МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра компьютерных систем

Станкявичуте Кристина Сергеевна

ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ И ЗАЩИЩЕННОСТИ СЕТИ WI-FI

БАКАЛАВРСКАЯ РАБОТА
по основной образовательной программе подготовки бакалавров
по направлению 09.03.02 – Информационные системы и технологии

г. Владивосток
2018

Студент гр. Б8418 _____
подпись
«_____» _____ 2018 г.

Научный руководитель к.ф.-м.н., доцент
(должность, ученое звание)
_____ Е.В. Пустовалов
(подпись) (и.о.ф)
«_____»_____ 2018 г.

Защищена в ГАК с оценкой _____

Секретарь ГАК

_____ _____
подпись И.О.Фамилия

«_____» _____ 2018 г.

«Допустить к защите»

Заведующий кафедрой ___к.ф.-м.н., доцент___
(ученое звание)

_____ Е.В. Пустовалов
(подпись) (и. о.ф)

«_____»_____ 2018 г

Аннотация

Выпускная квалификационная работа на тему: «Оптимизация производительности и защищенности сети Wi-Fi»

Автор: Станкявичуте Кристина Сергеевна, студентка 4 курса

Выпускная квалификационная работа 44 с., 3 ч., 16 рис., 3 табл., 10 источников.

КЛЮЧЕВЫЕ СЛОВА

Беспроводная сеть Wi-Fi, оптимизация, безопасность, производительность, факторы, уязвимость, стандарты 802.11, тестирование.

Цель выпускной квалификационной работы: улучшить качество сигнала и безопасность исследуемой сети Wi-Fi

Цель выпускной квалификационной работы может быть достигнута путем решения следующих задач:

- Исследование основных принципов работы сети
- Исследование факторов, влияющих на производительность и защищенность беспроводной сети
- Поиск и изучение средств тестирования производительности и защищенности беспроводной сети
- Анализ и оптимизация используемой сети с применением найденных средств

Выпускная квалификационная работа состоит из введения, трех глав и заключения.

В введении обосновывается актуальность выбранной темы, формулируются цели, и ставится основная задача работы.

В первой главе выполняется обзор основных программных средств для тестирования производительности и защищенности сети Wi-Fi.

Во второй главе подробно описывается возможные методы достижения поставленной цели и обосновывается выбор лучшего из них.

В третьей главе представлена реализация решения поставленной задачи.

Заключение содержит выводы, основанные на полученных результатах.

Введение

В последнее время все больше пользователей предпочитают использовать сети Wi-Fi для подключения к Интернету. Что неудивительно, так как Wi-Fi позволяет получить доступ с любого устройства, не заставляя пользователя задумываться о подключении кабеля.

Но этим пользуются и злоумышленники, которые все чаще используют Wi-Fi для проведения атак на различные системы. Что вызвано не только удобством в использовании технологии, но и тем, что безопасностью беспроводных сетей часто пренебрегают. Например, на последней пресс-конференции форума Positive Hack Days 8 эксперт Positive Technologies представил доклад о том, что при проведении специалистами тестирования на проникновение беспроводных сетей российских и зарубежных компаний, они смогли успешно попасть в систему в 68% случаев.

Все вышесказанное подтверждает актуальность темы, так как именно в разгар развития информационного общества и технологий в целом, необходимо следить за безопасностью используемых сетей Wi-Fi и не забывать о производительности для обеспечения эффективной защиты.

Вследствие чего, была сформулирована основная цель выпускной квалификационной работы: проанализировать и протестировать имеющийся маршрутизатор для принятия решения о необходимых действиях для улучшения его работы, безопасности и качества передаваемого им сигнала беспроводной сети.

Для выполнения поставленной цели необходимо решить следующие задачи:

- Исследовать основные принципы работы беспроводной сети
- Исследовать факторы, влияющие на производительность и защищенность беспроводной сети
- Поиск и изучение средств тестирования производительности и защищенности беспроводной сети

- Анализ и оптимизация используемой сети с применением найденных средств.

.

Глава 1. Обзор средств тестирования производительности и защищенности сетей Wi-Fi

1.1 Средства тестирования защищенности Wi-Fi сети

Чаще всего для тестирования защищенности применяются различные дистрибутивы Linux с установленным пакетом утилит. Дальше будут рассмотрены самые популярные из них.

1.1.1 Kali Linux

Kali Linux — это один из дистрибутивов Linux, разработанный для хакеров и специалистов информационной безопасности. Согласно разработчикам дистрибутив предназначен: «Для тестирования на проникновения и этичного хакинга».

Kali Linux наполнен различными программами и инструментами для тестирования безопасности. Есть графические программы, а есть команды терминала, также в систему включено несколько базовых утилит, таких, как просмотр изображений, калькулятор, и текстовый редактор. Но нет офисных программ, почтовых клиентов и органайзеров.

По умолчанию пользователь дистрибутива root. Это необходимо, так как многим программам для работы нужны права суперпользователя.

Вот примеры программ, которые установлены по умолчанию на Kali Linux и могу быть использованы в тестировании сети на защищенность.

1.1.1.1 Утилиты Aircrack-ng

Утилиты Aircrack-ng позволяют взламывать ключи WEP, выполнять мониторинг трафика, перебирать ключи WPA-PSK, и захватывать ключи установки соединения Wi-Fi.

1.1.1.2 Kismet

Утилита-детектор беспроводных сетей для выявления вторжения. Также может использоваться для выявления скрытых сетей и взлома паролей.

1.1.1.3 Wireshark

Инструмент для анализа и захвата сетевого трафика. Позволяет находить проблемы и уязвимости в работе сети [1].

1.1.2 BlackArch Linux

BlackArch Linux – специализированная модификация Arch Linux, созданная для проведения тестирования на возможность проникновения специалистами по безопасности. Она спонсируется хакерской группой NullSecurty.

BlackArch обладает списком в более чем 1900 различных программ и утилит для тестирования безопасности. Функционал многих из них схож между собой, что создает некоторые трудности для неопытных пользователей в работе с данным дистрибутивом.

Так же, как и в Kali Linux, данный дистрибутив не обладает «обычными» программами для работы, что делает его нелучшим вариантом в качестве основной системы. Но его легкая графическая оболочка позволяет установить дистрибутив на слабый/низкопроизводительный компьютер в качестве постоянной рабочей системы специалиста по безопасности [1].

1.1.3 Parrot Security OS

Parrot Security OS – дистрибутив, нацеленный как на тестирование на проникновение, так и на анонимную работу в интернете. Довольно прост в освоении как новичкам, так и профессионалам.

Благодаря легкости и эффективности его все чаще используют вместо довольно потребительной Kali Linux.

По функционалу он похож на Kali Linux, здесь тоже вместе с системой поставляется огромное количество специального программного обеспечения для тестирования безопасности. Из отличительных особенностей можно назвать больший, нежели в Kali, уклон в анонимность: интеграция I2P (invisible internet project) и предустановленные сервисы TOR.

Parrot разрабатывали в сотрудничестве с Caine, и в нем лучший инструментарий в области цифровой криминалистики, с наилучшими средствами анализа, предоставления доказательств и отчетности. Также в

дистрибутив включили несколько инструментов шифрования для защиты данных.

В отличие от предыдущих двух дистрибутивов, Parrot Security OS вполне подходит в качестве дистрибутива для ежедневной работы [1].

1.1.4 WifiSlax

WifiSlax – это специализированный дистрибутив с подборкой инструментов для проверки безопасности систем Wi-Fi-сетей и проведения криминалистического анализа. Дистрибутив построен на базе Slackware Linux.

В настоящее время, это один из наиболее часто используемых инструментов для аудита Wi-Fi сетей, в него включено большинство популярных утилит для анализа защищенности беспроводных сетей [1].

1.1.5 PentestBox

PentestBox – это сборка утилит для тестирования безопасности сети, работающая в Windows окружении.

PentestBox содержит достаточно большое количество популярных утилит, облегчающих процесс тестирования на проникновение. Утилиты разбиты по группам, облегчающим их поиск и использование — от сбора информации и разведки, веб-сканеров, bruteforce утилит до утилит анализа Android-приложений и Wi-Fi.

Сборка очень просто изменяется «под себя»: можно добавлять и удалять утилиты в зависимости от надобности. Обновления тоже не составят никаких сложностей. Интерфейс выполнен в виде командной строки с «классическим» зеленым шрифтом на черном фоне.

Этот вариант отлично подходит для пользователей, не готовых к работе с виртуальными машинами и Linux.

Также, кроме дистрибутивов, можно использовать и отдельные утилиты для анализа безопасности сети. Приведем некоторые из них [1].

1.1.6 Elcomsoft Wireless Security Auditor

Wireless Security Auditor – это программа для тестирования беспроводной сети на защищенность, также помогает проверить сеть на устойчивость к внешним и внутренним атакам.

Проверка безопасности сети происходит за счет того, что программа пытается проникнуть в нее снаружи или изнутри. Также она производит аудит сети и пытается восстановить пароль к ней за заданный промежуток времени. Если программе это не удается, сеть может считаться защищенной.

При этом, работа аудитора никак не сказывается на функционировании тестируемой беспроводной сети [2].

1.1.7 Nmap

Nmap – это набор инструментов для сканирования сети и проверки безопасности.

Nmap использует множество различных методов сканирования. Nmap также поддерживает большой набор дополнительных возможностей, а именно: определение операционной системы удалённого хоста с использованием отпечатков стека TCP/IP, «невидимое» сканирование, динамическое вычисление времени задержки и повтор передачи пакетов, параллельное сканирование, определение неактивных хостов методом параллельного ping-опроса, сканирование с использованием ложных хостов, определение наличия пакетных фильтров, произвольное указание IP-адресов и номеров портов сканируемых сетей.

В последних версиях добавлена возможность написания произвольных сценариев [3].

1.2 Средства тестирования производительности Wi-Fi сети

Существует множество различных инструментов для анализа и тестирования производительности и качества беспроводной сети. Рассмотрим ниже некоторые из них.

1.2.1 Netspot

NetSpot – утилита, предназначенная для анализа беспроводных сетей и создания карт покрытия Wi-Fi сетей.

Программа работает в двух режимах: Discover (Режим обзора сети) и Survey (Режим карты).

В режиме Discover NetSpot выводит детальную информацию о доступных точках доступа в виде таблицы. Сканирование сети Wi-Fi осуществляется с интервалом 10, 30 и 60 секунд, и работает в течение всего времени, пока открыта программа. В таблице при этом отображается актуальная информация на данный момент.

Режим Survey предназначен для составления схемы помещений и наложения на нее карты покрытия Wi-Fi. Работает это очень просто - вручную рисуется схема, после чего отмечается местоположение ноутбука на ней, затем NetSpot сканирует сети и создает область на карте. Затем ноутбук перемещается в другую точку на схеме и снова сканируется сеть. Чем больше будет таких точек, тем точнее будет карта покрытия. После завершения сканирования NetSpot укажет на карте предполагаемое размещение точки доступа [4].

1.2.2 Acrylic W-Fi

Acrylic Wi-Fi – это анализатор Wi-Fi сетей со встроенным сниффером. Предназначена для анализа, обнаружения и разрешения проблем безопасности и функционирования беспроводных сетей.

Есть две версии программы: бесплатная и платная.

В бесплатной версии программы отображается основная информация об окружающих точках доступа беспроводной сети, а именно: имя точки доступа, MAC-адрес, уровень сигнала, максимальная скорость передачи, тип используемого шифрования, статус WPS (включен или нет), также программа выводит график изменения уровня сигнала от различных точек доступа.

В платной версии функционал более обширный. Например, программа может указывать, какие точки доступа негативно влияют на качество вашей сети,

позволяет генерировать подробные отчеты с детальной характеристикой Wi-Fi сетей об их состоянии. Также в данной версии программа может производить диагностику проблем с сетью, диагностировать состояние безопасности сети и т.д [5].

1.2.3 Wi-Fi Scanner

Wi-Fi Scanner – анализатор беспроводных сетей. Так же, как и выше представленные утилиты показывает информацию об окружающих точках доступа, но с дополнительными колонками. Кроме основных данных об имени точки доступа, MAC-адресе, уровне сигнала, максимальной скорости и т.д. мы можем увидеть информацию о реально достижимой скорости передачи данных, используемой ширине канала, загруженности канала передачи данных и более расширенную информацию об используемых протоколах безопасности.

Как и Acrylic Wi-Fi, имеет две версии: бесплатную и платную. Но у Wi-Fi Scanner функционал версий никак не отличается. Также можно отметить, что в бесплатной версии Wi-Fi Scanner доступны все функции, представленные в платной версии Acrylic Wi-Fi [5].

1.2.4 Homedale

Homedale – это программа-анализатор беспроводной сети.

Программа отображает основную техническую информацию о точках доступа Wi-Fi сети: имя, MAC-адрес, уровень сигнала, канал, битрейт, тип шифрования и т.д.

Основное преимущество данной программы – наличие портативной версии. Но оно очень сильно проигрывает ее недостаткам в виде глюков и зависаний. Также отмечают, что ее не выйдет использовать для постоянного наблюдения за беспроводной сетью, так как утилита замедляет Интернет-соединение во время работы [5].

1.2.5 InSSIDer

InSSIDer – программа для диагностики Wi-Fi сетей и загруженности каналов.

Утилита отображает скорость и загруженность Wi-Fi сети, поможет узнать силу сигнала, имя сети, тип шифрования, MAC-адрес точки доступа, производителя устройства и т.д.

Программа может работать только с беспроводными сетями с частотой 2.4 и 5 ГГц. Также она не показывает устройства, которые могут негативно влиять на качество сигнала сети [6,7].

Заключение

В ходе выполнения практической части выпускной квалификационной работы были выполнены основные задачи и достигнуты следующие результаты.

Изучение основных принципов сети позволило повысить знания о предметной области для более углубленного понимания темы для дальнейшего выполнения практики.

Основные изученные принципы сети были использованы для выявления основных факторов, влияющих на производительность и безопасность сети Wi-Fi, а именно стандарты 802.11, используемый диапазон частот, канал и ширина канала – для производительности; протокол защищенности, сложность пароля, статус режима WPS – для безопасности.

Выявленные факторы производительности и безопасности беспроводной сети в дальнейшем были использованы для поиска и анализа программных средств для тестирования показателей сети Wi-Fi: для безопасности – дистрибутив для проведения теста на проникновения с программами airmon-ng, airodump-ng, reaver, pyrit; для производительности – Acrylic Wi-Fi, сервис www.speedtest.net.

Найденные программные средства были применены для тестирования состояния исследуемой беспроводной сети и анализа ее состояния. В итоге тестирования было выявлено, что главная угроза безопасности данной сети Wi-Fi – это используемый ранее слабый пароль; основной причиной низкой скорости соединения является установленный в автоматическом режиме стандарт 802.11. Для дальнейшей оптимизации сети было принято решение увеличить сложность используемого пароля и в процессе анализа всех возможных для маршрутизатора стандартов 802.11 выбрать самый оптимальный.

На основе проведения анализа решений, принятых для оптимизации беспроводной сети, был сделан вывод о целесообразности использования более надежного пароля по причине повышения безопасности сети путем усложнения задачи перебора пароля при попытке его взлома. Для повышения реальной

скорости соединения было принято решение об использовании стандарта беспроводной сети 802.11n с шириной канала до 40 МГц, данный способ позволил увеличить скорость до 22 Мбит/с при изначальной скорости 7 Мбит\с.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра компьютерных систем

ОТЗЫВ РУКОВОДИТЕЛЯ

на выпускную квалификационную работу студентки Станкявичуте Кристины Сергеевны
по основной образовательной программе подготовки бакалавров по направлению 09.03.02 - Информационные системы и технологии группа Б8418
Руководитель ВКР к.ф.м.н., доцент Е.В.Пустовалов

на тему _ ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ И ЗАЩИЩЕННОСТИ СЕТИ WI-FI
Дата защиты ВКР «21» июня 2018г.

В последнее время все более чаще используются беспроводные способы передачи данных. Защищённость таких каналов связи одна из актуальных задач.

Целью работы является улучшение качества сигнала и безопасность сети Wi-Fi. Были поставлены следующие задачи: исследовать основные принципы работы сети; исследование факторов, влияющих на производительность и защищенность беспроводной сети; поиск и изучение средств тестирования производительности и защищенности беспроводной сети; Анализ и оптимизация используемой сети с применением найденных средств.

В результате был выполнен анализ возможностей сети Wi-Fi, предложены методы, повышающие ее производительность и защищенность.

Выпускная квалификационная работа полностью соответствует заданию.

Результаты могут использоваться в организациях, активно использующих Wi-Fi. Станкявичуте К.С. продемонстрировала высокую степень самостоятельности, умение анализировать, обобщать, делать выводы, проявила ответственность и работоспособность.

К недостаткам можно отнести ошибки в оформлении, а также отсутствие информации по аналогичным роутерам.

Несмотря на указанные недостатки Станкявичуте К.С. заслуживает присвоения соответствующей квалификации, а дипломная работа оценки «отлично».

Руководитель ВКР к.ф.м.н., доцент _____ Е.В.Пустовалов

«20»___июня____2018г.