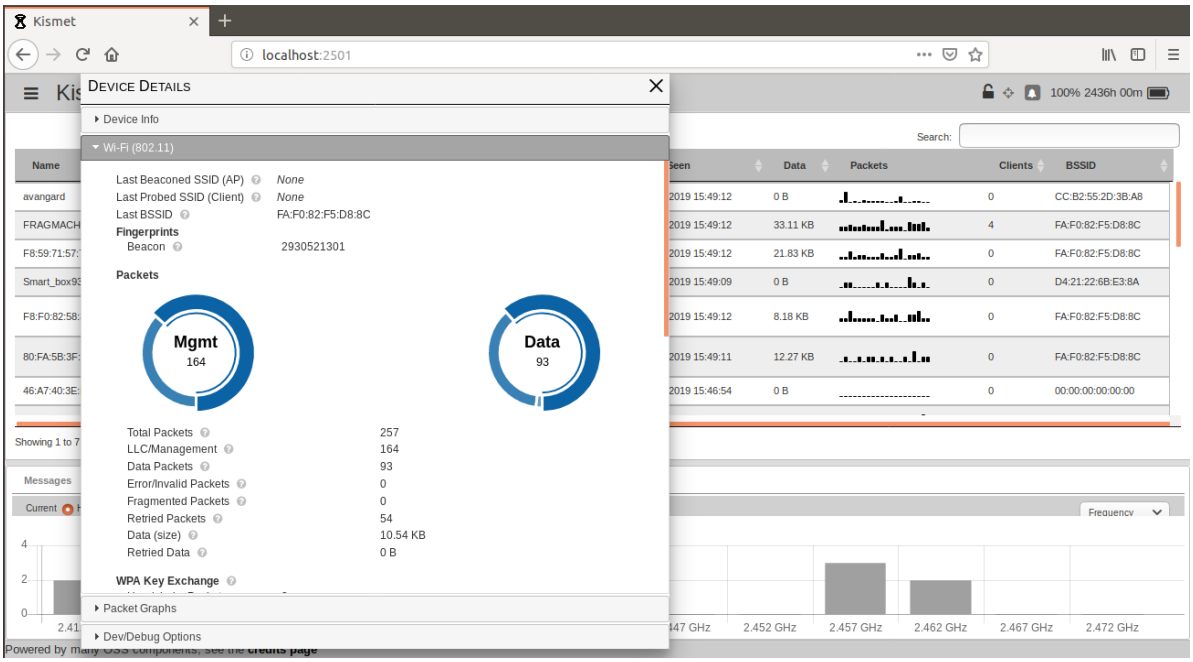

Рисунок 16 – информация о скрытой сети FRAGMACHINE.

Сценарии атак на WEP/WPA

Для атак будет использована связка программ Kismetи Aircrack-NG. Алгоритм показан на рисунке 17.Для атаки на WEP, запускаем Kismetи ищем сети с типом шифрования WEP. Найдя, переписываем BSSIDи Channeladрес сети. Цель выбрана, теперь нужно заняться ловлей пакетовдля расшифровки при помощи Aircrack-NG. Запускаем утилиту командой:

sudoairodump-ng –i --bssid (здесь вписываем ранее записанный SSID) –c (здесь вписываем ранее записанный Channel)–w (имя файла для пойманных пакетов) (интерфейс).

Ловля пакетов запущена. В теории для подбора ключа может хватить и двух пакетов, но в реальности нужно более десяти тысяч пакетов. После того как наберется нужное число пакетов, запускаем программу подбора ключей:

aircrack-ng (имя файла пойманных пакетов)

Если все прошло успешно, то программа выдаст ключ, если нет, то напишет при каком количестве пакетов нужно будет повторить поиск ключа.[21]

Рисунок 17 – Блок схема проведения атаки на WEP

ВслучаеатакинаWPA/WPA2 всевыглядитнамногопроще, ноприйтикконечномурезультатугораздо сложнее. Алгоритм показан на рисунке 18. Для начала находим нужную нам сеть через Kismetи выписываем MACадреса точки и клиентов, подключенных к данной сети. Теперь, чтобы начать перебор пароля, нам нужно поймать рукопожатие, для этого отключаем клиента от сети командой:

aireplay-ng -0 1 -a (MACточкидоступа) -c(MACклиента)(интерфейс)

После отключения клиента от станции, он подключится обратно, тогда-то программа перехватит рукопожатие и уведомит об этом сообщением «WPA handshake: (MAC адрес точки доступа)». Если этого не произошло, то снова используем aireplay-ng, пока не добьемся положительного результата. Когда же рукопожатие будет поймано, то запускаем aircrackс использованием словаря командой:

aircrack-ng -w (имясловаря.lst) -b (MACадресточкидоступа) (файлрукопожатия.cap)

В данном случае результат зависит напрямую от наличия нужного пароля в используемом словаре, поэтому шансы получить пароль прямо пропорциональны размеру и качеству словаря.

Рисунок 18 – Блок схема алгоритма проведения атаки на WPA/WPA2

Лабораторная работа 1. Ознакомление с программой Kismet.

1 Задание

Ознакомиться с назначением и основами работы с программой Kismet.

2 Теоретические сведения

Описано в разделах 2.3, 2.7, 2.8 ВКР.

3 Порядок выполнения работы

1. Запустить программу и выбрать источник данных.
2. Включить точки доступа в разных режимах: открытая-видимая, открытая-скрытая, закрытая-видимая, закрытая-скрытая.
3. Подключиться к точкам доступа.
4. Ознакомиться со списком точек доступа.
5. Посмотреть клиентов и к каким сетям они относятся.
7. Сохранить лог файл программы и открыть его в Wireshark.

4 Содержание отчета

1. Титульный лист согласно приложению.
2. Скриншот каждой сети и их клиентов.
3. Сделать выводы о сетях по перехваченным пакетам.
4. Приложить лог файлыKismetв форматах pcap, xml.

5 Контрольные вопросы

1. Открытые и закрытые точки доступа

2. 802.11b
3. 802.11g
4. 802.11n
5. 802.11ac

Лабораторная работа 2. Изучение перехваченных пакетов.

1 Задание

Изучение работы и возможностей утилиты Kismet.

2 Теоретические сведения

Описано в разделах 2.3, 2.7 ВКР.

3 Порядок выполнения работы

1. Постройте сеть, топология которой представлена на рисунке 18.

Рисунок 18 – топология сети

2. Включите и настройте ТД на разные каналы и имена сетей. Также включите внутренний DHCP сервер ТД.
3. Подключите 2 компьютера к разным сетям.
4. Запустите Kismetна 3 компьютере, посмотрите обнаруженные сети.
5. Определите каналы для каждой ТД.

6. Посмотрите, какие типы пакеты перехватываются, когда компьютеры ассоциированы, но не активны. Наблюдайте за графиком количества перехваченных пакетов в секунду.
7. Подключите к 3 компьютеру дополнительный беспроводной интерфейс и ассоциируйте его с одной из точек доступа.
8. Выполните взаимодействие между двумя компьютерами, находящимися в одной сети (например, скопируйте файл с помощью scp). Какие типы пакетов появились в эфире? Как изменился график?
9. Определите клиентов обнаруженных сетей.

4 Содержание отчета

1. Титульный лист.
2. Рисунок топологии сети со всеми адресами.
3. Сделать выводы по графику перехваченных пакетов, когда клиенты не активны и во время передачи данных.
4. Приложить логфайлыKismet в формате pcap, xml.

3.2.5Контрольные вопросы

1. Фреймы управления
2. Фреймы контроля
3. Фреймы данных

Лабораторная работа 3. Проведение и обнаружение атаки с помощью программ Kismetи Aircrack-NG.

1 Задание

Используя полученные навыки в прошлых лабораторных работах по программе Kismetобнаружить атаку, произведенную на сеть с помощью программы Aircrack-ng.

2 Теоретические сведения

Описано в разделах 1.4.3, 2.3, 2.6, 2.9 ВКР

3 Порядок выполнения работы

1. Построить сеть показанную на рисунке 19.

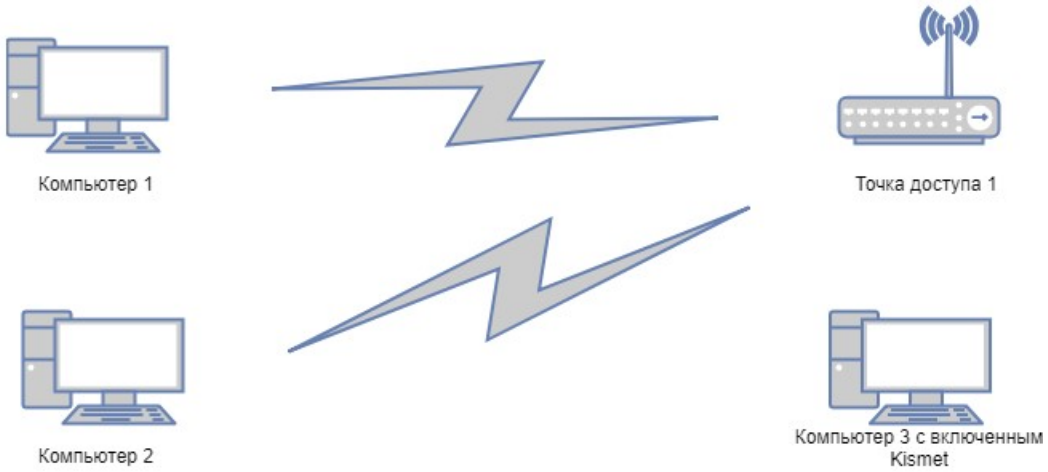

Рисунок 19 – топология сети

2. Настроить точку доступа и подсоединиться к ней первым компьютером.
3. Настроить Kismetдля обнаружения посторонних соединений посредством изменения файла kismet_alerts.conf.
4. Включить Kismetв режиме мониторнинга.

5. Включить Aircrack-ngна компьютере 2 и произвести атаку на сеть.
6. Обнаружить атаку в Kismet.

4. Содержание отчета

1. Титульный лист.

2. Рисунок топологии сети со всеми адресами.

3. Сделать выводы по графику перехваченных пакетов, когда клиенты не активны и во время передачи данных.

4. Также приложить лог-файл Kismet в формате xml.

5.Контрольные вопросы

1. Атака на WEP.
2. Атака на WPA2.
3. Атака человек-посередине.