ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ
КОЛЛЕДЖ АВТОМАТИЗАЦИИ
И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ № 20

КУРСОВАЯ РАБОТА

По ПМ.03 «Программно-аппаратные и технические средства защиты информации»

Тема: Исследование методов и средств анализа защищенности беспроводных сетей.

Студент Илларионов Иван Игоревич Курс, группа ОИБ225

Дата защиты «20» апреля 2021г. Оценка _____

Руководитель курсовой работы _____ М.Д. Круглов

Москва
2021

Содержание:

Введение

В современном мире проблематика защищенности беспроводных сетей стоит наиболее остро. Даже если беспроводное соединение устаревает – оно иногда возвращается в новом виде. Такое произошло с Bluetooth или с инфракрасным каналом передачи информации. Bluetooth перестал быть способом передачи контента, но стал способом транслирования музыки. ИК-порт, который исчез из телефонов, теперь его используют в схемах умных домов.

В настоящее время почти невозможно найти человека, который не пользовался беспроводной сетью. Первое появление беспроводного способа передачи информации датируется 1895 годом. В этом году изобрели радио. На основе этого изобретения и появились первые беспроводные способы передачи информации.

Почти все беспроводные соединения используют радиоканал (радиочастоты). Для несанкционированного доступа к информации используется различные средства перехвата радиосигнала: антенны (Wi-Fi или Bluetooth), модули ближнего бесконтактного соединения (Near Field Communication (NFC)), программно-определяемая радиосистема, анализаторы трафика (Снифферы), перехватчик International Mobile Subscriber Identity (IMSI) и сопутствующие приложения. Подобные устройства и программы могут находиться на любом уровне сети. Саботаж возможен: на уровне провайдера, любого сайта, в узле сети.

У большого числа современных пользователей имеется хотя бы 2-3 устройства использующие беспроводные сети. Телефон, часы, наушники, фитнес-браслеты, банковские карты, и т.д. Каждое подобное устройство нуждается в защите. Даже те устройства, которые на первый взгляд защищать и не нужно. Таким примером является телевизор. Если телевизор использует беспроводное соединение к нему возможно подключиться и внедрить троян [1].

Аналогично примеру с телевизором угрозе подвергаются: телефоны с технологией NFC[2], устройства с Bluetooth[3], любой гаджет, использующий Wi-Fi соединение.

Стоит отметить, что угрозы в большинстве своем гипотетические, но из них могут вырасти угрозы реальные. Чтобы избежать подобного, необходимо постоянно анализировать

---

[1] Журнал «Хакер»; «Hack TV: взлом телевизора». – Режим доступа: https://xakep.ru/2011/07/04/56127/
[2] Журнал «Хакер»; «Доступ к смартфону по NFC». – Режим доступа https://xakep.ru/2012/07/31/59074/
[3] Издание «Лента»; «Миллиарды гаджетов оказались под угрозой взлома по BlueTooth».
– Режим доступа: https://lenta.ru/news/2020/05/20/bias/

средства и методы защиты беспроводных сетей, уровень их защищенности, заниматься пропагандой правильного поведения пользователей, а также постоянно отслеживать новостные ресурсы в поисках информации о новых уязвимостях.

Беспроводная сеть, в отличие от проводной сети, транслирует данные в эфир по радиоканалу, поэтому количество возможных уязвимостей растет, в сравнении, с проводной. Но если подойти к вопросу защиты беспроводной сети комплексно, проводить аудиты безопасности квалифицированными лицами и провести комплексный анализ – возможно добиться уровня защиты, сравнимым с проводной сетью.

Несмотря на все недостатки беспроводных сетей компании и обычные люди продолжают ими пользоваться. Главный аргумент – удобство. Не требуется прокладывать провода, настраивать коммутаторы и локальную сеть, закупать необходимое оборудование, постоянно находится рядом с техникой для ее настройки и взаимодействия с ней. Например, если принтер поддерживает беспроводное соединение – возможна настройка и удаленный запуск печати, находясь на значительном расстоянии от него.

Исходя из вышесказанного необходимо сделать вывод – беспроводные сети подвержены большим рискам, если не подходить к вопросу безопасности ответственно. Беспрерывно появляются новые угрозы и способы взлома, поэтому очень важно постоянно исследовать методы и средства защищенности беспроводных сетей.

Объектом курсовой работы – беспроводные сети.

Предмет – методы защиты беспроводных сетей.

Цель курсовой работы – проанализировать методы и средства защищенности беспроводных сетей.

Задачи курсовой работы:

1) Провести обзор источников информации, стандартов безопасности, специализированных журналов;

2) Исследовать принципы и виды беспроводного соединения;

3) Рассмотреть способы взлома беспроводной сети и перехвата трафика;

4) Установить оптимальные методы защиты соединения от несанкционированного доступа.

Раздел 1. Теоретический обзор распространенных уязвимостей беспроводных сетей

1.1 Прямые угрозы беспроводной сети.

Угрозы беспроводной сети разделяются на два типа - прямые и косвенные. Прямые угрозы возникают при передачи информации по стандарту связи разработанным институтом инженеров электротехники и электроники (Institute of Electrical and Electronics Engineers) - IEEE 802.11.

Самые распространенные виды прямых угроз:

1) *Человек посередине* – это вид атаки, когда злоумышленник перехватывает конфиденциальную информацию через существующую беспроводную сеть. Этот способ напоминает принцип работы стационарного телефона с несколькими устройствами – человек имеющий одно из устройств(телефон) сети имеет возможность слушать разговор и даже что-то сказать.

Атака «человек посередине» имеет несколько способов реализации в проводной сети и два вида в беспроводной:

• Перехват Wi-Fi. Существует два варианта реализации: с помощью уже существующей точки или создание собственной. Принцип в обоих случаях одинаков: с помощью анализатора трафика или подмены страницы - перехватить конфиденциальную информацию.

• Перехват сеанса. В данном случае, злоумышленник охотится за сессионными файлами (cookie). С их помощью возможно зайти в учетную запись человека, чьи сессионные файлы были украдены.

2) *Мошенническое устройство (Rogue Device[4]) (Чужаки)* – вид угрозы через устройства внутри сети. Аналогично с прошлым пунктом, есть несколько способов реализации данной угрозы:

1. С помощью чужеродной точки доступа (Rogue Access Point) – самый частый пример: сотрудник принес свой маршрутизатор и подключил его в сетевую розетку. Данная точка превращается в канал утечки информации из общий корпоративной сети. Существует вариант, когда злоумышленник создает точку доступа с аналогичным уникальным идентификатором

[4] Сайт компании «ManageEngine». «What is Rogue Device detection & prevention?». – Режим доступа https://www.manageengine.com/products/oputils/rogue-detection-and-prevention.html

сети (Service Set Identifier (SSID)) с помощью которой он имеет возможность перехватить данные сотрудников или клиентов, которые подключились к этой сети по ошибке.

2. С помощью устройств, которые попали за пределы компании. Реализация этой угрозы возможна в случае, если на предприятии реализуется модель BYOD (Bring Your Own Device). Например: сотрудник взял домой рабочий ноутбук и в домашней сети поймал вирус. После этого сотрудник возвращает ноутбук в компанию. Теперь вирус имеет возможность попасть в корпоративную сеть. Другой пример: Сотрудник потерял или продал свой рабочий телефон, имеющий доступ к корпоративной беспроводной сети. Злоумышленник, который получил данное устройство, может беспрепятственно попасть в корпоративную сеть (находясь в зоне ее работы).

3) *Перехват и взлом рукопожатий (handshake).* Рукопожатия в беспроводной сети – это обмен информацией между точкой доступа и устройством. Эта информация может включать в себя пароль от сети Wi-Fi, в случае, подключения пользователя к беспроводной сети. Эта информация закодирована (хэширована) и поэтому злоумышленнику потребуется некоторое время для декодирования информации. Процесс перехвата происходит следующим образом:

a) Некое устройство с антенной переводится в режим мониторинга и начинает перехватывать файлы из эфира определенной точки доступа;

b) Злоумышленник ждет, пока пользователь подключится к сети. Имеется возможность отключения пользователей, для инициирования подключения;

c) Перехватывается файл рукопожатия;

d) Файл «очищают» от ненужных данных и начинается процесс подбора пароля (брут) с помощью оборудования: видеокарт и процессора;

e) В случае успешного подбора пароля – злоумышленник получает пароль от сети;

f) Реализуются угрозы беспроводной сети, связанные с получением тотального контроля над сетью.

Для ускорения процесса перебора злоумышленник имеет возможность использовать маску. Это происходит в том случае, если ему известны некоторые данные о пароле: количество символов, вид символов, часть пароля. Хорошим способом защиты от такой угрозы является использование длинного пароля (16 символов), смена пароля каждые полгода, не позволять сотрудникам разглашать или получать информацию о пароле.

4) *Распределенный отказ в обслуживании (Distributed Denial of Service) (DDOS)*. Этот вид атаки применятся для ухудшения работы беспроводной сети. Существует два вида атаки:

• На устройства, подключенные к сети. Используется либо для получения файлов рукопожатия (пункт 3) или для улучшения качества сети одного пользователя сети, за счет, отключения других.

• На точку доступа. Используется для реализации угрозы RogueAP (пункт 2). У клиентов и сотрудников остается только подмененная точка доступа и они начинают подключаться к ней. В это время злоумышленник может использовать комплекс атак и получить конфиденциальную информацию достаточную для получения данных из корпоративной сети.

В редких случаях DDOS атака на точку доступа используется для подавления ее работы без цели получения конфиденциальных данных. Это могут быть места, где использование Wi-Fi сети запрещено или для освобождения эфира.

5) *Утечки проводной сети.* Почти любой вид беспроводного соединения подключается к проводному соединению. Все угрозы, связанные с проводным соединением, могут быть реализованы и в беспроводной сети.

1.2 Косвенные угрозы

Косвенные – угрозы, возникающие из-за наличия Wi-Fi сетей рядом с предприятием, связанные с организационными мерами, особенности оборудования, и так далее.

Косвенные угрозы:

• Активность в нерабочее время. Правильным решением будет отключать беспроводную сеть физическим образом в нерабочие часы. Любые попытки использовать сеть вне времени работы – должны помечаться, как подозрительные и расследоваться.

• Интерференция. В случаях, когда в частоте точки доступа находится устройство достаточно мощное – может произойти ситуация с отказом оборудования. Угроза косвенная переходит в разряд прямой угрозы (пункт 4).

• Скорости. Чем больше скорость передачи, тем ближе необходимо находится к точке доступа. Например: офис территориально ограничен. Все пользователи пользуются интернетом на определенной скорости (выше 5 мбит/с). Если к сети подключен пользователь, который пользуется сетью на скорости 1-2 мбит/с, то необходимо срочно принимать меры.

• Особенности функционирования беспроводных сетей.

Беспроводная сеть, как и оговаривалось выше – менее защищены от проводных. Поэтому необходимо постоянно заниматься мониторингом трафика, анализом оборудования, поиском новых уязвимостей.

1.3 Теоретическое введение в стандарты безопасности Wi-Fi

На данный момент существуют 6 видов стандартов безопасности wifi:

1) *Wi-Fi protected access Personal Key (PSK)* - Для подключения к точке необходимо только ввести пароль, иногда - SSID, если сеть скрыта. Данный стандарт безопасности использует устаревший способ шифрования данных Temporal Key Integrity Protocol (TKIP), который невозможно использовать на новых сетевых интерфейсах, из-за соображений безопасности;

2) *WPA Enterprise* - Вход организуется через логин и пароль, данные о которых хранятся в базе данных сервера. Используется в компаниях, в образовательных организациях, на предприятиях. Принцип работы показан на рисунке 1.

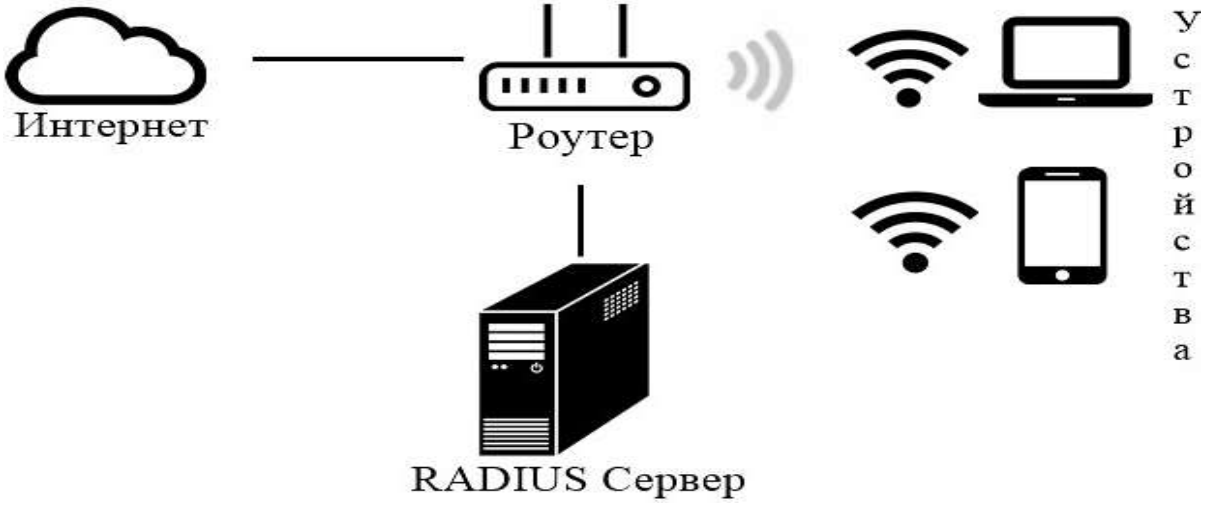

Рис 1. Принцип работы WPA Enterprise.

Из рисунка следует, что в случае подключения устройства, маршрутизатор отправляет на проверку данные в RADIUS сервер, и, если устройство и учетная запись имеет доступ к сети становится возможным выход в интернет;

3) *WPA2-PSK* – В отличии от WPA:

• Используется стандарт шифрования Advanced Encryption Standard (AES)/CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol);

- Требуется пароль от 8 символов;
- Необходимо использовать более мощное оборудование.

4) *WPA2 Enterprise* – аналогично примеру с WPA2-PSK отличия наблюдаются в использовании нового способа шифрования AES. Присутствует возможность использования современных настроек и способов защиты беспроводного соединения. Но в данный момент существуют способы взлома этого стандарта, в основном, с помощью *мошеннической точки доступа (RogueAP)*[5];

5) *WPA3-Simultaneous Authentication of Equals (SAE)* – самый актуальный стандарт безопасности, который был создан в 2018 году компанией Wi-FI Alliance.

Основные изменения:

- Реализуется способ шифрования Opportunistic Wireless Encryption (OWE);
- Новый способ аутентификации устройств SAE[6];
- Ликвидирует концептуальные недоработки стандарта WPA2;
- Новый протокол SAE устраняет уязвимость, связанную с файлами рукопожатия;[7]

6) *WPA3-Enterprise* – самое актуальное решение для предприятий и организаций. В отличии от WPA2, WPA3 предусматривает возможность использования ста девяноста двух битов при шифровании данных. Однако, возможность использования стандартных ста двадцати восьми битов осталась – этот вариант подойдет тем компаниям, где нецелесообразно использование настолько мощного способа шифрования[8].

Исходя из вышесказанного возможно сделать вывод: беспроводные сети вышли на новый уровень безопасности. Но вместе с этим развиваются способы взлома и поиска уязвимостей. Невозможно предсказать возможные и будущие угрозы. Поэтому необходимо постоянно проводить анализ новых уязвимостей и заниматься аудитом безопасности беспроводной сети. Эти мероприятия позволяют ликвидировать большинство угроз, обеспечить необходимый уровень безопасности и минимизировать расходы на устранение последствий.

---

[5] Информационный портал SecurityLab. «Как взлмывают корпоративный Wi-Fi: новые возможности». - Режим доступа: https://www.securitylab.ru/analytics/471816.php

[6] Институт инженеров электротехники и электроники. 802.11-2016 - IEEE Standard for Information technology —Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 2016.

[7] Веб-сайт «Хабр». «Wi-Fi становится безопаснее». Режим доступа - https://habr.com/ru/post/424925/

[8] Веб-сайт «Wi-Fi.org». «Discover Wi-Fi. Security». Режим доступа - https://www.wi-fi.org/discover-wi-fi/security

1.4 Способы и методы защиты беспроводных сетей

Начать стоит с того, что любая система защиты подвергается самой массовой угрозе – человеческому фактору. Любые мероприятия по предотвращению угроз безопасности становятся бесполезными, если пользователь пренебрежет правилам использования сети. Поэтому в первую очередь необходимо обращать внимание именно на этот аспект. Мерами защиты в данном случае могут послужить:

- Осведомленность пользователей сети в предотвращении основных угроз;
- Сокращение времени работы беспроводной сети в нерабочее время;
- Создание и популяризация правил безопасности для пользователей сети.

Естественно, организационные меры не способны обеспечить должный уровень безопасности от внешних угроз. Но с их помощью возможно избежать некоторые виды угроз.

Способы и методы защиты беспроводной сети, аналогично видам угроз возможно разделить на прямые и косвенные:

Прямые способы и методы – специально созданы и направленны на защиту сети от несанкционированного доступа.

Косвенные – технологии, которые не были изначально созданы для защиты сети, но косвенным образом усложняющие взлом сети.

К прямым способам и мерам защиты относятся:

1) Скрытие SSID Wi-Fi сети. В настройках большинства маршрутизаторов, есть функция скрытия имени Wi-Fi сети (Hide SSID). Эта функция не способна спрятать сеть от специальных инструментов и программ, но позволяет отключить открытое оповещение о существовании этой сети. Злоумышленнику будет необходимо использовать дополнительные затраты по времени и знать где эта сеть находится, но для этого придется приложить дополнительные усилия;

2) Фильтрация по Media Access Control (Контроль доступа к среде) адресам. Реализуется с помощью списка доступа (Access Control List (ACL)). Те устройства, чей MAC адрес есть в списке – могут беспрепятственно подключаться к точке доступа. Если к сети будет пытаться подключиться устройство, которого нету в списке – не смогут это сделать. Современные технологии позволяют подменить MAC адрес, но это создает ряд трудностей:

• Необходимо узнать адрес устройства имеющее доступ к сети;

• Некоторые антивирусы способны заметить подмену MAC и предпринять необходимые защитные меры[9];

• Это требует дополнительных затрат времени и ресурсов.

3) Поиск Rogue AP. Обращаясь к пункту 1.1 известно, что мошеннические точки доступа способны ввести в заблуждение пользователей и подвергнуть всю сеть угрозе. Современные технологии защиты позволяют своевременно обнаружить мошеннические точки доступа и принять соответствующие меры[10];

4) Отключение функции Wi-Fi Protected Setup (WPS). WPS – это быстрый способ подключения к сети, позволяющий обойти ввод пароля при подключении устройств. Принцип работы WPS: чтобы не вводить пароль на устройстве, которое пытается подключится к сети – есть возможность нажать специальную кнопку (рис.2) на маршрутизаторе. Это облегчает подключение к сети, но очень сильно сказывается на безопасности. Дело в том, что при включенной функции WPS – присоединение к сети возможно организовать с помощью кода, указанного на самом маршрутизаторе. Код состоит из 8 цифр. Из этого следует, что количество комбинаций 100.000.000. Но из-за недоработки стандарта количество этих вариантов резко сокращается, если знать алгоритм с помощью, которого этот код создается.[11] Об этой уязвимости знают, и создатели специальных программ с помощью, которых этот перебор осуществляется. Все, что требуется злоумышленнику – открыть программу и подобрать код. Стоит отметить, что если злоумышленнику удалось получить доступ к маршрутизатору по WPS, то он сможет посмотреть пароль, который был установлен для защиты точки. В итоге, на руках у злоумышленника окажется не только доступ к точке, но и установленный пароль.

Но вышесказанное – это не все уязвимости функции WPS. В 2015 году обнаружилось, что некоторые разработчики маршрутизаторов, при генерации пароля использовали слишком просто алгоритм, который легко взламывается[12].

---

[9] Сайт компании «Kaspersky». «Защита от атак типа MAC-спуфинг». Режим доступа: https://support.kaspersky.com/KESWin/11.4.0/ru-RU/174954.htm

[10] Сайт компании «Tp-Link». «Configure rogue AP detection on EAP/Omada Controller». Режим доступа: https://www.tp-link.com/ru/support/faq/1013/

[11] Сайт «sviehb.files.wordpress.com». «Brute forcing Wi-Fi Protected Setup» - Режим доступа: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

[12] Форум дистрибутива Linux «Kali». «WPS pixie Dust Attack». Режим доступа: https://forums.kali.org/showthread.php?24286-WPS-Pixie-Dust-Attack-(Offline-WPS-Attack)

Современные производители маршрутизаторов изменили отношение к WPS. Теперь при попытке перебора – эта функция отключается. Выходят новые версии WPS, которые относительно безопасно использовать. Способ генерации пароля теперь сложнее. Но старые устройства подвергаются этой угрозе, поэтому очень желательно сразу выключить эту функцию при настройке беспроводной сети;

Рис 2. Кнопка WPS на маршрутизаторе.

5) Использование современного оборудования. Из примеров выше следует, что большинство устаревших стандартов и функций – создают огромный пласт уязвимостей. Необходимо целесообразно обновлять свое оборудование, отключать функции, которые не используются или подвержены угрозам;

6) Установка пароля в 16 символов. На взлом пароля, состоящего из 8-ми цифр злоумышленнику, потребуется не более суток. На взлом пароля, состоящего из 16-ти символов с использованием спецсимволов – уйдет около триллиона лет. Но тут необходимо учитывать ряд факторов:

- Пароль должен быть уникальным и придуман человеком лично;
- Для компаний – необходимо контролировать получение паролей сотрудниками. О пароле компании должны знать только сотрудники безопасности и доверенные лица;
- Желательно менять пароль раз в полгода.

Предоставленные меры защиты являются необходимыми для обеспечения удовлетворительного уровня безопасности для домашней сети, но недостаточными для защиты корпоративной сети. Во-втором случае, требуется специальный отдел безопасности, занимающийся анализом и защитой беспроводной сети, так как любая беспроводная сеть нуждается в постоянном мониторинге за трафиком и подозрительными действиями. Стоит отметить, что любые меры – должны быть целесообразны и экономически оправданы.

К косвенным способам и методам относятся:

1) Использование нового диапазона частот в 5 гигагерц. Современные маршрутизаторы поддерживают и рекомендуют работать в диапазоне 5Ггц, так как это ускоряет передачу данных и улучшает качество связи. Исходя из основ физики – чем выше частота, тем хуже она проходит через препятствия. Это значит, что беспроводная сеть становиться очень ограниченной по радиусу распространения сигнала. Тем самым, злоумышленнику потребуется находиться очень близко к источнику беспроводного сигнала, что сильно усложняет реализацию методов воздействия на сеть;

2) Создание сети из нескольких точек доступа. Как и оговаривалось выше – частоты 5ггц плохо проходят через препятствия. Для решения этой проблемы используют несколько точек доступа, объединенных в одну сеть. Чаще всего применятся mesh-система. “Mash” в переводе с английского значит «Ячейка». Принцип работы подобной системы изображен на рис.3.

Рис.3. Реализация mash-системы в различных видах помещений.

Из рисунка следует, что mash-система позволяет ликвидировать главный недостаток диапазона в 5ггц – сигнал распространяется по всей территории помещения с помощью нескольких источников сигнала. Однако, дальность действия сильно ограничена, а значит злоумышленнику необходимо находится близко к источнику сигнала.

Но главное преимущество использования нескольких точек доступа – функция автоматического исцеления (Auto Healing). Данная функция позволяет автоматически проверяет источники сигнала и в случае, если один из них перестает работать – усиливает сигнал другого источника. Подобная технология позволяет усложнить реализацию уязвимости Rogue AP. Если злоумышленник начнет глушить один источник – другой начнет работать сильнее и пользователи смогут продолжить работу в сети;

3) Установка пороговых значений уровня сигнала для подключения и отключения пользователей. Эта функция чаще всего используется, когда есть несколько точек доступа. Ее предназначение – отключать пользователей с плохим уровнем сигнала от точки, чтобы инициировать подключение к другой. Пользователь, который перемещается по помещению отдаляется от одной точки и начинает приближается к другой. Задача функции – «передать» пользователя другой точке, которая будет ближе. Косвенная защита точки заключается в том, что при попытке подключения с дальнего расстояния – соединение будет разорвано. Аналогично примерам выше – злоумышленнику необходимо находится близко к источнику сигнала, так как в ином случае – система автоматически отключит его;

4) Повышение скорости передачи данных. Данный метод сам по себе не влияет на безопасность сети, но позволяет внедрять дополнительные меры защиты, которые сильно замедляют передачу данных. К таким мерам можно отнести – использование виртуальных частных сетей (Virtual Private Network (VPN)) и зашифрованных каналов связи;

5) Окраска базовых наборов услуг (Basic service set coloring). Раньше маршрутизаторы расшифровывали любые сигналы, полученные на своей частоте, это сильно сказывалось на работе устройства и на безопасности. Современные технологии позволяют добавить специальную подпись на пакеты данных, тем самым разделяя трафик и снижая нагрузку на маршрутизатор.

6) Обновление программного обеспечения. Чаще всего, обновления требуются для улучшения работы маршрутизатора в целом. Программный код оптимизируется, тем самым общая нагрузка на устройство снижается. Но в некоторых случаях обновления содержат в себе важные изменения в безопасности. Поэтому необходимо постоянно проверять свое оборудование на наличие новых версий программного обеспечения и по возможности обновлять его.

Следуя из вышесказанного, следует сделать вывод: современные технологии предоставляют различные методы и способы защиты беспроводных сетей. Комплекс прямых и косвенных методов позволяет организовать удовлетворительный уровень защиты. Но даже, подобные меры не гарантируют полную защиту сети от несанкционированного доступа. Злоумышленники каждый день развивают методы взлома беспроводных сетей. В свою очередь, производители программного обеспечения и оборудования стремиться, как можно быстрее реагировать на новые уязвимости и способы взлома.

Раздел 2. Практический анализ методов и средств защиты беспроводной сети

2.1 Реализация уязвимости файлов рукопожатия.

В теоретическом разделе была рассмотрена возможность перехвата и взлома handshake файлов (Раздел 1. Заголовок 1.1 Пункт 3.). Данная уязвимость позволяет злоумышленнику получить доступ к беспроводной сети, в случае успешного взлома. Уязвимость актуальна для стандартов: WPA-PSK и WPA2-PSK

Необходимое оборудование:

- Wi-FI адаптер, поддерживающий режим контроля (монитора);
- Мощное оборудование для подбора паролей;
- Желательно использование дистрибутива *Linux Kali*;
- Программное обеспечение.

План действий:

1) Произвести запуска дистрибутива *Kali Linux*;
2) Перевести адаптер в режим контроля (монитора) и выбрать цель атаки;
3) Перехватить Handshake-файл;
4) Конвертировать полученный файл в необходимый формат;
5) Взломать файл рукопожатия.

Реализация:

1) Запуск дистрибутива Linux;

Дистрибутив это форма расспространения программного обеспечения, которая содержит в себе предустановленные приложения для определенных целей и задач. Для того, чтобы запустить *Kali Linux* необходимо создать специальную флешку с помощью которой возможна установка или запуск операционной системы. Затем необходимо запустить компьютер с загрузочной флешкой. Есть возможность выбора: установить операционную систему или загрузиться с помощью LiveUSB. LiveUSB – это носитель, который включает в себя операционную систему и конфигурационные файлы с возможностью ее запуска.

2) Перевод адаптера в режим монитора и выбрать цель атаки;

Перед тем, как выполнить команду перевода адаптера в режим монитора необходимо завершить процессы, использующие Wi-Fi интерфейс. Для этого используется команда –

"airmon-ng check kill". Только после этой команды возможно перевести сетевой адаптер в режим монитора командой – "airmon-ng start wlan0".

Рис 4. Результат выполнения команд.

После выполнения команд сетевой адаптер перейдет в режим монитора и получит новое название с припиской «mon». Это значит, что адаптер находится в режиме контроля.

После перевода сетевого адаптера в режим монитора необходимо запустить процесс перехвата сетевых пакетов. Процесс запускается командой – airodump-ng wlan0mon.

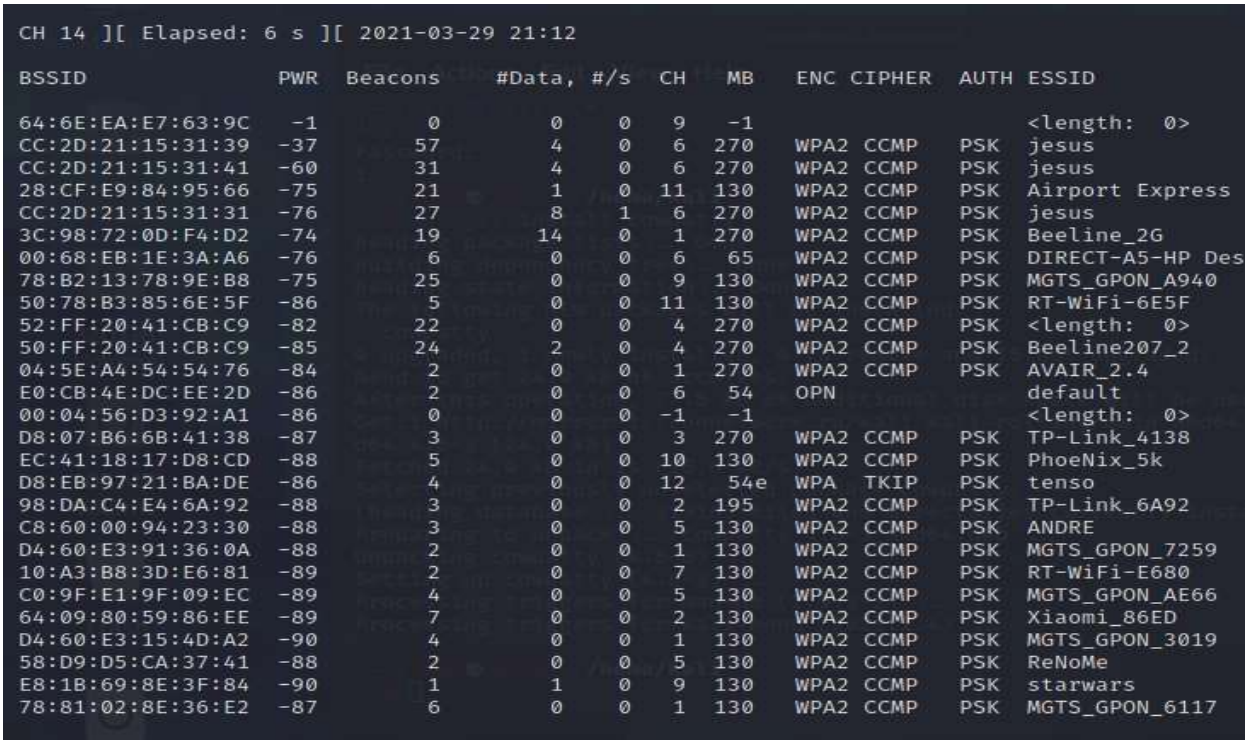

Рис 5. Итоговый вывод программы

Из рисунка следует, что получены данные о доступных точках доступа. К полученным данным относятся: MAC-адреса (1 столбик), мощность сигнала(2),количество маяков, которые точка доступа отправляет, сообщает о готовности доступа передавать сигнал(3), количество захваченных пакетов(4), количество пакетов данных в секунду, измеренных за последние 10 секунд (5), номер канала маршрутизатора (6), максимальная скорость передачи данных (7), используемый стандарт безопасности (8), способ шифрования(9), вид аутентификации (10), имя точки доступа (11).

На основе этих данных возможно выбрать цель атаки. Но взлом любой точки доступа, кроме своей является нарушением законодательства РФ[13]. Поэтому целью выбрана точка доступа «Jesus».

3) Перехватить Handshake-файл;

После выбора точки необходимо ввести команду, которая позволяет проанализировать трафик и перехватить файл рукопожатия. Команда выглядит следующим образом: airodump-ng wlan0mon (название адаптера) -w (префикс создает файл в который будет занесена перехваченная информация) jesus (название точки доступа) --bssid CC:2D:21:15:31:39 (MAC-адрес точки доступа) -c 6 (номер канала маршрутизатора).

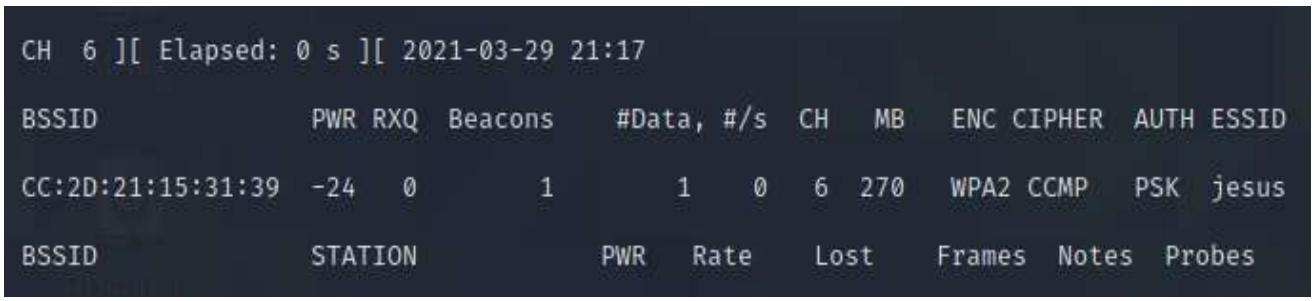

Рис 6. Результат работы команды

Имеется возможность ускорить процесс путем воздействия на устройство с помощью *распределенного отказа в обслуживании.* Тем самым вызвав деаутентификацию (отсоединения пользователя). Устройство пользователя после разрыва связи попытается вновь присоединиться к точке отправив файл рукопожатия, который возможно перехватить. Делается это с помощью команды – aireplay-ng.

[13] Уголовный кодекс РФ. Статья 272 “Неправомерный доступ к компьютерной информации.”

```
21:24:06  Sending 64 directed DeAuth (code 7). STMAC: [AC:64:CF:82:9D:18] [ 5
21:24:06  Sending 64 directed DeAuth (code 7). STMAC: [AC:64:CF:82:9D:18] [ 5
21:24:06  Sending 64 directed DeAuth (code 7). ^Z
zsh: suspended  aireplay-ng -0 100 -a CC:2D:21:15:31:39 -c AC:64:CF:82:9D:18
wlan0mon
```

Рис. 7 Работа программы airplay-ng

Через некоторое время airodump-ng сообщит об успешном перехвате файла. В терминале появится информация о файле рукопожатия.

```
File  Actions  Edit  View  Help

CH  6 ][ Elapsed: 48 s ][ 2021-03-29 21:27 ][ WPA handshake: CC:2D:21:15:31:39

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

CC:2D:21:15:31:39  -26  85      491      294    1   6  270   WPA2 CCMP   PSK  jesus

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

CC:2D:21:15:31:39  64:9A:BE:69:87:32  -35    1e-24      0      276  EAPOL
CC:2D:21:15:31:39  14:F6:D8:00:AE:BF  -48    0 - 2e     0      118
```

Рис. 8 Перехваченный файл рукопожатия

Если файл рукопожатия перехвачен, то его необходимо очистить от ненужных данных. Так как помимо информации о пароле он содержит бесполезные для взлома данные. Очистка выполняется программой «wpaclean» с помощью команды: wpaclean da (название файла, который будет содержать только необходимые данные) Jesus-03.cap (название файла, который создала программа для перехвата файлов рукопожатия).

```
┌──(root💀kali)-[/home/kali/hs]
└─# wpaclean da Jesus-03.cap
Pwning Jesus-03.cap (1/1 100%)
Net cc:2d:21:15:31:39 jesus
Done
```

Рис. 9 Успешная очистка файла

4) Конвертировать полученный файл в необходимый формат;

Данное действие является обязательным в том случае, если используется программа «hashcat». Дело в том, что эта программа работает только с форматом hccapx. Это нужно для того, чтобы программа удостоверилась в том, что файл рукопожатия содержит необходимые

данные для перебора пароля. Возможно использование других программ, но их главный недостаток – медленная скорость подбора. Поэтому целесообразным будет использование именно «hashcat». Процесс конвертации возможен прямо на сайте программы[14]

5) Взломать файл рукопожатия.

Полученный файл возможно взломать и на другой компьютере. Иногда злоумышленники поступают именно так: перехватывают файл рукопожатия с помощью небольшого устройства, а затем на более мощном компьютере перебирают пароли. Скорость подбора напрямую зависит от производительности устройства.

Работа с программой осуществляется через стандартное приложение «Windows ОС» - «Windows PowerShell». Необходимо ввести следующую команду: .\hashcat (название программы) -m (тип файла) 2500 -a (способ перебора) 3 1.hccapx (название файла) ?d?d?d?d?d?d?d?d (маска). Подробнее про некоторые префиксы:

Тип файла. Указывается в цифрах. «Hashcat» имеет возможность перебора и взлома различных типов файлов[15]. Необходимо указывать, какой конкретно файл используется.

Способ перебора. Существует 4 варианта перебора: по словарю (-a 0), комбинаторная атака по словарю (-a 1), полный перебор (-a 2), атака по маске (-a 3). Словари состоят из самых частых паролей. Имеется возможность создать словарь исходя из информации о человеке[16]. Атака по маске позволяет сократить время на перебор, если известны какие-либо данные о пароле (количество символов или некоторая часть пароля).

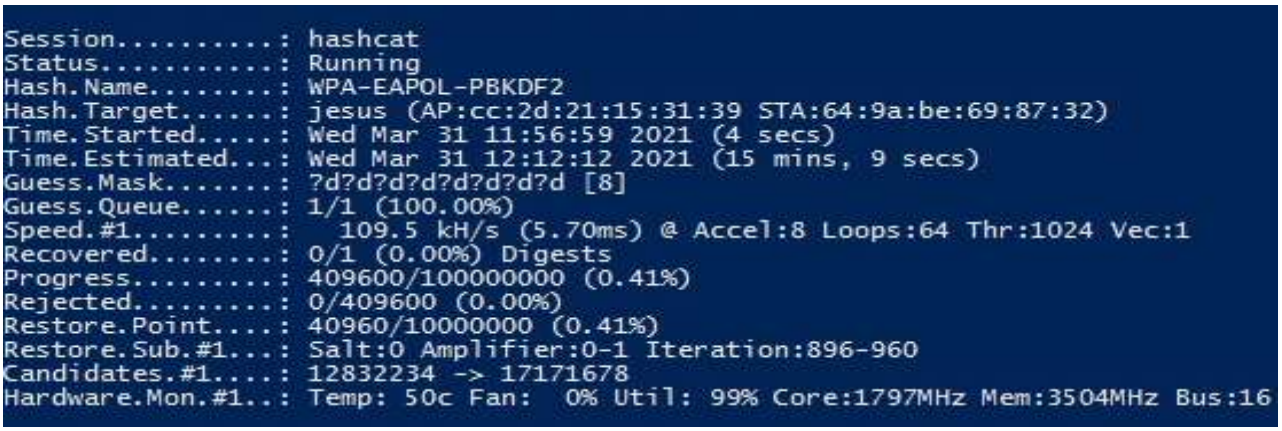

Рис. 10 Работа программы hashcat

[14] Сайт разработчика программы «Hashcat». Режим доступа: https://hashcat.net/cap2hccapx/
[15] Официальный сайт разработчика «Hashcat». «Example hashes». Режим доступа: https://hashcat.net/wiki/doku.php?id=example_hashes
[16] Сайт «Hackware». Продвинутые техники создания словарей. Режим доступа: https://hackware.ru/?p=15350#3

На рисунке видно, как программа выводит различные данные:

Session – название сессии. Чаще всего используется стандартное, имеется возможность изменить названия, когда сохраняется часть прогресса. К примеру: для перебора пароля злоумышленник использует рабочий компьютер и для того, чтобы каждый раз не начинать заново, есть возможность сохранить прогресс;

Status – свидетельствует о том, что программа работает успешно;

Hash.Name – тип файла (хэша). Хэшиование – это способ кодирования информации. Из рисунка следует, что используется тип хэша «WPA-EAPOL-PBKDF2». То есть, происходит перебор зашифрованного пароля стандарта «WPA/WPA2»;

Hash.Target – название сети, ее MAC-адрес и адрес устройства, которое подключилось к сети. То есть устройство, которое выполнило «рукопожатие» с точкой доступа;

Time.Started – дата и время начала работы программы;

Time.Estimated – Расчетное время на взлом;

Guess.Mask – используемая маска. В данном примере используется маска для перебора пароля, состоящего из 8 цифр.

Guess.Queue – Количество файлов в очереди.

Speed #1 – скорость перебора. Цифра один означает, что используется только одно устройство. 109 kh/s – означает, что перебирается около 109 тысяч хешей в секунду.

Progress – прогресс работы.

Rejected – количество отклоненных паролей. Для перебора хэшей «WPA» эта функция не используется.

Restore.Point – точка восстановления. Используется для сохранения процесса.

Restore.Sub #1 – Данная функция показывает используется, ли дополнительный способ шифрования с помощью случайного слова (соль). В данном случае не используется.

Candidates. #1 – показывает «кандидатов». То есть диапазон паролей, которые сейчас перебираются. В данном случае – от 12832234 до 17171678.

Hardware.Mon #1 – Показывает нагрузку на устройство, его загруженность.

В результате, если пароль будет подобран программа сообщит об этом и сохранит его в специальном файле.

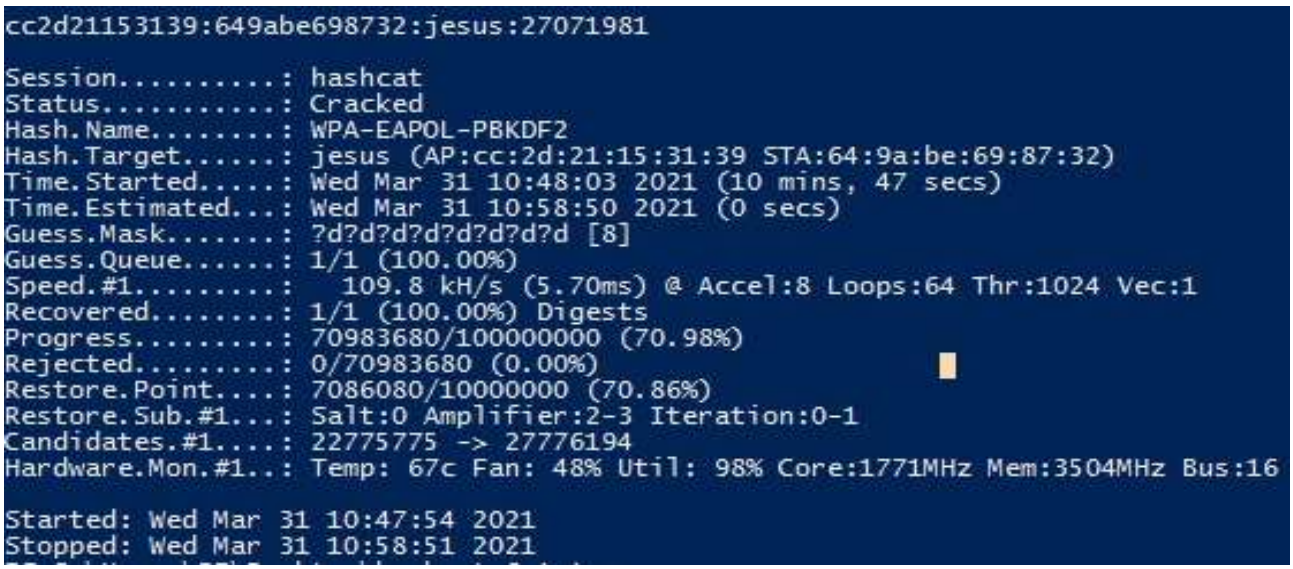

Рис. 11 Успешный подбор пароля

На рисунке видно, что статус сменился на «Cracked» (взломан). В самом вверху рисунка написан пароль от сети – 27071981. Сам процесс взлома занял 10 минут 47 секунд. То есть злоумышленнику для взлома пароля, состоящего из 8 цифр нужно не более 2-х часов. Поэтому рекомендуется устанавливать пароли, состоящие из 16 различных символов. На взлом подобного практически невозможен и нецелесообразен.

Для защиты беспроводной сети от уязвимости перехвата файлов рукопожатия целесообразно использовать новый стандарт безопасности WPA3. Современные способы шифрования обеспечивают необходимый уровень защиты. В случае если файлы рукопожатия будут перехвачены – на их взлом уйдет слишком много времени и это будет бесполезно, так как при каждом новом соединении устанавливается новый шифрующий пароль.

2.2 Практическое применение уязвимости функции WPS

Как и оговаривалось выше функция «WPS» позволяет подключится к беспроводной сети Wi-Fi без необходимости ввода пароля. Но проблема данной функции в том, что пароль возможно подобрать. Современные маршрутизаторы защищены от этого:

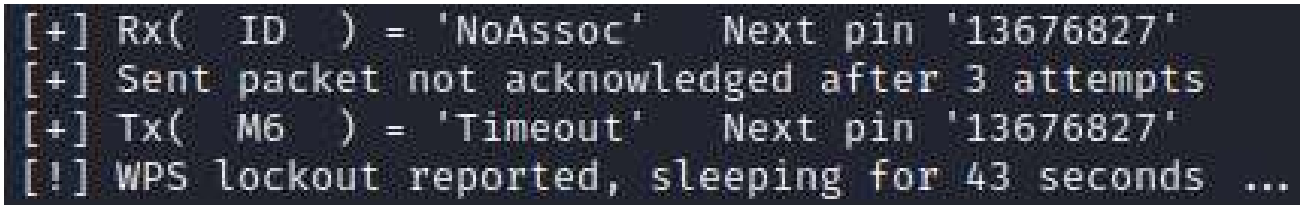

Рис. 12 Блокировка функции WPS

В последней строчке на представленном рисунке видно, что функция WPS заблокировалась после нескольких неудачных попыток подбора. Но в некоторых случаях злоумышленникам удается получить доступ к устройству с помощью 1-2 попыток[17]. Исходя из этих данных необходимо сделать вывод – функция WPS остается уязвимой к взлому на сегодняшний день.

Для практической реализации обхода пароля с помощью взлома WPS необходимые следующие действия

1) Запустить дистрибутив Kali Linux или parrot ОС;

2) С помощью команд и программ проанализировать точки доступа поблизости с включенной функцией WPS;

3) Выбрать цель для атаки;

4) Провести атаку на точку доступа.

В отличие от уязвимости с использованием файлов рукопожатия – в этом случае мощное оборудование не требуется. Так как перебор происходит с небольшой скоростью.

1) Запустить дистрибутив Kali Linux или parrot ОС;

Настоящее действие является рекомендуемым, но реализация данной уязвимости возможна и на «Windows ОС»[18]. Но в использование дистрибутивов Linux имеет ряд плюсов:

- Возможен анализ точки доступа и предоставление информации текущей версии WPS, мощности сигнала и об используемом стандарте защиты;
- Существуют программы, которые реализуют уязвимость с помощью, которой возможно подобрать пароль с 1-2 попытки;
- Программа для «Windows ОС» обладает меньшим функционалом.

Исходя из этих аспектов возможно сделать вывод: целесообразнее использовать представленные дистрибутивы Linux.

2) С помощью команд и программ проанализировать точки доступа поблизости с включенной функцией WPS;

[17] Сайт «HackWare». «Эффективный подбор WPS ПИНа». Режим доступа: https://hackware.ru/?p=4080
[18] Сайт «Wi-Fiгид». «Тот же WiFi Warden, только для Windows». Режим доступа: https://wifigid.ru/vzlom/wifi-dumpper

Перед этим действием необходимо перевести адаптер в режим монитора. Информация об этом содержится выше. Для реализации этого пункта существует команда: "airodump-ng wlan0 --wps" которая позволяет отобразить информацию о wps.

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	WPS	ESSID
90:F6:52:B9:74:3A	-57	54	0	0	2	130	WPA2	CCMP	PSK	1.0 ETHER,LAB,PBC	Nikitos
CC:2D:21:15:31:39	-23	41	5	0	6	270	WPA2	CCMP	PSK	0.0	jesus
CC:2D:21:15:31:41	-59	23	2	0	6	270	WPA2	CCMP	PSK	0.0	jesus
78:B2:13:78:9E:B8	-80	12	0	0	8	130	WPA2	CCMP	PSK	Locked	MGTS_GPON_A940
3C:98:72:0D:F4:D2	-74	15	0	0	1	270	WPA2	CCMP	PSK	0.0	Beeline_2G
28:CF:E9:84:95:66	-69	16	0	0	11	130	WPA2	CCMP	PSK	0.0	Airport Express
CC:2D:21:15:31:31	-70	14	131	0	6	270	WPA2	CCMP	PSK		jesus
D8:EB:97:21:BA:DE	-80	7	0	0	12	54e	WPA	TKIP	PSK	Locked	tenso
50:FF:20:41:CB:C9	-80	1	0	0	9	270	WPA2	CCMP	PSK	Locked	Beeline207_2
50:78:B3:85:6E:5F	-83	4	0	0	11	130	WPA2	CCMP	PSK	2.0	RT-WiFi-6E5F
60:A4:4C:28:08:B8	-85	0	6	0	11	-1	WPA			0.0	<length: 0>
A0:CF:F5:C7:C8:6E	-86	3	0	0	11	130	WPA2	CCMP	PSK	2.0 LAB,DISP,PBC,KPAD	MGTS_GPON_1027
00:04:56:D3:92:A1	-86	0	0	0	-1	-1				0.0	<length: 0>
04:5E:A4:54:54:76	-86	3	0	0	7	270	WPA2	CCMP	PSK	0.0	AVAIR_2.4

Рис. 13 Дополнительная информация о wps

На представленном рисунке видно, что появился новый столбец – wps. В нем содержаться данные о версии wps или информация о том, что wps заблокирован. Данная информация позволяет злоумышленнику или аудитору безопасности проанализировать беспроводные подключения на возможность атаки с помощью подбора пинкода.

3) Выбрать цель для атаки;

Исходя из представленных данных целесообразно реализовывать уязвимость на сети «Nikitos». В этой сети используется устаревшая версия протокола WPS в котором нету защиты от полного перебора. После выбора цели необходимо скопировать ее MAC адрес и канал передачи информации. Это информация необходима для специальной программы.

4) Провести атаку на точку доступа.

Существует несколько программ для проведения атаки на точку доступа. Из них самые популярные: bully, reaver и airgeddon. Целесообразнее использовать именно последнюю программу так как она включает в себя первые две. Подобное решение позволяет мгновенно переключатся между программами. Для того, чтобы воспользоваться airgeddon необходимо ввести команду - bash airgeddon.sh.

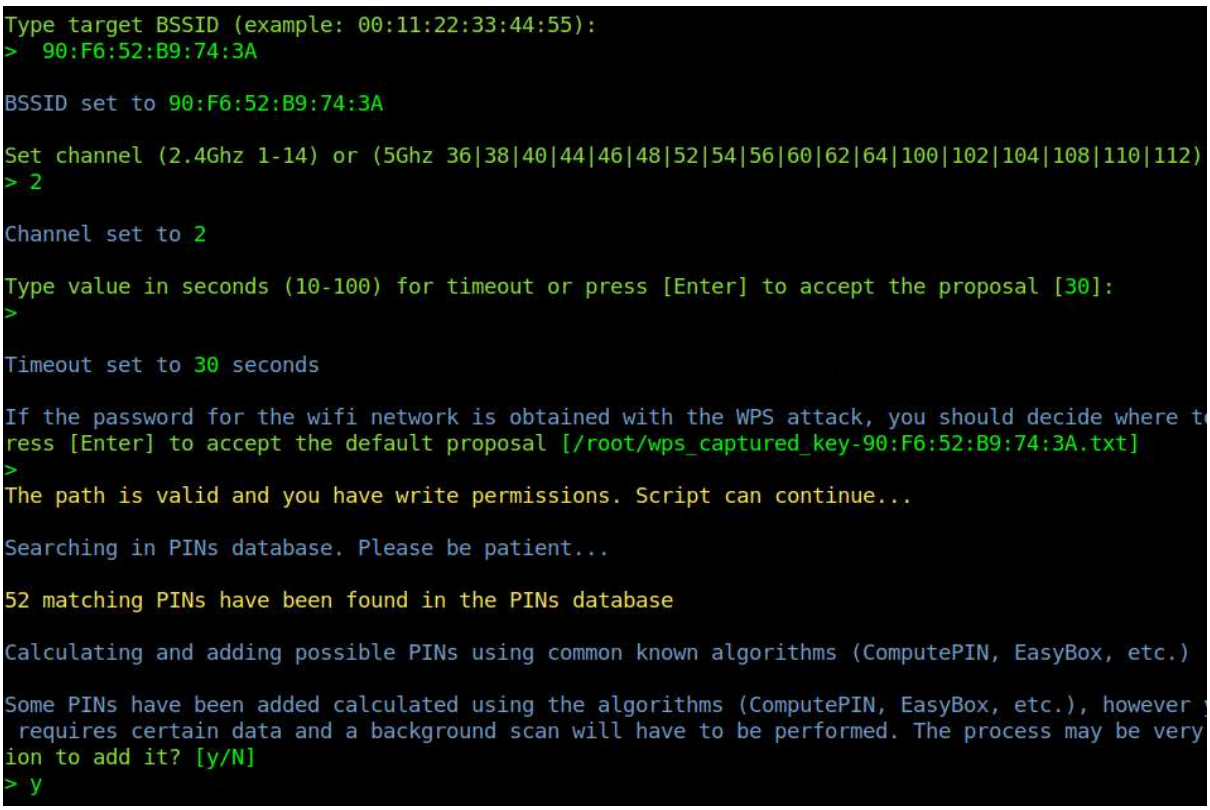

Рис. 14 Внешний вид программы

Первое, что просит программа – ввести MAC адрес сети. Как и оговаривалось выше – его необходимо скопировать из 2 пункта (рис. 12). Затем требуется ввести канал и подтвердить сохранение пароля в специальный файл. Программа предупредит о том, что процесс взлома будет проходить медленно - необходимо согласиться. Начнется процесс перебора.

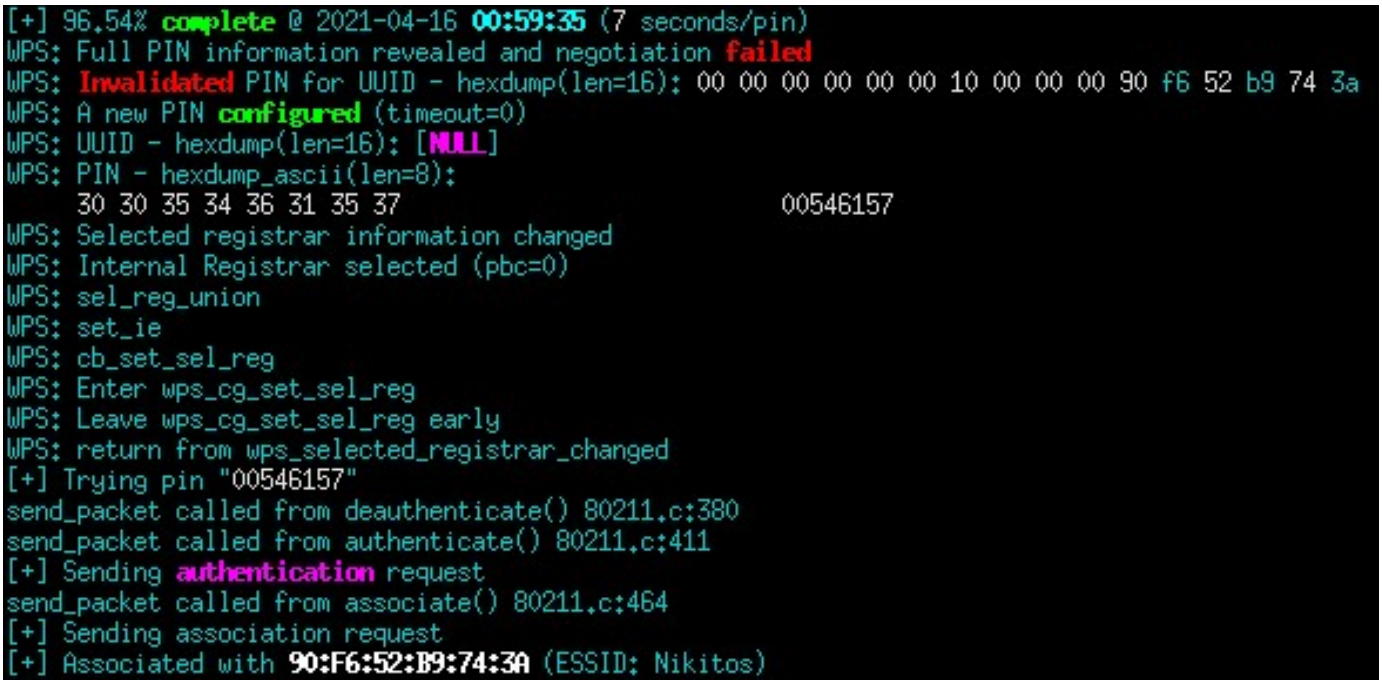

Рис. 15 Работа программы airgeddon

Из рисунка следует, что программа почти завершила процесс перебора. 96.54 процента выполнено и это заняло 59 минут 35 секунд. Скорость подбора – один код раз в 7 секунд. Далее идет информация про текущий пин на рисунке – 00546157. Затем о том, что идет запрос на аутентификацию по пину и, если он не подходит программа пробует следующий.

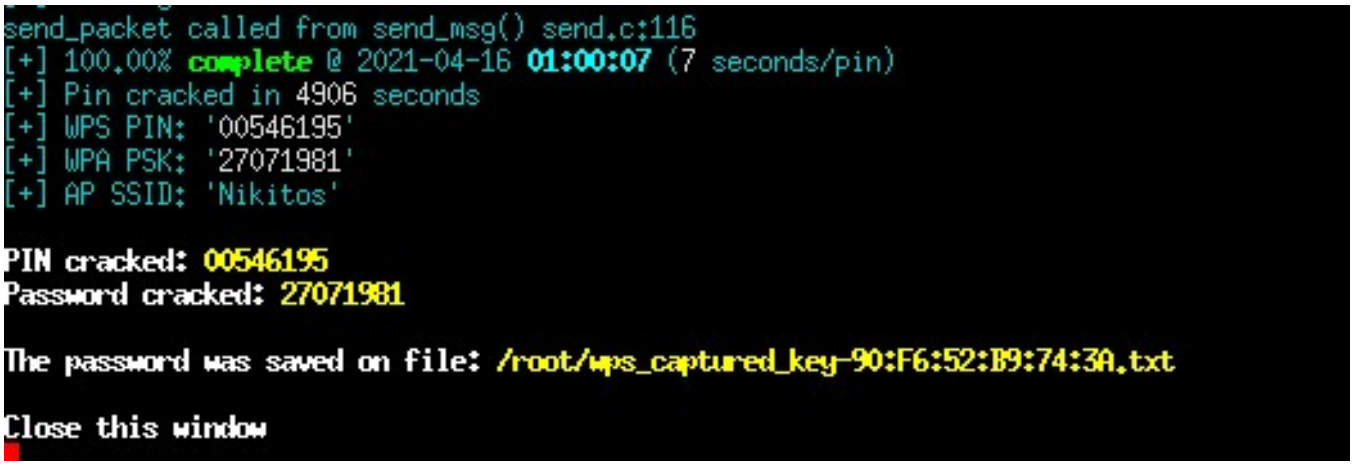

Рис. 16 Итог работы программы

На рисунке видно, что пароль подобрался за 1 час 7 секунд. Код от подключения по WPS – 00546195, а пароль от сети Wi-Fi – 27071981. Пароль сохранен в специальный файл, который имеет расширение txt. Злоумышленнику даже не приходиться получать пароль от сети, программа автоматически его получает и показывает. Данные от сети действительно совпадают с данными на маршрутизаторе:

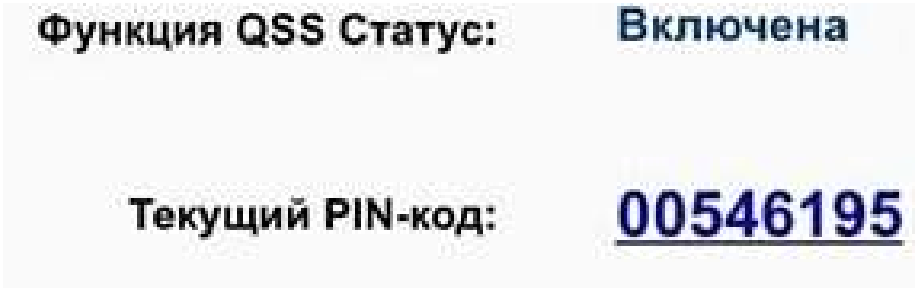

Рис. 17 Пинкод совпадает с полученным

WPS – действительно удобная функция для пользователя, однако, она несет за собой риски связанные с безопасностью. Некоторые маршрутизаторы защищены от подобных методов подбора и автоматически блокируют попытки взлома. Но функция WPS остается очень уязвимой, постоянно появляются новые способы подбора пинкода. Существуют методы позволяющие взломать WPS буквально за минуту. Поэтому в любой беспроводной сети – домашней или корпоративной, эту функцию необходимо отключать. Аудитору безопасности беспроводных сетей стоит обращать внимание в первую очередь на WPS.

Заключение

Данная курсовая работа состоит из вводной, теоретической и практической частей. В курсовой работе были рассмотрены: основные уязвимости, связанные с использованием беспроводных сетей, практическая реализация некоторых угроз и стандарты, и меры защиты беспроводного соединения.

Как показало проведенное исследование способов и методов защиты беспроводных сетей: к вопросу безопасности необходимо подходить комплексно и ответственно. Требуется проведение аудитов безопасности, мониторинг подключенных пользователей, постоянный анализ сети на возможные уязвимости.

Несмотря на возможные угрозы безопасности беспроводной сети, их продолжают использовать и развивать. В действительности, большинство уязвимостей без особых проблем возможно избежать, если использовать современное оборудование, не игнорировать советы безопасности и использовать надежные пароли. Для компаний важным аспектом защиты является – контроль сотрудников и их действий. Любая система безопасности рушится при безответственном отношении к правилам и установкам отдела безопасности.

В заключении следует отметить, что несмотря на важность методов и средств защиты беспроводного соединения, к вопросу безопасности необходимо подходить целесообразно. Большинству обычных пользователей хватит выполнения трех действий: применение стандарта WPA2, отключение WPS и использование длинного пароля.

Заявленная в начале курсовой работы цель исследования: «Проанализировать методы и средства защищенности беспроводных сетей» - была достигнута. Были рассмотрены основные уязвимости и способы их ликвидации с помощью методов и средств анализа беспроводных сетей. Был проведен обзор источников информации: стандартов безопасности, специализированных журналов и специализированных вебсайтов.

Результаты курсовой работы рекомендуется использовать пользователям беспроводных сетей, небольшим предприятиям и начинающим специалистам безопасности, которые в ходе своей деятельности сталкиваются с необходимостью анализа и защиты беспроводных сетей. Вероятность избежать уязвимостей полностью отсутствует, что делает эту проблему актуальной каждый день.

Список используемых источников

Нормативно технические документы:

1) 802.11-2016 - IEEE Standard for Information technology —Telecommunications and information exchange between systems Local and metropolitan area networks—Specific re-quirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 2016.

2) Министерство Связи и Массовых Коммуникаций Российской Федерации приказ от 14 сентября 2010 года N 124 Об утверждении Правил применения оборудования радиодоступа. Часть I. Правила применения оборудования радиодоступа для беспроводной передачи данных в диапазоне от 30 МГц до 66 ГГц (с изменениями на 6 июля 2020 года)

Электронные ресурсы:

3) Журнал «Хакер»; «Hack TV: взлом телевизора». – Режим доступа: https://xakep.ru/2011/07/04/56127/

4) Журнал «Хакер»; «Доступ к смартфону по NFC». – Режим доступа https://xakep.ru/2012/07/31/59074/

5) Издание «Лента»; «Миллиарды гаджетов оказались под угрозой взлома по BlueTooth». – Режим доступа: https://lenta.ru/news/2020/05/20/bias/

6) Сайт компании «ManageEngine». «What is Rogue Device detection & prevention?». – Режим доступа https://www.manageengine.com/products/oputils/rogue-detection-and-prevention.html

7) Информационный портал SecurityLab. «Как взлмывают корпоративный Wi-Fi: новые возможности». - Режим доступа: https://www.securitylab.ru/analytics/471816.php

8) Веб-сайт «Хабр». «Wi-Fi становится безопаснее». Режим доступа - https://habr.com/ru/post/424925/

9) Веб-сайт «Wi-Fi.org». «Discover Wi-Fi. Security». Режим доступа - https://www.wi-fi.org/discover-wi-fi/security

10) Сайт компании «Kaspersky». «Защита от атак типа MAC-спуфинг». Режим доступа: https://support.kaspersky.com/KESWin/11.4.0/ru-RU/174954.htm

11) Сайт компании «Tp-Link». «Configure rogue AP detection on EAP/Omada Controller». Режим доступа: https://www.tp-link.com/ru/support/faq/1013/

12) Сайт «sviehb.files.wordpress.com». «Brute forcing Wi-Fi Protected Setup» - Режим доступа: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

13) Форум дистрибутива Linux «Kali». «WPS pixie Dust Attack». Режим доступа: https://forums.kali.org/showthread.php?24286-WPS-Pixie-Dust-Attack-(Offline-WPS-Attack)

14) Сайт разработчика программы «Hashcat». Режим доступа: https://hashcat.net/cap2hccapx/

15) Официальный сайт разработчика «Hashcat». «Example hashes». Режим доступа: https://hashcat.net/wiki/doku.php?id=example_hashes

16) Сайт «Hackware». Продвинутые техники создания словарей. Режим доступа: https://hackware.ru/?p=15350#3

17) Сайт «HackWare». «Эффективный подбор WPS ПИНа». Режим доступа: https://hackware.ru/?p=4080

18) Сайт «Wi-Fигид». «Тот же WiFi Warden, только для Windows». Режим доступа: https://wifigid.ru/vzlom/wifi-dumpper