МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Кафедра систем информационной безопасности

«ДОПУЩЕН К ЗАЩИТЕ»
Зав. кафедрой к.п.н., доцент Р. Ш. Бердибаев
_____ «_____» _____2019 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Уязвимости и способы защиты беспроводных сетей
Специальность: 5В100200 – “Системы информационной безопасности”
Выполнил Пахретдинов Руслан Адылжанович Группа СИБ-15-2
Научный руководитель Маргаров Геворг Иванович

Консультант:
по экономической части:
к. э. н., профессор Ахметбаева Т. Г.
(ученая степень, звание, Ф.И.О)
подпись «20» мая 2019 г.
(подпись)

по безопасности жизнедеятельности:
д. т. н. ст. преп. Бекбасаров Ш. Ш
(ученая степень, звание, Ф.И.О)
_____ «20» мая 2019 г.
(подпись)

по применению вычислительной техники:
к. т. н, доцент Сатпаева Е. Т.
(ученая степень, звание, Ф.И.О)
_____ «28» мая 2019 г.
(подпись)

Нормоконтролер:
Ст. преподаватель, м. т. н., Аскарова Н. Ш.
(ученая степень, звание, Ф.И.О)
_____ «29» 05 2019 г.
(подпись)

Рецензент:
_____
(ученая степень, звание, Ф.И.О)
_____ «_____» _____2019 г.
(подпись)

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Институт систем управления и информационных технологий

Кафедра систем информационной безопасности

Специальность 5В100200 – “Системы информационной безопасности”

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Пахретдинову Руслану Адылжановичу

Тема проекта Уязвимости и способы защиты беспроводных сетей

Утверждена приказом по университету №_124_ от «_26_» _октября_ 2019 г.

Срок сдачи законченного проекта «_____» _____ 2019 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): проект подразумевает проведение исследований уязвимостей беспроводных сетей Wi-Fi и их эксплуатирование, а также способы защиты от возможных атак на данные сети. В качестве проверки уязвимостей реализованы действующие атаки на различные протоколы, обход разных способов защиты Wi-Fi сетей и уязвимостей, связанных с аппаратным обеспечением точек доступа, а также поиск новых способов получения несанкционированного доступа в беспроводную сеть и возможные варианты развития атак. Для защиты будут использоваться стандартные методы, которые может обеспечить функционал любого маршрутизатора, для предотвращения различных атак.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: дипломный проект включает в себя 5 глав, разделенных на подглавы, каждая из которых освещает определенную тематику, используемую для реализации атак и защиты беспроводных сетей.

В первой главе дипломного проекта представлена общая информация по беспроводным сетям: различные протоколы, функции, плюсы и минусы, надежность и безопасность Wi-Fi сетей, а также некоторые хитрости для более простого взаимодействия.

Во второй главе дипломного проекта представлены различные виды атак, с последующей их реализацией и пояснением, использование уже известных

уязвимостей, а также практическая реализация уязвимостей представленных в виде теорий.

В третей главе подробно описывается функционал маршрутизаторов, позволяющий защитить беспроводную сеть

В четвертой главе приводится технико-экономическое обоснование, показывающее актуальность исследования с финансовой точки зрения.

В пятой главе рассматриваются необходимые условия для комфортного проведения исследования.

Перечень графического материала (с точным указанием обязательных чертежей):

1 графическое обоснование протоколов;

2 скрины реализации атак;

3 скрины реализации защиты;

4 скрины;

5 скрины с последующим воздействием на сеть.

Основная рекомендуемая литература:

1 Аманжолова К. Б., Алибаева С. А. Экономика предприятии телекоммуникации: Учебное пособие. - Алматы: АИЭС, 2003

2 Голубицкая Е. А., Жигульская Г. М. Экономика связи. – М. Радио и связь, 2000

3 Мерритт, М. Безопасность беспроводных сетей / М. Мерритт. - М.: 282

4 Защита беспроводных сетей URL: https://habr.com/ru/post/224955/

5 Что такое беспроводная сеть и принципы ее работы URL: http://posetke.ru/wifi/besprovodnie-seti-klassifikaciya-princip-raboti.html

6 Нормы микроклимата URL: http://adilet.zan.kz/rus/docs /V050003789

Конструкции по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Безопасн. жизнедеятель.	Бекбасаров И.Ш.	05.03-20.05	
Экономика	Алибаева т.с.т.	04.03 - 20.05	
Вычисл. техника	Сатимова Б.Т.	04.03 - 24.05	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Протокол WEP	1.02.2019 - 3.02.2019	
Протокол TKIP	4.02.2019 - 5.02.2019	
Протокол CCMP	7.02.2019 - 9.02.2019	
Стандарт WPS	12.02.2019 - 15.02.2019	
Проведение атаки на WEP	16.02.2019 - 17.02.2019	
Проведение атаки на WPA2	18.02.2019 - 20.02.2019	
Использование фишинга	22.02.2019 - 24.02.2019	
Атак PMKID	25.02.2019 - 28.02.2019	
Уязвимость WPS	29.02.2019 - 3.03.2019	
Уязвимости маршрутизаторов	4.03.2019 - 7.03.2019	
Защита с использование NAC	9.03.2019 - 10.03.2019	
Сложность пароля	12.03.2019 - 15.03.2019	
Сокрытие точки доступа	17.03.2019 - 19.03.2019	
Изоляция	22.03.2019 - 24.03.2019	
WPA3 новый стандарт	24.03.2019 - 29.03.2019	
Последствия проникновения	30.03.2019 - 4.04.2019	
Технико-экономическое обоснование	7.04.2019 - 11.04.2019	
Безопасность жизнедеятельности	13.04.2019 - 17.04.2019	

Дата выдачи задания «___» _____2019 г.

Заведующий кафедрой _____ (_____)
(Подпись) (Ф.И.О)

Научный руководитель проекта _____ (Сайтимова Б.Т.)
(Подпись) (Ф.И.О)

Задание принял к исполнению студент _____ (Тахтодинов Р.А.)
(Подпись) (Ф.И.О)

АННОТАЦИЯ

Целью данной дипломной работы является проведение научного исследования беспроводных сетей. Поиск уязвимостей и способов защиты, в частности рассмотрение самого распространенного протокола WPA2 с целью способов получения несанкционированного доступа к беспроводной сети. Проведение практических атак на беспроводные сети, успешная попытка взлома нового протокола WPA3 путём специальной настройки уже существующих инструментов, а также компрометация часто используемых роутеров, атака, связанная с уязвимости в аппаратном обеспечении. А также реализация следующих шагов после получения несанкционированного доступа в сеть, сканирование доступных устройств и их последующий взлом. Построение правильной защиты беспроводной сети, с целью обеспеченья целостности и конфиденциальности, используя различные инструменты обеспечения безопасности.

АНДАТПА

Бұл дипломдық жұмыстың мақсаты сымсыз желілерге ғылыми зерттеу жүргізу болып табылады. Осалдықтар мен қорғау тәсілдерін іздеу, атап айтқанда сымсыз желіге рұқсатсыз кіру жолдарын алу мақсатында WPA2 ең таралған протоколын қарау. Сымсыз желілерге практикалық шабуылдар жүргізу, Қолданыстағы құралдарды арнайы баптау жолымен жаңа WPA 3 хаттамасын бұзуға сәтті әрекет ету, сондай-ақ жиі пайдаланылатын роутерлерді ымыралау, аппараттық қамтамасыз етудегі осалдыққа байланысты шабуыл. Сондай-ақ желіге рұқсатсыз кіруді алғаннан кейін келесі қадамдарды іске асыру, қол жетімді құрылғыларды сканерлеу және оларды кейіннен бұзу. Қауіпсіздікті қамтамасыз етудің түрлі құралдарын пайдалана отырып, тұтастық пен құпиялылықты қамтамасыз ету мақсатында сымсыз желіні дұрыс қорғауды құру.

ANNOTATION

The purpose of this thesis is to conduct scientific research of wireless networks. Search for vulnerabilities and security methods, in particular consideration of the most common WPA2 Protocol for ways to gain unauthorized access to the wireless network. Carrying out practical attacks on wireless networks, a successful attempt to break the new WPA 3 Protocol by special configuration of existing tools, as well as compromising frequently used routers, an attack related to a vulnerability in hardware. As well as the implementation of the next steps after obtaining unauthorized access to the network, scanning of available devices and their subsequent hacking. The creation of a right protection of a wireless network, with the aim of ensuring integrity and confidentiality using various tools to ensure security.

Содержание

Введение

WiFi – это возможность передачи данных между устройствами на короткие дистанции без помощи проводов. Устройства, подключенные по беспроводной технологии, образуют сеть.

Технология WiFi одна из самых перспективных на сегодняшний день в области компьютерной связи. WiFi (Wireless Fidelity) – в переводе с английского – «беспроводная преданность». Технологией Wi-Fi называют один из форматов передачи цифровых данных по радиоканалам.

Изначально устройства WiFi были предназначены для корпоративных пользователей, чтобы заменить традиционные кабельные сети. Для проводной сети требуется тщательная разработка топологии сети и прокладка вручную многих сотен метров кабеля.

Сеть WLAN (Wireless Local Area Network – беспроводная локальная сеть) – вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами высокочастотные радиоволны, а не кабельные соединения. Это гибкая система передачи данных, которая применяется как расширение – или альтернатива – кабельной локальной сети внутри одного офиса, здания или в пределах определенной территории.

Данная технология позволяет экономить Ваши средства за счет отсутствия необходимости прокладывать метры кабеля, а простота установки не отнимает время на сложные ремонто-технические работы. Расширение и реконфигурация сети для WLAN не является сложной задачей: пользовательские устройства можно интегрировать в сеть, установив на них беспроводные сетевые адаптеры.

Беспроводные сети используют радиочастоты, поскольку радиоволны внутри помещения проникают через стены и перекрытия. Диапазон или область охвата большинства систем WLAN достигает 160 м, в зависимости от количества и вида встреченных препятствий. Беспроводные сети обычно более надежны, чем кабельные. Скорость работы сравнима со скоростью кабельной сети. Точно так же, как и в обычной сети, пропускная способность сети WLAN зависит от ее топологии, загрузки, расстояния до точки доступа и т.д. Количество пользователей практически неограниченно. Его можно увеличивать, просто устанавливая новые точки доступа. С помощью перекрывающихся точек доступа, настроенных на разные частоты (каналы), беспроводную сеть можно расширить за счет увеличения числа пользователей в одной зоне.

Ядром такой сети является точка доступа (Access Point). Вокруг неё образуется территория радиусом 50-100 метров, называемая хот-спотом, или зоной Wi-Fi.

На сегодняшний день можно уверенно сказать, что WiFi технологии проникли глубоко в нашу жизнь. Так как ежедневно по всему миру используется стандарт 802.11, благодаря которому мы получаем беспроводной выход в интернет, с довольно неплохой скоростью (зависит от

оборудования). Постепенно стандарт 802.11 эволюционирует, увеличивается скорость работы, изменяются способы защиты, так как со временем появляются различные уязвимости, как в аппаратном, так и в программном обеспечении, в связи с этим алгоритмы защиты становятся все сложнее, но при этом все же находятся различные уязвимости. Сейчас сети WiFi востребованы по всему миру, они используются как в личных потребностях, так и в огромных компаниях, для обычного доступа в сеть интернет, так и для доступа во внутреннюю сеть, даже официанты теперь работают с телефона оформляя заказы через сеть. Но не всегда эта сеть довольно хорошо защищена.

1 Теоретическая часть

Термин Wi-Fi не является техническим, но активно применяется современными пользователями. Под аббревиатурой Wi-Fi (от английского сочетания Wireless Fidelity, которое можно дословно перевести как высокая точность беспроводной передачи данных) в настоящее время понимается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Другими словами, под термином Wi-Fi пользователи подразумевают технологии беспроводных локальных сетей – Wireless Local Area Network (WLAN, Wireless LAN). Эти технологии позволяют объединять компьютеры в локальные сети без помощи проводов (т.е. используя радиоволны) и подключать их к Интернету.

Наиболее правильное определение термина Wi-Fi – это торговая марка консорциума Wi-Fi – объединение крупнейших производителей компьютерной техники и беспроводных устройств Wi-Fi. Эта организация курирует коммерческое развитие технологии Wi-Fi на базе стандартов, разработанных и ратифицированных институтом IEEE (группа стандартов 802.11).

Беспроводные локальные сети имеют ряд преимуществ перед проводными локальными сетями:

-быстрое развертывание, что очень удобно в условиях работы вне офиса (например, при проведении презентаций);

-легкое перемещение пользователей мобильных устройств при подключении к локальным беспроводным сетям в рамках действующих зон сети без разрыва соединения благодаря функции роуминга между точками доступа;

-использование современных сетей за счет высоких скоростей для решения очень широкого спектра задач;

-простота организации беспроводной локальной сети в случае, когда прокладка кабеля невозможна.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это, как правило, меньшая скорость и расстояние передачи данных по сравнению с проводными сетями, подверженность влиянию помех и более сложная схема обеспечения безопасности передаваемой информации.

Беспроводные сети могут использоваться как самостоятельно, так и входить в состав сложной архитектуры, содержащих как беспроводные, так и проводные сегменты.

Наиболее часто сети Wi-Fi используются для решения следующих задач:

-беспроводное подключение пользователей к проводным сетям;

-объединение пространственно-разнесенных подсетей в одну общую сеть там, где кабельное соединение подсетей невозможно или нежелательно;

-подключение пользователей к сетям провайдеров интернет услуг.

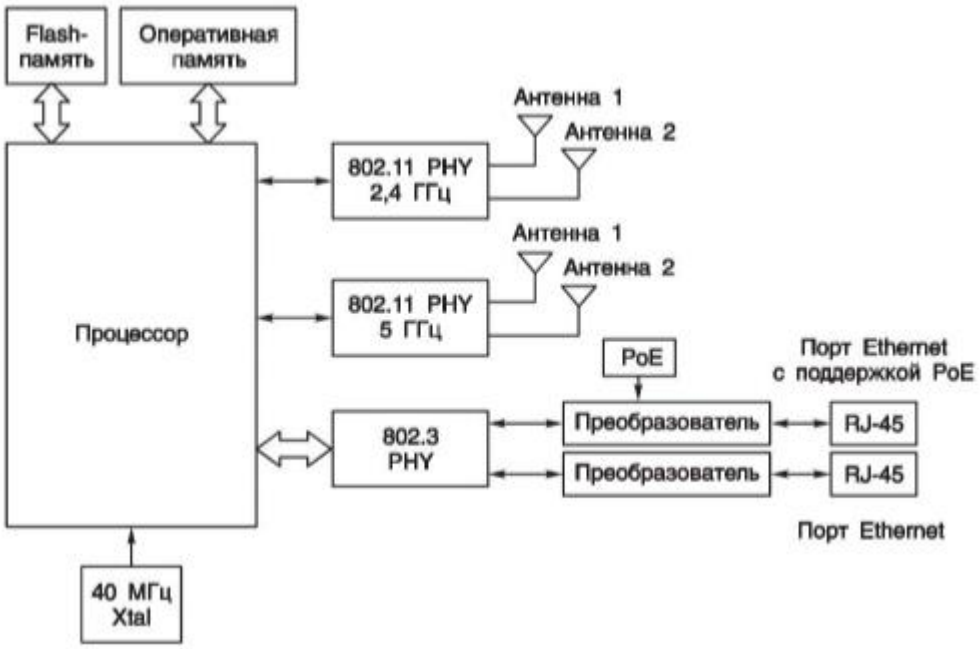


Рисунок 1 - Архитектура точки доступа

Точка доступа изображена на рисунке 1 является основным компонентом инфраструктуры беспроводной сети. Через нее осуществляется обмен информацией между беспроводными клиентскими устройствами, а также подключение к общей распределительной системе (обычно сети Ethernet), для чего у точки доступа имеется сетевой интерфейс Ethernet (uplink port) с разъемом 8p8c (RJ45). Через этот же интерфейс может осуществляться и ее настройка. Точки доступа могут работать как в одном (2.4 или 5 ГГц), так и в обоих диапазонах частот (dual-mode). При этом работа в разных частотных диапазонах может осуществляться параллельно (concurrent dual-mode), если такая функциональность поддерживается точкой доступа.

В зависимости от типа архитектуры беспроводной сети точки доступа можно разделить на два класса: автономные и унифицированные.

Автономные точки доступа (Autonomous Access Point) – это традиционные устройства, которые используются в домашних сетях, сетях небольших офисов, учебных классов, кафе, ресторанов, т.е. там, где не требуется большой зоны покрытия. Автономные точки доступа самостоятельно реализуют все сервисы 802.11 и поэтому работают в сети независимо друг от друга, даже если соединены через коммутаторы.

Унифицированные точки доступа (Unified Access Point) могут работать как автономно друг от друга, реализуя все сервисы 802.11 самостоятельно, так и централизованно контролироваться беспроводным контроллером.

Беспроводной контроллер (Wireless Controller) представляет собой устройство, основной функцией которого является управление, контроль и настройка точек доступа, присутствующих в сети.

Беспроводные контроллеры поддерживают такие функции, как роуминг, управление доступом, шифрование данных, мониторинг клиентов и точек доступа, управление радиочастотными характеристиками.

Основным строительным блоком беспроводных сетей стандарта IEEE 802.11 является базовый набор услуг (Basic Service Set, BSS), который состоит из нескольких станций (station, STA), реализующих общий протокол MAC и состязающихся за доступ к разделяемой среде и передачи данных. Зона покрытия, внутри которой станции, являющиеся членами BSS, остаются на связи, называется базовой зоной обслуживания (Basic Service Area, BSA) (рисунок 2).

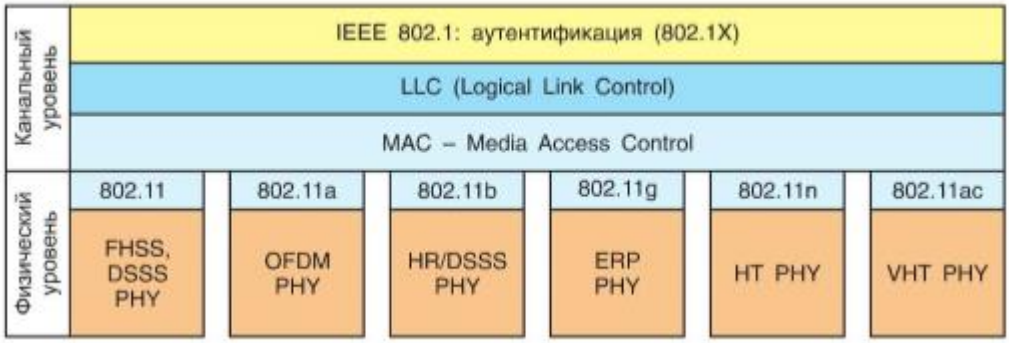


Рисунок 2 – Разновидности стандарта 802.11

Стандарт IEEE 802.11 определяет набор услуг (сервисов), которые должна предлагать беспроводная сеть для обеспечения возможностей, аналогичных функциям проводных сетей. Весь набор разделен на две группы: услуги, предоставляемые станцией, и услуги, предоставляемые распределительной системой.

Услуги первой группы реализуются на каждой станции 802.11, в том числе на станциях, являющихся точками доступа:

-аутентификация;

-отмена аутентификации;

-конфиденциальность данных;

-доставка MSDU;

-динамический выбор частоты (DFS);

-управление мощностью передатчика (TPC);

-синхронизация таймеров верхнего уровня;

-планирование трафика (качество обслуживания, Qos);

-радиочастотные измерения;

-динамическое разблокирование станции (DSE).

Услуги распределительных систем предлагаются между базовыми наборами услуг (BSS). Эти услуги могут быть реализованы на точках доступа

или других специализированных устройствах, подключенных к распределительной системе:

-ассоциация;
-разрыв ассоциации;
-распределение;
-интеграция;
-повторная ассоциация;
-планирование трафика (Qos);
-динамическое разблокирование станции (DSE).

1.1 Протокол WEP

WEP (Wired Equivalent Privacy) – алгоритм обеспечения конфиденциальности и целостности данных, определенный а оригинальном стандарте IEEE 802.11. Конфиденциальность и целостность данных обеспечиваются на основе алгоритма симметричного потокового шифрования RC4 (Rivest's Cipher v.4, код Ривеста).

Алгоритм WEP работает по принципу электронной кодовой книги, в которой каждый блок открытого текста заменяется блоком шифрованного текста. Шифрование начинается после передачи секретных ключей взаимодействующим устройствам. Поскольку WEP является симметричным алгоритмом шифрования, один и тот же ключ используется как для шифрования, так и для дешифрования передаваемых данных (рисунок 3).

WEP использует ключи длиной 40 и 104 бит. Они задаются вручную при настройке шифрования на точках доступа и клиентских устройствах. Ключ длиной 40 бит представляет собой 5 ASCII-символов или 10 шестнадцатеричных чисел. Ключ длинной 104 бит представляет собой 13 ASCII-символов или 26 шестнадцатеричных чисел. При этом обмен пользовательскими данными между взаимодействующими устройствами возможен только в том случае, если они используют одинаковые ключи шифрования. В противном случае клиент не сможет правильно шифровать передаваемые данные и они будут отброшены, точкой доступа или дешифровать кадры, полученные от точки доступа (рисунок 4).

Рисунок 3 – Схема симметричного шифрования

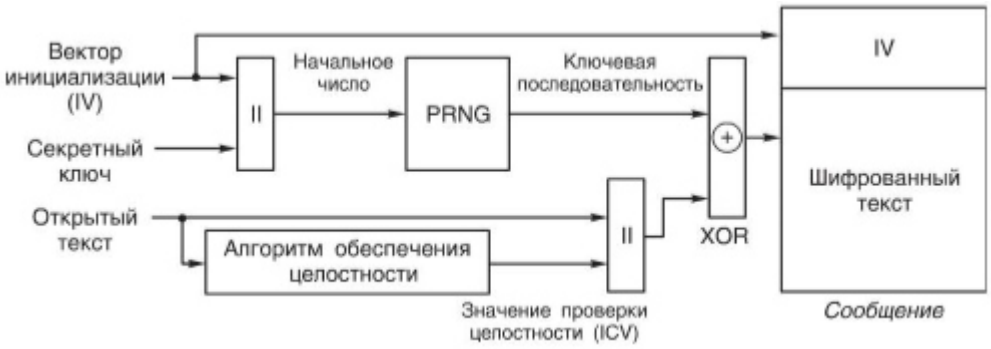


Рисунок 4 – процесс шифрования WEP

Программы сертификации WPA/WPA2

Безопасность беспроводных сетей является весьма важным вопросом, поэтому в 2000 году Wi-Fi Alliance запустил программу сертификации, определяющую требования к безопасности беспроводных сетей, включая поддержку WEP. Быстрое развитие беспроводных технологий, а также уязвимость WEP привели к необходимости разработки новых механизмов защиты.

В дополнение к функциям безопасности, существовавшим в оригинальном стандарте IEEE 802.11, рабочая группа IEEE 802.11 разработала набор расширенных функций безопасности. Wi-Fi Protected Access(WPA) основывалась на проекте стандарта IEEE 802.11i и представляла собой набор механизмов безопасности, которые позволяли решить большинство проблем с обеспечением защиты сетей 802,11. Вместо протокола WEP в WPA использовали протокол TKIP. Также WPA включала поддержку проверки целостности сообщений. Аутентификация выполнялась на основе протокола IEEE 802.11X с EAP корпоративных пользователей и на основе PSK для домашних пользователей и пользователей небольших офисов.

1.2 Протокол TKIP

Протокол TKIP (Temporal Key Integrity Protocol – протокол целостности временного ключа) был разработан с целью изменения программного обеспечения устройств, аппаратная часть которых способна поддерживать только протокол WEP. TKIP усиливает криптографическую стойкость WEP благодаря использованию нескольких дополнительных функций (рисунок 5). Протокол TKIP предоставляет два сервиса:

-целостность сообщений;

-конфиденциальность данных.

Рисунок 5 – процесс шифрования TKIP

В отличии от WEP, использующего статический базовый ключ, в TKIP применяется усовершенствованный механизм управления ключами. TKIP использует временные ключи, которые генерируются в процессе аутентификации на основе стандарта IEEE 802.11X или на основе PSK. Сгенерированный в процессе аутентификации ключ PMK используется механизмом четырехстороннего рукопожатия для генерации ключа PTK, который является составным и включает несколько ключей.

В 2004 году стандарт IEEE 802.11i был ратифицирован. Параллельно Wi-Fi Alliance представил программу сертификации WPA2, основанную на WPA, но вместо протокола TKIP использующую более криптоустойчивый протокол шифрования CCMP. Аутентификация так же, как и в WPA, выполняется на основе протоколов IEEE 802.X с EAP или PSK. WPA2 позволяет защитить не только кадры данных, но и кадры управления.

1.3 Протокол CCMP

Протокол CCMP (CTR with CBC – MAC Protocol) является обязательным для реализации протоколом работы современных беспроводных устройств и основан на режиме CCM (Counter Mode with CBC – MAC) алгоритм шифрования AES (Advanced Encryption Standart). Требования к алгоритму: симметричный, блочный, должен поддерживать длину блока 128 бит и длину ключа 128, 192, и 256 бит. В итоге в качестве AES был выбран алгоритм Rijndael (рисунок 6).

Режим CCM представляет собой комбинацию режима счета блоков шифра (CTR, Counter) и кода аутентификации сообщения из блочного шифра(Cipher Block Chaining Message Authentication Code, CBC – MAC).

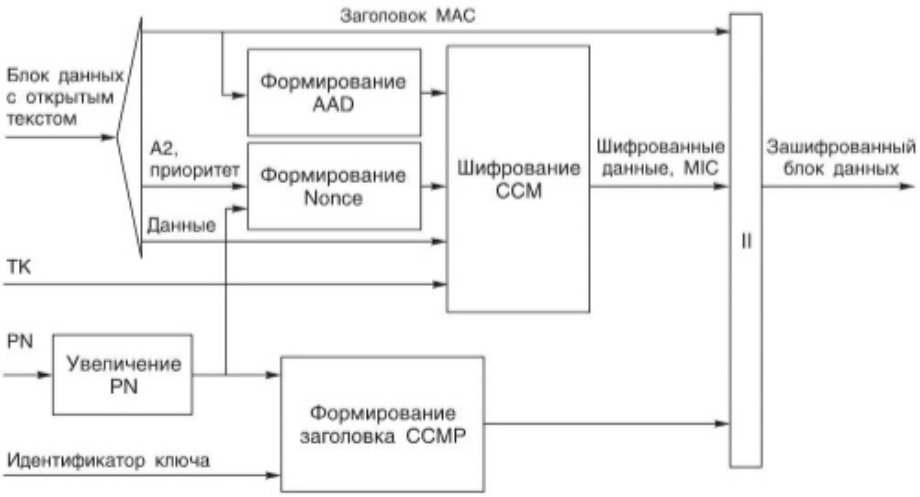


Рисунок 6 – процесс шифрования CCMP

Таблица – 1.1 Виды существующих протоколов

	WEP	WPA	WPA2
Протокол шифрования	Алгоритм RC4 с ручным назначение ключей	Протокол TKIP, основанный на RC4	Протокол CCMP с ключами AES длинной 128 бит
Целостность данных	Линейная хэш-функция	Криптографическая хэш-функция	
Управление ключами	Нет	Да	
Обнаружение атаки типа Replay	Нет	Да	

Таблица – 1.2 разновидности WPA2

WPA/WPA2-Personal	WPA/WPA2-Enterprise
Централизованно неуправляемый режим аутентификации на основе PSK (используется вводимая вручную парольная фраза, общая для всех пользователей сети)	Каждому пользователю назначаются индивидуальные права доступа после IEEE 802.11X-аутентификации
Не требуется сервер аутентификации	Требуется сервер аутентификации IEEE 802.11X AAA с поддержкой EAP и база аутентификационных данных
Ключи шифрования данных уникальны для каждой сессии	

1.4 WPS

Для упрощения настройки возможностей WPA2 в домашних сетях и сетях небольших офисов в 2007 году Wi-Fi Alliance представили дополнительную программу сертификации Wi-Fi Protected Setup (WPS). WPS является методом автоматической настройки параметров WPA2 (в режиме WPA2-Personal) на беспроводных устройствах, предназначенных для рынка SOHO. Основной задачей WPS является обеспечение простоты подключения беспроводных устройств к сети с соблюдением всех требований безопасности и шифрования для пользователей, не обладающих знаниями в области сетевых технологий. При необходимости пользователь может выполнить все настройки WPA2 на WPS-совместимом устройстве вручную.

Устройства с поддержкой WPS предлагают пользователям один из трех методов настройки WPA2:

-Personal Identification Number (PIN): этот метод является обязательным для точек доступа и клиентских устройств. Для создания соединения пользователь через интерфейс настройки устройства вводит персональный идентификационный номер (PIN), который может быть указан на самом устройстве или сгенерирован динамически.

-Push Button Configuration (PBC): этот метод является обязательным для точек доступа и опциональным для клиентских устройств. Используя этот метод, пользователь нажимает на кнопку WPS (физическую или виртуальную) на точке доступа и соответствующем клиентском устройстве, запуская тем самым автоматическую процедуру безопасного соединения.

-Near Field Communication (NFC): этот метод является опциональным. Пользователь при это использует NFC-токен или физически соединяет точку доступа с клиентским устройством.

2 Атаки

2.1 WEP (Wired Equivalent Privacy)

В первую очередь рассмотрим атаку на беспроводные точки доступа, использующие WEP защиту. WEP довольно старый способ защиты беспроводных точек доступа, весь алгоритм был расписан ранее, но ключевая уязвимость кроется в недостатках шифра RC4. Для реализации атаки на точку Wifi защищенной WEP шифрованием, достаточно всего лишь программы aircrack-ng. Данная программа имеет огромные возможности взаимодействия с беспроводной сетью, такие как:

Таблица - 2.1 Возможности aircrack-ng

Имя	Описание
aircrack-ng	Взламывает ключи WEP и WPA (Перебор по словарю).
airdecap-ng	Расшифровывает перехваченный трафик при известном ключе.
airmon-ng	Выставление различных карт в режим мониторинга.
aireplay-ng	Пакетный инжектор (Linux и Windows).
airodump-ng	Анализатор трафика: Помещает трафик в файлы PCAP или IVS и показывает информацию о сетях.
airtun-ng	Создаёт виртуальный интерфейс туннелирования.
packetforge-ng	Создаёт шифрованные пакеты для инъекции.
ivstools	Инструменты для слияния и конвертирования.
airbase-ng	Предоставляет техники для атаки клиента.
airdecloak-ng	Убирает WEP-маскировку с файлов pcap.
airolib-ng	Хранит и управляет списками ESSID и паролей, вычисляет парные мастер-ключи.
airserv-ng	Открывает доступ к беспроводной сетевой карте с других компьютеров.
buddy-ng	Сервер-помощник для easside-ng, запущенный на удалённом компьютере.
easside-ng	Инструмент для коммуникации с точкой доступа без наличия WEP-ключа.
tkiptun-ng	Атака WPA/TKIP.
wesside-ng	Автоматический инструмент для восстановления WEP-ключа.

В первую очередь нужно выбрать сетевой интерфейс, который будет переведен в режим мониторинга сети, в данном случае используется внешний сетевой адаптер Alfa (рисунок 7).

Используем команды “sudo ifconfig”.

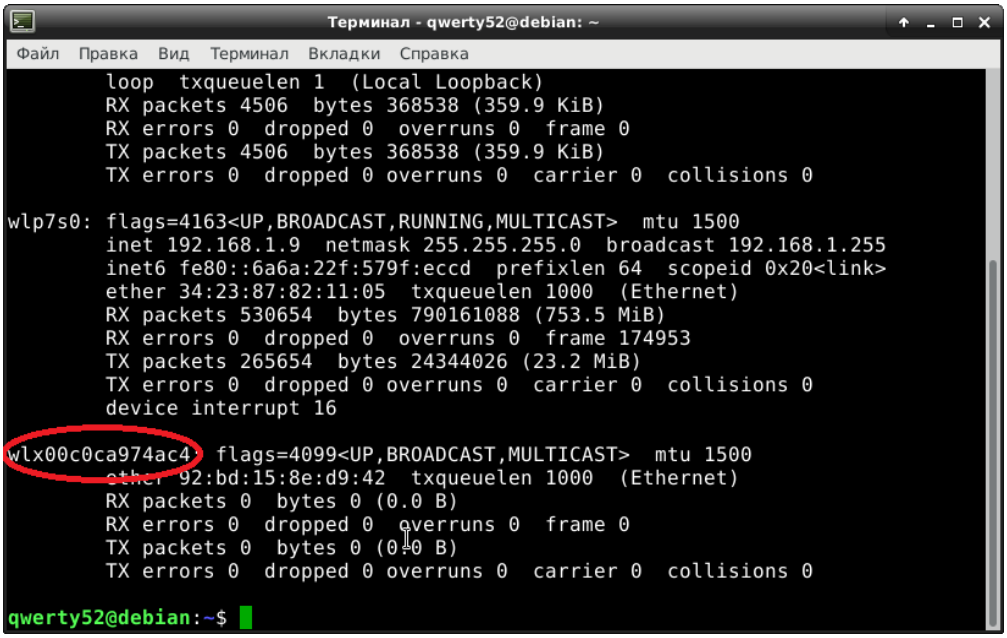


Рисунок 7 – Выбор сетевого интерфейса

Далее выбранный сетевой адаптер переводиться в режим мониторинга с помощью команды “sudo airmon-ng start wlx00c0ca974ac4 (название сетевого адаптера)”, после чего программа сообщает нам о то что сетевой адаптер переведен в режим мониторинга, обращаться к нему мы можем под названием wlan0mon (название сетевого адаптера в режиме мониторинга) (рисунок 8).

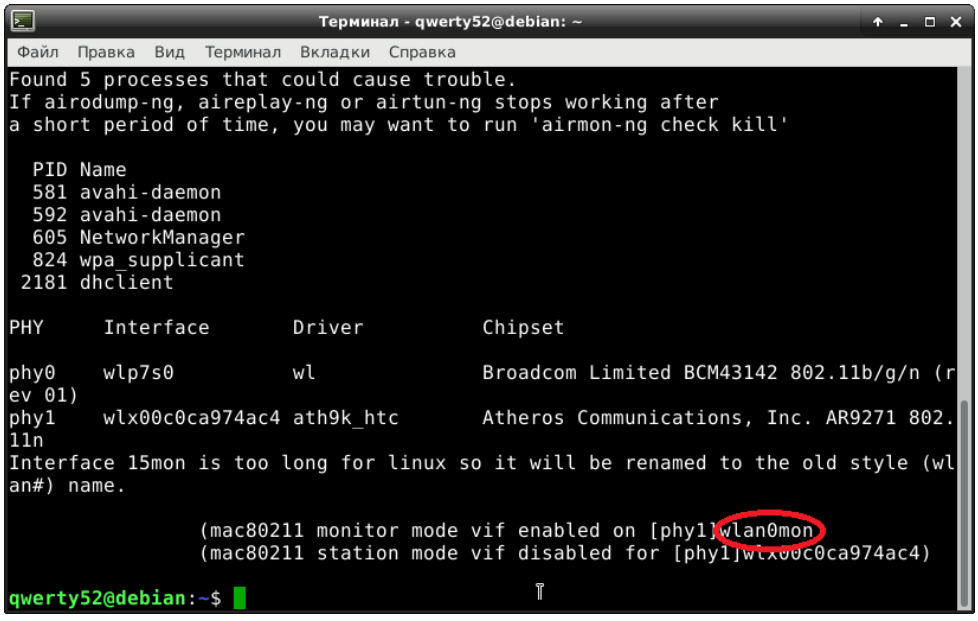


Рисунок 8 –Перевод сетевого адаптера в режим мониторинга

Далее запускаем сканирование ближайших точек доступа wifi при помощи команды “sudo airodump-ng wlan0mon” (указывается интерфейс для сканирования), здесь мы можем увидеть MAC-адрес точки доступа (BSSID), уровень сигнала (PWR), количество пакетов объявлений или маяков (Beacons), количество отловленных пакетов (#Data), число пакетов данных за последние 10 секунд (#/s), канал на котором работает точка доступа (CH), максимальное скорость поддерживаемая AP (MB), используемый алгоритм шифрования (ENC), обнаруженный шифр (CIPHER),используемый протокол аутентификации (AUTH), название точки доступа (ESSID) (рисунок 9).

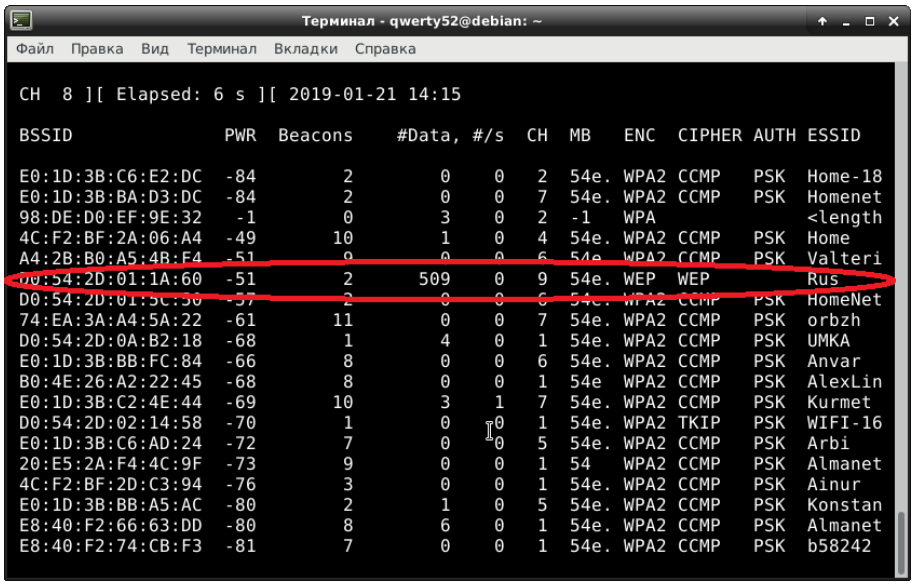


Рисунок 9 – сканирование всех доступных точек доступа

Указываем диапазон каналов для сканирования при помощи команды “sudo airodump-ng –c 7-9 wlan0mon, что бы было проще выбрать цель атаки (рис 10.).

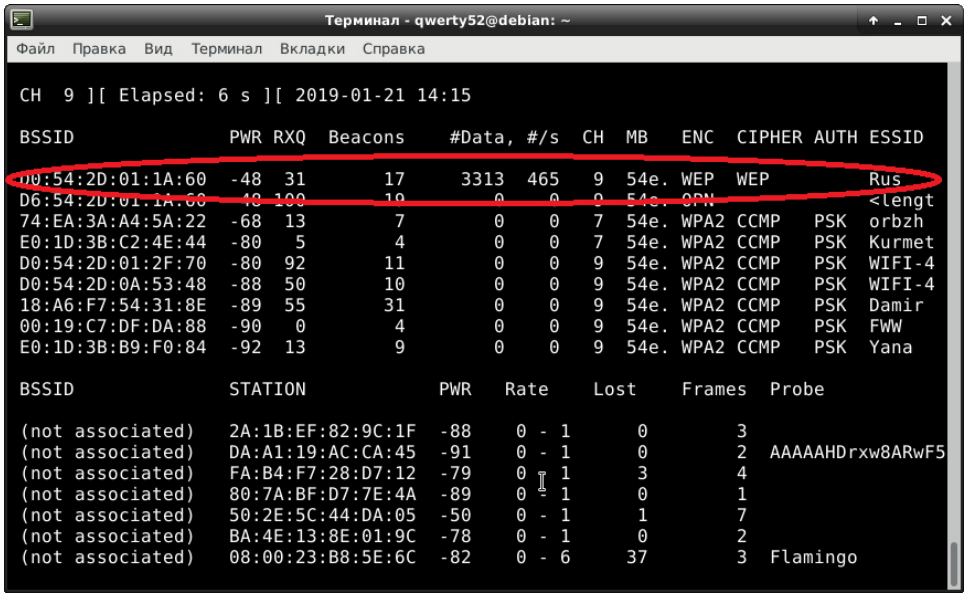


Рисунок 10 – сканирование определенных каналов беспроводных сетей

Выбираем жертву и начинаем мониторить и записывать только выбранную сеть, при помощи команды “sudo airodump-ng –c 9 –bssid D0:54:2D:01:1A:60 –w /home/qwerty52/Документы/ wlan0mon”, здесь мы можем увидеть MAC-адреса клиентов подключенных к данной точке доступа (рисунок 11).

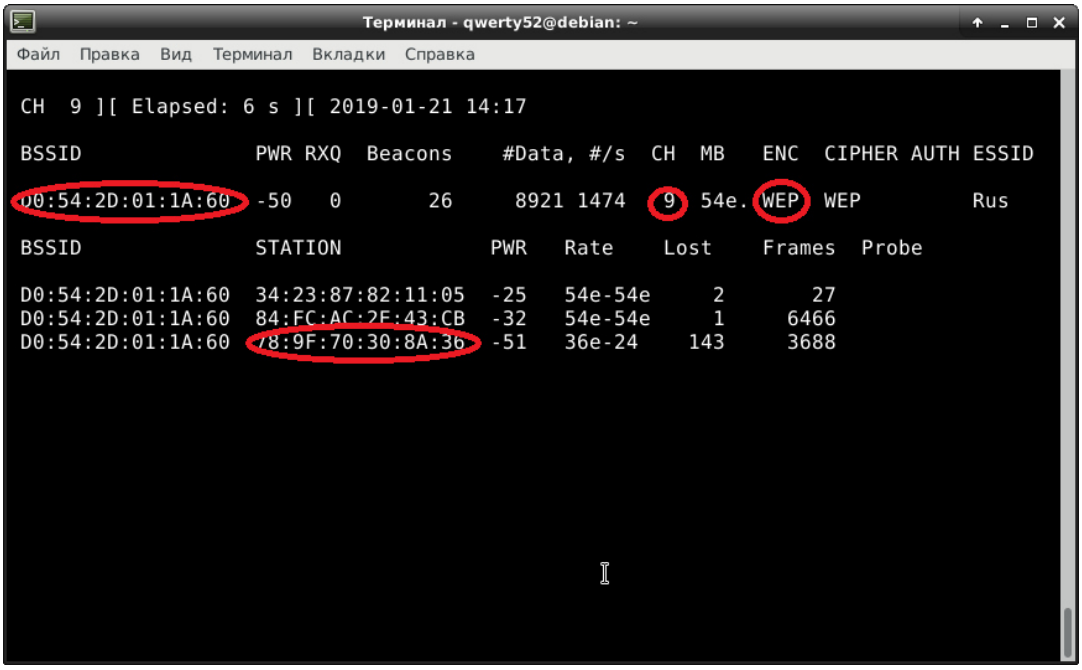


Рисунок 11 – сканирование выбранной точки доступа

Далее нам нужно получить рукопожатия, для этого требуется собрать как можно больше пакетов, так как в некоторых из них время от времени отправляется ключ, который нам нужен для доступа к сети (рисунок 12).

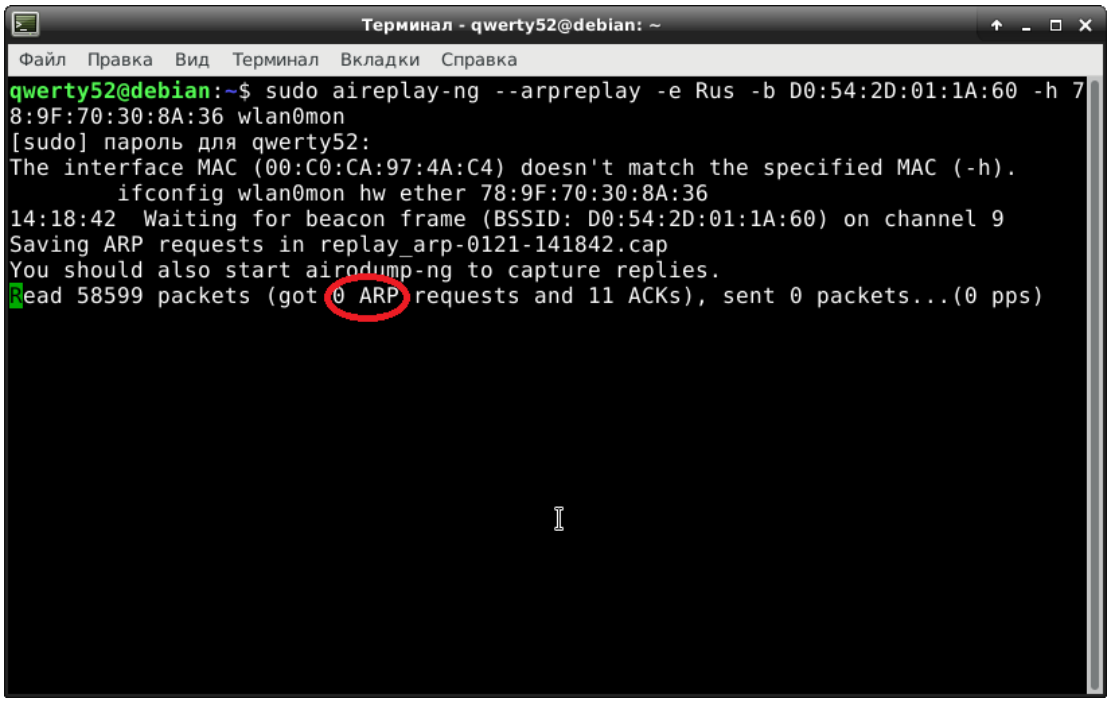


Рисунок 12 – сбор проходящих пакетов

Происходит запись проходящих пакетов от клиент а к точке доступа (рисунок 13).

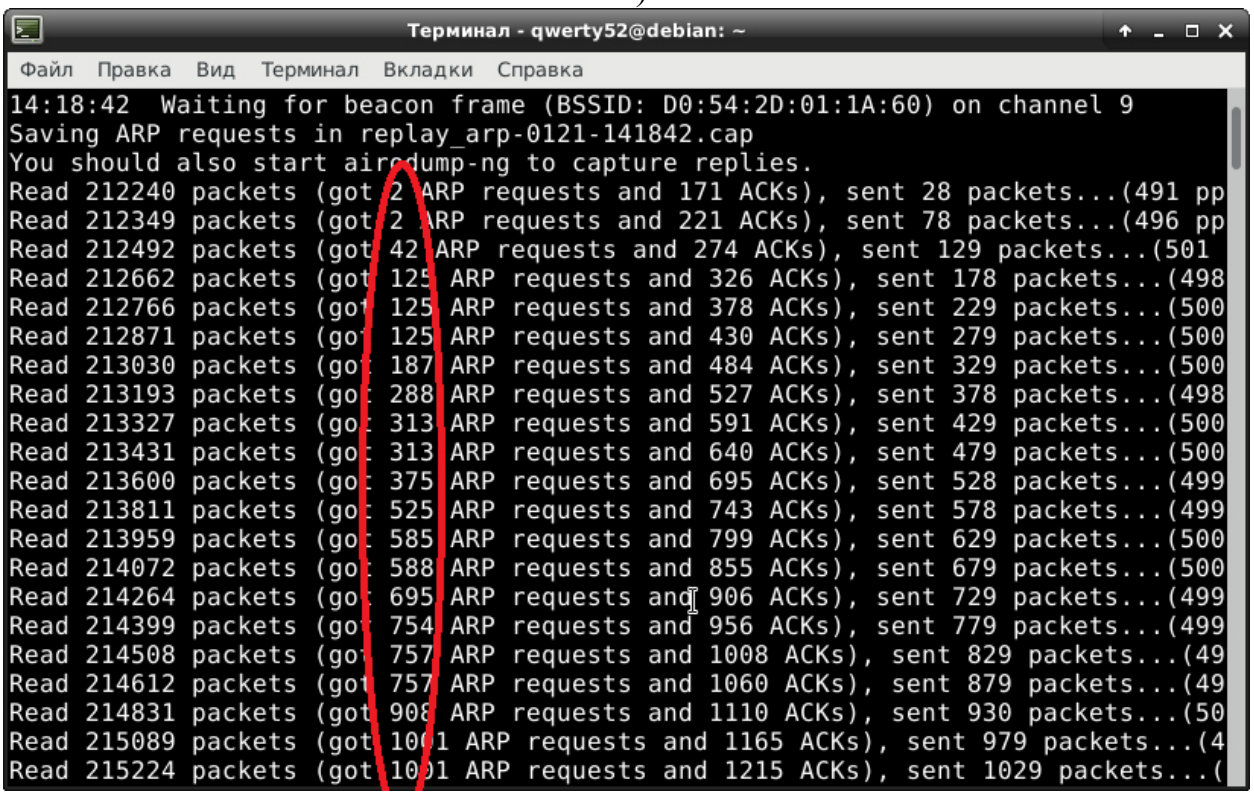


Рисунок 13 – сбор проходящих пакетов

Дальше запускаем программу для дешифрования полученного рукопожатия (рисунок 14).

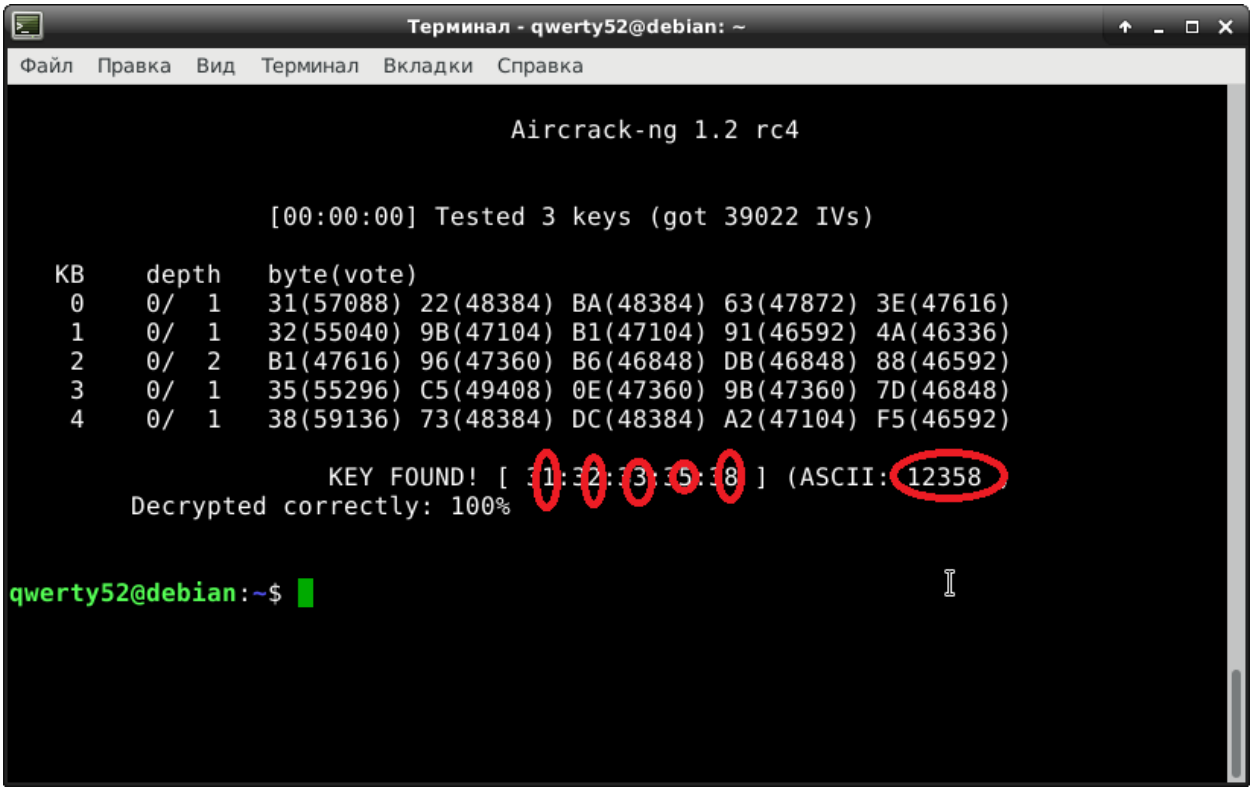


Рисунок 14 – результат дешифровки

Здесь мы видим какие параметры заданы на самом роутере, а также какой ключ используется (рисунок 15).

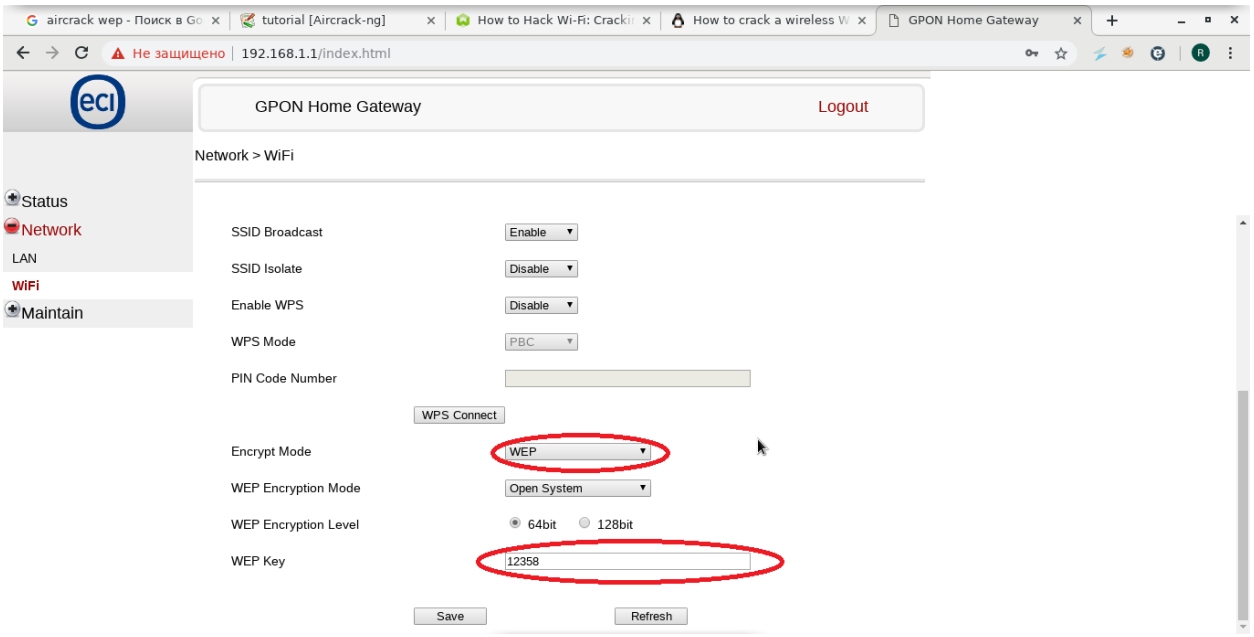


Рисунок 15 – настройки роутера

2.1 WPA2

Технология WPA (Wi-Fi® Protected Access) – это спецификация шифрования данных для беспроводной сети. Она превосходит функцию безопасности WEP благодаря защите доступа к сети за счет использования протокола EAP (Extensible Authentication Protocol), а также обеспечивая механизм шифрования для защиты данных при передаче. Технология WPA предназначена для использования с сервером проверки подлинности 802.1X, который распределяет различные ключи каждому пользователю. Однако ее также можно использовать в менее безопасном режиме "Pre-Shared Key (PSK)". Ключ PSK предназначен для домашних сетей и сетей небольших офисов, где для всех пользователей используется одинаковый пароль. Протокол WPA-PSK также называется WPA-Personal. Протокол WPA-PSK позволяет беспроводному устройству Brother обмениваться данными с точками доступа при помощи способа шифрования TKIP или AES. Протокол WPA2-PSK позволяет беспроводному устройству Brother обмениваться данными с точками доступа при помощи способа шифрования AES.

Протокол TKIP (Temporal Key Integrity Protocol) – это метод шифрования. Протокол TKIP обеспечивает попакетное шифрование, включающее проверку целостности сообщений и механизм повторного шифрования.

Алгоритм AES (Advanced Encryption Standard) – это одобренный Wi-Fi® стандарт надежного шифрования.

В режиме WPA-PSK/WPA2-PSK и TKIP или AES используется общий ключ (PSK) длиной 8 - 63 символа.

В первую очередь нужно выбрать сетевой интерфейс, который будет переведен в режим мониторинга сети, в данном случае используется внешний сетевой адаптер Alfa. Используем команды “sudo ifconfig” (рисунок 16).

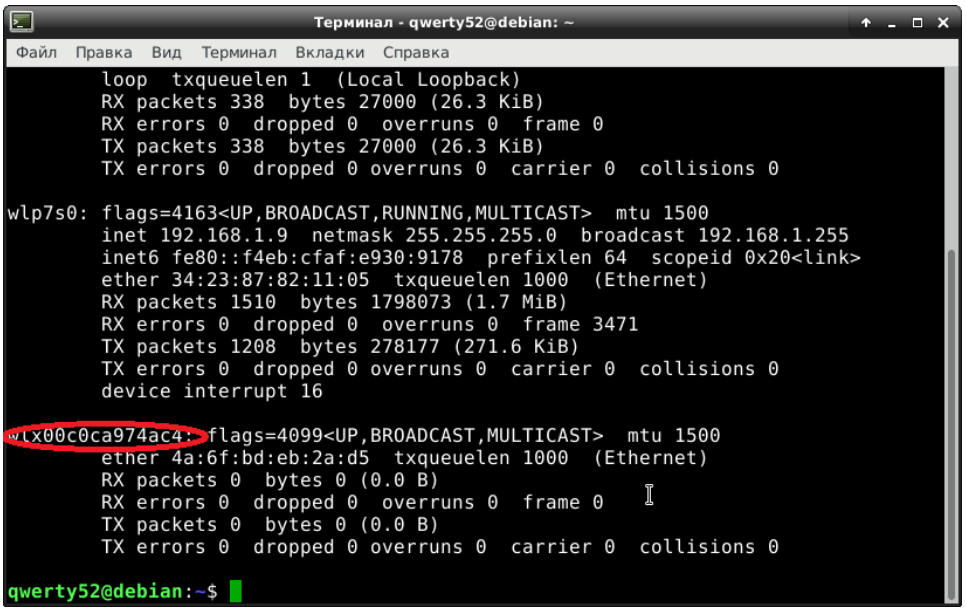


Рисунок 16 – выбор сетевого интерфейса

Далее выбранный сетевой адаптер переводиться в режим мониторинга с помощью команды “sudo airmon-ng start wlx00c0ca974ac4 (название сетевого адаптера)”, после чего программа сообщает нам о то что сетевой адаптер переведен в режим мониторинга, обращаться к нему мы можем под названием wlan0mon (название сетевого адаптера в режиме мониторинга) (рисунок 17).

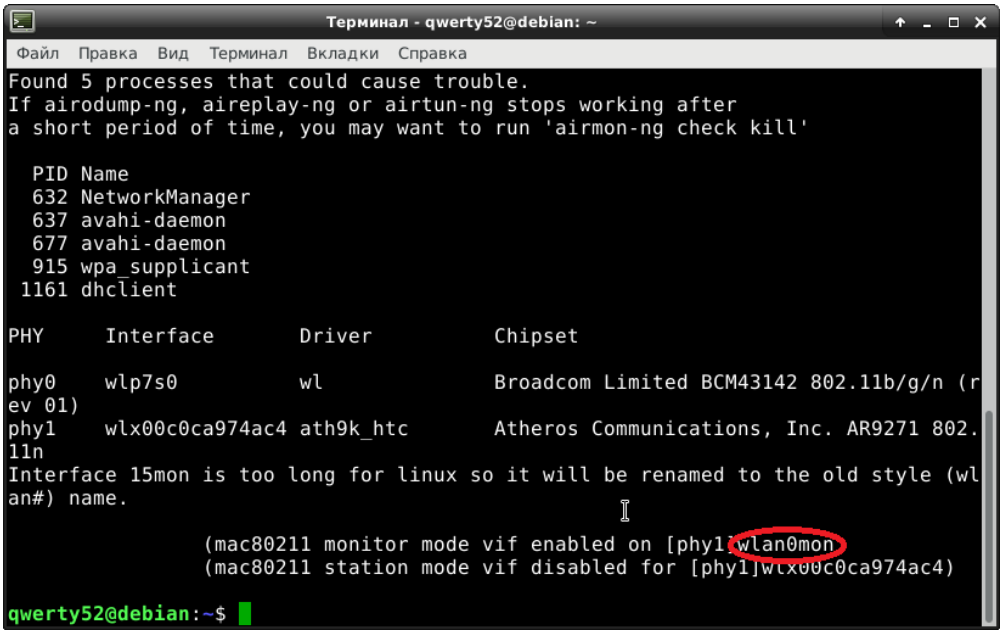


Рисунок 17 – интерфейс переведён в режим мониторинга и переименован в “wlan0mon”

Далее запускаем сканирование ближайших точек доступа wifi при помощи команды “sudo airodump-ng wlan0mon” (указывается интерфейс для

сканирования), здесь мы можем увидеть MAC-адрес точки доступа (BSSID), уровень сигнала (PWR), количество пакетов объявлений или маяков (Beacons), количество отловленных пакетов (#Data), число пакетов данных за последние 10 секунд (#/s), канал на котором работает точка доступа (CH), максимальное скорость поддерживаемая AP (MB), используемый алгоритм шифрования (ENC), обнаруженный шифр (CIPHER),используемый протокол аутентификации (AUTH), название точки доступа (ESSID) (рисунок 18).

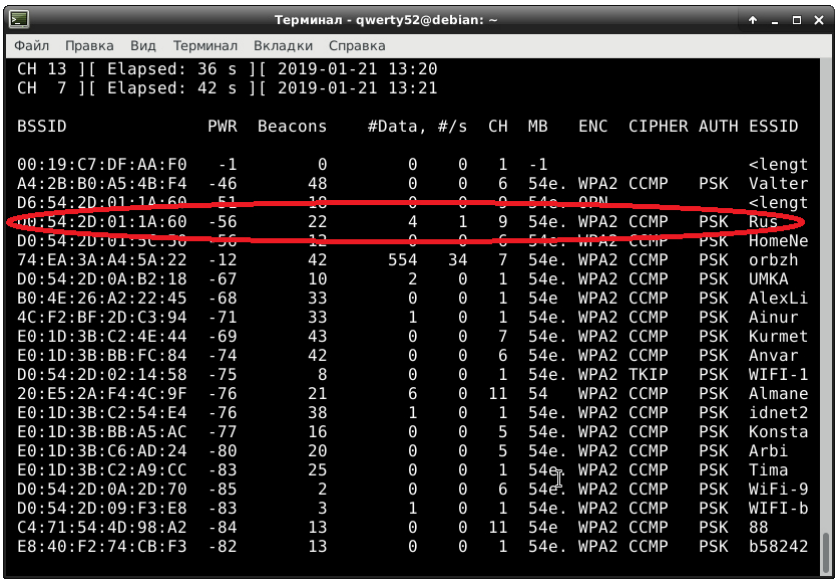


Рисунок 18 – сканирование ближайших точек доступа

Указываем диапазон каналов для сканирования при помощи команды “sudo airodump-ng –c 7-9 wlan0mon, что бы было проще выбрать цель атаки (рисунок 19).

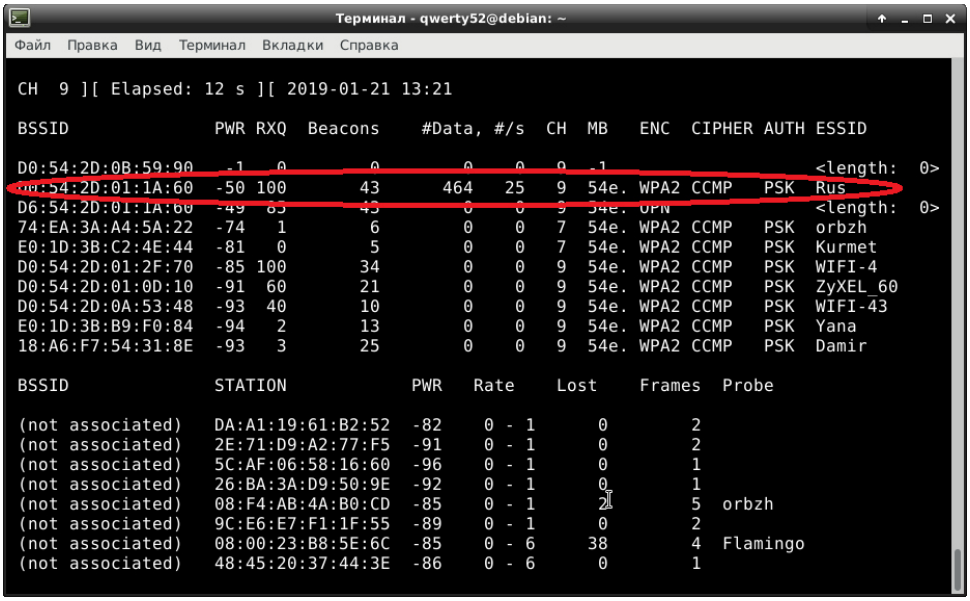


Рисунок 19 – отображение беспроводных сетей, работающих только с 7 по 9 каналы

Выбираем жертву и начинаем мониторить и записывать только выбранную сеть, при помощи команды “sudo airodump-ng –c 9 –bssid D0:54:2D:01:1A:60 –w /home/qwerty52/Документы/ wlan0mon”, здесь мы можем увидеть MAC-адреса клиентов подключенных к данной точке доступа (рисунок 20).

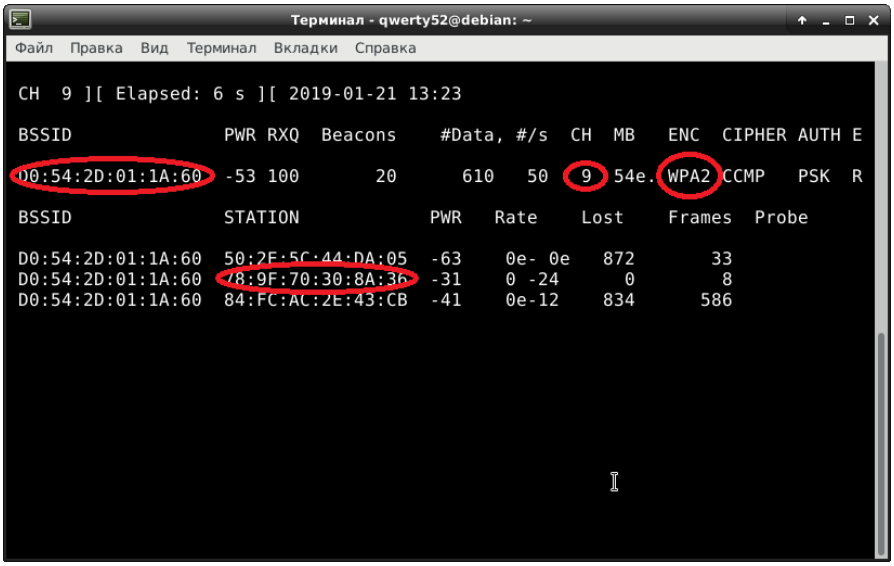


Рисунок 20 – сканирование выбранной точки доступа с записью

Далее выбираем подключенного к данной точке доступа клиента и пытаемся его деаутентифицировать(выкинуть с сети), для его повторного подключения, так как при подключении будет проходить рукопожатие, в котором будет передан зашифрованный пароль. Используется команда в которой параметр “-0” указывает на то что будет проведена деаутентификация, “10” указывает количество отправленных пакетов, “-a” здесь указывается MAC-адрес точки доступа, “-c” MAC-адрес клиента отключаемого от точки доступа (рисунок 21).

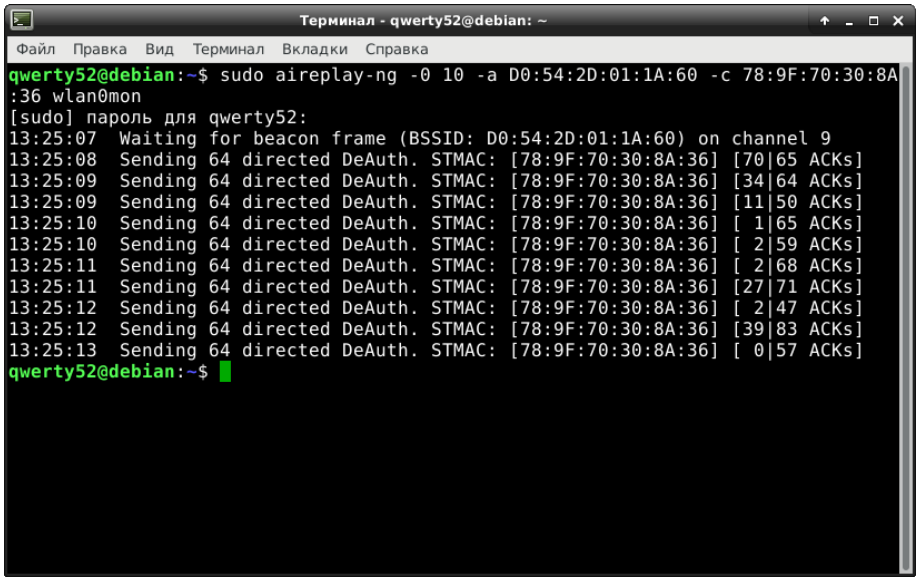


Рисунок 21 – деаутентификация клиента от точки доступа.

В правом верхнем углу появляется надпись о том, что рукопожатие перехвачено, следовательно, мы имеем пароль от точки доступа в зашифрованном виде (рисунок 22).

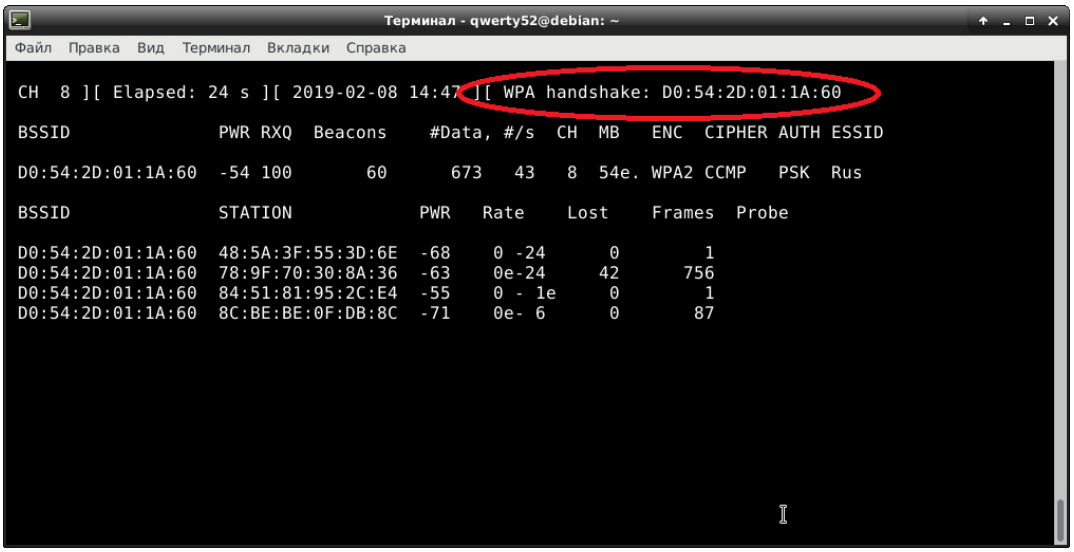


Рисунок 22 – Получение handshake

Далее нам остаётся дешифровать пойманный handshake, это можно сделать разными способами и программами, например aircrack-ng , ей достаточно словаря с возможными паролями, далее она сама генерирует зашифрованный handshake на основ MAC-адреса названия точки доступа, грубо говоря всех параметров которые нам известны, кроме пароля, пароль берётся из словаря и шифруется со всем остальным, после чего программа сверяет полученный шифр, при совпадении мы получаем пароль (рисунок 23).

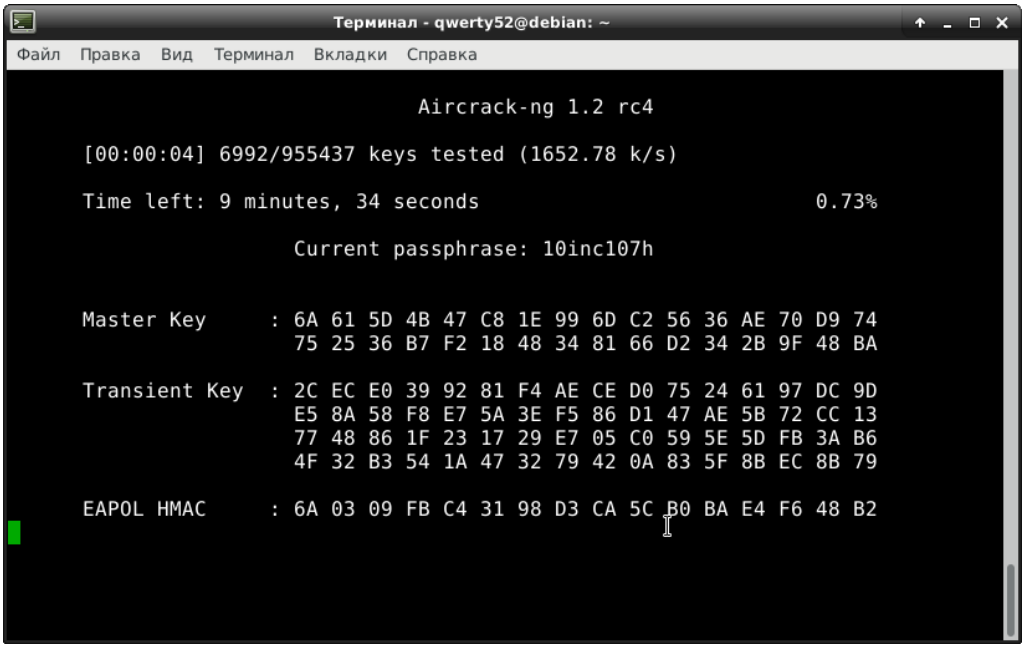


Рисунок 23 – дешифровка пароля

После чего мы получаем пароль в чистом виде (рисунок 24).

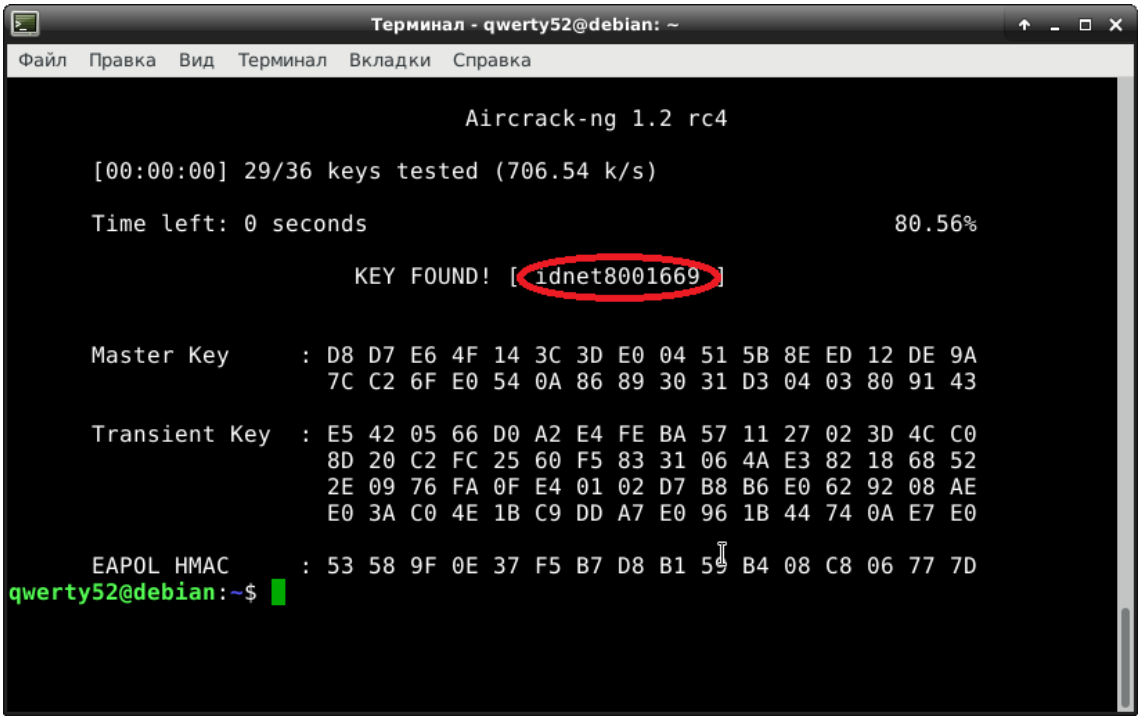


Рисунок 24 – результат дешифровки пароля

Вообще существуют разные способы перебора пароля, допустим aircrack-ng использует мощность процессора для перебора по словарю, но если пароль будет довольно сложным, перебирать он может от нескольких часов до нескольких дней, существуют так же аналоги данной программы такие как Pyrit или Hashcat, которые для перебора используют мощности видеокарты что примерно в 10-13 раз быстрее чем мощность процессора, хотя это зависит от мощности видеокарты, но в любому случае можно использовать внешние ресурсы , существуют веб сервисы по дешифрованию handshake.Достаточно залить туда .cap файл, полученный при сканировании точки доступа (рисунок 25).

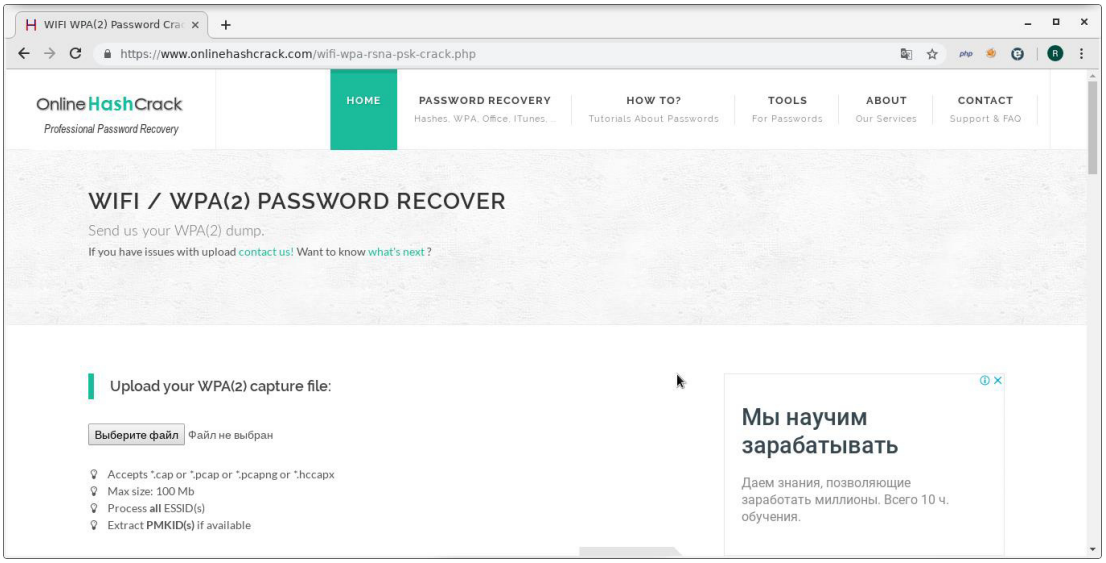


Рисунок 25 – Сервис для дешифровки.

По истечению 2 дней сервис даёт ответ, либо он может дешифровать за несколько минут. Так же предлагаются услуги использования более расширенного словаря с паролями (рисунок 26).

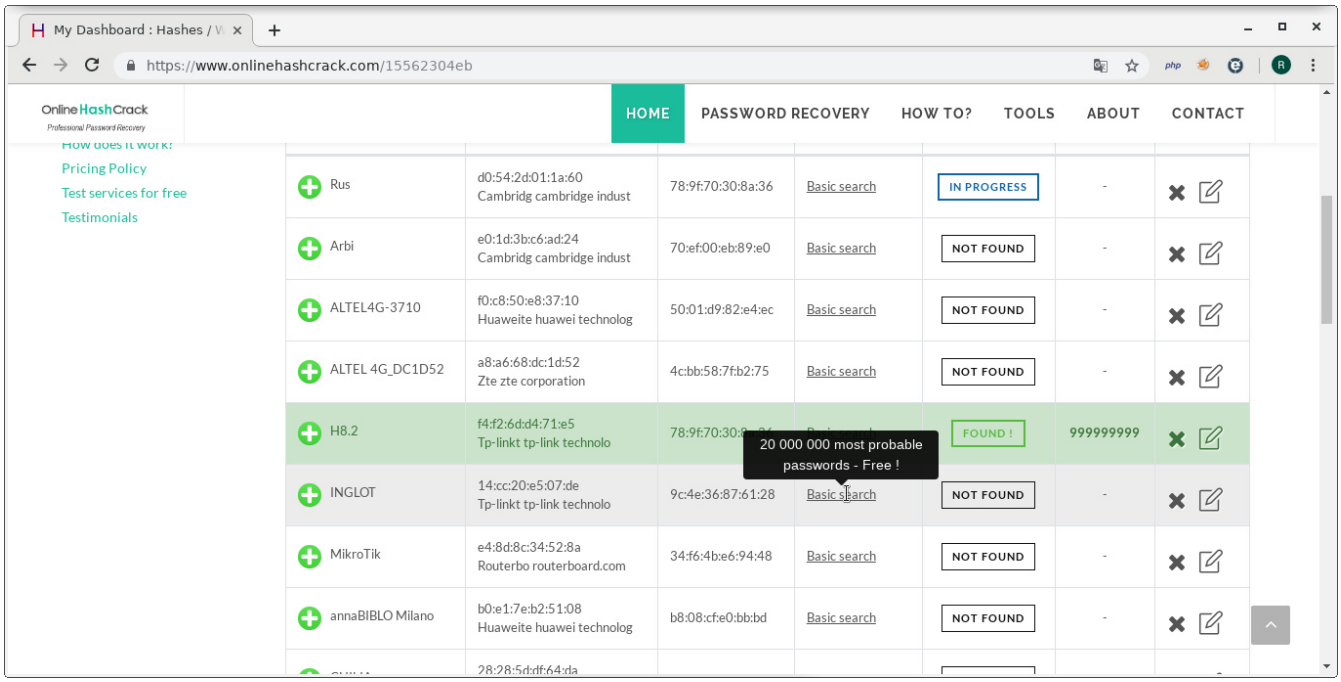


Рисунок 26 – Результат дешифровки

Здесь мы видим какие параметры заданы на самом роутере , а так же какой ключ используется (рисунок 27)

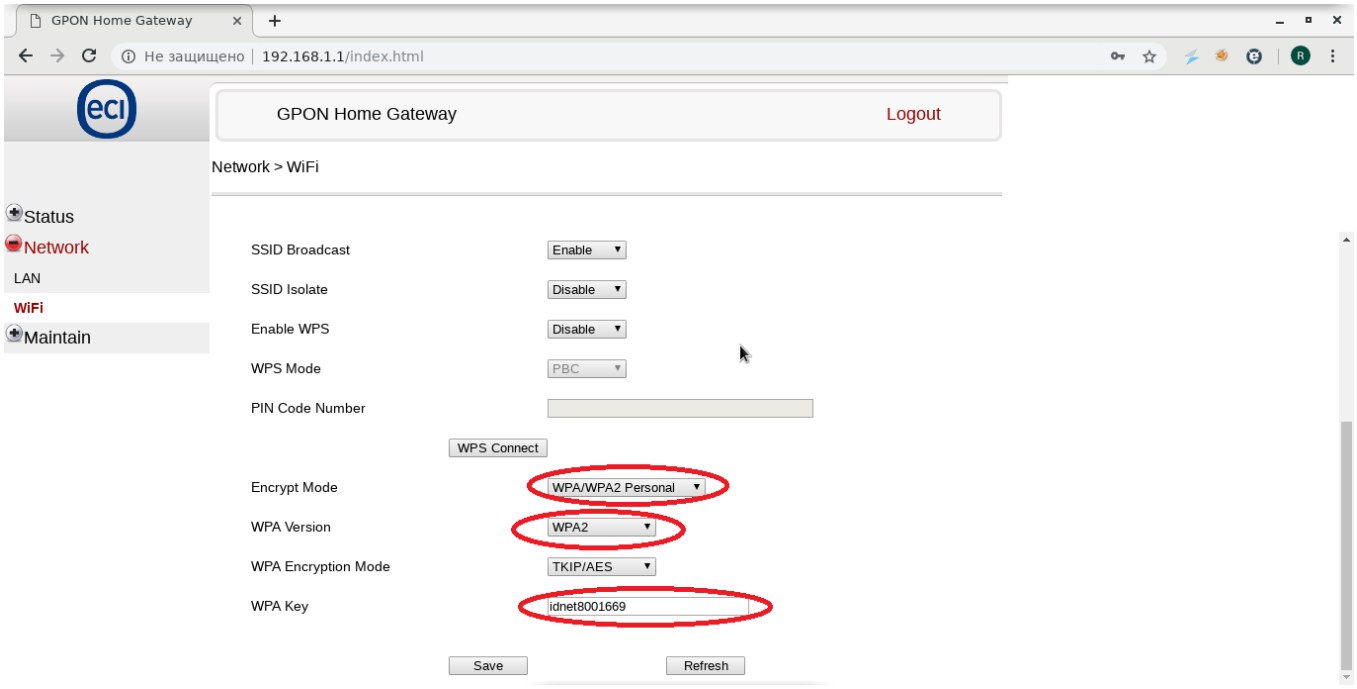


Рисунок 27 – Настройки роутера

2.3 Фишинг (Fishing)

Fluxion – это инструмент аудита безопасности и социальных исследований. Это римейк linset от vk496 с (надеюсь) меньшим количеством ошибок и большей функциональностью. Сценарий пытается извлечь ключ WPA / WPA2 из целевой точки доступа с помощью атаки социальной инженерии (фишинга). Это совместимо с последним выпуском Кали (прокатки). Настройка атак Fluxion в основном выполняется вручную, но экспериментальный автоматический режим обрабатывает некоторые параметры настройки атак.

Функционал:

Сканирует в поисках целевой сети;

Запускает атаку Handshake Snooper;

Захватывает рукопожатие (необходимо для верификации пароля);

Запускает атаку Captive Portal;

Поднимает мошенническую (фальшивую) ТД, которая притворяется оригинальной точкой доступа;

Запускает DNS сервер, перенаправляющий все запросы на хост атакующего, где запущен captive portal (перехватывающий портал);

Запускает веб-сервер, на котором размещён перехватывающий портал, с запросом к пользователю ввести его WPA/WPA2 ключ;

Запускает глушилку, деаутентифицирующую всех клиентов от оригинальной ТД, заманивая их в мошенническую ТД;

Все попытки аутентификации на перехватывающем портале проверяются по ранее захваченному рукопожатию;

Как только введён верный ключ, атака автоматически завершиться, ключ будет записан и клиентам будет позволено подсоединиться к целевой точке доступа.

Данная программа, как и предыдущие работает в терминале и имеет симпатичный интерфейс (рисунок 28).

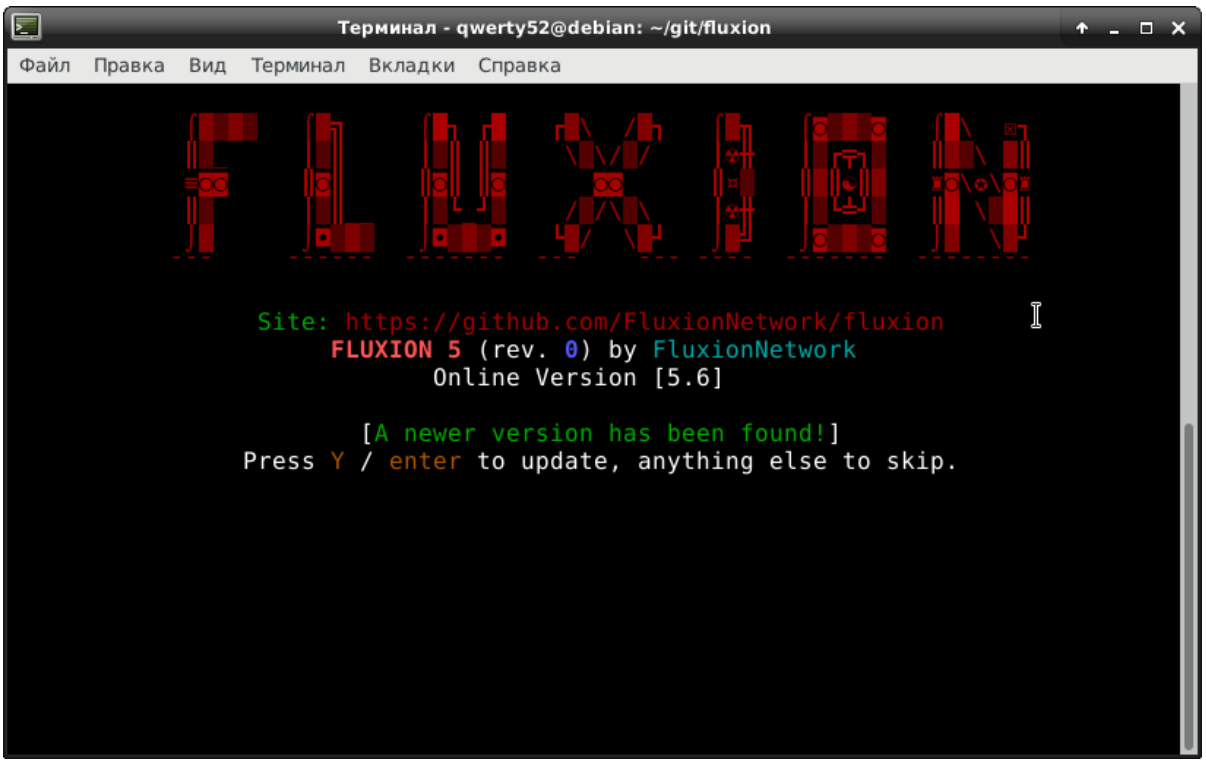


Рисунок 28 – запуск программы Fluxion

Далее программа даёт нам 2 вектора атаки, это создание фейковой точки доступа , либо перехват handshake для последующего создания фейковой точки доступа (рисунок 29).

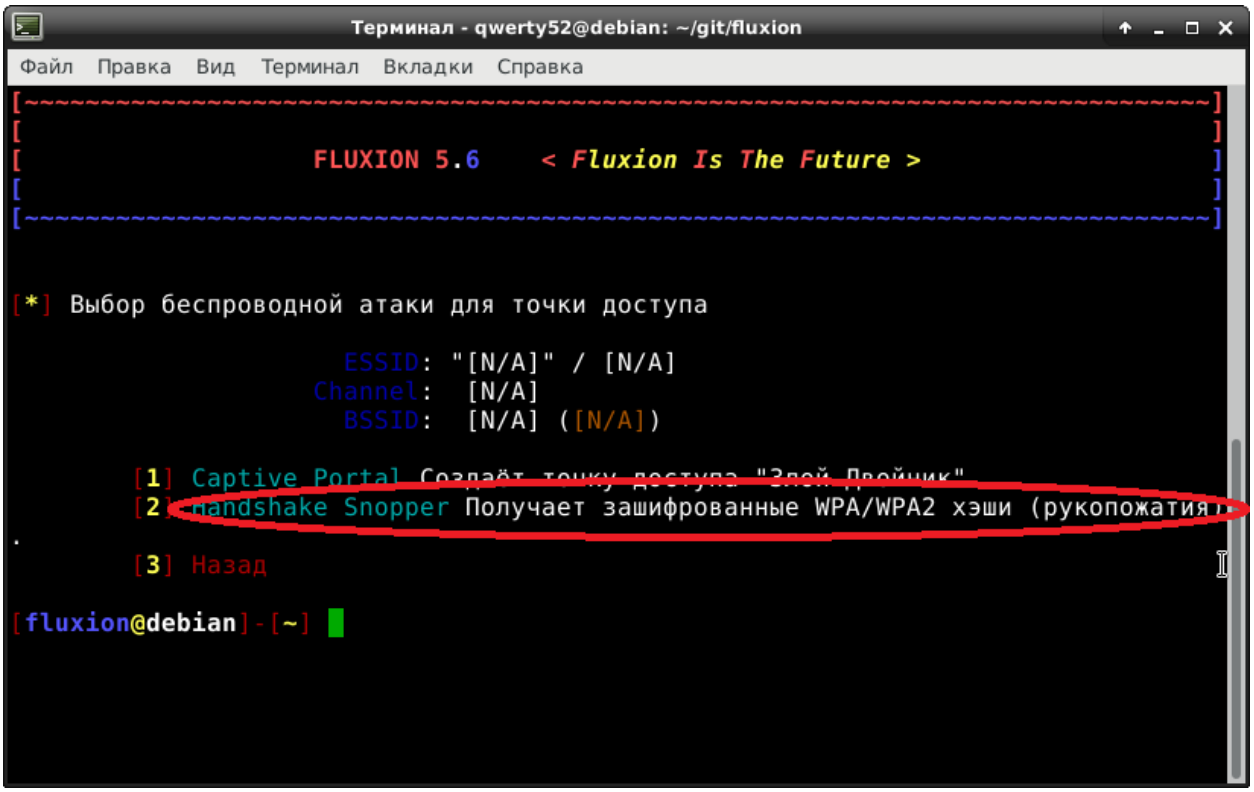


Рисунок 29 – векторы атаки

Далее нам нужно выбрать сетевой интерфейс для проведения мониторинга, в данном случае используется внешний сетевой адаптер Alfa awus036nha (рисунок 30).

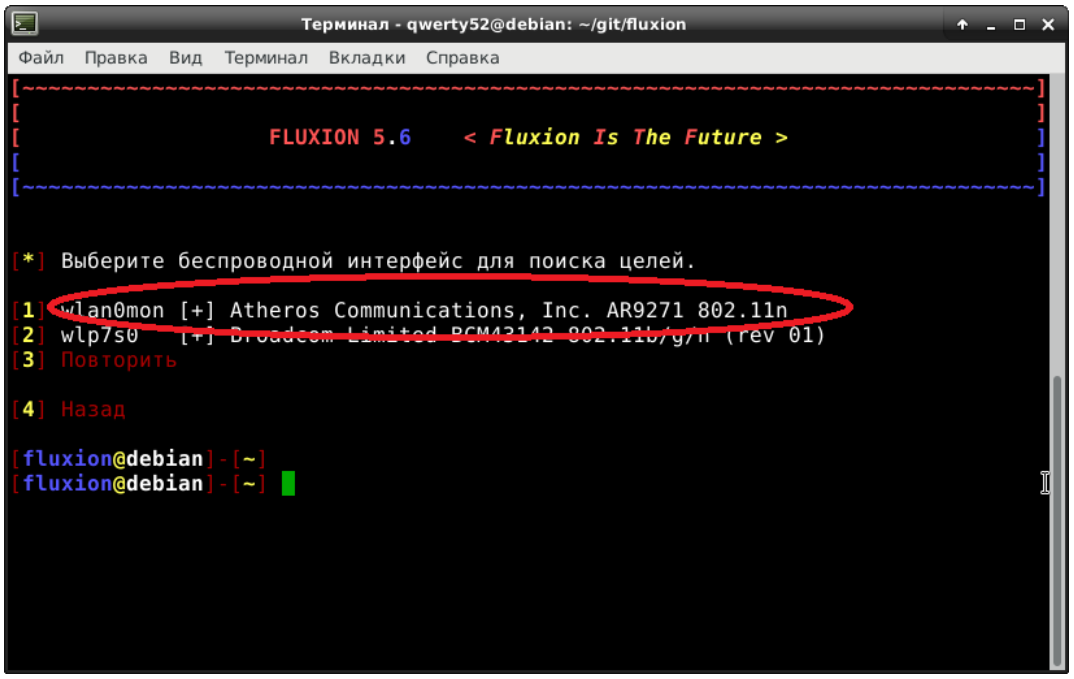


Рисунок 30 – выбор сетевого интерфейса для мониторинга

После чего выбирается канал для мониторинга, есть возможность выбрать определенный канал, либо весь диапазон каналов как 2.4 Ггц так и 5 Ггц (рисунок 31).

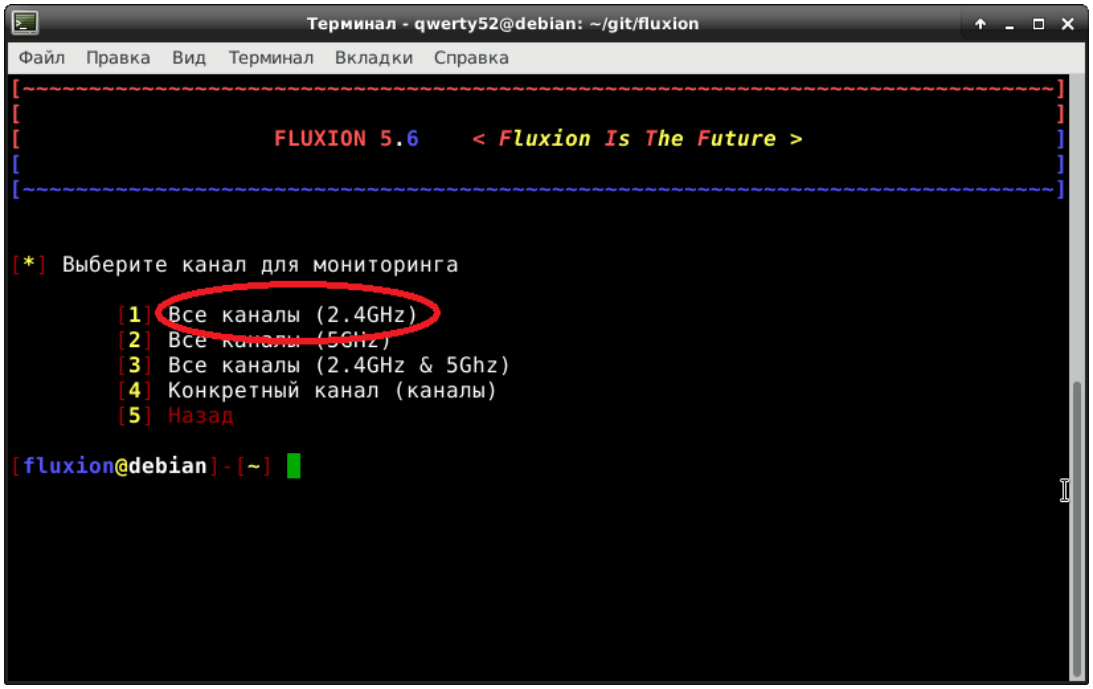


Рисунок 31 – выбор каналов для мониторинга

Далее запускается отдельное окно, в котором появляются ближайшие точки доступа, которые в данный момент сканируются (рисунок 32).

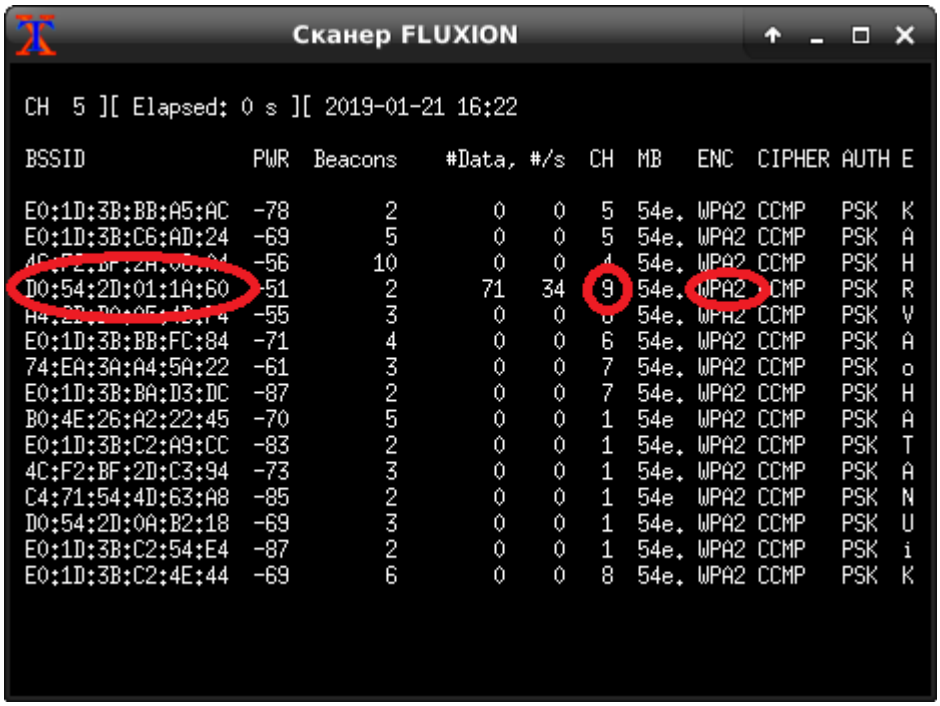


Рисунок 32 – сканирование беспроводных точек доступа

После чего предоставляется список для выбора цели атаки (рисунок 33).

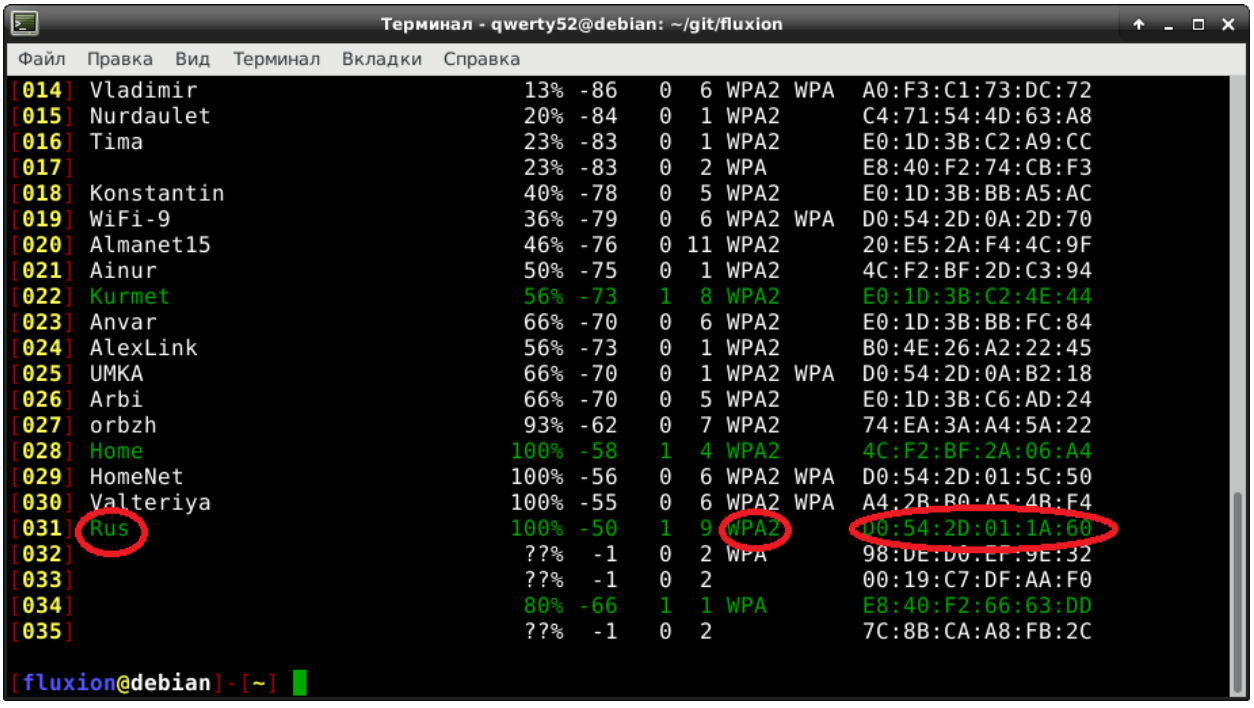


Рисунок 33 – выбор цели атаки

Далее нужно выбрать сетевой интерфейс для перехвата handshake (рисунок 34).

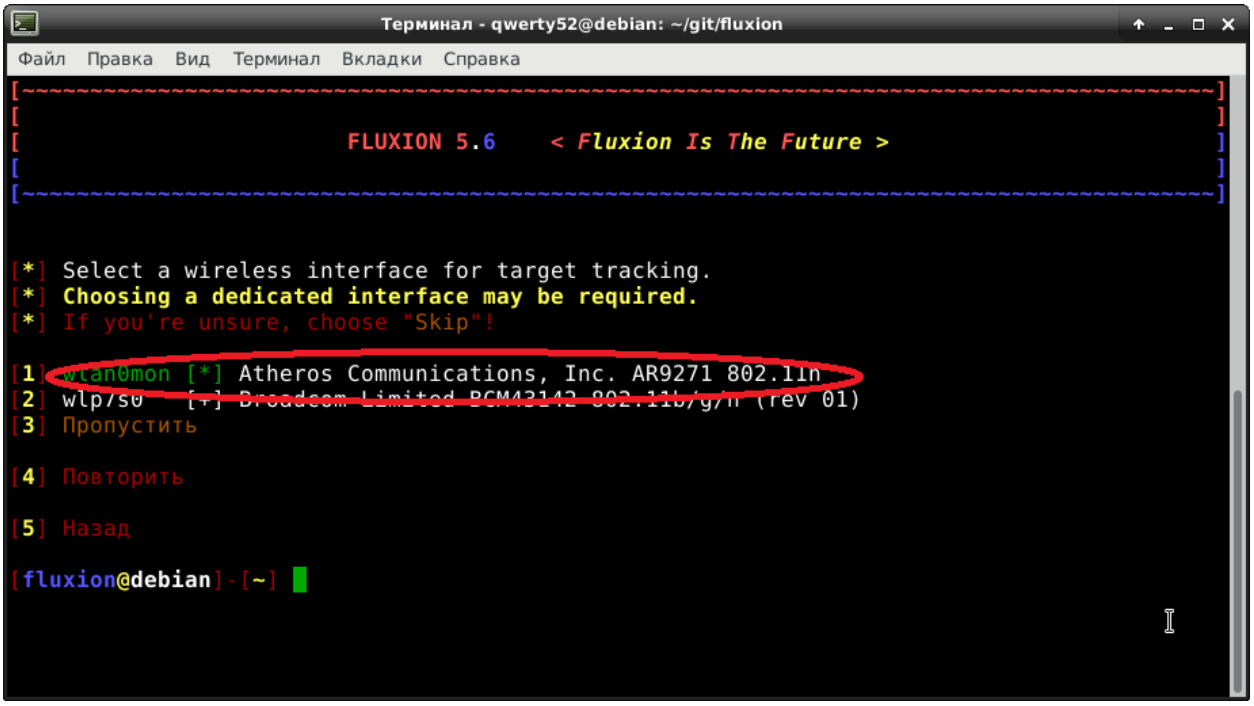


Рисунок 34 – выбор сетевого интерфейса для перехвата handshake

После чего нужно выбрать каким способом получать handshake, пассивным наблюдением за сетью со сбором огромного количества пакетов, так как в одном из них будет находиться пароль, либо деаутентифицировать подключенные устройства и при их повторном подключении к точке доступа будет украден handshake, так же есть возможность выбрать какая программа будет этим заниматься aircrack-ng или mdk3 (рисунок 35)

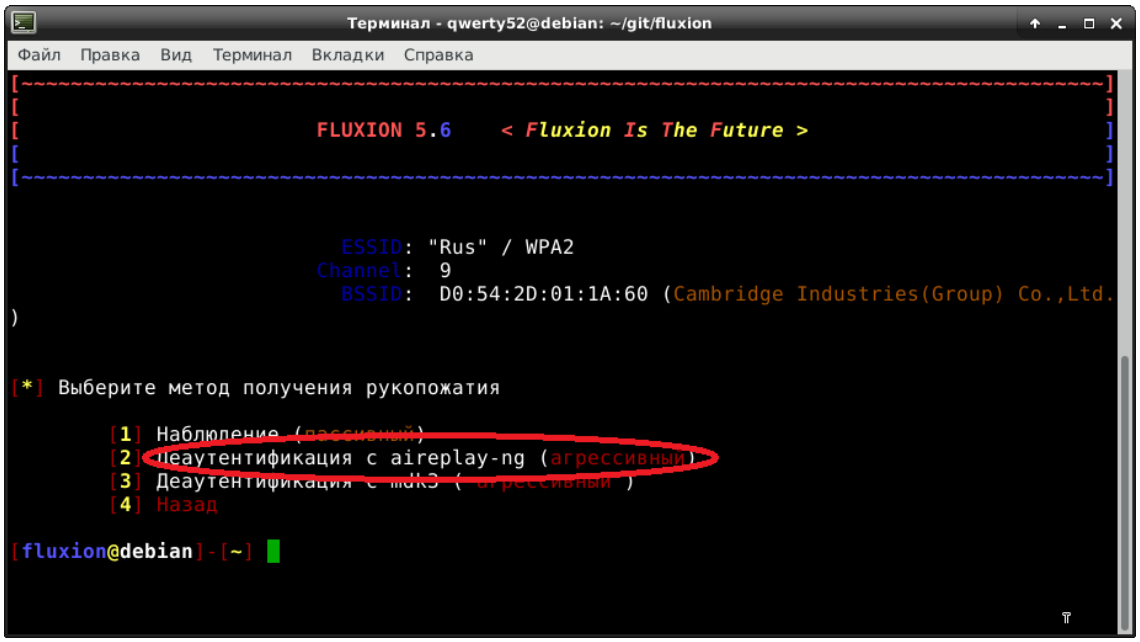


Рисунок 35 – выбор способа получения handshake

Далее нужно выбрать с помощью какого приложения будет проходить проверка рукопожатия, aircrack –ng, cowpatty или pyrit (рисунок 36).

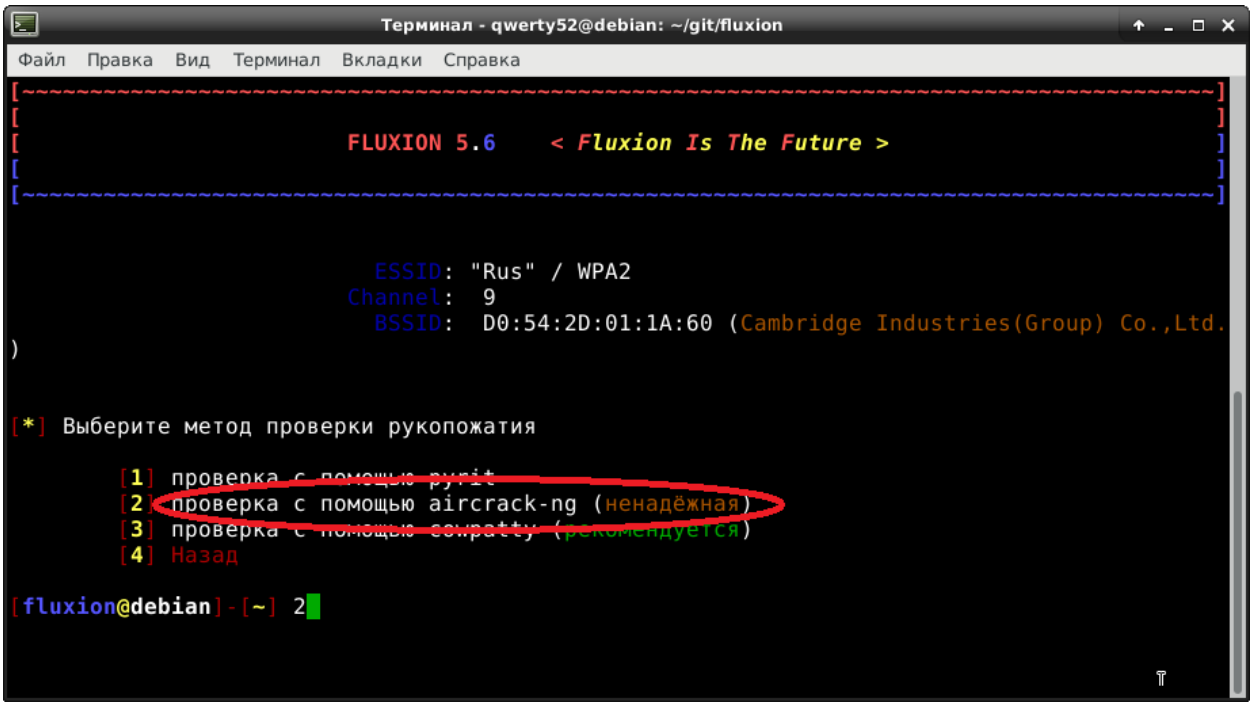


Рисунок 36 – выбор программы для проверки рукопожатия

После чего выбирается промежуток проверки, получено ли рукопожатие (рисунок 37).

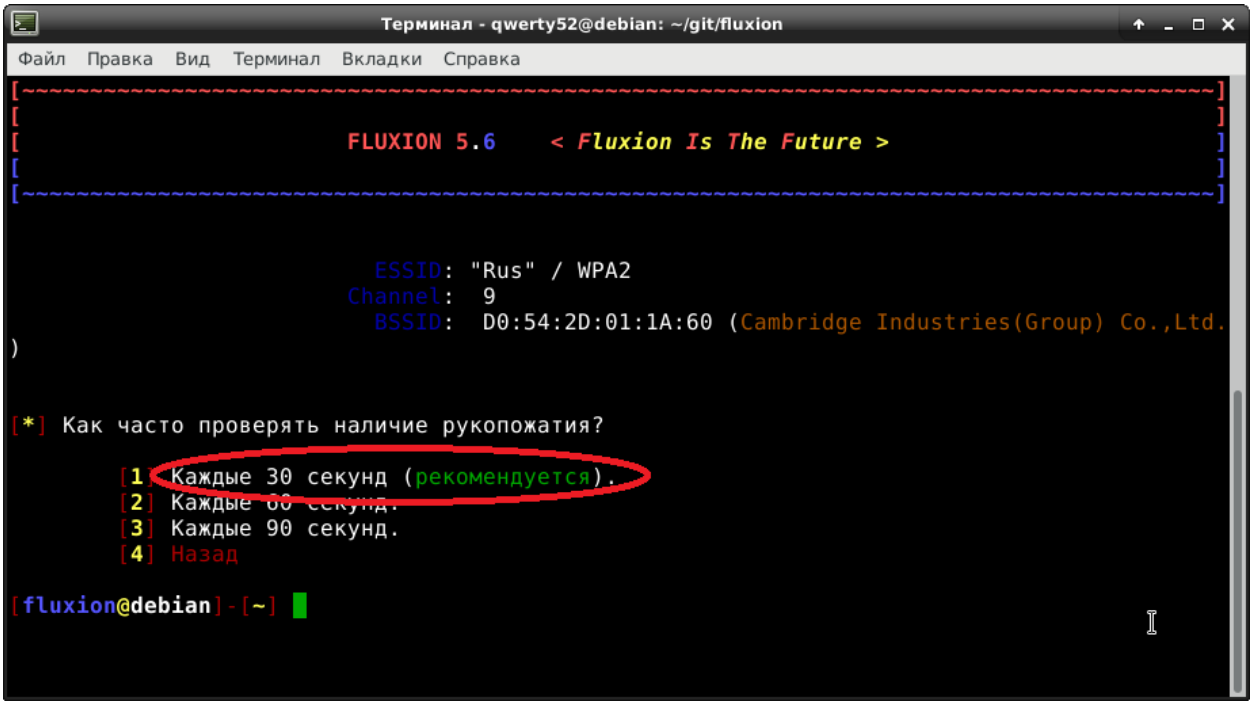


Рисунок 37 – время проверки получено ли рукопожатие

Далее появляется возможность выбрать как должна проходить верификация, синхронно или асинхронно (рисунок 38).

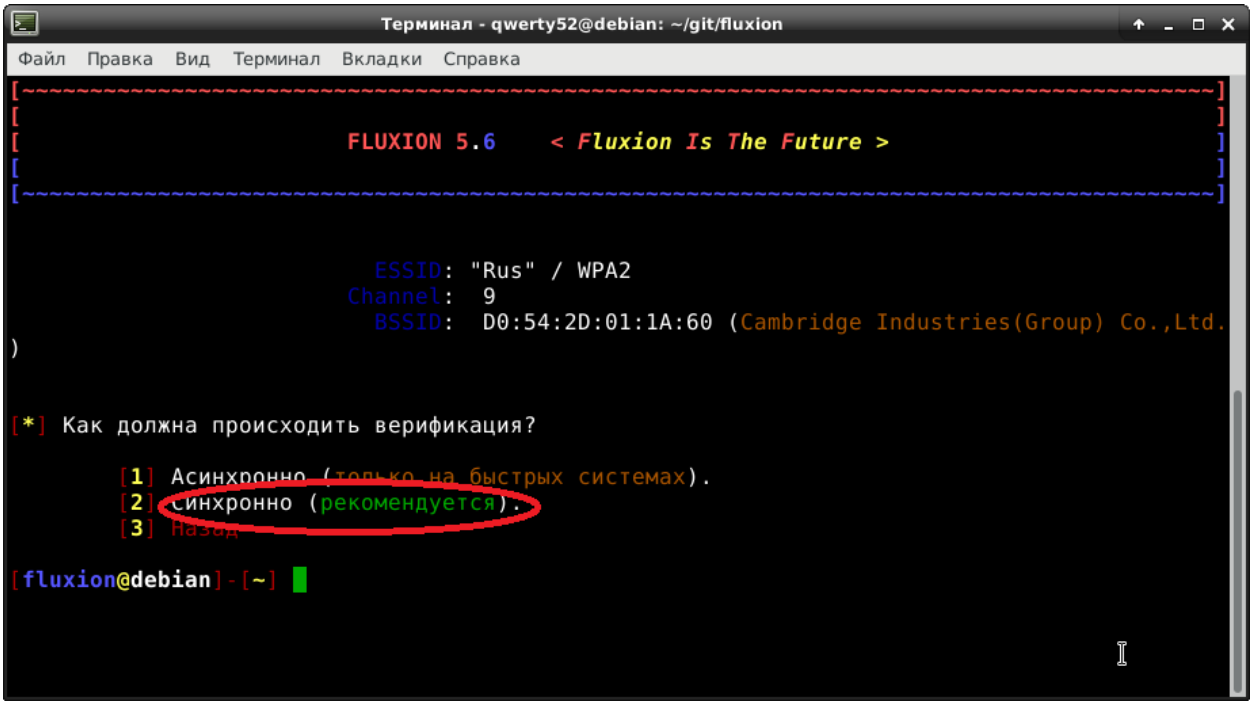


Рисунок 38 – выбор типа верификации

На следующем этапе происходит сама атака запускается 3 дополнительных окна, в которых мониторится выбранная точка доступа, в следующем происходит деаутентификация пользователей и в последнем показывается проверка получения рукопожатия (рисунок 39).

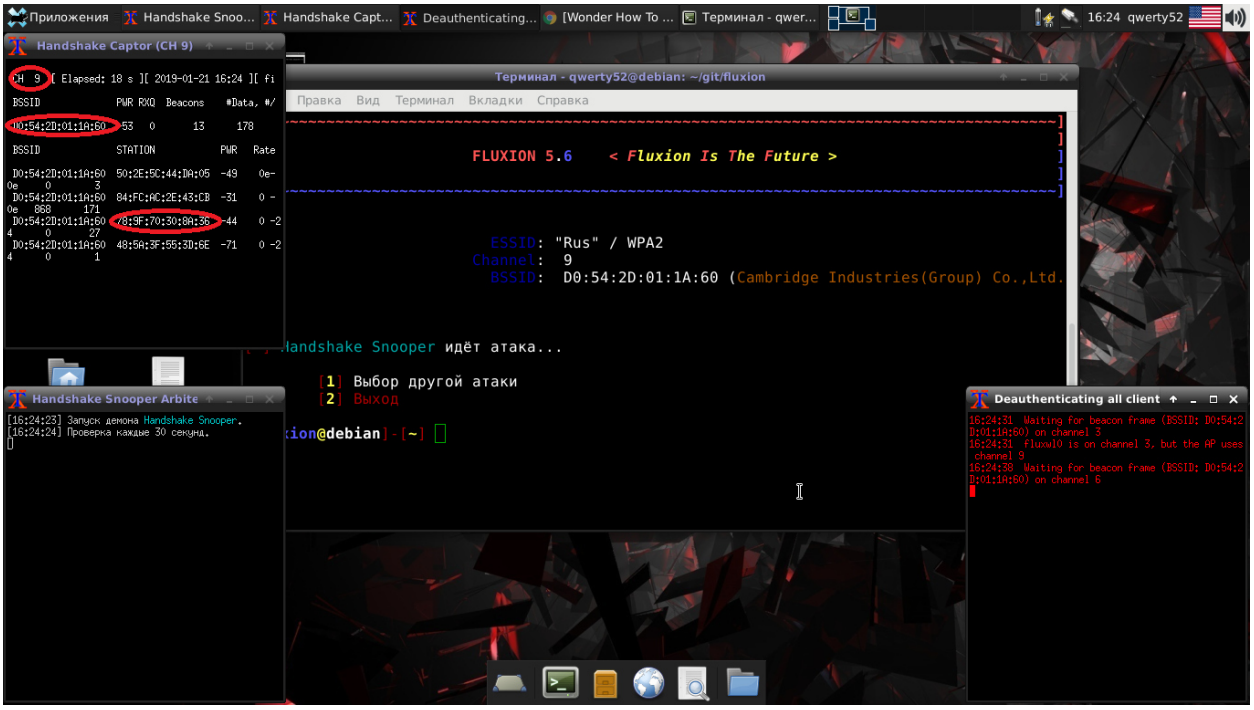


Рисунок 39 – перехват handshake(рукопожатия)

Далее появляется уведомление о том что handshake(рукопожатие) перехвачено (рисунок 40).

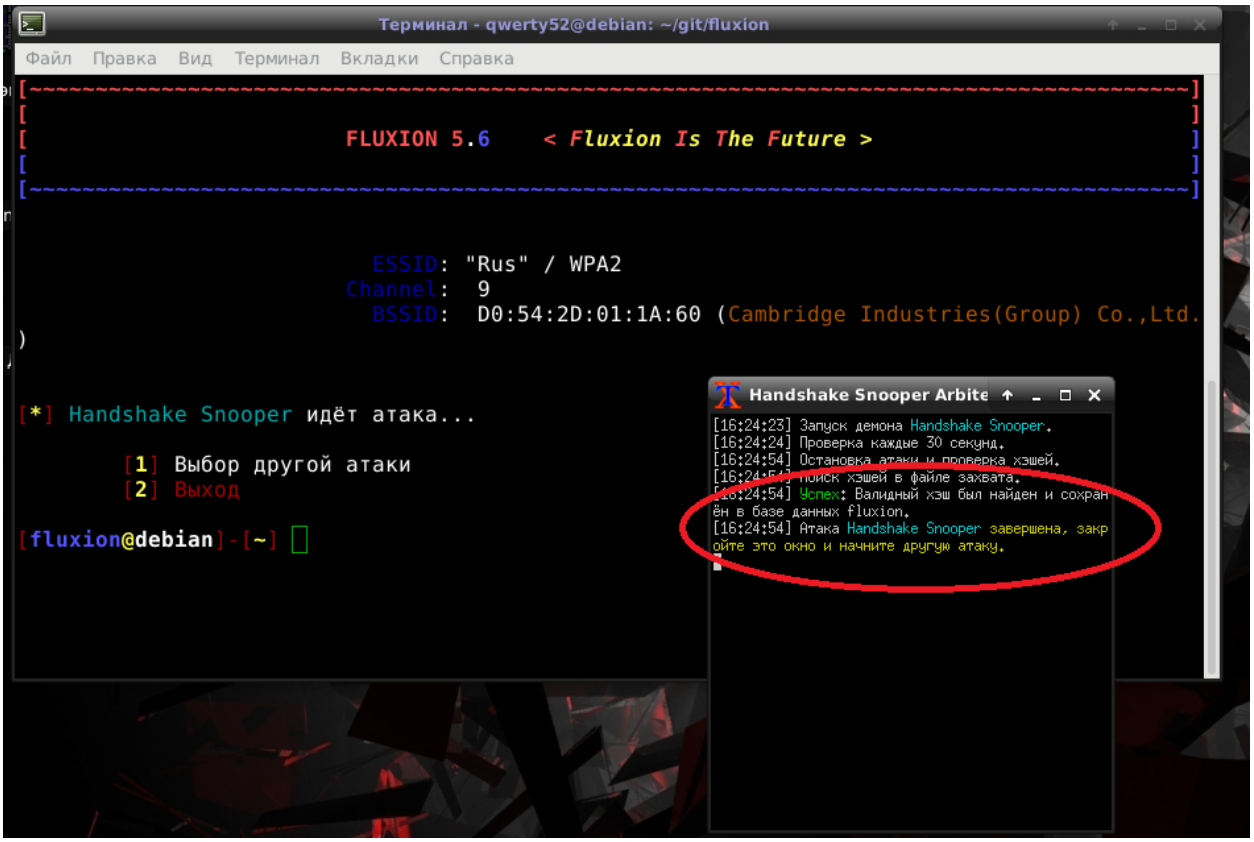


Рисунок 40 – результат проделанной атаки

После чего мы выбираем другой вид атаки (рисунок 41).

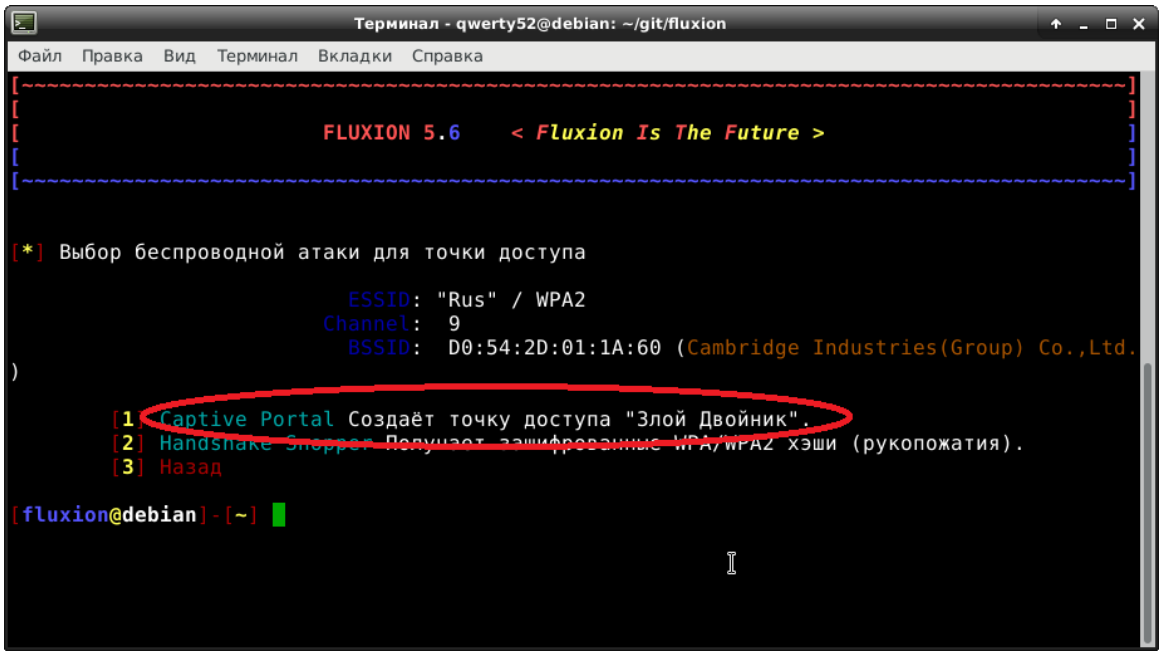


Рисунок 41 – выбор следующего типа атаки

Программа сразу предлагает продолжить работу с выбранной сетью (рисунок 42).

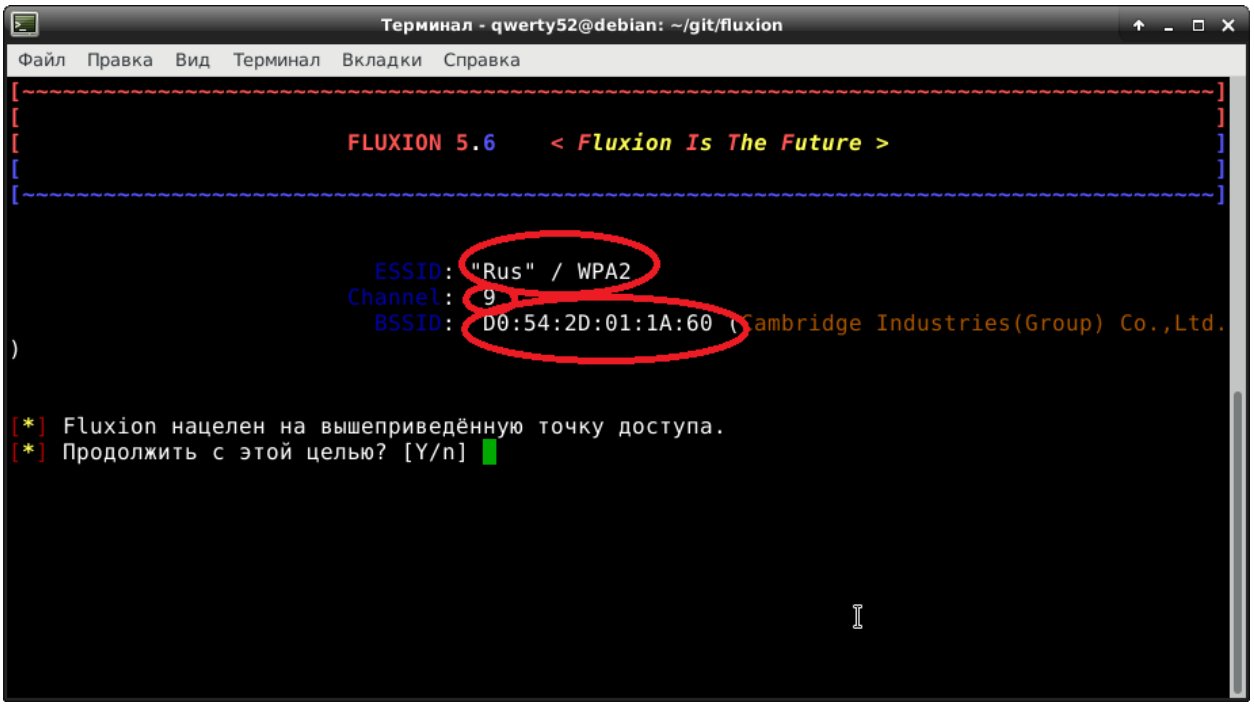


Рисунок 42 – выбор атакуемой сети

После чего требуется выбрать сетевой интерфейс для глушения точки доступа wifi (рисунок 43).

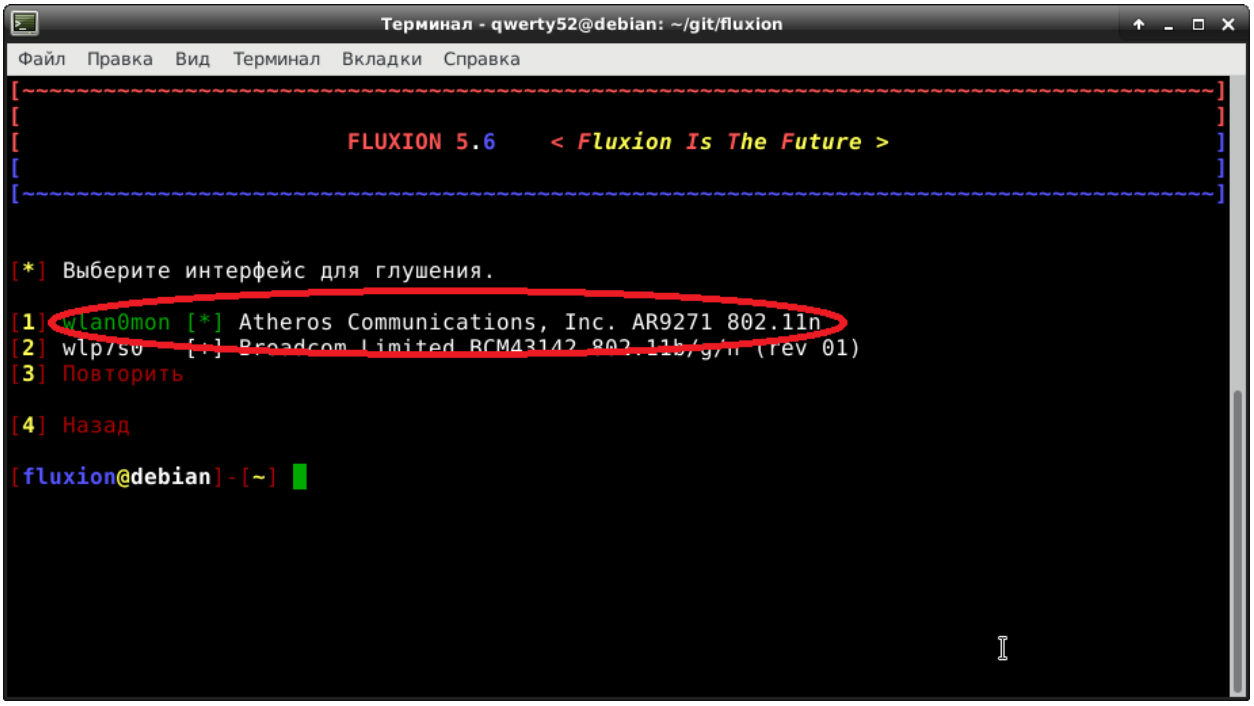


Рисунок 43 – выбор сетевого интерфейса для глушения

Далее нужно выбрать сетевой интерфейс для поднятия фейковой точки доступа (рисунок 44).

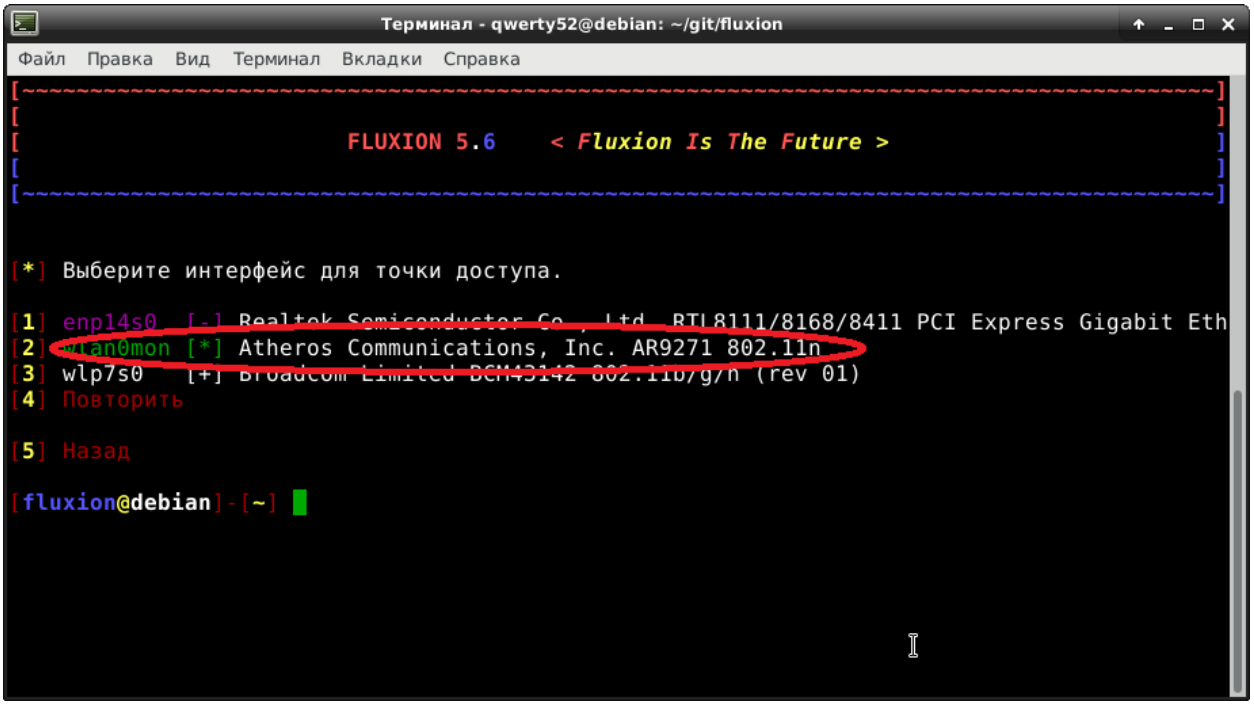


Рисунок 44 – выбор сетевого интерфейса для поднятия фейковой точки доступа

Далее нужно выбрать службу которая будет запускать фейковую точку доступа , доступно airbase-ng и hostapd (рисунок 45).

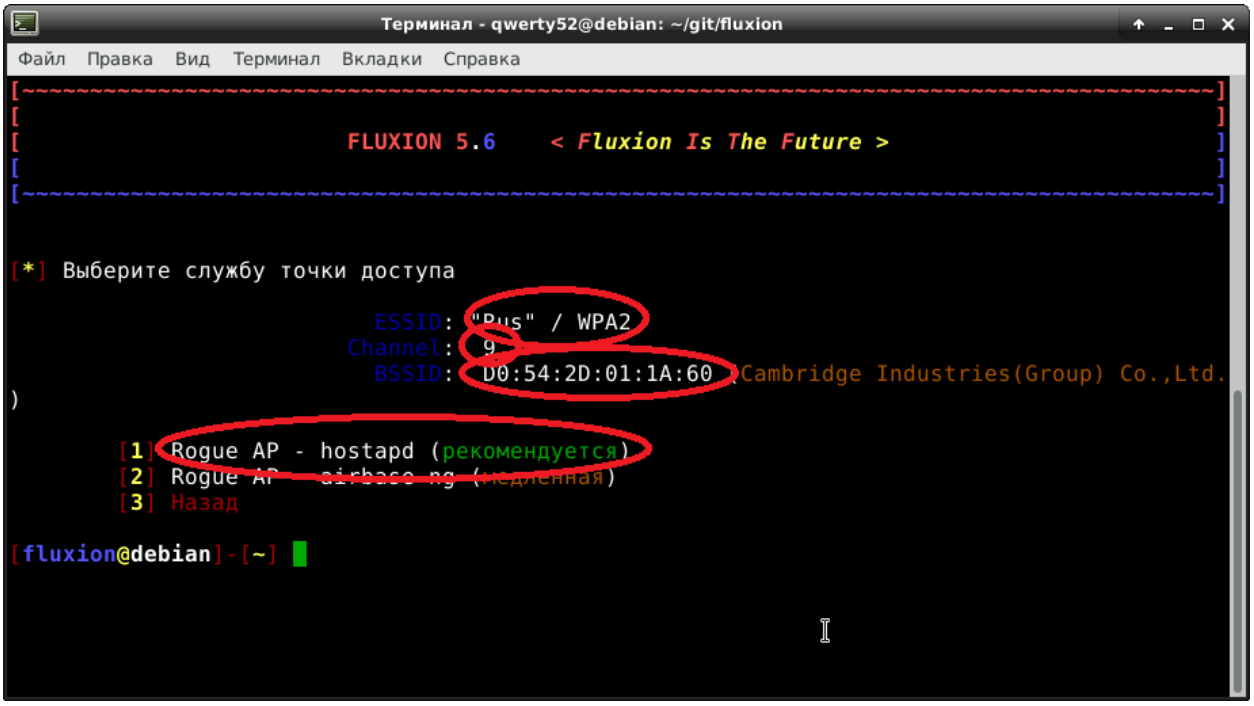


Рисунок 45 – выбор службы для поднятия фейковой точки доступа

После чего нужно выбрать рукопожатие, полученное в последней атаке либо указать путь до другого рукопожатия (рисунок 46).

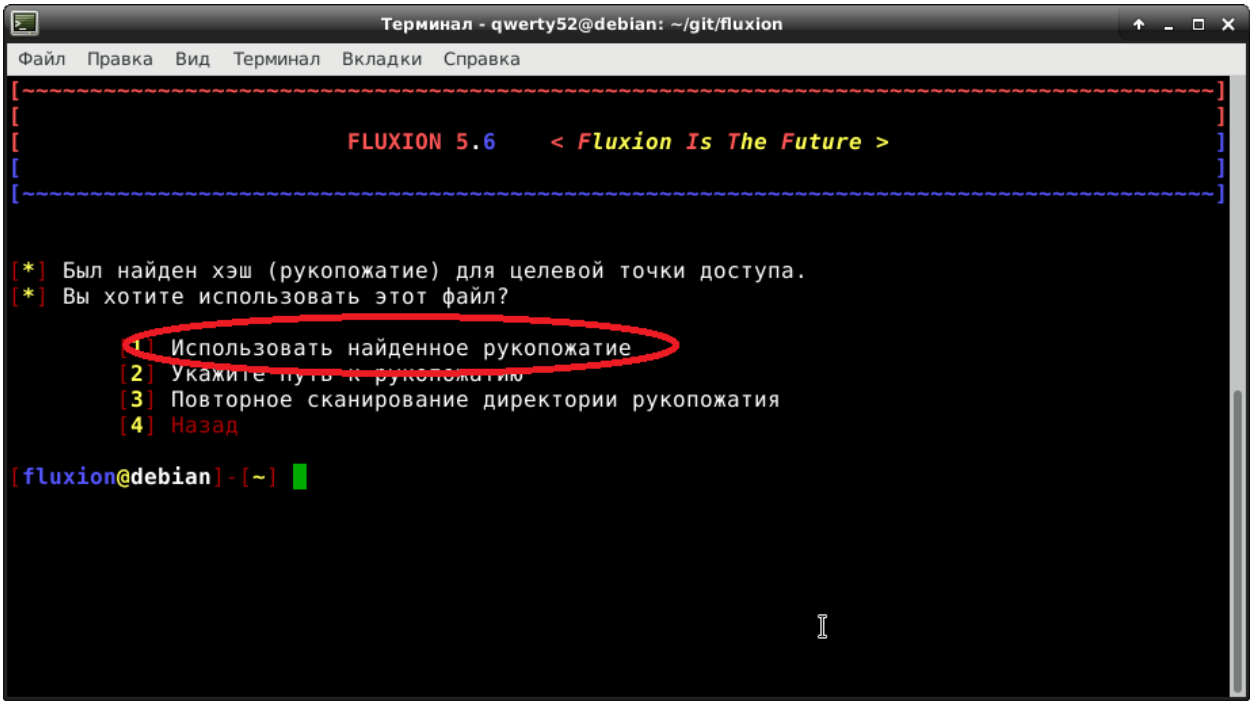


Рисунок 46 – выбор рукопожатия(handshake)

Далее нужно выбрать программу для проверки рукопожатия(handshake), aircrack-ng, cowpatty или pyrit. Для сверки с существующей точкой доступа (рисунок 47).

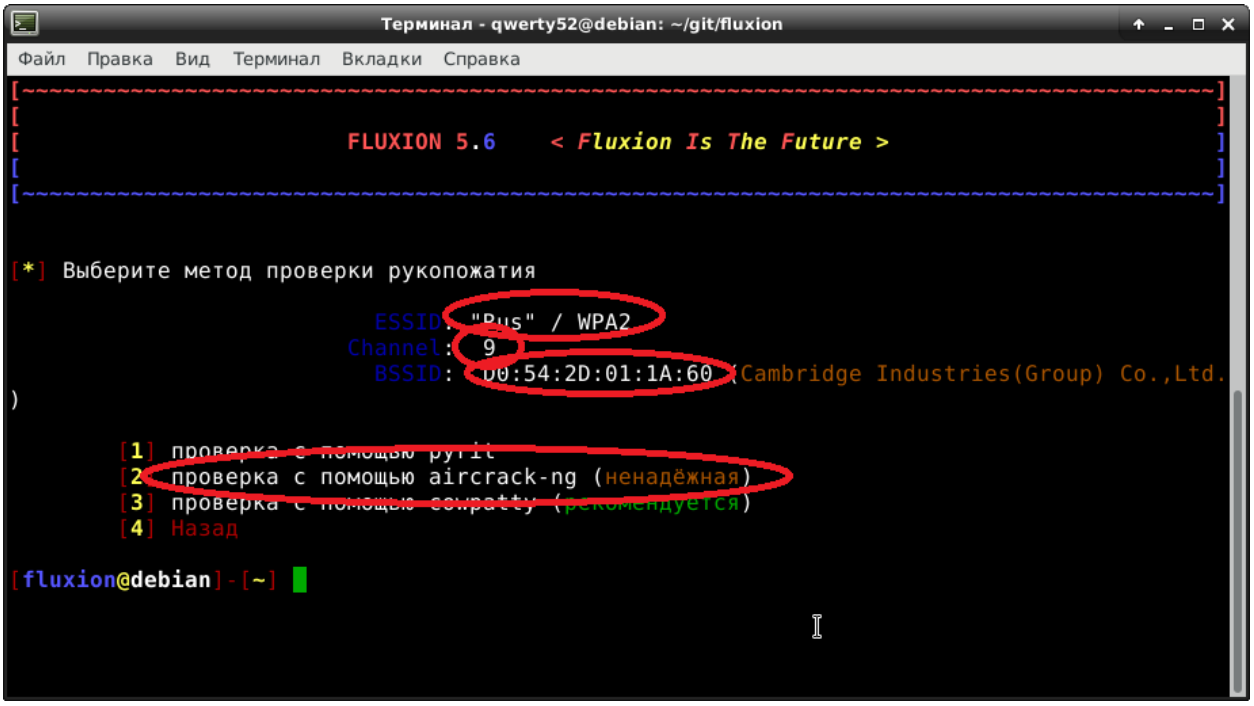


Рисунок 47 – выбор программы для проверки рукопожатия(handshake)

Далее нужно выбрать или создать сертификат для перехватывающего портала (рисунок 48.)

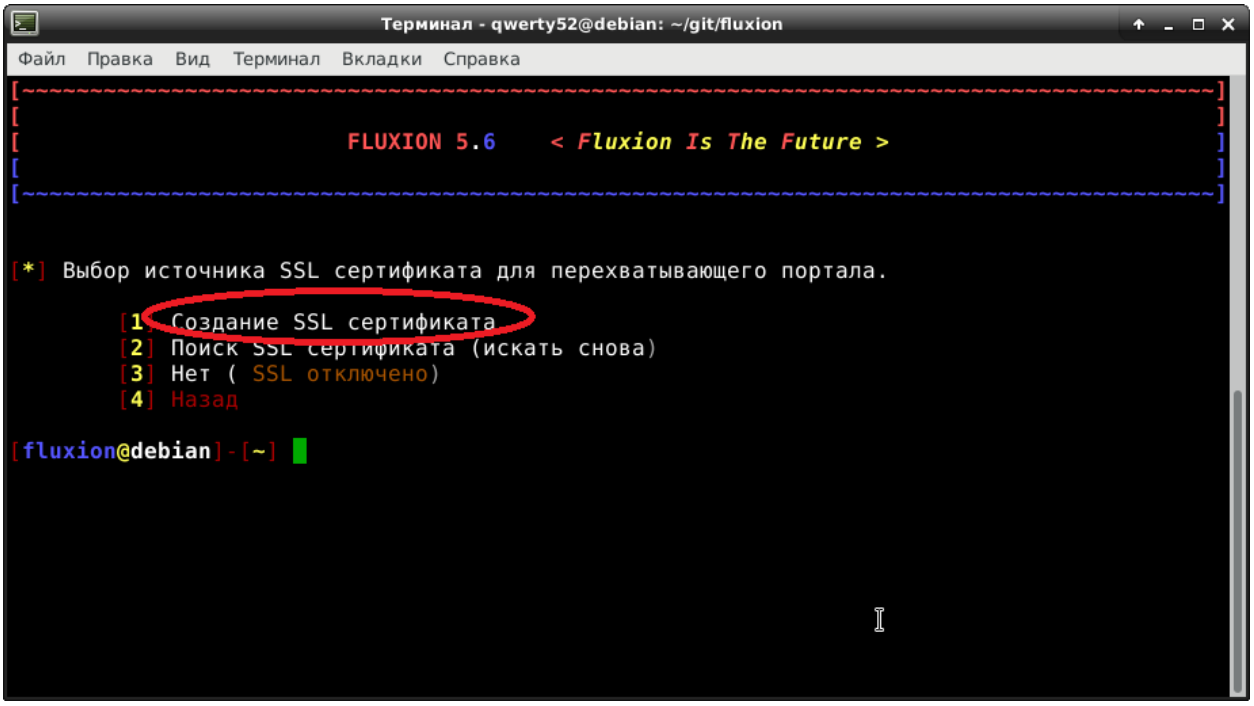


Рисунок 48 – выбор сертификата

После чего нужно выбрать будет ли выход в интернет у созданной фейковой точки доступа (рисунок 49).

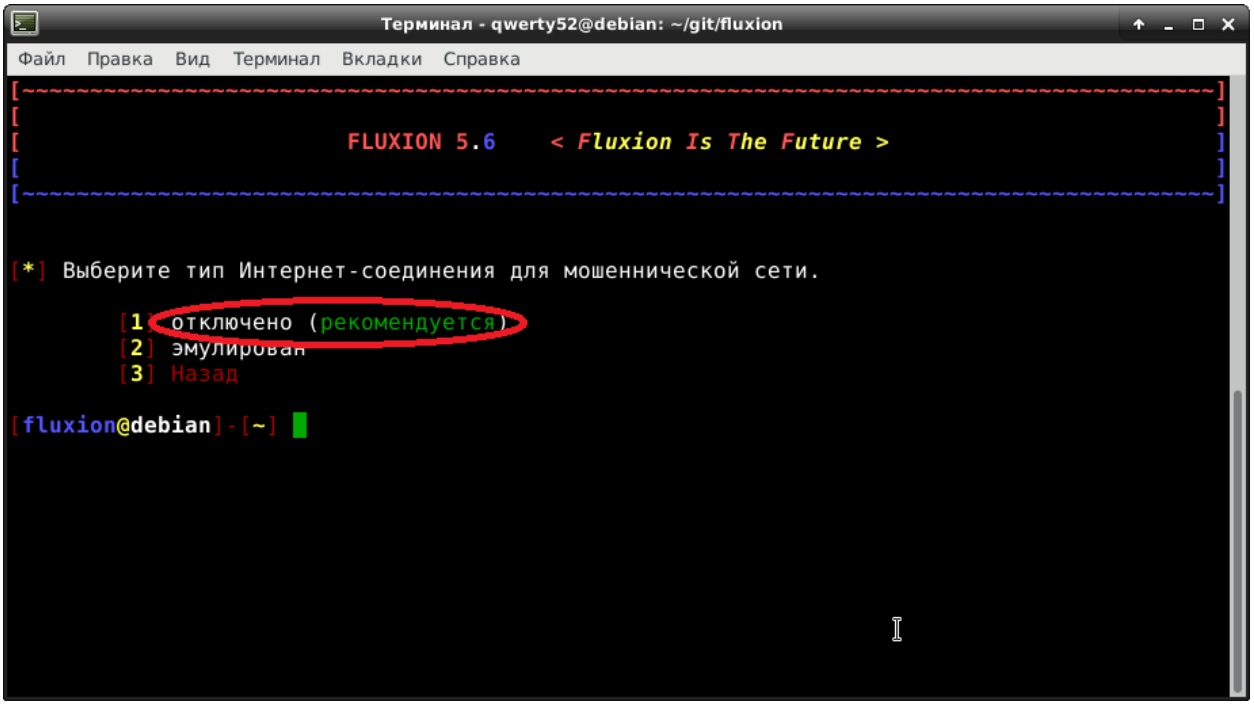


Рисунок 49 – выбор доступности в глобальную сеть

Далее нужно выбрать каким будет перехватывающий портал, его язык и тип роутера (рисунок 50).

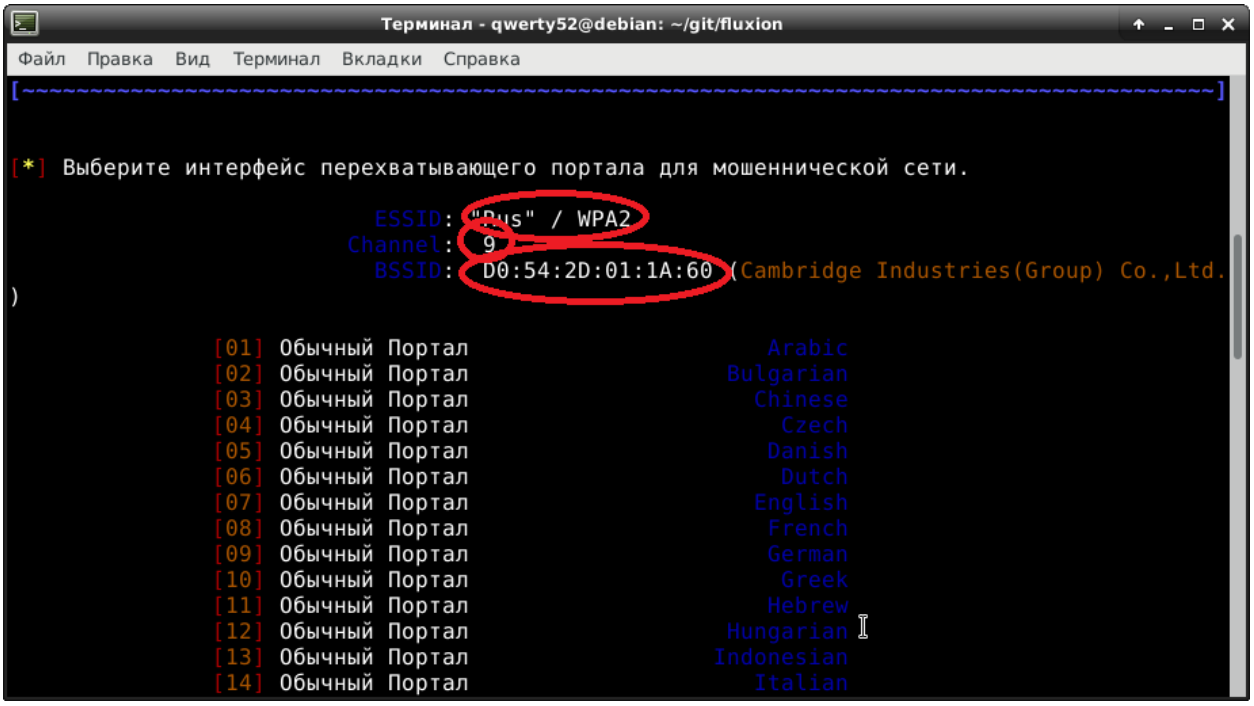


Рисунок 50 – выбор перехватывающего портала

После чего начинается атака, открываются дополнительные окна, которые следят за аутентификацией к фейковой точке доступа, мониторят саму точку доступа , распределением ip адресов (dhcp сервис), web сервисом, dns сервисом, а так же jammer для перехвата введенных данных (рисунок 51).

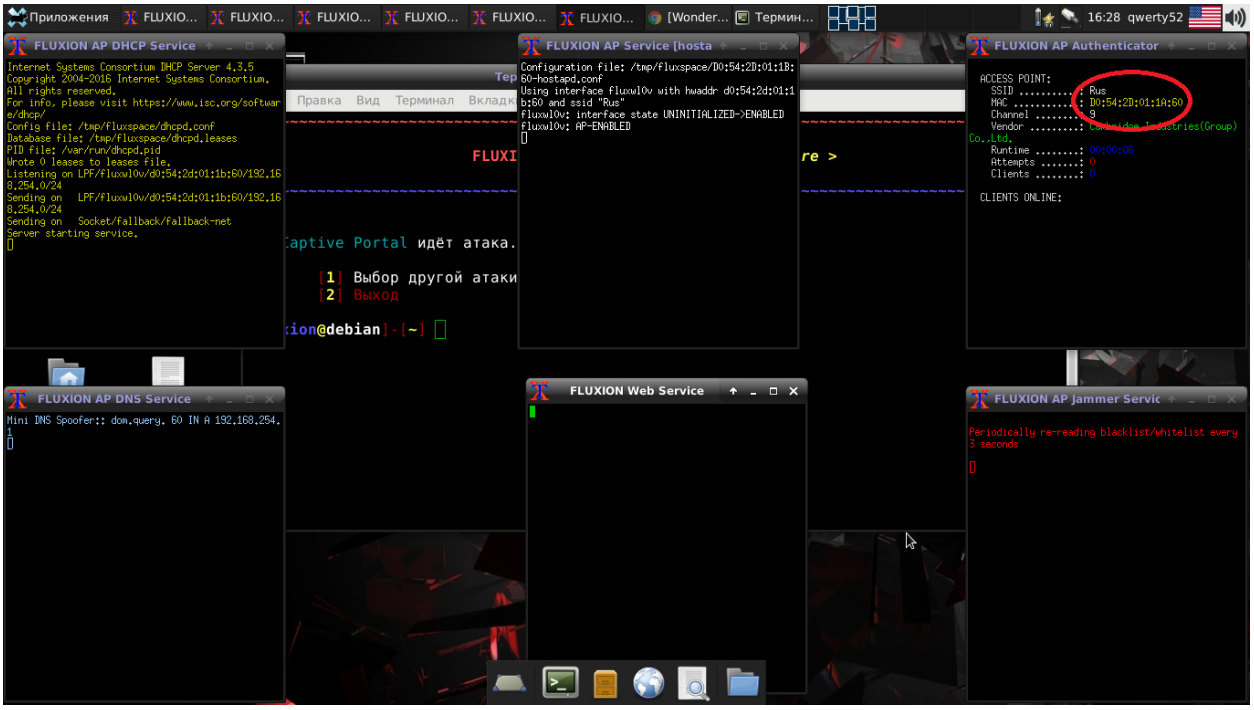


Рисунок 51 – реализация атаки

Далее появляется фейковая точка доступа имеющая то же самое название, все те же самые параметры , Mac-адрес, канал на котором работала настоящая точка доступа, но отсутствует пароль у этой точки доступа, а оригинальная точка доступа просто пропала, так как заглушена (рисунок 52).

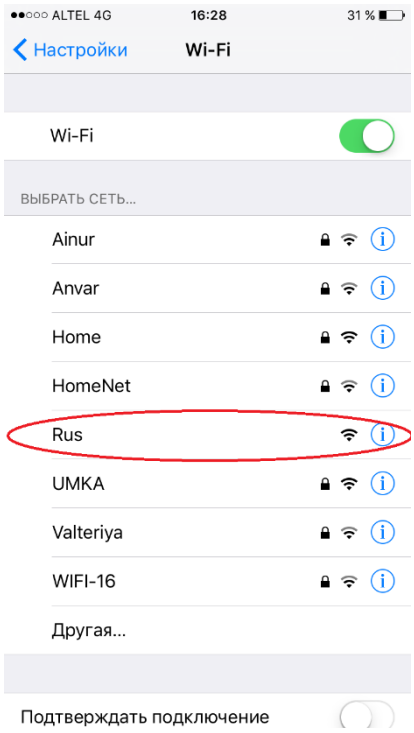
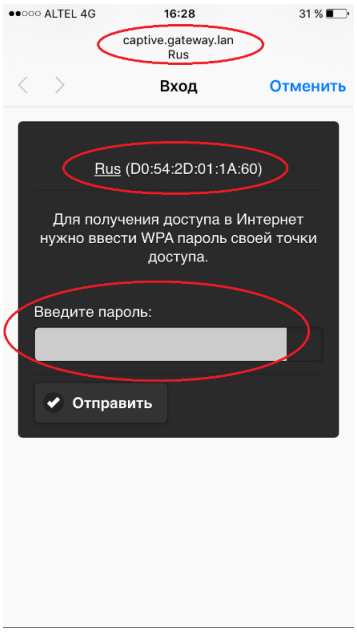


Рисунок 52 – результат создания фейковой точки

Дальше жертва подключается к выбранной точке доступа, сразу же всплывает окно авторизации, то есть созданный портал, с выбранным интерфейсом (рисунок 53).



Риунок 53 – открытие портала для хищения пароля

После чего мы видим аутентифицированную жертву, то есть название устройства, выделенный ей ip адрес , MAC-адрес устройства, запросы которые отправляются на web сервис (рисунок 54).

Рисунок 54 – реализация атаки

После введения жертвой пароля от точки доступа, всплывает уведомление о перехвате пароля, а так же путь где он находится (рисунок 55).

Рисунок 55 – результат проделанной атаки

Далее проходим по адресу указанном программой, и видим всю информацию о точке доступа (рисунок 56).

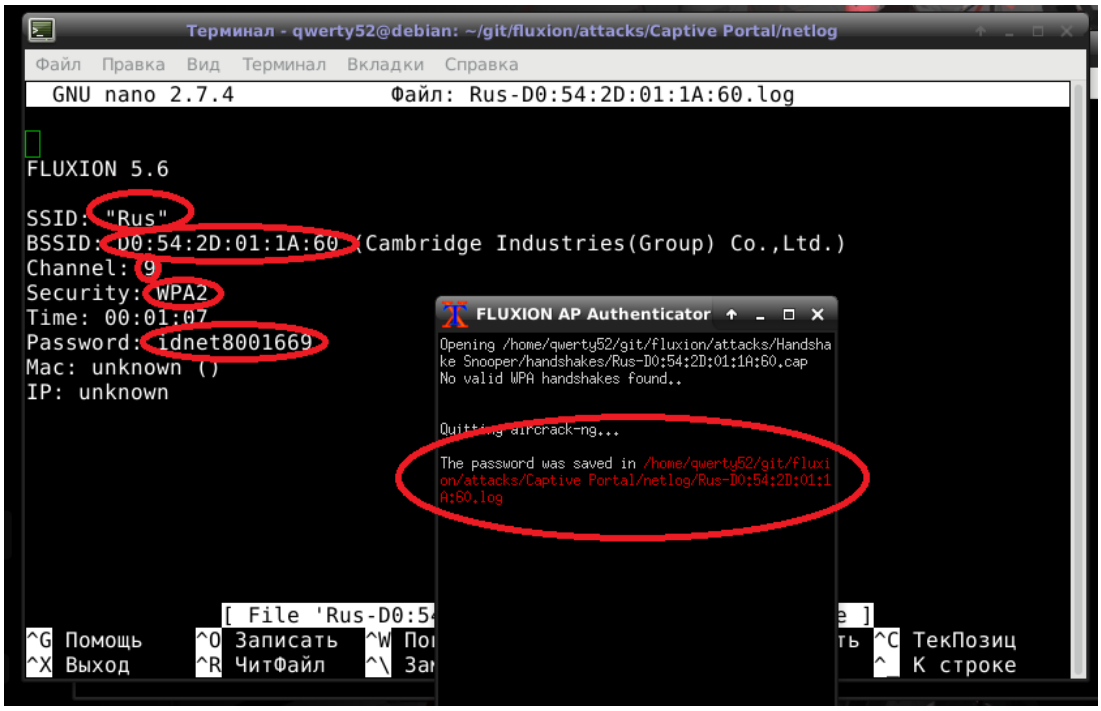


Рисунок 56 – результат проделанной атаки

2.4 PMKID

Основными преимуществами этой атаки являются следующие:

- Больше не требуется регулярных пользователей – потому что злоумышленник напрямую связывается с AP.
- Больше не нужно ждать полного 4-стороннего рукопожатия между обычным пользователем и AP.
- Отсутствие дополнительных повторных передач кадров EAPOL.
- Меньшая вероятность неверного пароля.
- Больше нет потерянных кадров EAPOL, когда обычный пользователь или AP находится слишком далеко от исследователя.
- Больше не требуется фиксировать значения nonce и replaycounter.
- Больше нет специального формата вывода (pcap, hccapx и так далее) - окончательные данные будут отображаться как обычная строка с шестнадцатеричным кодированием.

В первую очередь нужно выбрать сетевой интерфейс, который будет переведен в режим мониторинга сети, в данном случае используется внешний сетевой адаптер Alfa. Используем команды “sudo ifconfig” (рисунок 57).

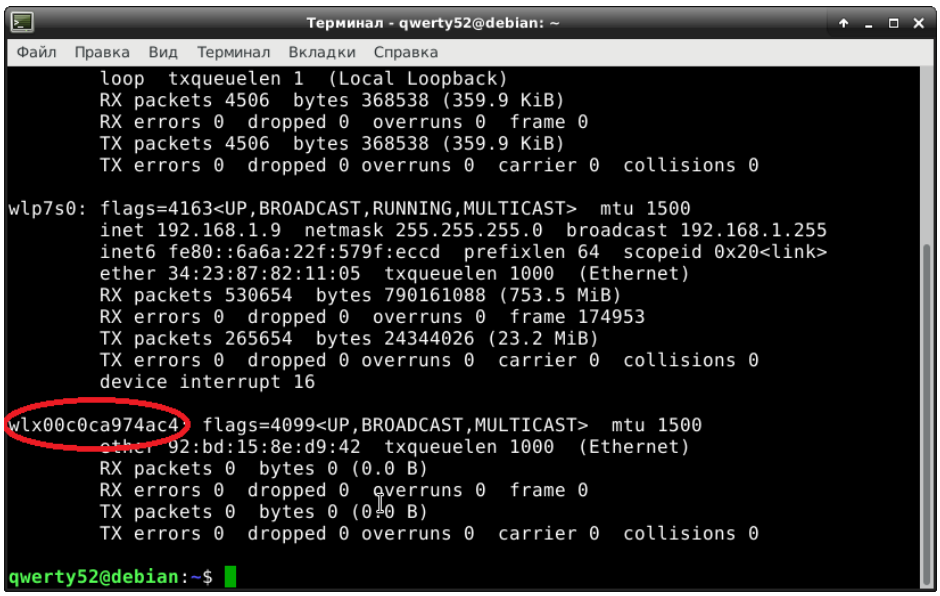


Рисунок 57 – Выбор сетевого интерфейса

Далее выбранный сетевой адаптер переводиться в режим мониторинга с помощью команды “sudo airmon-ng start wlx00c0ca974ac4 (название сетевого адаптера)”, после чего программа сообщает нам о то что сетевой адаптер переведен в режим мониторинга, обращаться к нему мы можем под названием wlan0mon (название сетевого адаптера в режиме мониторинга) (рисунок 58).

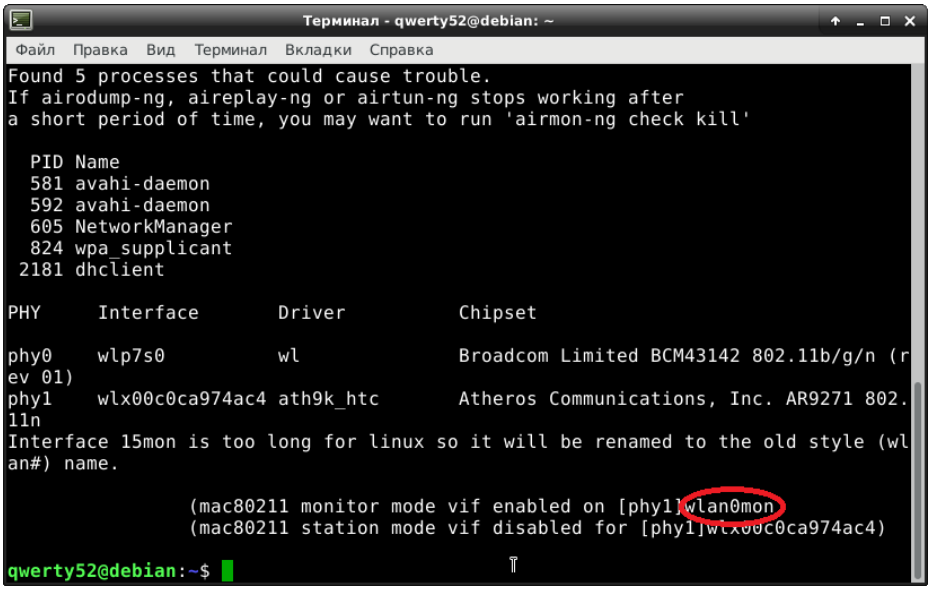


Рисунок 58 –Перевод сетевого адаптера в режим мониторинга

Далее запускаем сканирование ближайших точек доступа wifi при помощи команды “sudo airodump-ng wlan0mon” (указывается интерфейс для сканирования), здесь мы можем увидеть MAC-адрес точки доступа (BSSID), уровень сигнала (PWR), количество пакетов объявлений или маяков (Beacons), количество отловленных пакетов (#Data), число пакетов данных за последние 10 секунд (#/s), канал на котором работает точка доступа (CH),

максимальное скорость поддерживаемая AP (MB), используемый алгоритм шифрования (ENC), обнаруженный шифр (CIPHER),используемый протокол аутентификации (AUTH), название точки доступа (ESSID). В данном случае нас интересует только MAC адрес точки доступа (рисунок 59).

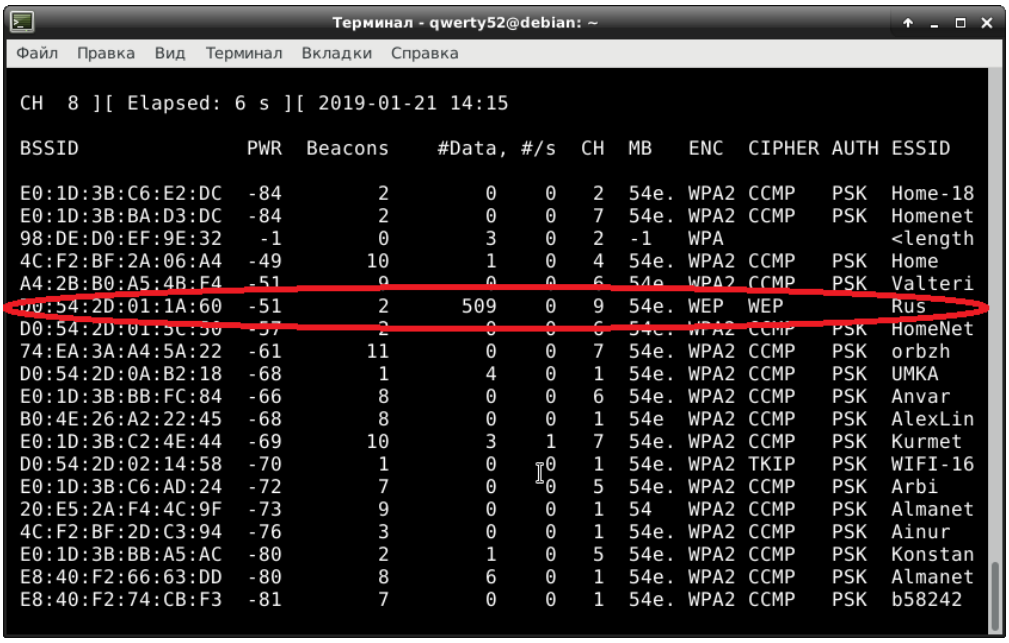


Рисунок 59 – сканирование всех доступных точек доступа

Далее MAC-адрес записывается в обычный файл формата txt без двоеточий, файл назван Filter.txt (рисунок 60).

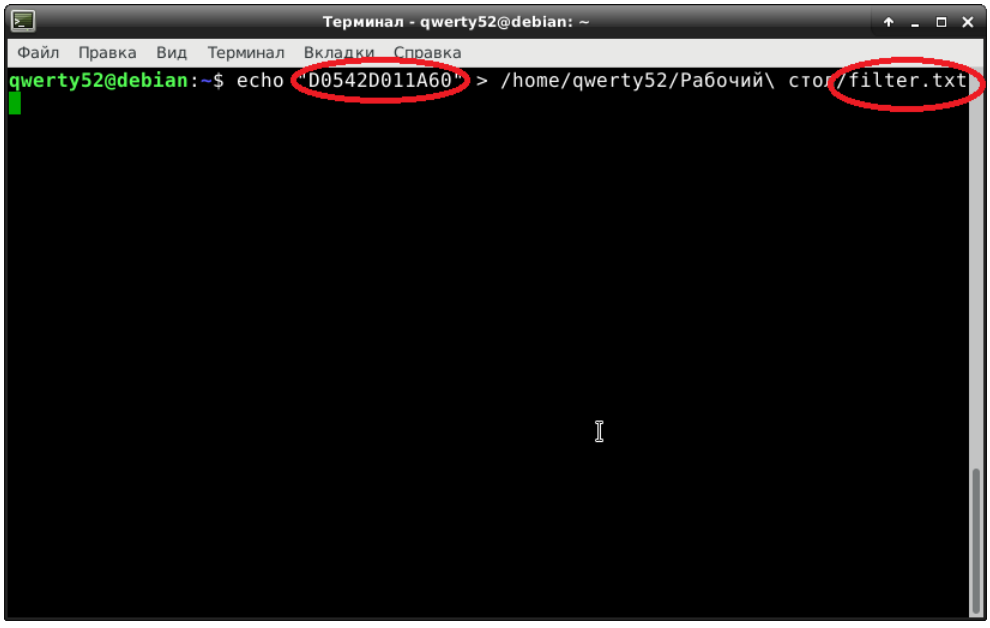


Рисунок 60 – Создание файла для фильтрации

Далее запускаем приложение hcxdumptool, которое позволяет нам перехватывать пакет EAPOL в которых находится нужный нам PMKID. Используется следующая команда (рисунок 61).

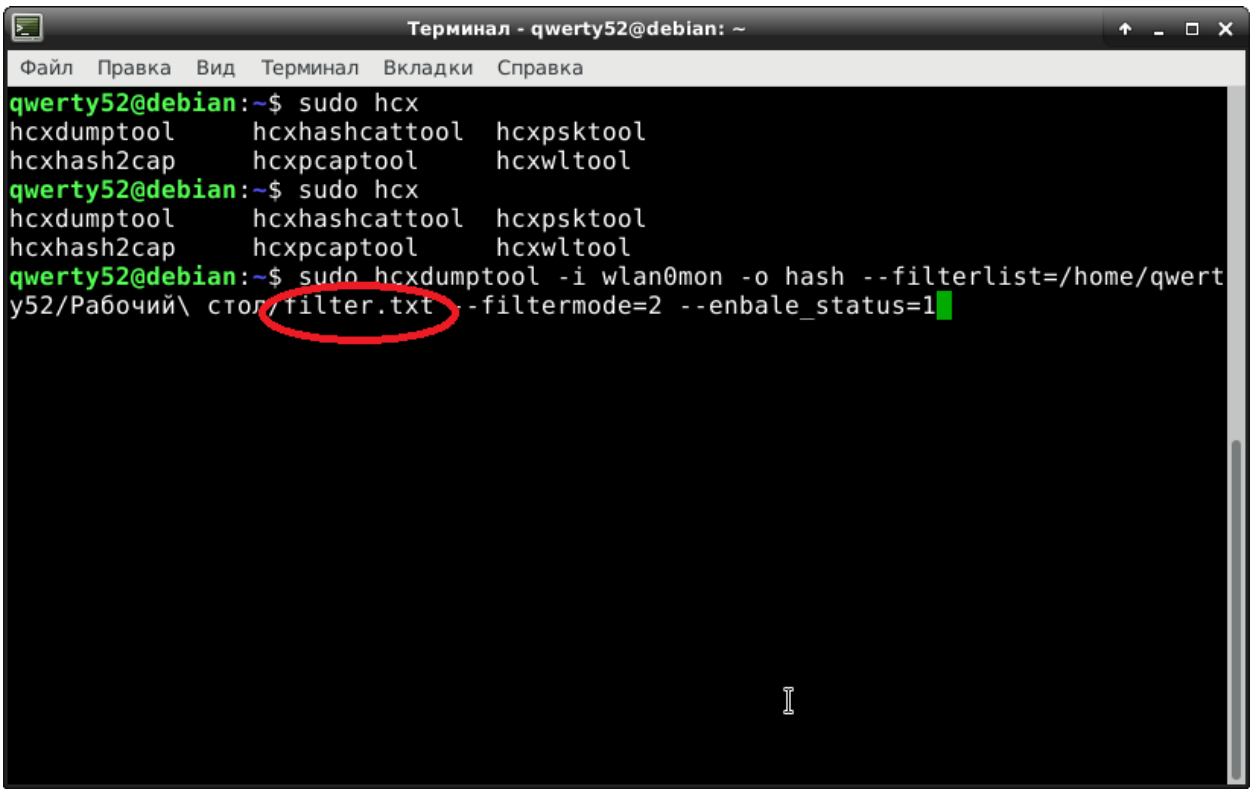


Рисунок 61 – Запуск hcxdumptool для перехвата пакета EAPOL

После запуска программа начинает захват пакетов, при получении пакета она уведомляет об этом, появляется надпись “FOUND PMKID” (рисунок 62,63).

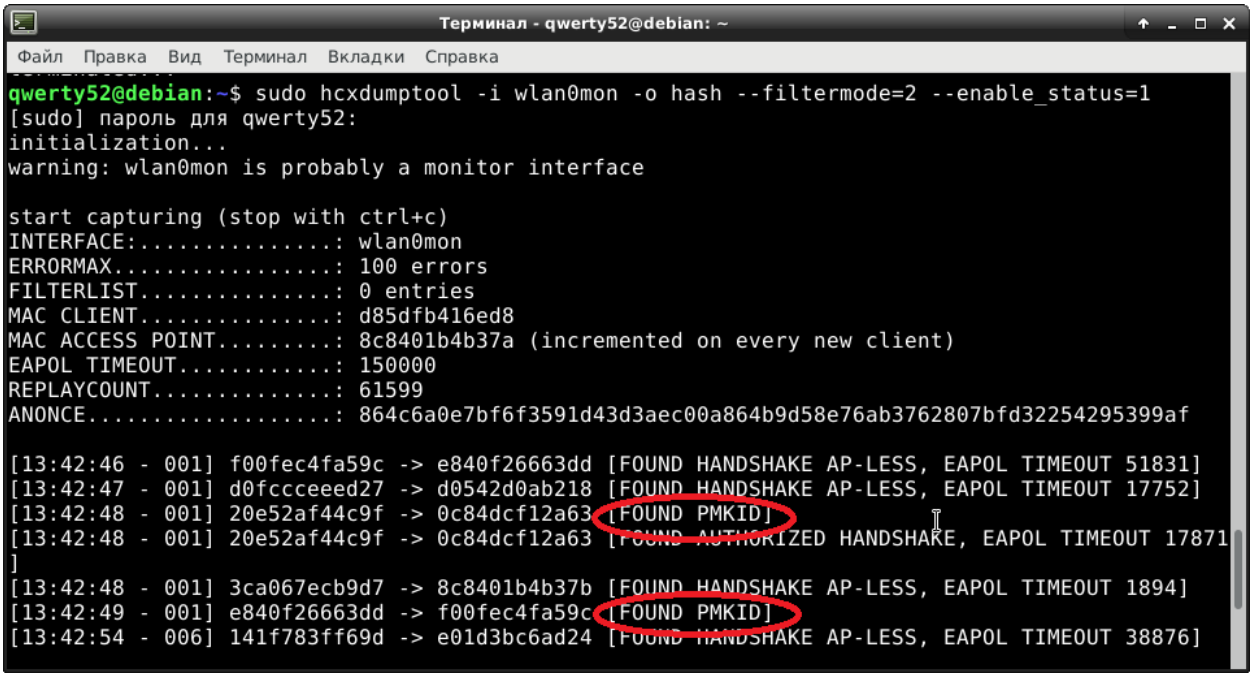


Рисунок 62 – Процесс захвата пакетов EAPOL

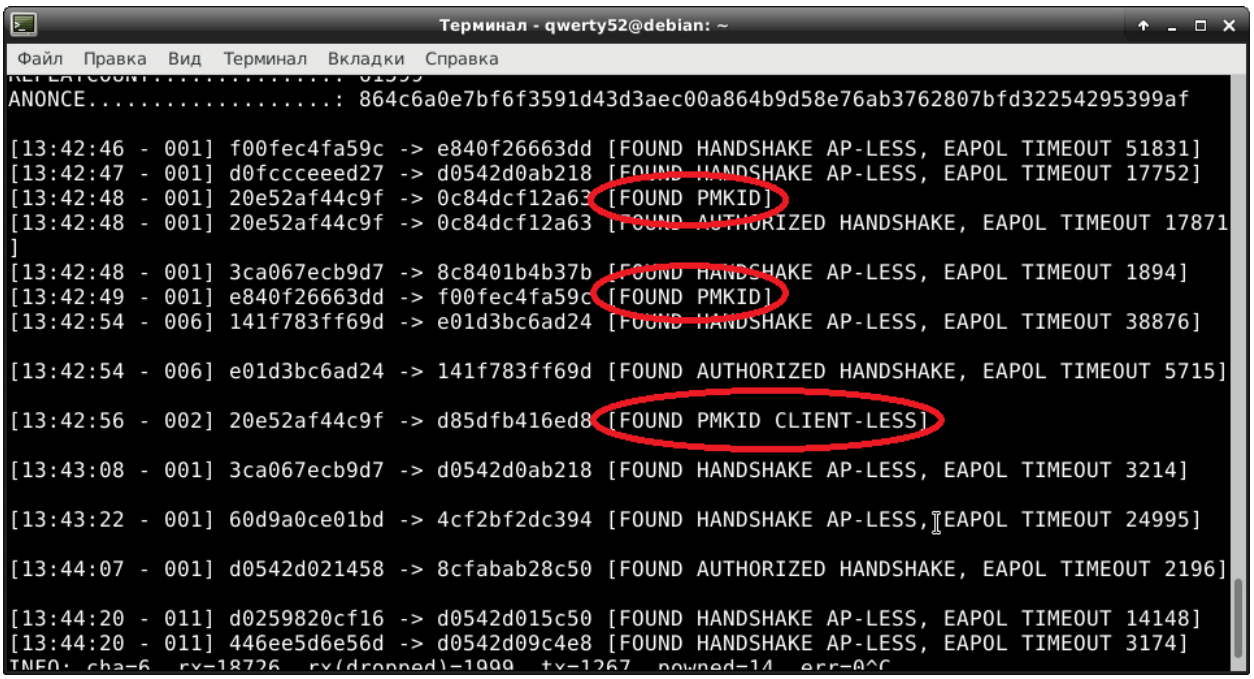


Рисунок 63 – Результат работы программы Hcxdumptool

Через Wireshark можно наглядно увидеть, что проходит в данном пакете, если подробно его рассмотреть, как указано ниже на скриншоте (рисунок 64).

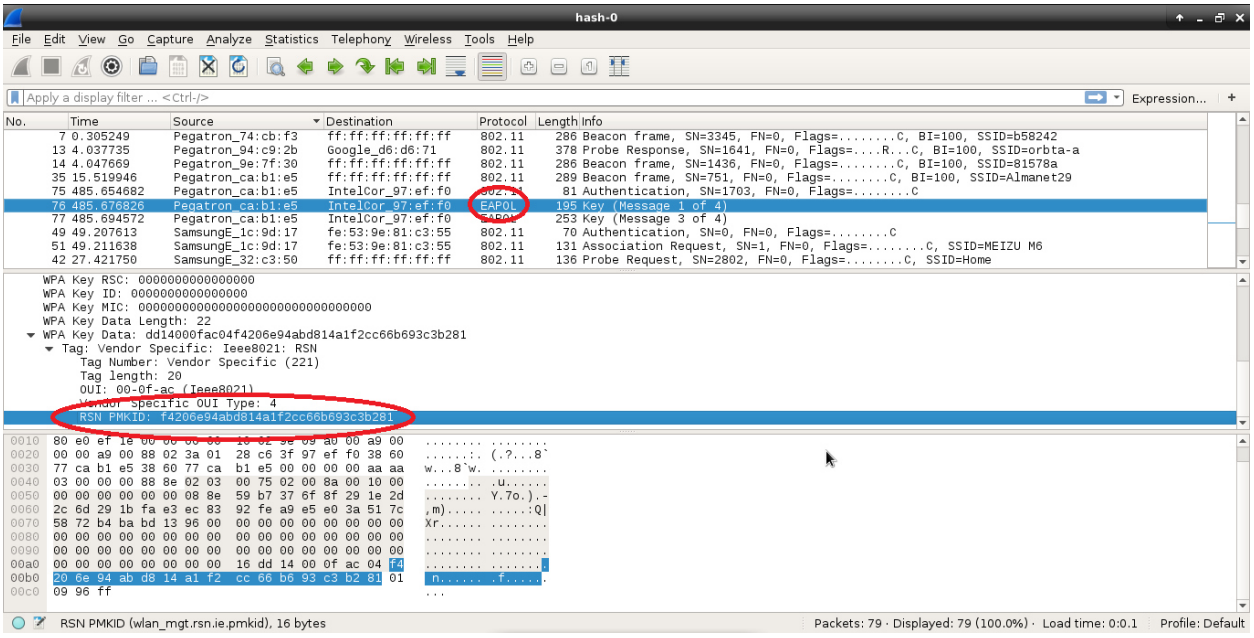


Рисунок 64 – Просмотр содержимого пакета EAPOL

Далее используется утилита Hcxcaptool которая позволяет откинуть всё лишнее оставив, только нужный нам PMKID и записать его в формате, доступном для перебора через hashcat (рисунок 65).

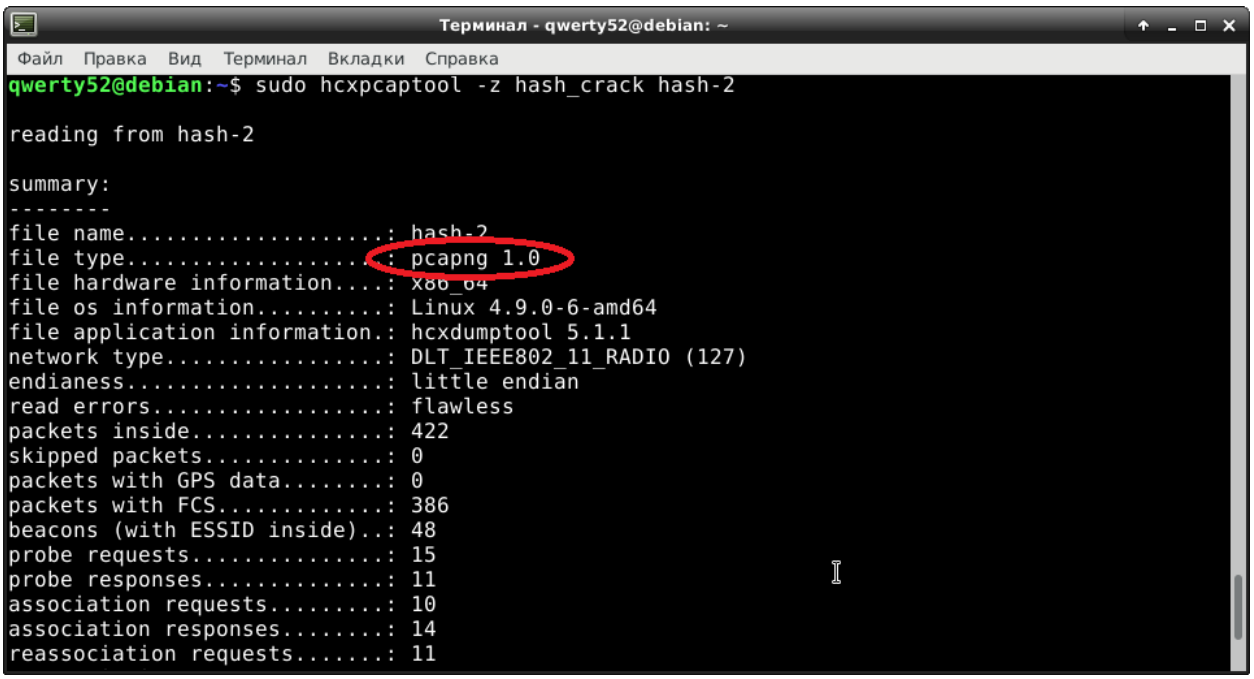


Рисунок 65 – Запуск программы hcxcaptool для записи в формате pcapng

В результате программа распишет все данные находящиеся в перехваченных пакетах и перезапишет существующие PMKID в отдельный файл с заданным названием (рисунок 66).

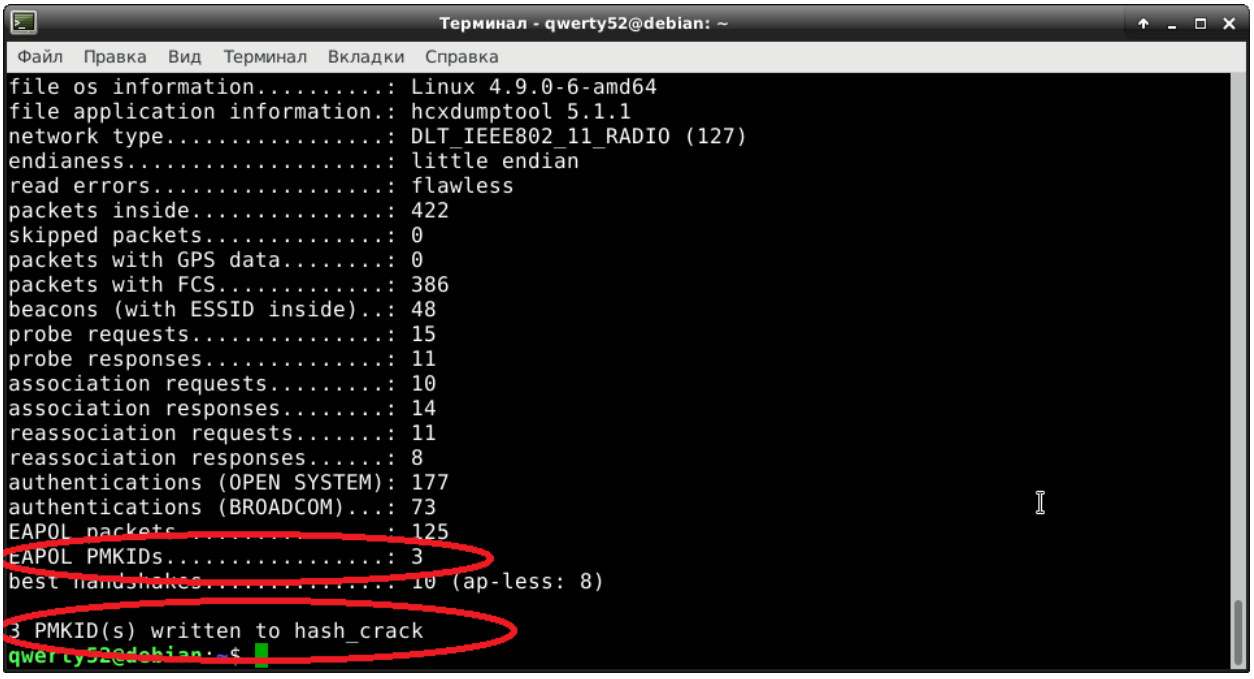


Рисунок 66 – Запись PMKID в отдельный файл

Если открыть обычным редактором то можно наглядно увидеть все 3 PMKID (рисунок 67).

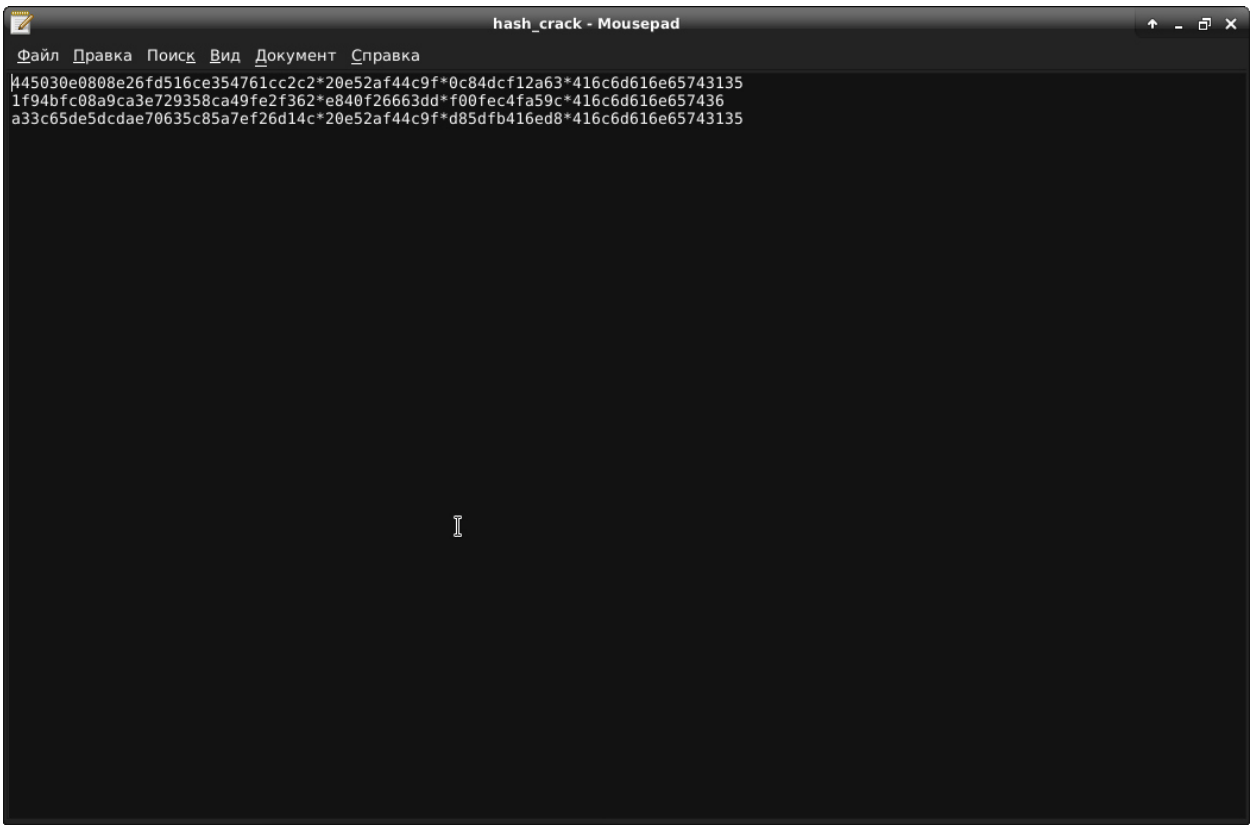


Рисунок 67 – Результат работы программы Hcxcaptool

Далее используется hashcat для перебора пароля по словарю (brute force) (рисунок 68,69).

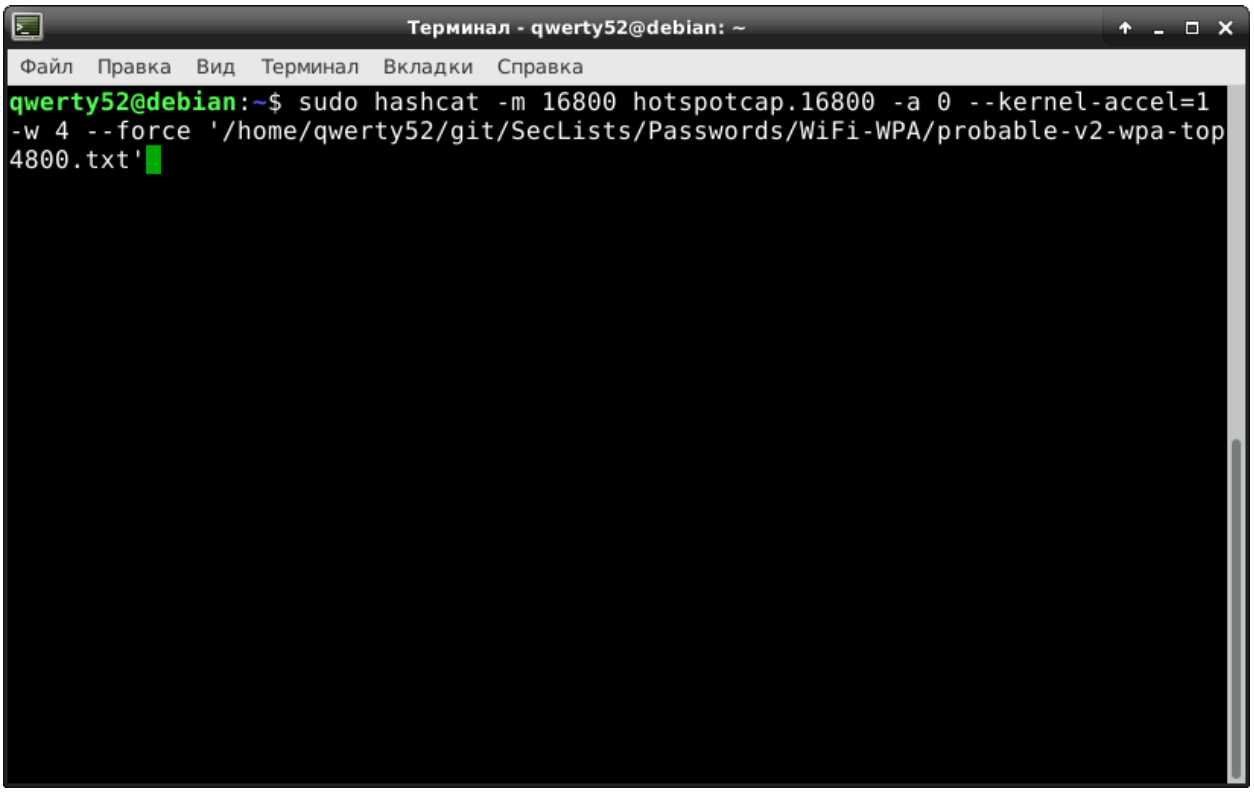


Рисунок 68 – Запуск программы Hashcat

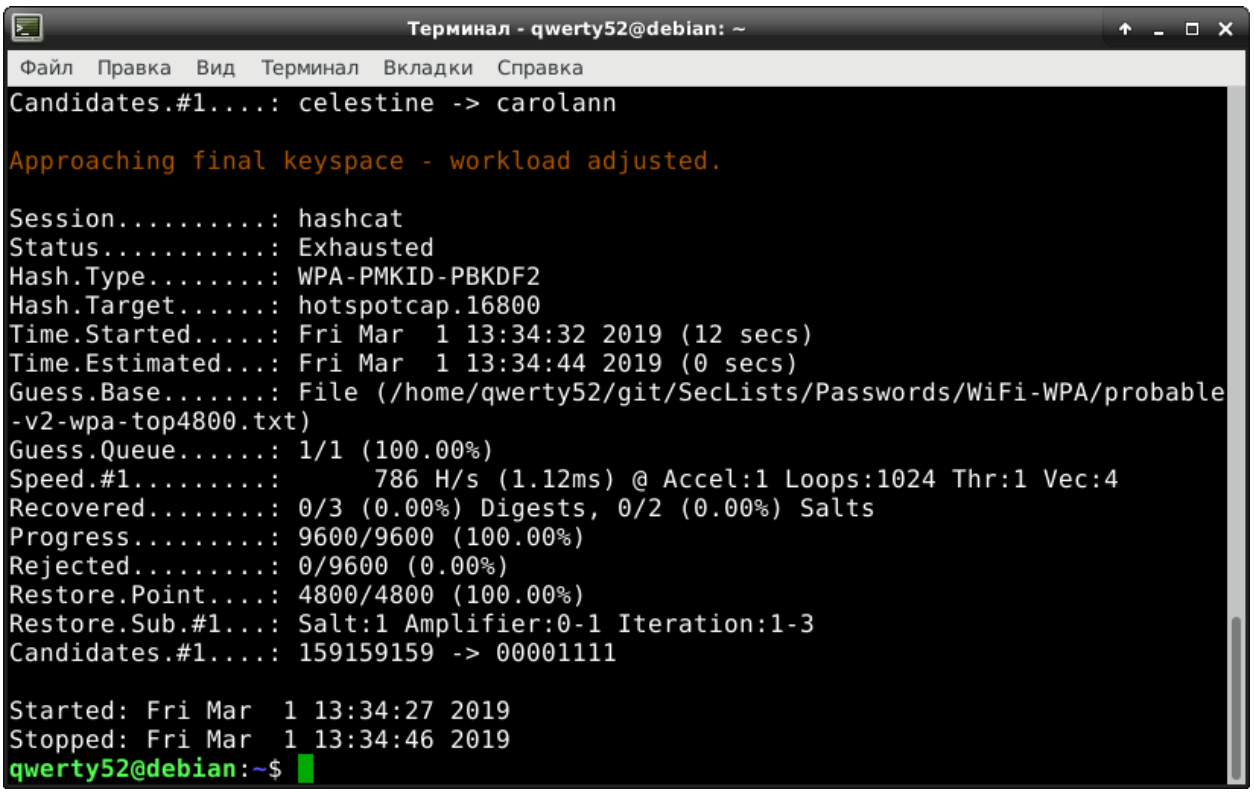


Рисунок 69 – Процесс работы программы hashcat

2.5 WPS

В первую очередь нужно выбрать сетевой интерфейс, который будет переведен в режим мониторинга сети, в данном случае используется внешний сетевой адаптер Alfa. Используем команды “sudo ifconfig” (рисунок 70).

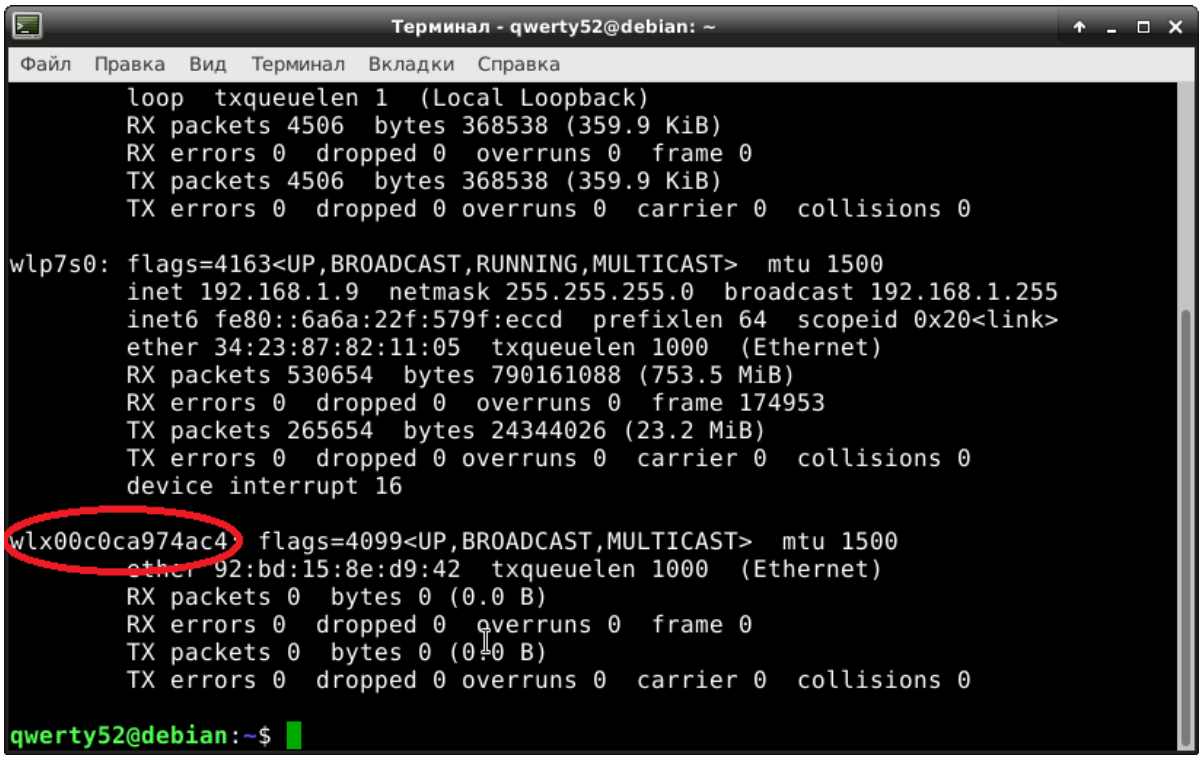


Рисунок 70 – Выбор сетевого интерфейса

Далее выбранный сетевой адаптер переводиться в режим мониторинга с помощью команды “sudo airmon-ng start wlx00c0ca974ac4 (название сетевого адаптера)”, после чего программа сообщает нам о то что сетевой адаптер переведен в режим мониторинга, обращаться к нему мы можем под названием wlan0mon (название сетевого адаптера в режиме мониторинга) (рисунок 71).

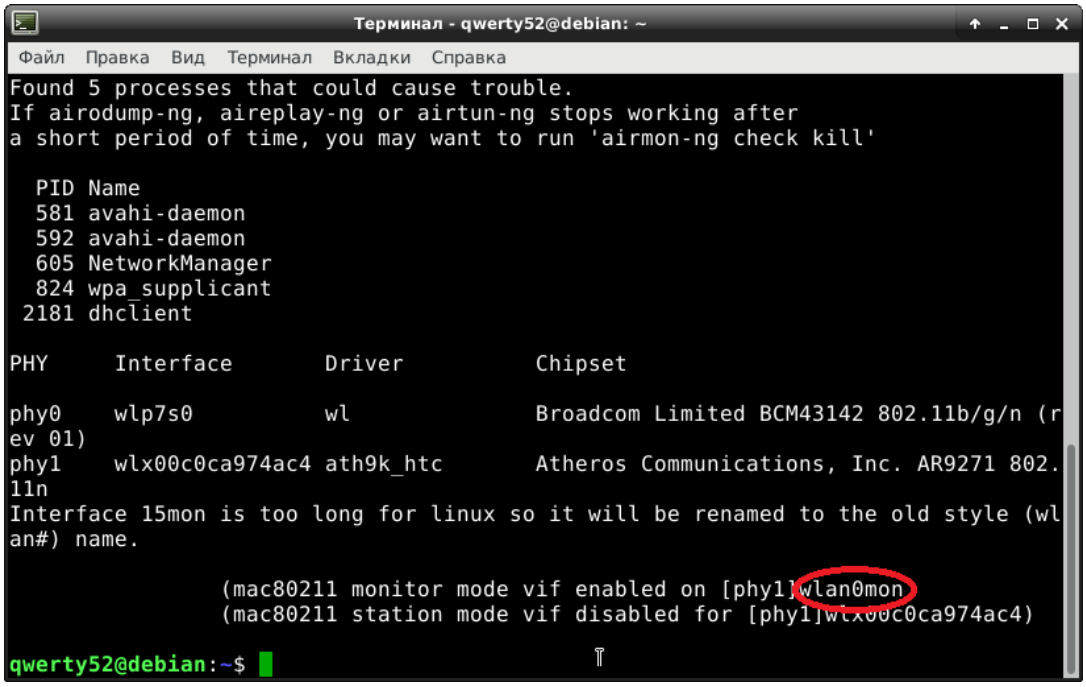


Рисунок 71 –Перевод сетевого адаптера в режим мониторинга

После чего запускаем программу для сканирования доступных точек WiFi в которых включена функция WPS (рисунок 72).

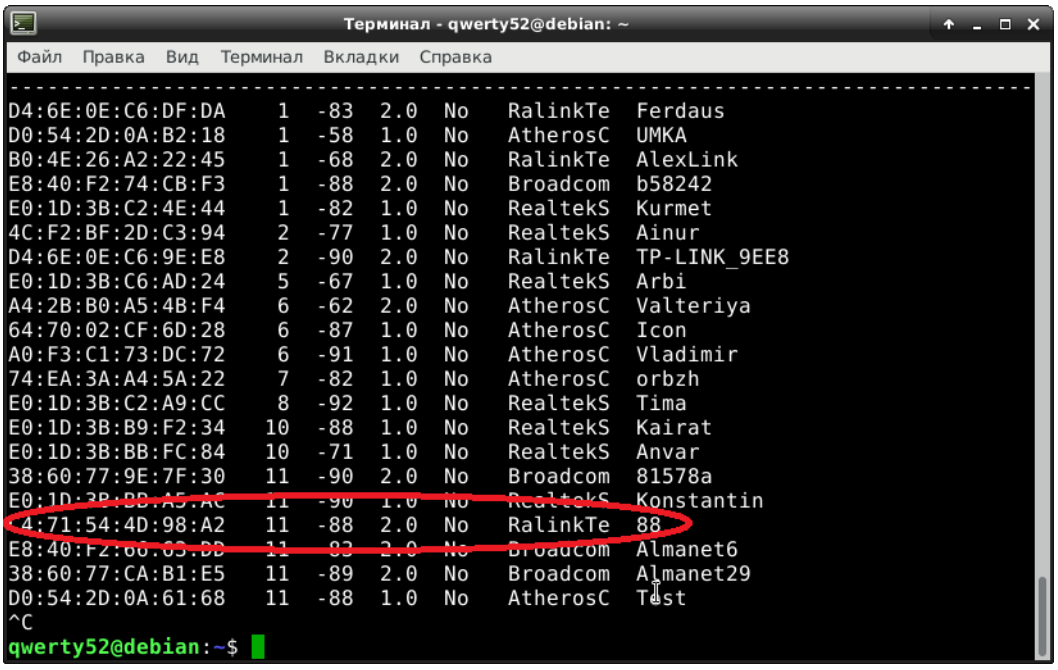


Рисунок 72 – сканирование точек с включенным WPS

Далее используется программа bully в сочетании с pixidust, которые позволяют нам получить WPS pin точки доступа, используя лишь bssid (MAC адрес точки) и канал на котором она работает (рисунок 73).

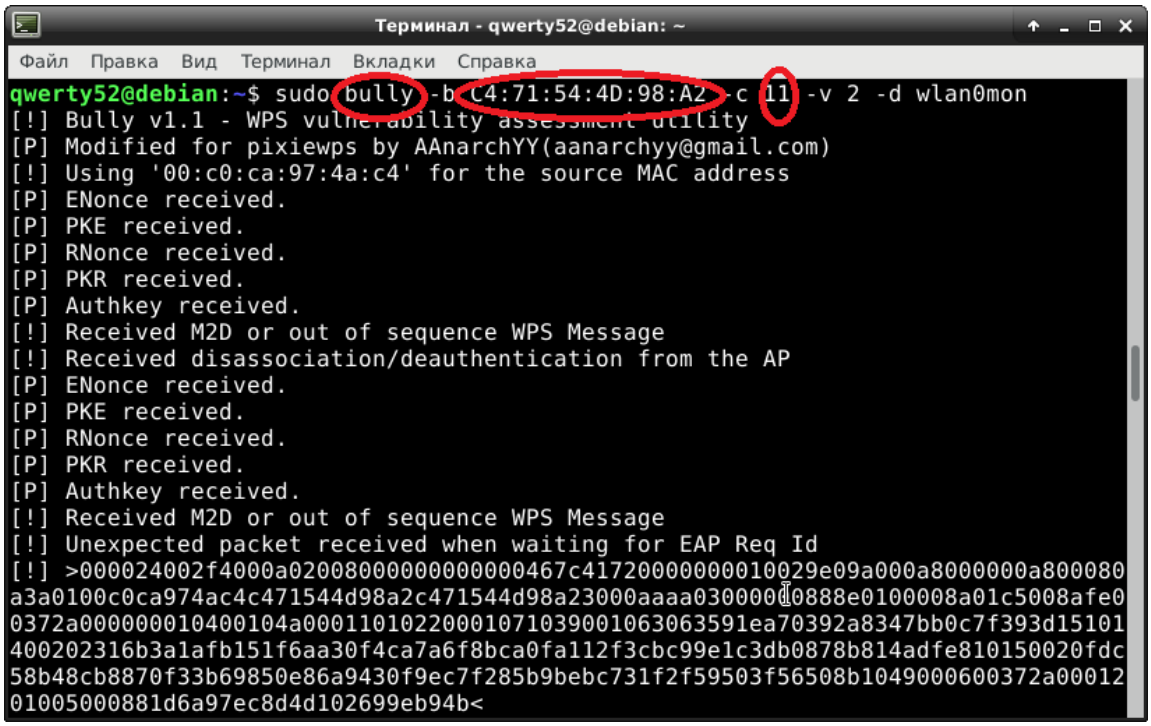


Рисунок 73 – запуск программы bully

В результате работы программы мы получаем WPS pin в открытом виде (рисунок 74).

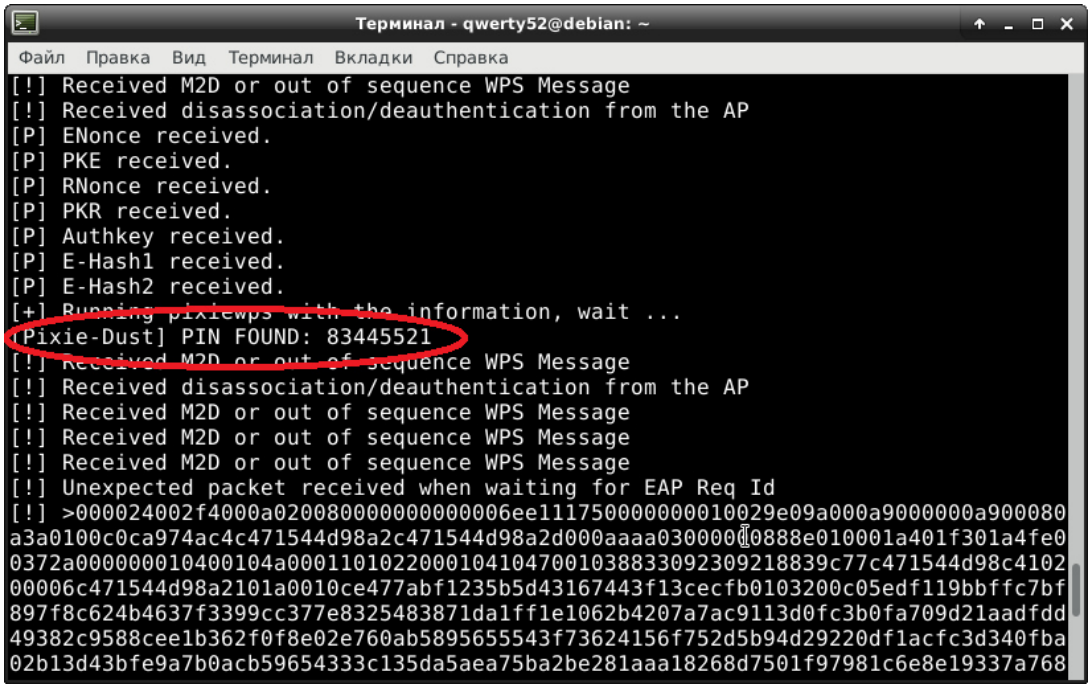


Рисунок 74 – результат работы программы bully

Далее используем программы reaver для подключения через WPS pin к точке доступа, так же указывается bssid (MAC адрес точки доступа) и канал на котором она работает (рисунок 75).

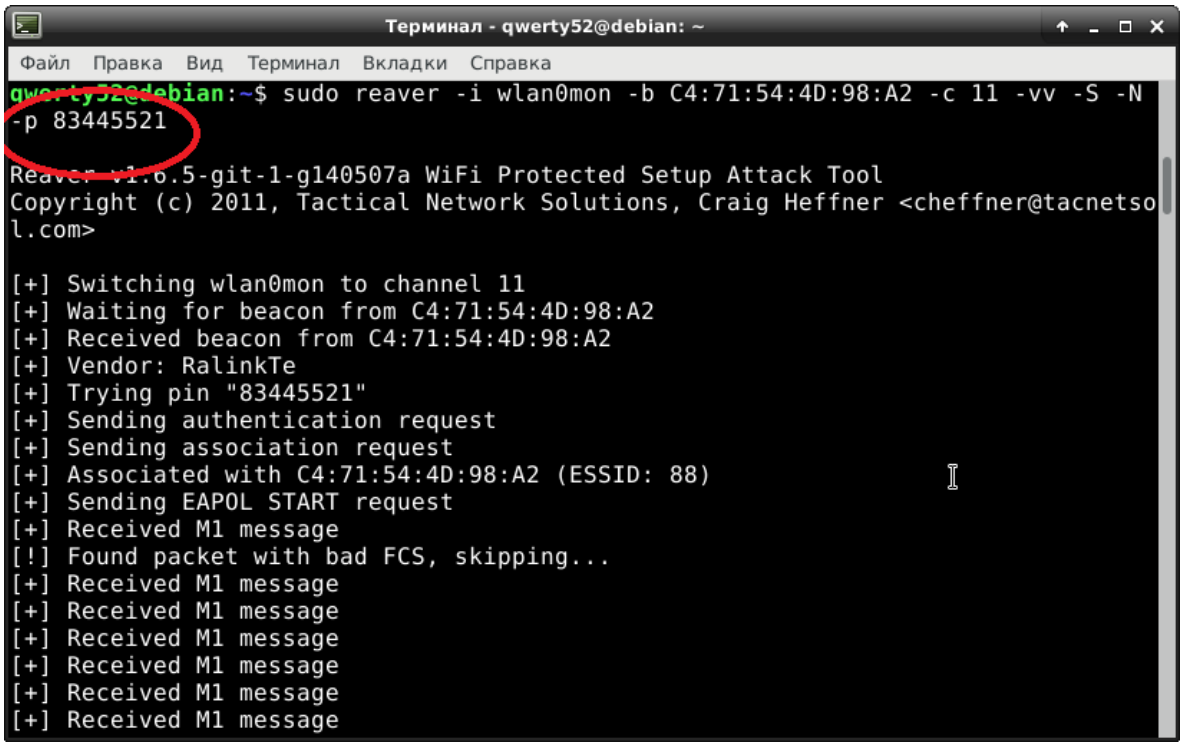


Рисунок 75 – подключение с помощью WPS pin

В результат мы получаем ключ от точки доступа в открытом виде (рисунок 76).

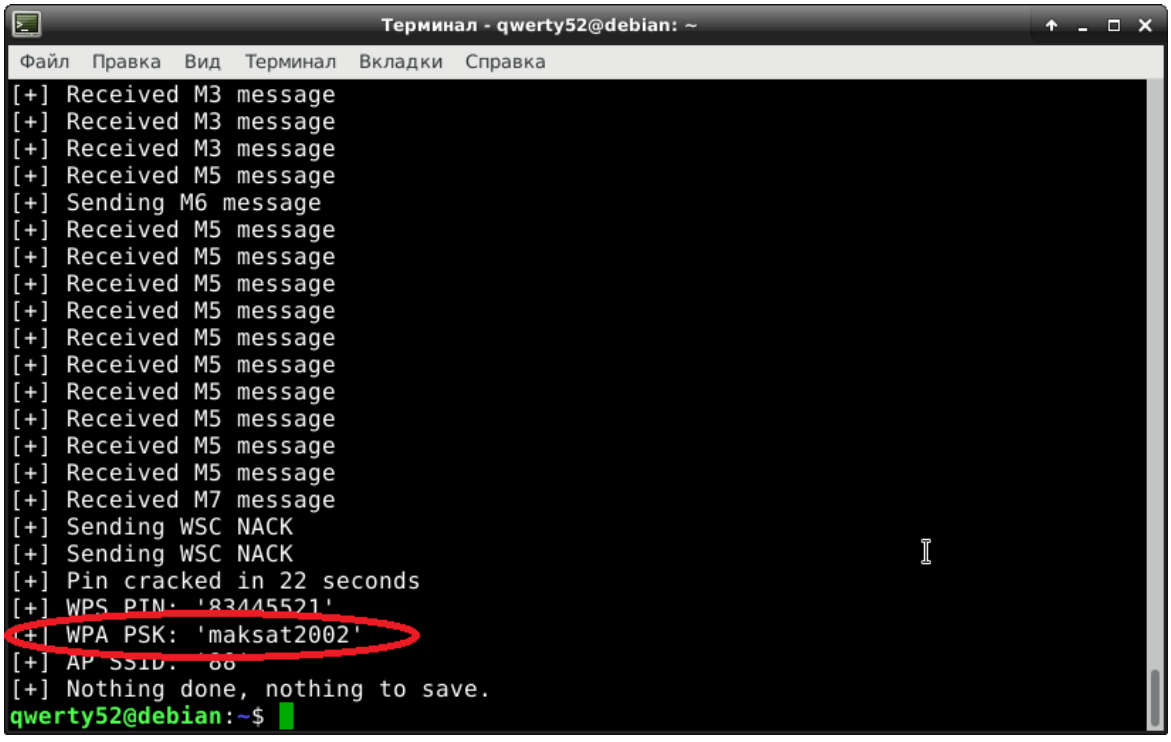


Рисунок 76 – Результат работы программы reaver

2.6 Использование уязвимостей маршрутизаторов

Данный способ атаки нацелен на определенную модель маршрутизаторов, а точнее GPON. Были выбраны маршрутизаторы именно этого производителя для проведения атаки, так как они очень широко распространены на территории Республики Казахстан, по причине того, что провайдер поставляет данные маршрутизаторы при подключении интернета, тем самым снабжая пользователей уязвимыми маршрутизаторами. Не так давно была найдена очень опасная уязвимость в данных маршрутизаторах, ей был присвоен индикатор CVE-2018-10561. Данная уязвимость позволяет обойти механизм аутентификации, путём добавления “?images/ к URL адресу страницы.

Для проведения атаки был написан небольшой скрипт с использованием curl, который собирал пароли, со всех маршрутизаторов, заданных в определённом диапазоне.

```
curl -k -d
"XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=\`$2\`;$2
&ipv=0" $1/GponForm/diag_Form?images/
echo "[+] Waiting...."
sleep 3
echo "[+] Retrieving the ouput...."
curl -k $1/diag.html?images/ 2>/dev/null | grep 'diag_result = ' | sed -e
's/\\n/\n/g'
```

В последствии был собран список, с названием, паролем и ip адресом точек доступа, в которых присутствует данная уязвимость (рисунок 77).

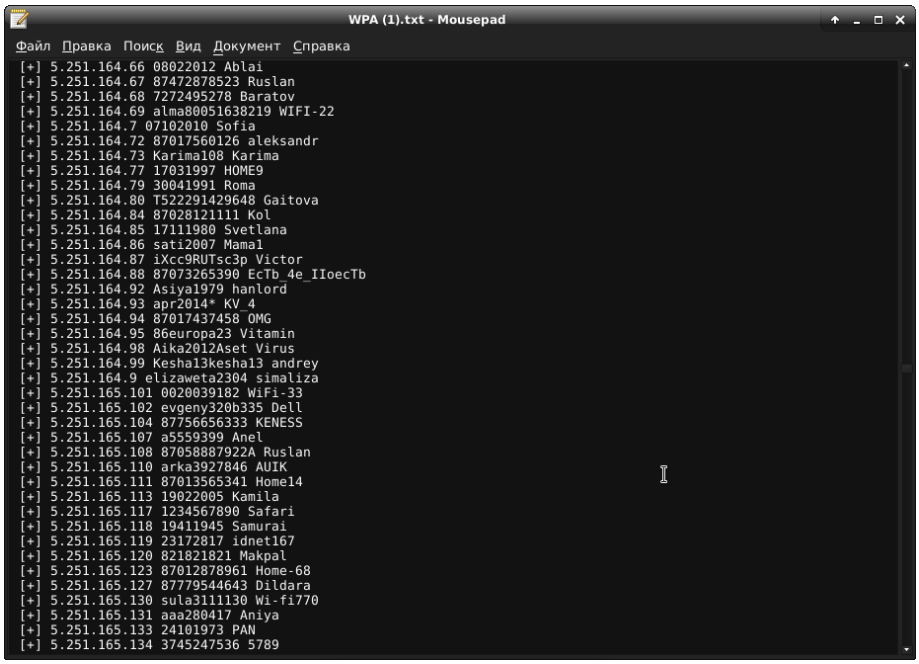


Рисунок 77 – список уязвимых точек доступа

3 Защита

3.1 Защита с использованием MAC-адреса

Один из наиболее распространенных способов защиты, это конечно же привязка по MAC адресу устройства. Данный способ может как разрешать, так и запрещать подключение к беспроводной сети какого-либо устройства, достаточно указать его MAC адрес. После чего выбрать Black list или White list. Само собой, Black list это ограничение подключения к точке доступа, а White list его противоположность.

Изначально все выглядело вот так (рисунок 78).

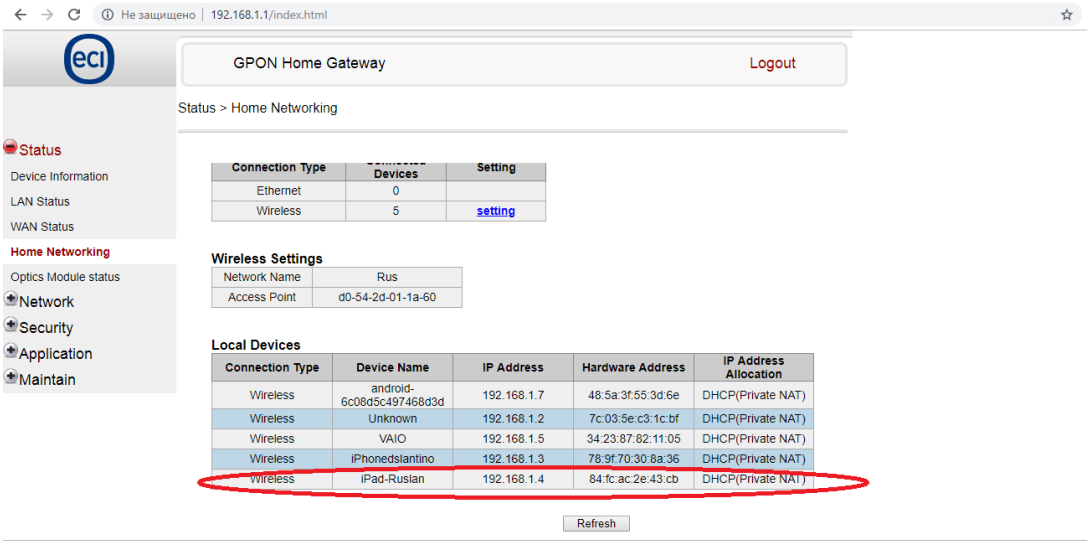


Рисунок 78 – список подключенных устройств

Далее добавляется устройства в Black list (рисунок 79).

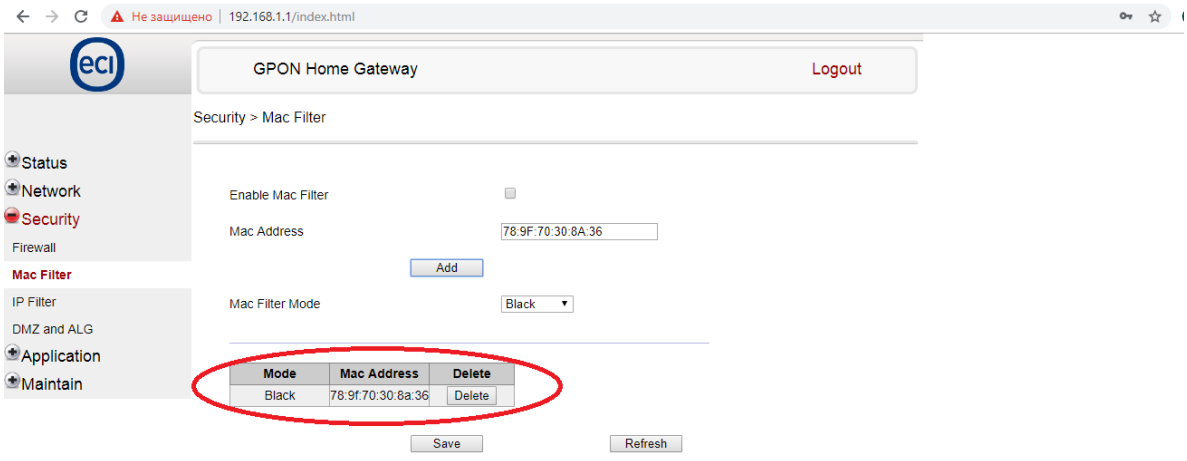


Рисунок 79 – добавление устройства в black list

После чего устройство отключается от беспроводной сети, и не может к нему подключится, так как стоит ограничение по MAC адресу, данного устройства (рисунок 80).

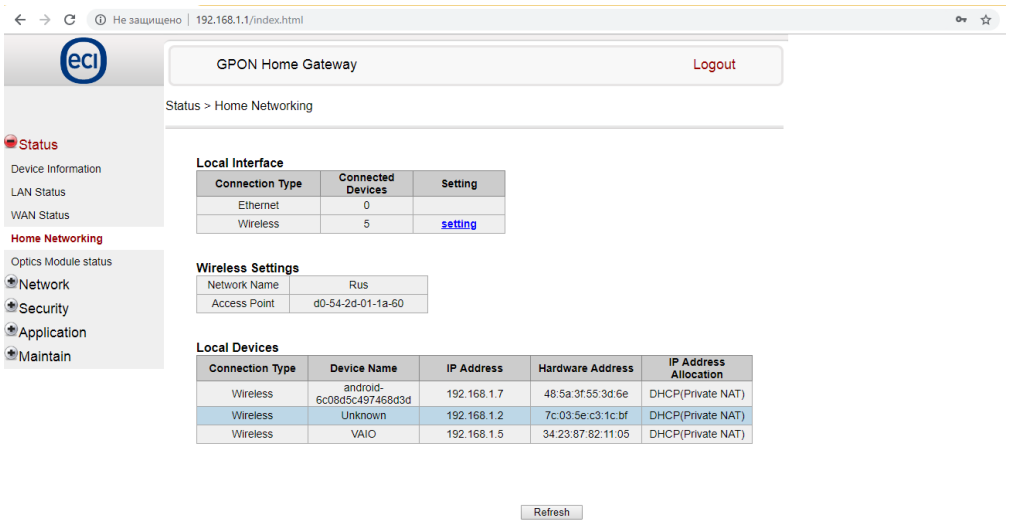


Рисунок 80 – результат работы MAC фильтра

3.2 Использование сложного пароля

Конечно не мало важной составляющей является сложность выбранного пароля, для беспроводной сети, чем длиннее и сложнее он будет, тем меньше шансов что вашу сеть смогут взломать, приоритетно иметь в пароле буквы разных регистров, цифры и различные спецсимволы, что довольно сильно усложнит получение несанкционированного доступа сети.

3.3 Сокрытие точки доступа

Следующий способ защиты, это сокрытие точки доступа, то есть отключение транслирования имени беспроводной сети. Для получения доступа в такую сеть помимо пароля, так же нужно знать название точки доступа и способ шифрования для прохождения аутентификации. Данный способ позволит сокрыть беспроводную сеть от нежелательных подключений.

Для этого нужно отключить SSID broadcast в настройках роутера (рисунок 81).

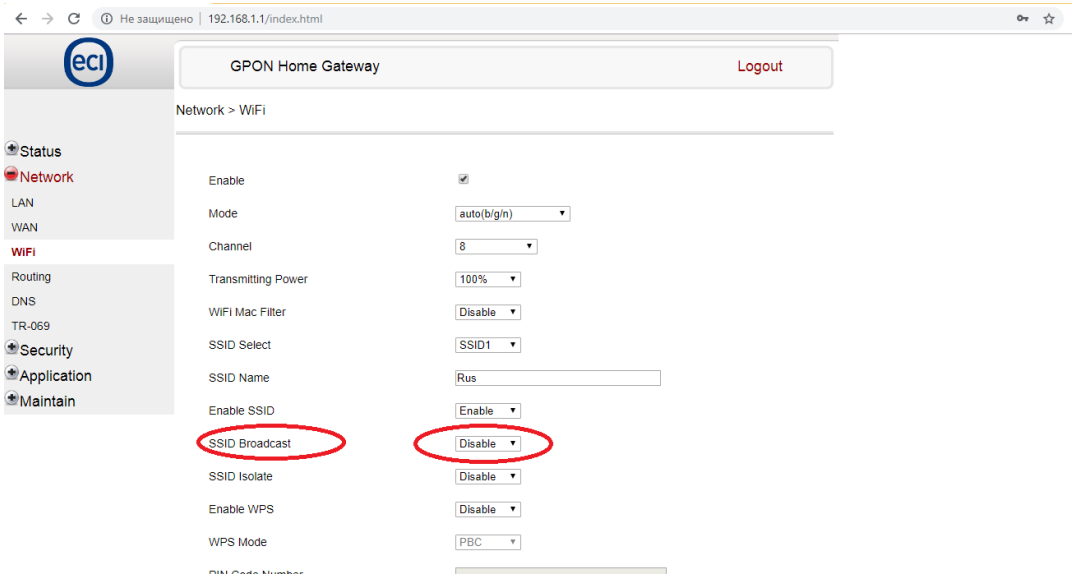


Рисунок 81 – отключение SSID broadcast

После чего беспроводная сеть исчезнет из списка доступных сетей, так как не будет отображаться ее SSID (название) (рисунок 82).

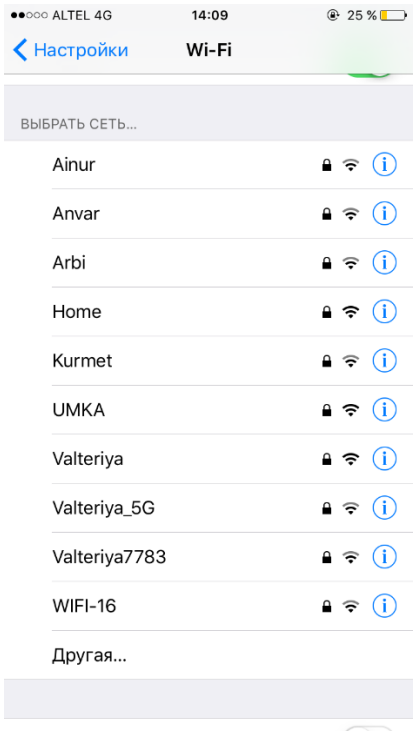


Рисунок 82 – отсутствие нужной беспроводной сети

Далее для подключения к такой сети нужно будет указать название сети (SSID), пароль и способ шифрования (рисунок 83).

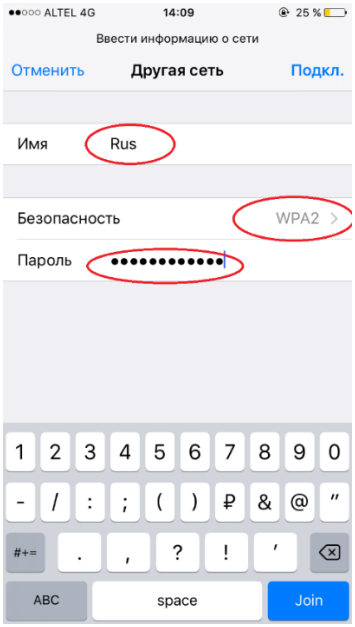


Рисунок 83 – подключение к скрытой беспроводной сети

3.4 Изоляция

Один из способов защиты беспроводной сети, так же является SSID isolate, то есть изолирование подключенного клиента от локальной сети, давая ему выход только во внешнюю сеть, тем самым можно уберечь многие устройства, подключенные к сети, от несанкционированного доступа.

Для начала просканируем локальную сеть на наличие, других устройств (рисунок 84).

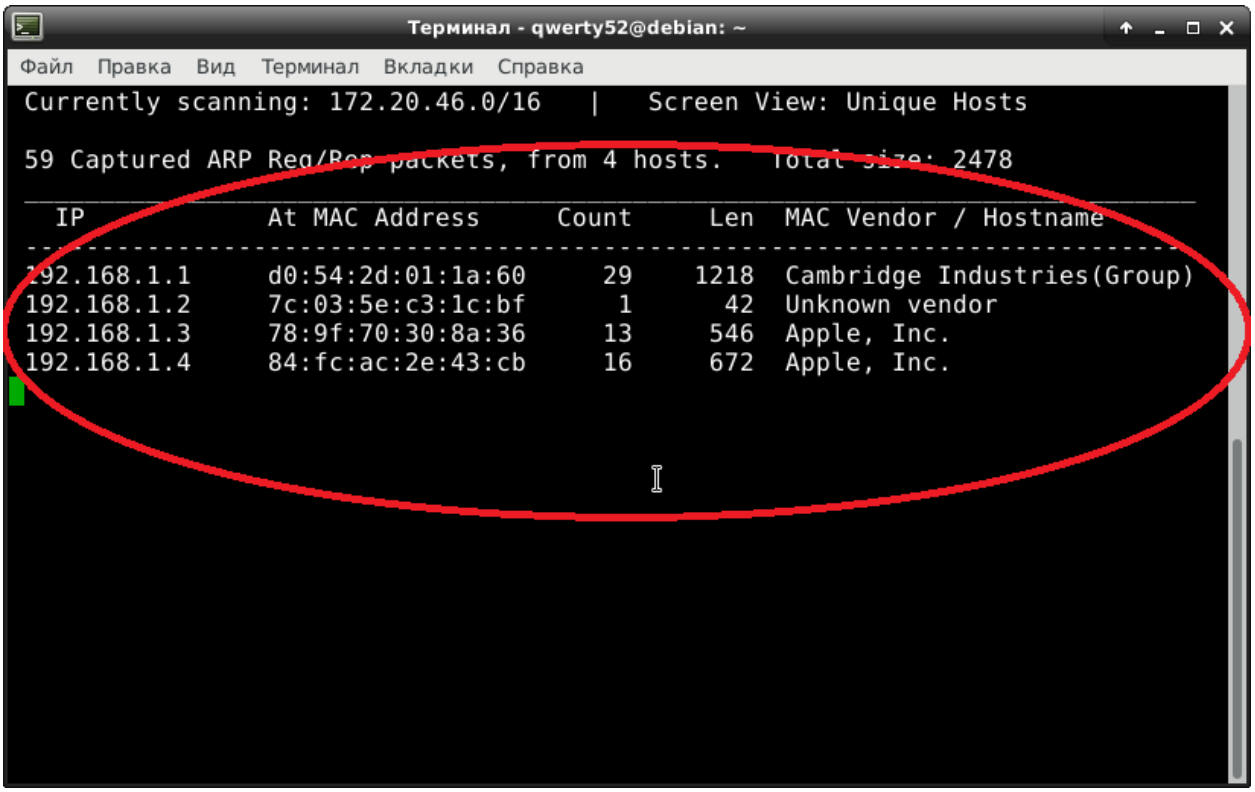


Рисунок 84 – сканирование локальной сети

Данная функция так же доступна в настройках роутера. Теперь включаем SSID isolate (рис 85.).

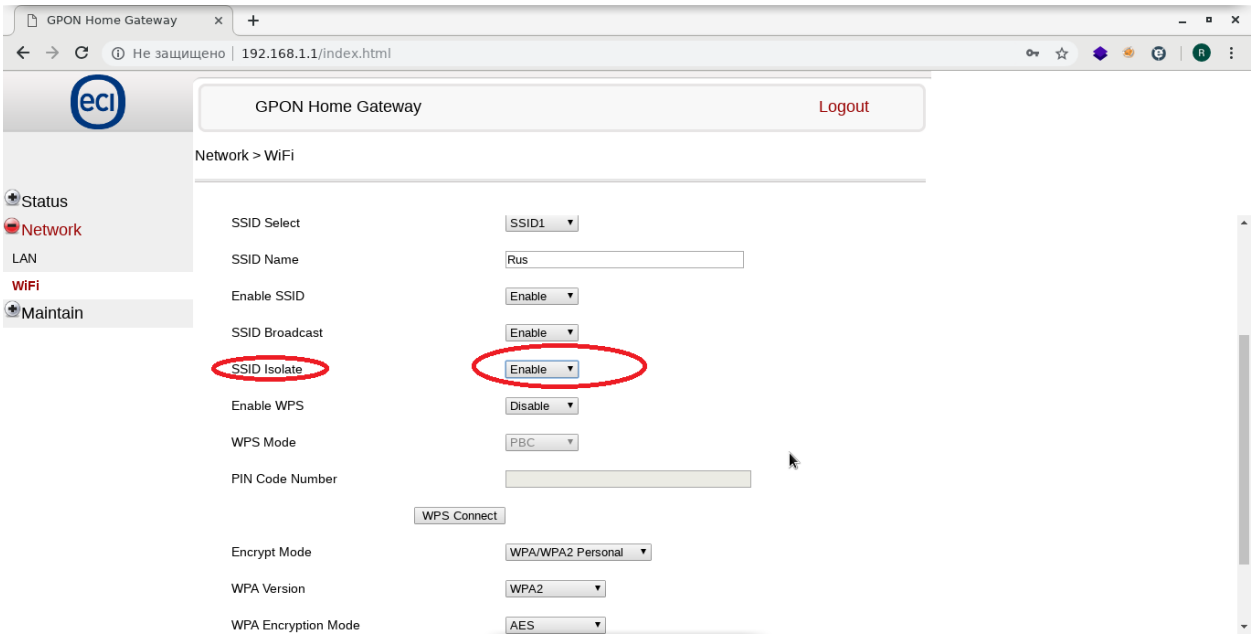


Рисунок 85 – включение SSID isolate

И снова пытаемся просканировать локальную сеть (рисунок 86).

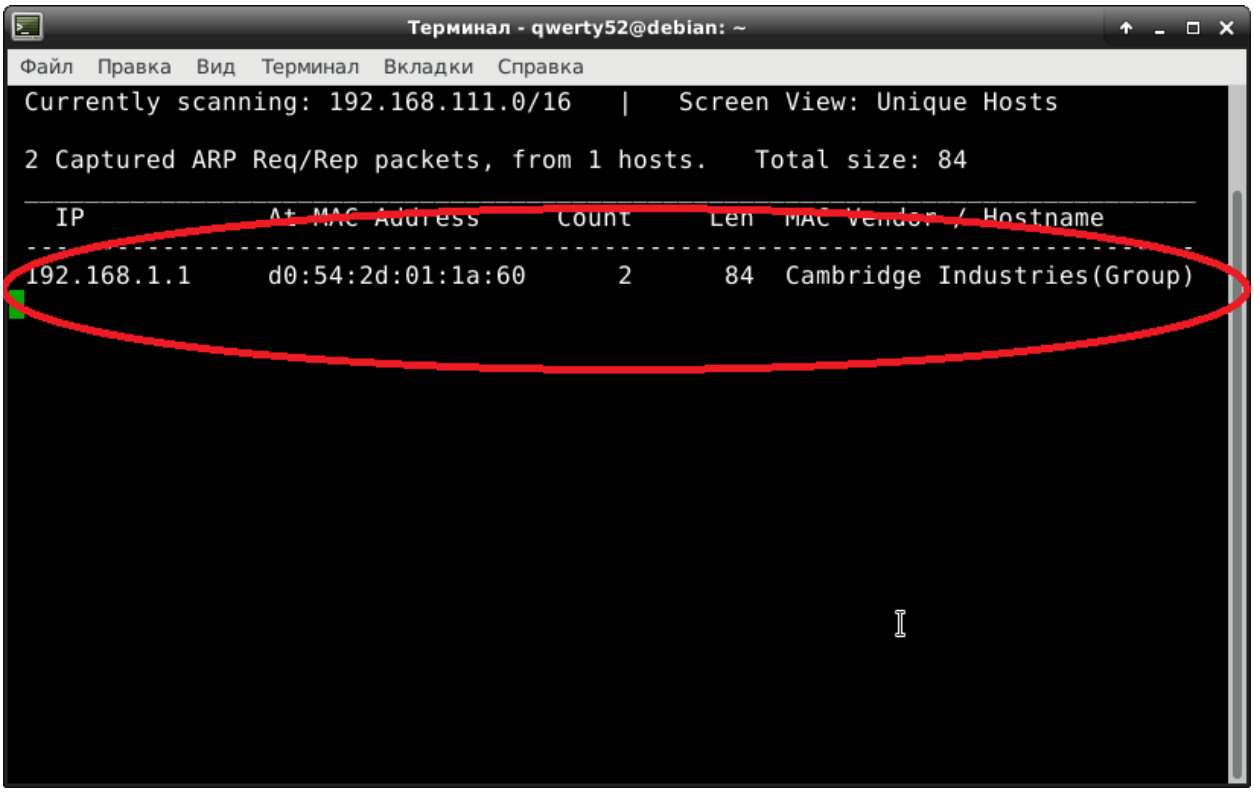


Рисунок 86 – сканирование локальной сети

В результате мы видим, только роутер который находится по адресу 192.168.1.1 , остальные устройства просто не отображаются так, как включена

функция SSID isolate, которая ограничивает доступ к локальной сети, всем устройствам.

3.5 WPA3

27 июня 2018 года альянс Wi-Fi объявил об окончании разработки нового стандарта безопасности – WPA3. Это одновременно и новый протокол безопасности, и название соответствующей программы сертификации.

Прежде чем на том или ином оборудовании появится лейбл «WPA3», ему необходимо будет пройти огромное количество тестов – это гарантирует корректную работу с другими устройствами, получившими ту же метку. С точки зрения пользователя стандарт WPA3 можно назвать и протоколом безопасности, но подразумевается под этим не аппаратная реализация, а соответствие нормативам.

Отличия WPA3 от WPA2

Создатели WPA3 попытались устранить концептуальные недоработки, которые всплыли с появлением KRACK. Новый стандарт, как и во всех предыдущих случаях, основан на технологиях его предшественника. В анонсе WPA3 представители альянса Wi-Fi говорили о применении четырех новых технологий, призванных встать на защиту беспроводного соединения. Но в итоге лишь одна из них стала обязательной для реализации производителями.

Поскольку ключевая уязвимость скрывалась в четырехстороннем рукопожатии, в WPA3 добавилась обязательная поддержка более надежного метода соединения – SEA, также известного как Dragonfly. Технология SEA (Simultaneous Authentication of Equals) уже применялась в mesh-сетях и описана в стандарте IEEE 802.11s. Она основана на протоколе обмена ключами Диффи - Хеллмана с использованием конечных циклических групп.

SEA относится к протоколам типа PAKE и предоставляет интерактивный метод, в соответствии с которым две и более стороны устанавливают криптографические ключи, основанные на знании пароля одной или несколькими сторонами. Результирующий ключ сессии, который получает каждая из сторон для аутентификации соединения, выбирается на основе информации из пароля, ключей и MAC-адресов обеих сторон. Если ключ одной из сторон окажется скомпрометирован, это не повлечет компрометации ключа сессии. И даже узнав пароль, атакующий не сможет расшифровать пакеты.

Еще одним новшеством WPA3 будет поддержка PMF (Protected Management Frames) для контроля целостности трафика. Но в будущем поддержка PMF станет обязательной и для WPA2.

Не попали в сертификацию WPA3 программы Wi-Fi Easy Connect и Wi-Fi Enhanced Open. **Wi-Fi Easy Connect** позволяет реализовать упрощенную настройку устройств без экрана. Для этого можно использовать другое, более продвинутое устройство, уже подключенное к беспроводной сети. Например, параметры сети для датчиков и умной домашней утвари можно будет задавать со смартфона, сфотографировав QR-код на корпусе девайса.

Easy Connect основан на применении аутентификации по открытым ключам (в QR-коде передается открытый ключ) и может использоваться в сетях с WPA2 и WPA3. Еще одна приятная особенность Wi-Fi Easy Connect – возможность замены точки доступа без необходимости перенастраивать все устройства.

Wi-Fi Enhanced Open подразумевает шифрование всех потоков данных между клиентом и точкой доступа. Эта технология позволит защитить приватность пользователя в публичных сетях, где не требуется аутентификация. Для генерации ключей в таких сетях будет применяться процесс согласования соединения, реализуемый расширением Opportunistic Wireless Encryption.

Поддержка обеих технологий не обязательна для сертификации по WPA3, но производитель может при желании сам включить их поддержку в продукт.

Как и в WPA2, в WPA3 предусмотрено два режима работы: WPA3-Personal и WPA3-Enterprise.

WPA3-Personal обеспечит надежную защиту, в особенности если пользователь задал стойкий пароль, который нельзя получить словарным перебором. Но если пароль не совсем тривиальный, то должно помочь новое ограничение на число попыток аутентификации в рамках одного рукопожатия. Также ограничение не позволит подбирать пароль в офлайновом режиме. Вместо ключа PSK в WPA3 реализована технология SEA.

WPA3-Enterprise подразумевает шифрование на основе как минимум 192-разрядных ключей, соответствующих требованиям CNSA (они выработаны комитетом NSS для защиты правительственных, военных и промышленных сетей). Для аутентифицированного шифрования рекомендовано применение 256-разрядных ключей GCMP-256, для передачи и подтверждения ключей используется HMAC с хешами SHA-384, для согласования ключей и аутентификации - ECDH и ECDSA с 384-разрядными эллиптическими кривыми, для защиты целостности кадров - протокол BIP-GMAC-256.

На официальном сайте альянса Wi-Fi уже опубликован список устройств с поддержкой WPA3, но пока что их всего шесть штук. Однако наличие такого списка означает, что до появления WPA3 осталось ровно столько времени, сколько необходимо для интеграции протокола в новые устройства. По прогнозам альянса Wi-Fi, ожидается, что устройства с поддержкой WPA3 получат распространение на рынке в 2019 году вместе с устройствами с поддержкой Wi-Fi-802.11ax (или Wi-Fi 6 согласно новой схеме наименования).

3.6 Последствия проникновения в сеть

Последствия проникновения в беспроводную сеть

После получения пароля от беспроводной нести, злоумышленник может нанести огромный ущерб.

В первую очередь проверить устройства находящиеся в этой сети с помощью netdiscover (рисунок 87).

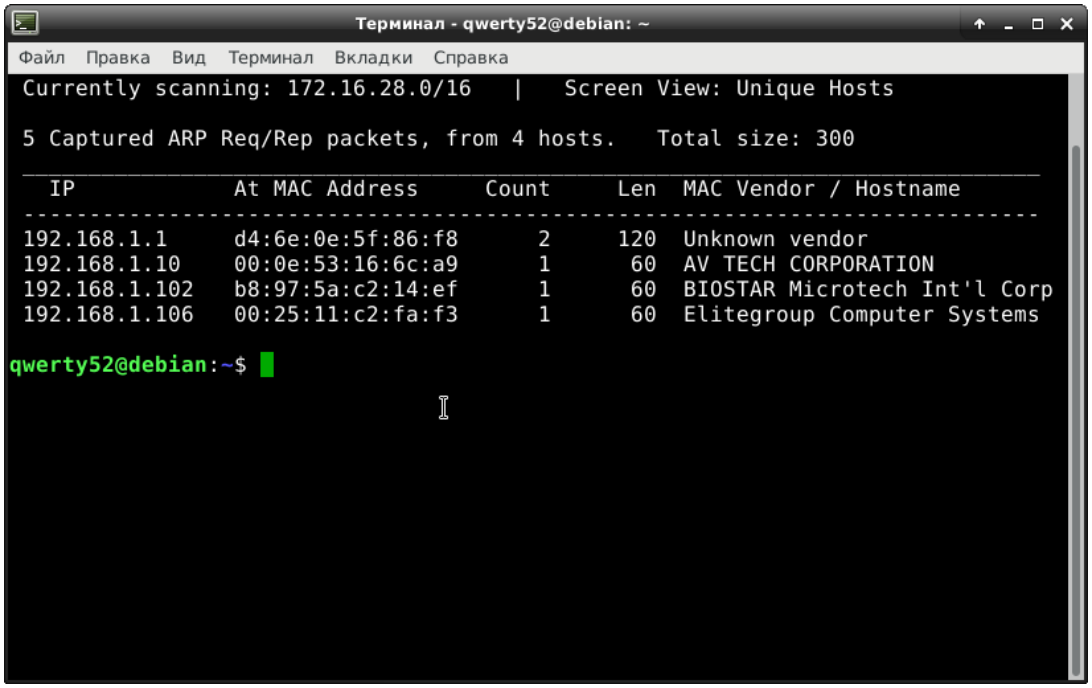


Рисунок 87 – Сканирование устройств, подключенных к беспроводной сети

Сразу же тут можно заметить то, что здесь имеются камеры, компьютер это первое что бросается в глаза.

Далее не сложно получить доступ к данным камерам (рисунок 88).

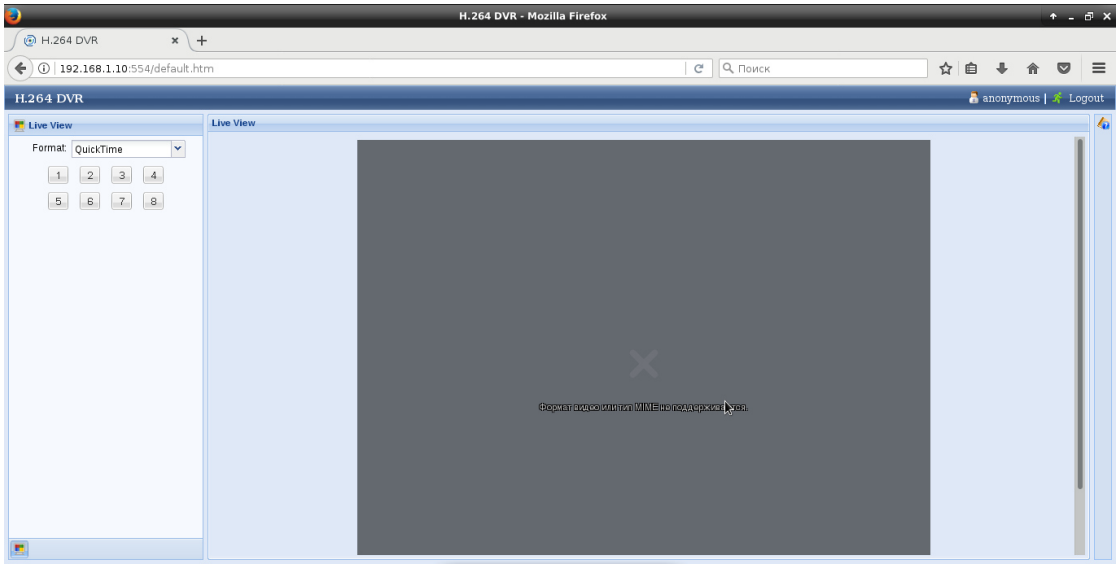


Рисунок 88 – Получение доступа к камерам

После чего можно просканировать доступный компьютер на открытые порты (рисунок 89).

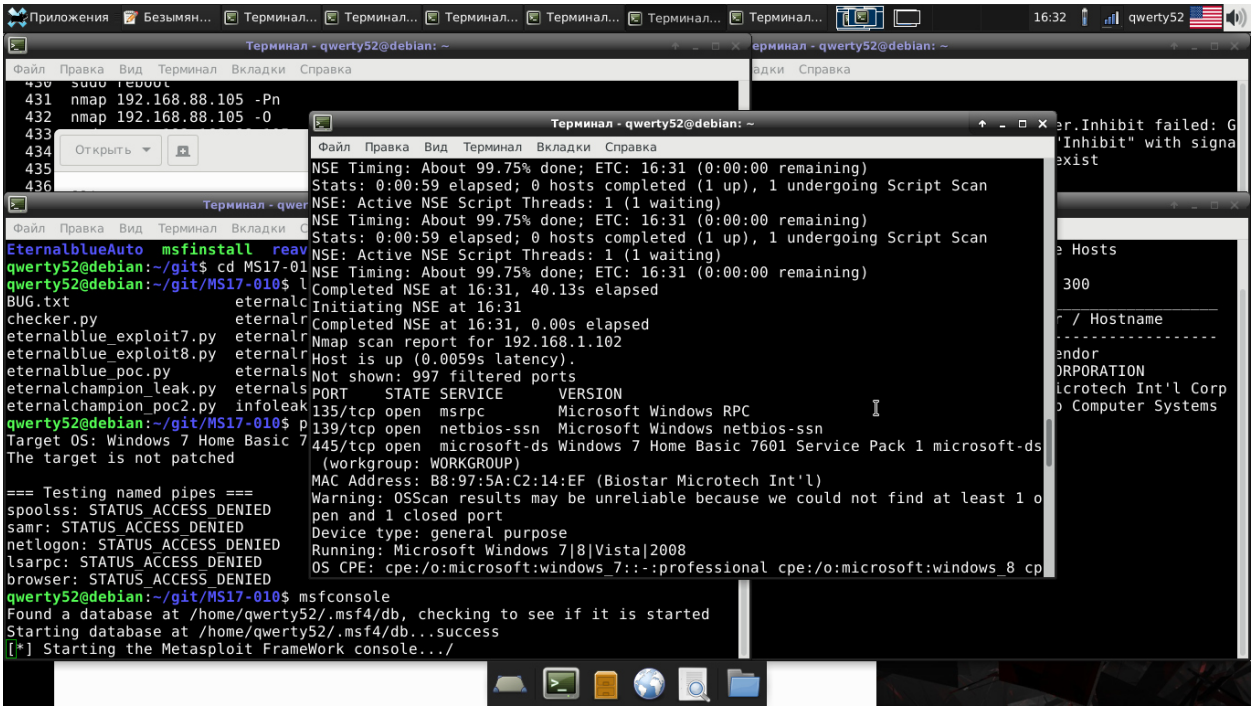


Рисунок 89 – сканирование открытых портов

В данном случае открыт порт 445, можно использовать эксплойт **ms17-010-eternalblue**, для получения удаленного доступа к этому компьютеру (рисунок 90).

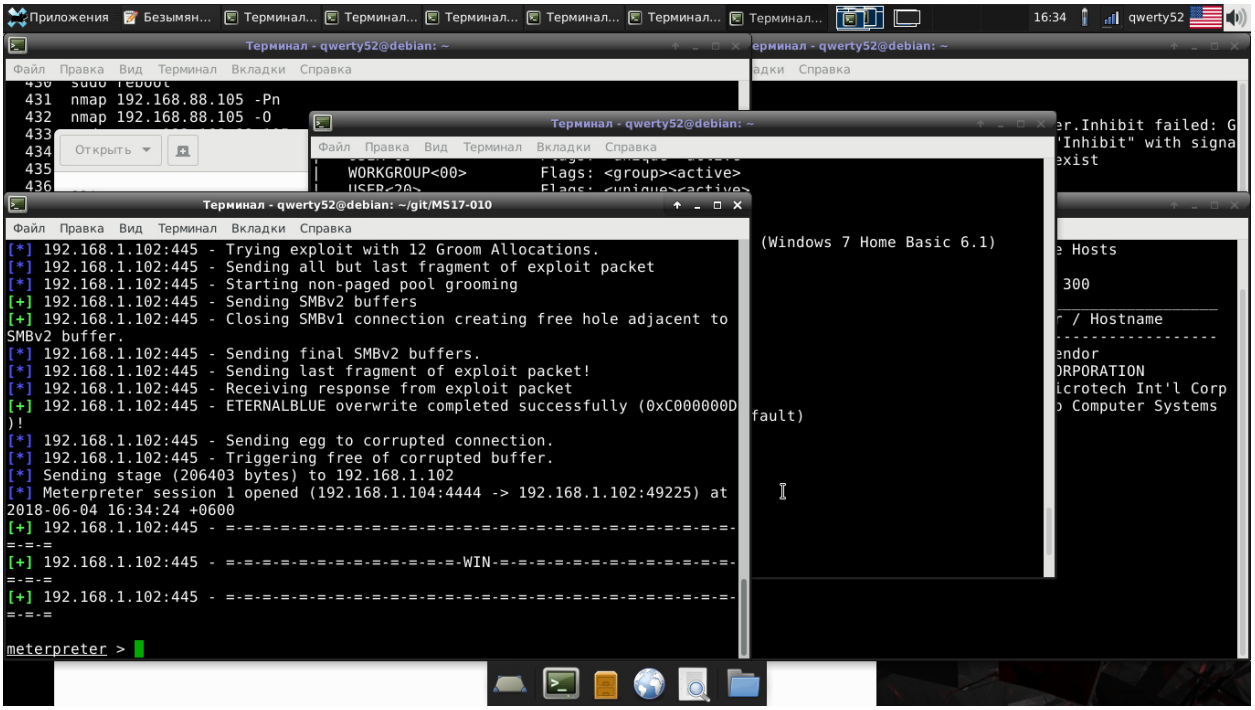


Рисунок 90 – Результат работы эксплойта, получение удаленного доступа

Возможно вытащить пароли от учетных записей на этом компьютере, к сожалению пароли не задавались (рисунок 91).

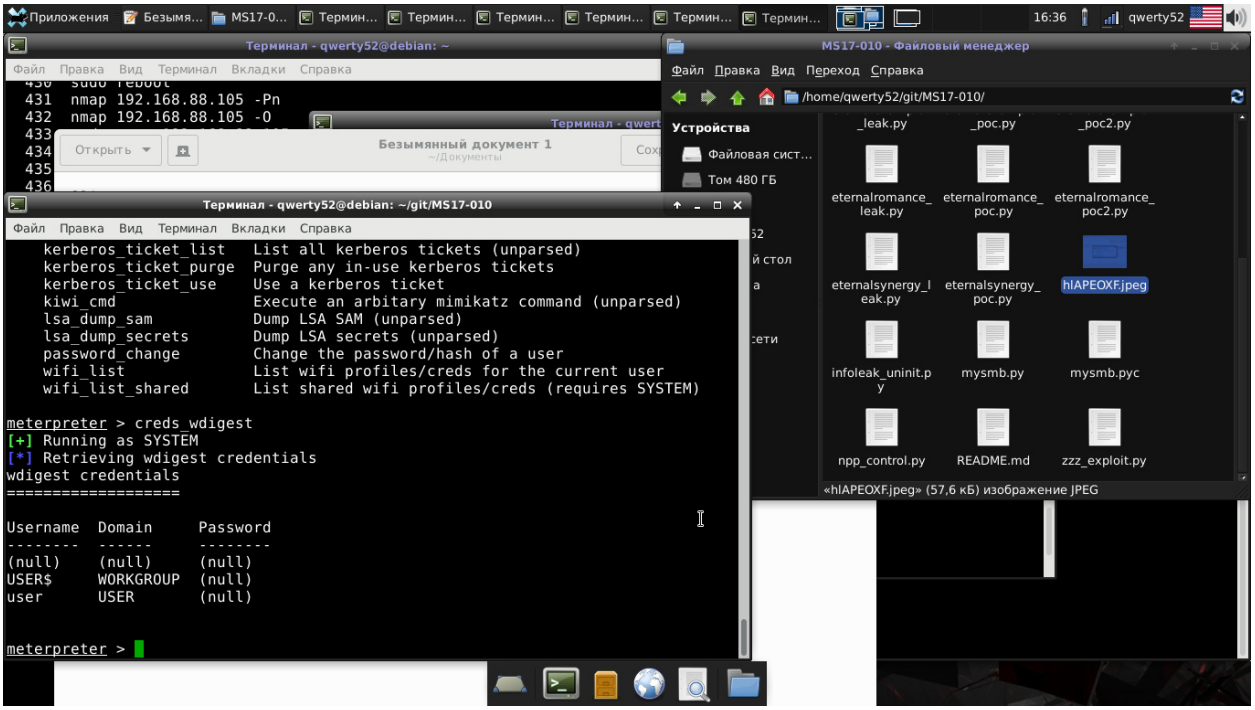


Рисунок 91 – Получение паролей от данного компьютера

Так же для понимания для чего этот компьютер, можно сделать скриншот экрана (рисунок 92).

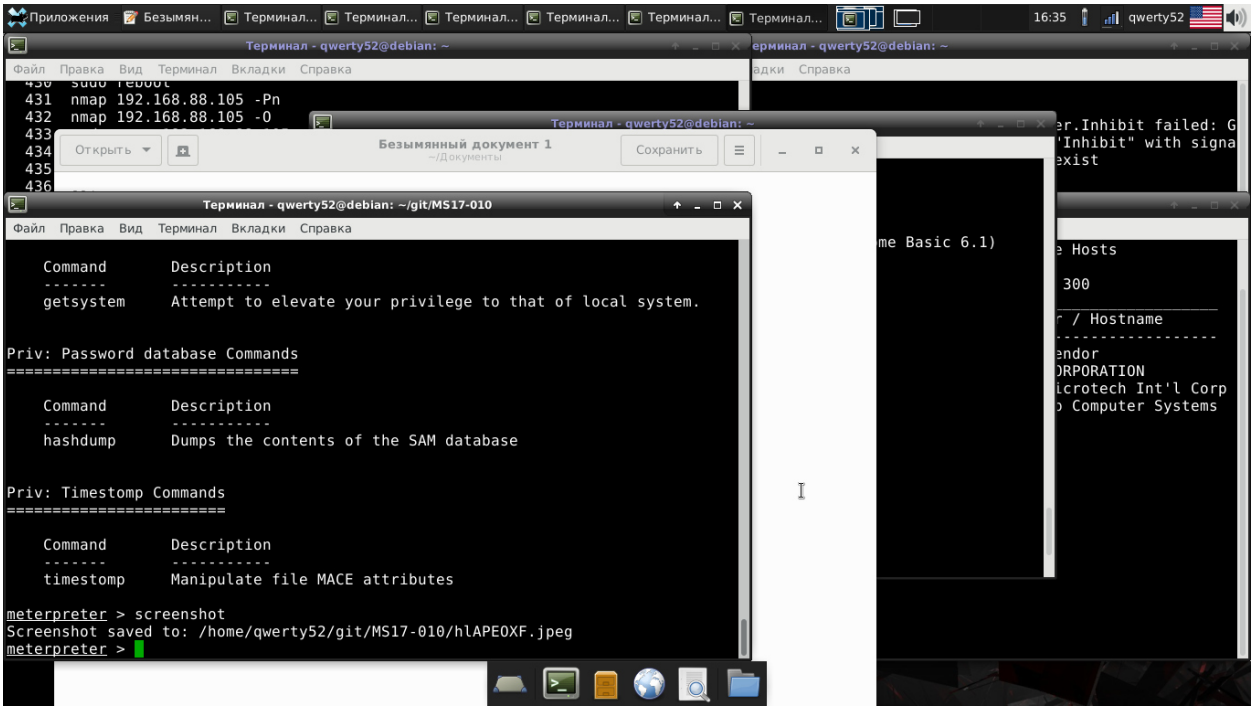


Рисунок 92 – Команда для выполнения скриншота

В результат мы видим, что данный компьютер, используется как кассовый аппарат(рисунок 93).

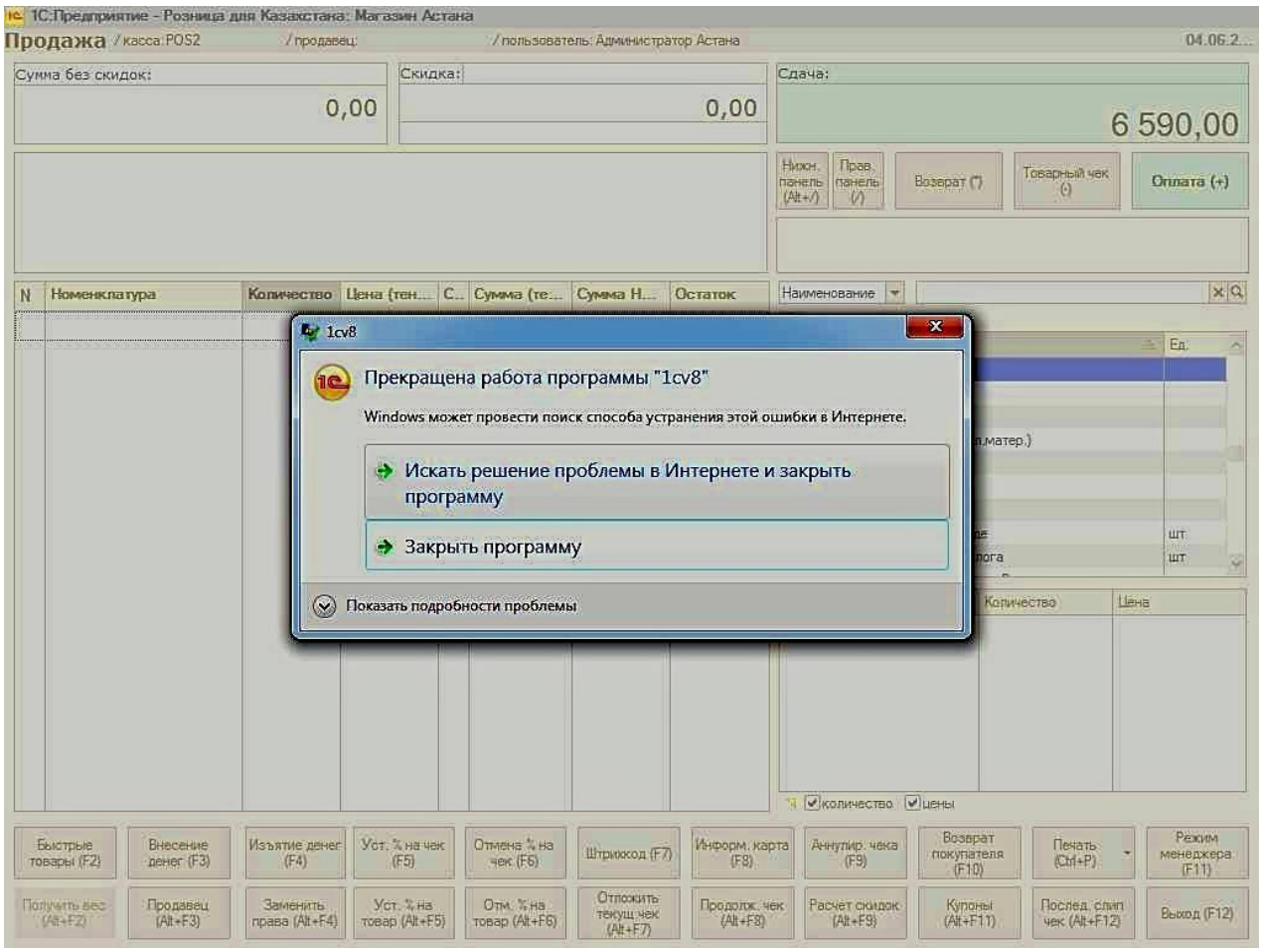


Рисунок 93 – Скриншот с компьютера

Так же можно использовать различные виды атак, такие как MITM(Man-in-the-middle), достаточно переустановить ключ шифрования, это позволит полностью прослушивать траффик, который будет проходить по сети.

4 Экономическая часть

Технико-экономическое обоснование

Главной задачей дипломного проекта является исследование уязвимостей и способов защиты беспроводных сетей. На сегодняшний день информация имеет огромную ценность, важно уметь правильно взаимодействовать с ней, но при нарушении конфиденциальности, целостности или доступности, это может вылиться в огромные убытки для владельца информации. Конечно же существует огромное множество способов обхода защиты беспроводных точек доступ, поэтому мониторинг беспроводных сетей довольна важен, так как по ним проходят огромные объёмы важной информации. Во время мониторинга используют различные возможности для защиты, такие как: фильтрация по MAC-адерсу, изоляция, шифрование и многое другое.

Программный проект рассчитан на единственного разработчика, так как, достаточно одного человека для обеспечения защиты беспроводных сетей, его задачами будет: проводить мониторинг беспроводных сетей, взаимодействие с определенным программным обеспечением, обеспечивать защищенность сети, проведение теста на проникновение в сеть (пентест/аудит) и т.д.

Технико-экономическое обоснование состоит из:

- установление трудоемкости выполнения пентеста/аудита и защиты;
-расчёт материальных затрат
-амортизация
-расчёт фондов оплаты труда

Расчет трудоемкости исследования

Указан список стадий и типов работ, необходимых для нахождения точной степени трудоемкости проведения аудита/пентеста и обеспечения защиты. В соответствии с общепризнанными методами трудоемкость. Этапы приведены в таблице 4.1.

Таблица 4.1– Распределение работ по этапам и оценка их трудоемкости

Этапы проведения работ	Тип работ	Трудоемкость разработки, чел. х ч.
1 этап	Постановка задач	18
2 этап	Разработка и утверждение технического задания на проникновение и защиту	22
3 этап	Ознакомление с методиками взлома и обеспечения защиты	28
4 этап	Изучение специализированной литературы	22
5 этап	Изучение необходимого программного обеспечения для обеспечения защиты и проведения атак	24
6 этап	Проведение практической части проекта	25
7 этап	Написание теоретической части на основе проведенной практической части	19
8 этап	Реализация проекта	34
9 этап	Написание выводов о проделанной работе	19
10 этап	Подведение итогов исследования	16
ИТОГО		227

$$\frac{227}{8} = 28{,}375 = 29 \text{ дней}, \quad (4.1)$$

Используя стандартный 8-ми часовой трудовой день, получаем то, что на реализацию проекта нужно затратить 29 рабочих дней.

Расчет затрат на исследование

Установление затрат на исследование уязвимостей и способов защиты беспроводных сетей, расчет происходит из составленной сметы, которая содержит следующие метки:

-материальные затраты;

-затраты на оплату дополнительного софта;

-прочие затраты.

Метка «Материальные затраты» это список из основных и второстепенных материалов, предназначенных для проведения исследования. Материальные затраты приведены в таблице 4.2.

Таблица 4.2 – Затраты на материальные ресурсы

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Внешняя сетевая карта	Alfa Awus036NAH	штук	1	18 100,00	18 100,00
Блокнот	"LIFE IS HERE"(РАЗМЕР А5) ТИРАЖ 2018-2019 Г	штук	1	2650,00	2 650,00
Ручка	Ручка шариковая ZEBRA "OLA "	упаковка		800,00	800,00
Компьютерная мышь (беспроводная)	Мышь A4Tech G3-310N, Black-Silver, USB	штук	1	6870,00	6870,00
Итого					28 420,00

Для проведения исследование использовался ноутбук Sony Vaio SVF1421P1RW, так как этот ноутбук при его приобретении имеет уже встроенную ОС Windows 8.1 и ПО Microsoft office, то затраты на их покупку не целесообразны. А также затраты не производились на вспомогательное ОС Debian так как она имеет бесплатную лицензию, как и ПО используемое для проведения работ.

Таблица 4.3 – Затраты на ОС и ПО, необходимые для проекта

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Ноутбук	Sony SVFP1521RW	Шт.	1	273000,00	273000,00
Принтер	HP laserjet 1020	Шт.	1	67000,00	67000,00
Модем	Модем ASUS DSL-AC68U	Шт.	1	91900,00	91900,00
Итого					431900,00

По данной формуле рассчитывается сумма расходов на программное обеспечение, а также исследование:

$$Зм = \sum Pi \times Ци, \quad (4.2)$$

где Pi - расход i-го вида материального ресурса, натуральные единицы;

Ци - цена за единицу i-го вида материального ресурса, тг;

i - вид материального ресурса;

n - количество видов материальных ресурсов.

Зм =28420+431900= 460 320 (тг)

Общие затраты для реализации проекта составляют: 460 320 тенге.

Расчет затрат на электроэнергию

Само собой, при проведении исследования, используется различное оборудование, которое потребляет электроэнергию, поэтому стоит рассчитать ее расход.Используя таблицу 1, получаем время, затрачиваемое для реализации исследования, так как принтер не нужен, на протяжении всего исследование, стоит ограничить его время работы до 3-х часов.

$$Э = Зэл.эн.обор + Здоп.нуж, \quad (4.3)$$

где $З_{эл.эн.обор}$ – затраты на электроэнергию оборудования;

$З_{доп.нуж.}$ – затраты электроэнергии на дополнительные нужды.

Расходы электроэнергии на оборудование определяются в соответствие с формулой:

$$З_{эл.эн.обор} = \sum W \times К_{исп} \times S \times T, \quad (4.4)$$

где W – потребляемая мощность, Вт;

$К_{исп}$ – коэффициент использования ($К_{исп}$ = 0,7..0,9);

T – время работы;

S – тариф (1кВт/ч = 26,71).

Результаты расчетов затрат на электроэнергию находятся в таблице 4.

Таблица 4.4 – Затраты на электроэнергию

Наименование приборов	Паспортная мощность, кВт	Коэффициент мощности	Время работы оборудования, ч	Цена ЭЭ тг/ кВтч	Сумма, тг
Ноутбук	0,7	0,8	227	23,85	3031,81
Модем	0,09	0,9	172	23,85	332,27
Принтер	0,4	0,9	5	23,85	42,93
Кондиционер	0,9	0,9	184	23,85	3554,60
Освещение	0,4	0,7	184	23,85	1228,75
Итого					8190,36

$З_{эл.эн.обор}$ = 3031,81+332,27+42,93+3554,60+1228,75= 8190,36 (тенге)

Дополнительные расходы считаются по увеличенному показателю около 5% относительно оборудования:

$$З_{доп.нуж} = 5\% \times З_{эл.эн.обор}, \quad (4.5)$$

Расчёт дополнительных затрат происходит по формуле :

$З_{доп.нуж}$ = 0,05 × 8190,36 =409,52 (тенге)

В итоге затрачиваемые средства составляют:

Э = 8190,36 +409,52 = 8599,88(тенге)

Таблица 4.5 – Затраты на оплату труда

Категория работника	Квалификация	Трудоемкость разработки ПП, чел.×ч	Часовая ставка, тг/ч	Сумма, тг
Высшая	Программист	227	1190	270130
ИТОГО затраты на оплату труда				270130

Часовую ставку сотрудника можно рассчитать по следующей формуле:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i}, \quad (4.6)$$

где $ЗП_i$ - месячная заработная плата i-го работника, тг;
$ФРВ_i$ - месячный фонд рабочего времени i-го работника, час.

$$ЧС_{программист} = \frac{276080}{29 * 8} = 1190 \text{ тг/ч}$$

Амортизация основных фондов и прочие затраты

Обычно годовые амортизационные нормы ОФ опираться на налоговый кодекс РК или создаются опираясь на показателях возможного срока полезного действия ОФ.

Формула для амортизации основных фондов

$$Аг=\frac{Соб \cdot На}{100}, \quad (4.7)$$

где, $С_{об}$ – стоимость оборудования;

$Н_А$ – норма амортизации (норма амортизация = 25);

Далее рассчитывается сумма нужная для амортизационных отчислений в течении года, отдельно для ноутбука:

$$Аг = \frac{273000 \times 25}{100} = 68250 \text{ тг}$$

Амортизационная сумма за время исследования:

$$Аг = \frac{68250 \times 26}{365} = 5796{,}6 \text{ тг тг}$$

Расчёт суммы амортизации для оставшегося оборудования

Таблица 4.6 – Амортизация основных фондов (ОФ)

Наименование оборудования и ПО	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Сумма амортизации за год, тг	Сумма амортизации за время разработки, тг
Ноутбук	35 000	25	68250	5796,60
Принтер	67 000	25	16750	1193,15
Модем	91 900	25	22975	1636,57
ИТОГО			121500	8626,32

Расчет затрат по социальному налогу

Формула определения социального налога:

$$Сн = (Фот - ПО) * 0.095 , \quad (4.8)$$

Где, ПО – отчисления в пенсионный фонд=10% от фонда оплаты труда. Социальный налог согласно Налоговому кодексу РК равен 9.5% от фонда оплаты труда (Фот).

ПО=479 940*0.1=47 994 Тенге

$$Сн = (270130 - 27013) * 0.095 = 23\,096{,}11 \text{ тенге}$$

Таблица 4.7 – Социальный налог

Категория работника	Заработная плата, тг	Пенсионные отчисления, тг	Соц. Налог, тг
Программист	270 130	27 013	23 096,

			11
Итого:			23 096, 11

Смета расходов.

Используя полученные результат можно создать смету на проведения исследования, далее приведена диаграмма рабочих затрат

Таблица 4.8 – Смета затрат на исследование программного кода

Статьи затрат	Сумма, тг
Затраты на оборудование и материальные ресурсы	460320,00
Затраты на оплату труда	270130,00
Затраты на электроэнергию	8599,88
Социальные налоги	23096,11
Амортизация основных фондов	8626,32
Прочие расходы	14000,00
Итого	784772,31

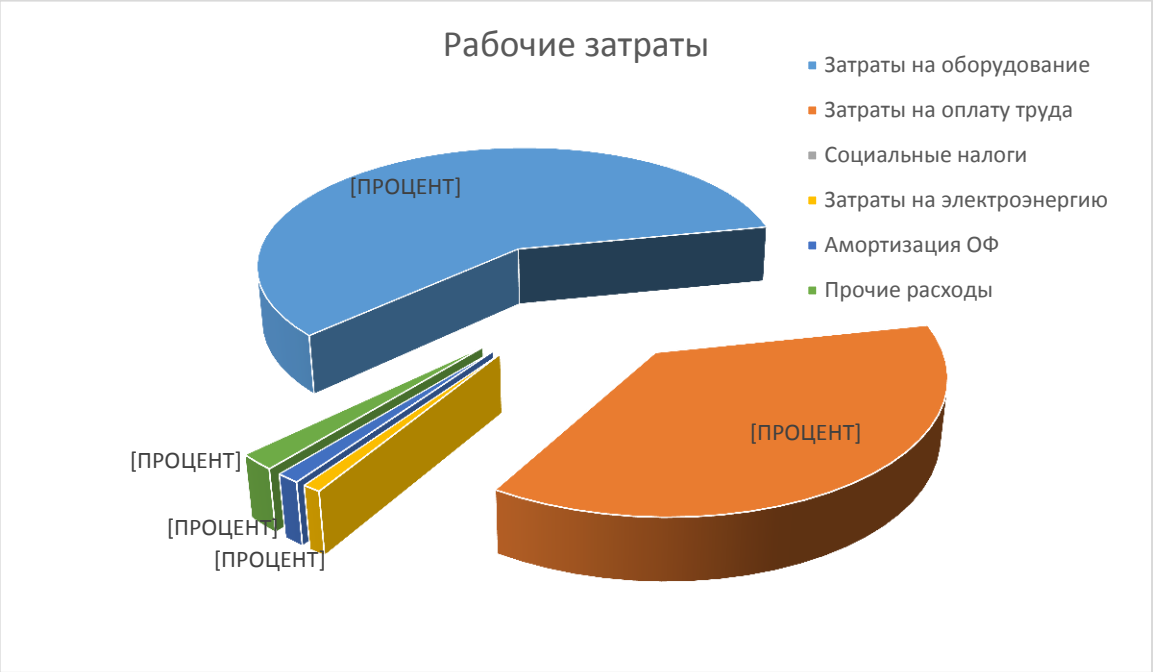


Рисунок 90 – Диаграмма рабочих затрат

Определение возможной (договорной) цены реализации

Стоимость реализации можно посчитать по следующей формуле:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \quad (4.9)$$

где $З_{нир}$ – затраты на проектирование, тг;

Р – средний уровень рентабельности, (%). Данный параметр принят равным 25%.

Прибыль = 784772,31* 0,25 = 196193,07 тенге

$$Ц_Д = 784772{,}31\left(1 + \frac{25}{100}\right) = 784772{,}31 + 784772{,}31 * 0{,}25 = 980965{,}38 \text{ тенге}$$

Далее необходимо определить стоимость реализации с учетом НДС, ставка НДС устанавливается законодательством РК. На 2019 года ставка НДС составляет 12%. Стоимость реализации учитывая НДС можно рассчитать по следующей формуле:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (4.10)$$

$$Ц_р = 980965{,}38 + 980965{,}38 * 0{,}12 = 1098681{,}23 \text{ тенге}$$

Результатом расчетов является: прибыль равна 196193,07 тенге
Себестоимость равна 784772,31 тенге
Стоимость с учётом НДС равна 1098681,23 тенге

Вывод

В данной главе дипломного проекта проведены вычисления различных затрат на покупку нужного оборудования, а также различных сопутствующих затрат, связанных с проведением проверки на уязвимость и обеспечения защиты беспроводных сетей. Произведены расчёты на такие затраты как: приобретение оборудования, расчёт трудоёмкости исследования, электроэнергию, амортизационные отчисления.

Проведение экономических расчетов необходимо, для того что бы узнать какие средства потребуются для реализации проекта, и последующего контроля средств во время его выполнения.

5 Безопасность жизнедеятельности

Данный дипломный проект будет реализован в компании «». После проведения анализа было выяснено, что освещение и вентиляция полностью соответствуют нормам, чего нельзя сказать о шуме. Так как на предприятии присутствуют электрогенераторы, которые нарушают акустические нормы. В этих расчетах будут приведены меры защиты и способы устранения шума.

Шум – это беспорядочное сочетание звуков различной частоты и интенсивности. Шум возникает при механических колебаниях в твердых, жидких и газообразных средах.

Шум ухудшает условия труда, оказывая вредное воздействие на организм человека. При длительном воздействии на организм человека происходят нежелательные явления: снижается острота зрения, слуха повышается кровяное давление, понижается внимание.

Сильный продолжительный шум может быть причиной функциональных изменений сердечно-сосудистой системы.

Условие задачи

В помещении на полу расположены несколько источников одинакового шума (Ф=1). Кабина замера находится 1,5 м в высоту и в 1 м от точки замера. Узнать октавные уровни в расчётной точке с использованием схем.

Результаты сравнить с допустимыми нормами. В случае превышения выбрать определённые меры по шум изоляции.

Начальные данные:
Оборудование: генератор
Количество: 5
r1= 3,5 м; r2= 4,2 м; r3= 5,3 м
Объем помещения, V: 1000 м3.
B/Sогр: 1,5
lmax: 1,2
Кабина наблюдения: 14 ×10×4 м
Окно S4= 3 м2
Стена, S1= 56 м2
Дверь, S3= 4 м2
Стена S2= 140 м2

Расчетная часть

Таблица 4.1. Уровни давления звука Lp теплоэнергетического оборудования /2/.

Источники шума на ТЭЦ	Среднегеометрические частоты октавных полос, Гц							
	63	125	250	500	1000	2000	4000	8000
генератор	105	105	98	97	98	92	90	92

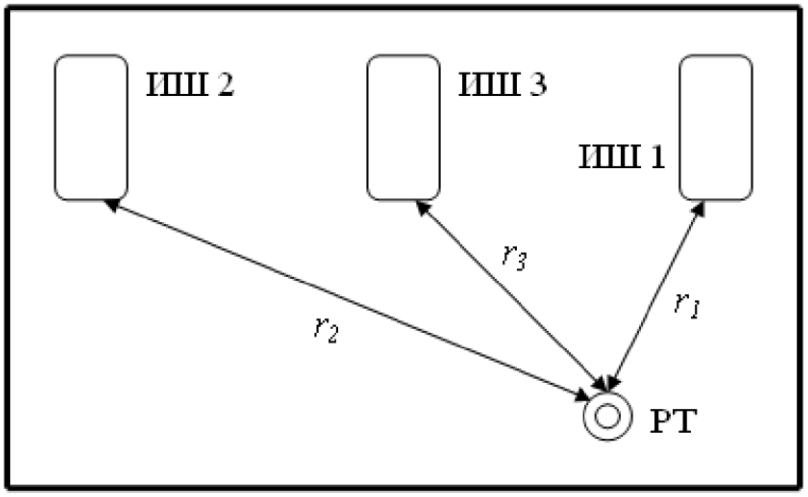


Рисунок 95 – Расположение расчетной точки и источников шума

Звуковое давление определяем по формуле:

$$L = 10 \cdot \lg\left(\sum_{i=1}^{m} \frac{\Lambda_i \chi_i \Phi_i}{S_i} + \frac{4\psi}{B}\sum_{i=1}^{n}\Lambda_i\right), \text{ где } \Lambda_i = 10^{0,1L_{pi}}, \qquad (5.1)$$

Lpi - звуковая мощность дБ;

где χ - коэффициент, влияния ближайшего акустического поля и принимаемый в зависимости от отношения r к lmax, lmax - максимальный габарит источника шума (Рисунок 2 /1/):

m= 3 - количество источников шума, ближайших к расчетной ($ri \leq 5 \cdot rmin$) поскольку для источников шума $ri < 4 \cdot rmin$ при rmin= 3,5 м.

n= 3 - общее количество источников шума в помещении;

$\chi 1$= 1, так как r1/lmax = 3,5/1,2 = 2,91;

$\chi 2$= 1, так как r2/lmax= 4,2/1,2 = 3,5;

$\chi 3$= 1, так как r3/lmax= 5,3/1,2 = 4,41;

Ф=1 - фактор напряженности источника шума;

S - площадь воображаемой поверхности. Для ИШ, у которых $2 \cdot lmax < r$ (в данном случае это условие выполняется для всех ИШ): при расположении ИШ в пространстве $S=4\pi r2$, на поверхности стен, перекрытия $S=2\pi r2$, в двухгранном углу, образованном ограждающими конструкциями $S=\pi r2$;

B - постоянная помещения, $B=B1000 \cdot \mu$, где B1000 - постоянная помещения на среднегеометрической частоте 1000 Гц. Для генераторного зала B1000= V/20 = 1000/20 = 40 (Таблица 3 /1/),

μ - частотный множитель (Таблица 4 /1/);

Таблица 4.2 - Частотные множители.

Объём помещения в м3	Частотный множитель μ при среднегеометрических частотах октавных полос в Гц							
	63	125	250	500	1000	2000	4000	8000

V=1000	0,65	0,62	0,64	0,75	1,0	1,5	2,4	4,2

ψ= 0,5 - коэффициент, учитывающий геометрические параметры ИШ, берется в зависимости от B/Sогр (Рисунок 3 /1/).

Находим суммарные уровни давлений Lсумм в равномерной точке от всех источников шума. Используем Lдоп, указанные в таблице 3, определяем требуемое снижение шума ΔLтр= Lсумм – Lдоп.

Таблица 4.3 – Допустимые уровни звукового давления (Таблица 2.7 /2/).

Допустимый уровень звукового давления	Среднегеометрические частоты октавных полос в Гц							
	63	125	250	500	1000	2000	4000	8000
Lдоп<	99	92	86	83	80	78	76	74

Производим расчет L для среднегеометрической частоты октавных полос 63 Гц:

$$L = 10 \times \lg(10^{0,1\times105} \times 1 \times 1 \times \left(\frac{1}{2\times3,14\times8.3^2} + \frac{1}{2\times3,14\times14^2} + \frac{1}{2\times3,14\times10^2}\right) + \frac{4\times0,5}{16,25} \times 3 \times 10^{0,1\times105})$$=101 дБ

ΔLтр= 101-99 = 2 дБ.

Результаты расчетов записываем в таблицу 4.4

Таблица 4.4 – Результаты расчета.

		Среднегеометрические частоты октавных полос, Гц							
		63	125	250	500	1000	2000	4000	8000
Lp	дБ	105	105	98	97	98	92	90	92
Lдоп	дБ	99	92	86	83	80	78	76	74
Λ		31,6·109	31,6·109	6,31·109	5,01·109	6,31·109	1,58·109	1,0·109	1,58·109
χ		1	1	1	1	1	1	1	1
Ф		1	1	1	1	1	1	1	1
r1	м	3,5	3,5	3,5	3,5	3,5	3,5	3,5	3,5
S1=2πr2	м2	433	433	433	433	433	433	433	433
r2	м	4,2	4,2	4,2	4,2	4,2	4,2	4,2	4,2
S2=2πr2	м2	1231	1231	1231	1231	1231	1231	1231	1231
r3	м	5,3	5,3	5,3	5,3	5,3	5,3	5,3	5,3
S3=2πr2	м2	628	628	628	628	628	628	628	628
ψ		0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
V	м3	1000	1000	1000	1000	1000	1000	1000	1000
μ		0,65	0,62	0,64	0,75	1	1,5	2,4	4,2
B	м2	16,25	15,5	16	18,75	25	37,5	60	105
Lсум	дБ	101	101	94	92	92	84	80	80
ΔL	дБ	2	9	8	9	12	6	4	6

Так как условия превышают нормы, требуется провести мероприятия по снижению шума.

Для начала нужно обезопасить работников, находящихся непосредственно около источников шума, выдав им наушники.

Расчет мероприятий по снижению шума

Нужно создать специальную кабину со следующими параметрами:

Кабина наблюдения - 14×10×4 м

Глухая стена, S1= 56 м2

Дверь, S3= 4 м2

Глухая стена S2= 140 м2

Окно S4= 3 м2

Воздушная изоляция шума Rтрi в дБ ограждающей конструкции в октавной полосе частот при проникновении из одного помещения в другое (формула (23) /1/): Rтрi= Lш-10·lg Ви+10·lg Si-Lдоп+10·lg n, где величина Ви - постоянная защищаемого от шума помещения в м2. Используя среднегеометрическую частоту октавных полос 63 Гц:

Vи= 14×10×4 = 560 м3, Ви1000= 800/20 = 40 м2, Ви= 40·0,65 = 26 м2.

Lш - октавный уровень звукового давления в не защищаемом от шума помещении, Lш= Lсум;

Si - площадь ограждающей конструкции (или отдельного ее элемента), через которую проникает шум в помещение;

n - общее количество ограждающих конструкций (или отдельных их элементов).

Rтр1= 101-10·lg 26+10·lg 86-99+10·lg 4 = 13 дБ;

Rтр2= 101-10·lg 26+10·lg 140-99+10·lg 4 = 16 дБ;

Rтр3= 101-10·lg 26+10·lg 4-99+10·lg 4 = 1 дБ;

Rтр4= 101-10·lg 26+10·lg 3-99+10·lg 4 = 0 дБ..

Таблица 4.5 – Результаты расчета значений воздушной изоляции.

		Среднегеометрические частоты октавных полос, Гц							
		63	125	250	500	1000	2000	4000	8000
Lдоп	дБ	99	92	86	83	80	78	76	74
Lсум	дБ	101	101	94	92	92	84	80	80
n		4	4	4	4	4	4	4	4
S1	м2	86	86	86	86	86	86	86	86
S2	м2	140	140	140	140	140	140	140	140
S3	м2	4	4	4	4	4	4	4	4
S4	м2	3	3	3	3	3	3	3	3
V	м3	800	800	800	800	800	800	800	800
μ		0,65	0,62	0,64	0,75	1	1,5	2,4	4,2
B	м2	26	24,8	25,6	30	40	60	96	168
Rтр1	дБ	13	20	19	19	21	13	9	9
Rтр2	дБ	16	23	22	22	24	16	12	12
Rтр3	дБ	1	8	7	7	9	1	-3	-3
Rтр4	дБ	0	7	6	6	8	0	-4	-4

По сделанным расчетам, при помощи таблиц 2.16 и 2.17, выберем параметры, обеспечивающие нужную нам изоляцию. С целью подавления шума, создаваемого оборудованием, проводятся следующие мероприятия:

Используем кирпичную кладку для стен и перекрытий (S1 и S2), оштукатуренную с 2-х сторон, толщиной в ½ кирпича, средняя поверхностная плотность, которого 100 кг/м2. Используется уплотненная дверь (S3) для шумоподавления. Окно можно использовать стандартное силикатное стекло. В итоге мы получаем полную изоляцию от шума в кабине наблюдения.

Заключение

В результате проделанной работы была полностью изучена беспроводная сеть Wi-Fi и все протоколы, способствующие обеспечить защиту. В итоге были проведены различные виды атак, для получения несанкционированного доступа к сети и последующего воздействия на сеть, так же были изучены способы обеспечения безопасности сети. Но в ходе изучения было изучено то, что в целом любая беспроводная сеть не может гарантировать 100% защищенность, так как существующие способы защиты уже устарели, и для их обхода не требуется больших стараний, а если брать современный новый протокол защиты, то он еще не доработан, так как тоже является уязвимым к различным атакам, по этой причине считаю не целесообразным использовать беспроводные сети. Благодаря данной работе можно понять все плюсы и минусы беспроводных сетей, а также разобрать способы их защиты используя стандартные инструменты, имеющиеся в любом роутере. Главным достоинством этой работы является практическое выполнение атаки при использовании пакета PMKID, так как данная атака была только теорией, в этой же работе есть практическое применение данной атаки, с использованием специальных параметров для уже известных инструментов, тем самым получив результат. В итоге была реализована одна из самых опасных атак на сегодняшний день, она актуальна как для старого WPA2, так и для нового недавно созданного WPA3, тем самым подвергая все беспроводные сети опасности, так как для этой атаки даже не нужны подключенные клиенты, это во многом упрощает её реализацию.

Список литературы

1 Что такое беспроводная сеть и принципы ее работы URL: http://posetke.ru/wifi/besprovodnie-seti-klassifikaciya-princip-raboti.html (дата обращения 17.03.19)

2 Защита беспроводных сетей URL: https://habr.com/ru/post/224955/ (дата обращения 04.04.19) 3 Мерритт, М. Безопасность беспроводных сетей. - М.: Радио и связь, 2008

4 Голубицкая Е. А., Жигульская Г. М. Экономика связи. – М.: Радио и связь, 2000

5 Аманжолова К. Б., Алибаева С. А. Экономика предприятии телекоммуникации: Учебное пособие. - Алматы: АИЭС, 2003

6 Нормы микроклимата URL: http://adilet.zan.kz/rus/docs /V050003789 (дата обращения 23.03.19)