# Взлом Wi-Fi сетей, Aircrack-ng, Kali Linux.

### **WPA/WPA2.**

**WPA** и **WPA2** (**Wi-Fi Protected Access**) собственно это протокол авторизации и шифрования данных в Wi-Fi сетях. На данный момент это самый популярный,  самый надежный протокол. Часто в домашних условиях и маленьких сетях используют   WPA2-PSK(Pre-Shared Key). В начале 2018 года международный альянс Wi-Fi Alliance анонсировал новейший протокол беспроводной безопасности — WPA3.

Основной и самый популярный метод атаки на этот протокол является брутфорс(метод грубой силы, перебор паролей).

### **handshake.**

Для того, чтобы устройство получило маркер доступа в сеть, на устройстве необходимо ввести специальную парольную фразу, называемую Pre-Shared Key. Длина должна быть от 8 до 32 символов, притом можно использовать специальные символы, а также символы национальных алфавитов. После ввода парольной фразы она помещается в специальный пакет ассоциации (пакет обмена ключами, handshake), который передается на точку доступа. Если парольная фраза верна, то устройству выдается маркер доступа в сеть.

Уязвимостью является возможность перехвата пакетов handshake, в которых передается Pre-Shared Key при подключении устройства к сети. По скольку Pre-Shared key шифруется, у злоумышленника остается только одна возможность – атака грубой силой на захваченные пакеты.   Также стоит обратить внимание, что для того, чтобы перехватить handshake злоумышленнику совсем не обязательно ждать того момента, как к сети будет подключено новое устройство. На некоторых беспроводных адаптерах, при использовании нестандартных драйверов, есть возможность посылки в сеть пакетов, которые будут прерывать сетевые соединения и инициировать новый обмен ключами в сети между клиентами и точкой доступа. В таком случае, для того, чтобы захватить требуемые пакеты, необходимо, чтобы к сети был подключен хотя бы один клиент.

### **Взлом.**

В наших примеров я использую **[Kali Linux](https://www.kali.org/" \t "/home/dima/Документы\\x/_blank)**(Kali Linux — GNU/Linux-LiveCD, возникший как результат слияния WHAX и Auditor Security Collection. Проект создали Мати Ахарони (Mati Aharoni) и Макс Мозер (Max Moser). Предназначен прежде всего для проведения тестов на безопасность). И пакет уже установленных программ**[Airocrack-ng](http://www.aircrack-ng.org/" \t "/home/dima/Документы\\x/_blank)** (Это полный набор инструментов для оценки безопасности сети Wi-Fi.)

Первым этапом нам надо перевести наш Wi-Fi адаптер в режим мониторинга. То есть чип адаптера переводиться в режим прослушивания эфира. Все пакеты которые отсылают друг другу в округе.

Сначала мы убьем все процессы которые используют Wi-Fi интерфейс:

****airmon-ng check kill****

Запустите беспроводной интерфейс в режиме мониторинга:

****airmon-ng start wlan0****

В результате у вас появиться новый интерфейс ****wlan0mon**** с ним дальше мы и будем работать (посмотреть доступные интерфейсы можно командой ****ifconfig**** ). Теперь мы можем посмотреть что же происходит вокруг:

****airodump-ng wlan0mon****

* ****BSSID**** — MAC адрес WI-Fi точки.
* ****PWR**** — Сила сигнала.
* ****Beacons**** — Фрейм Бикон (Beacon frame) /Точка доступа WiFi периодически отправляет Биконы для анонсирования своего присутствия и предоставления необходимой информации (SSID, частотный канал, временные маркеры для синхронизации устройств по времени, поддерживаемые скорости, возможности обеспечения QoS и т.п.) всем устройствам в зоне ее покрытия. Радиокарты пользовательских устройств периодически сканируют все каналы 802.11 и слушают биконы, как основу для выбора лучшей точки доступа для ассоциации. Пользовательские устройства обычно не посылают биконы, за исключением ситуации, когда выполняется процедура участия в IBSS (Independent Basic Service Set) или, по другому, в одноранговом соединении типа Ad-hoc.
* ****CH**** — Номер канала точки доступа.
* ****ENC-****Используемый алгоритм. OPN = нет шифрования, «WEP?» = WEP или выше (недостаточно данных для выбора между WEP и WPA/WPA2), WEP (без знака вопроса) показывает статичный или динамичный WEP, и WPA или WPA2 если представлены TKIP или CCMP или MGT.
* ****CIPHER**** — Обнаруженный шифр. Один из CCMP, WRAP, TKIP, WEP, WEP40, или WEP104. Не обязательно, но обычно TKIP используется с WPA, а CCMP обычно используется с WPA2. WEP40 показывается когда индекс ключа больше 0. Стандартные состояния: индекс может быть 0-3 для 40 бит и должен быть 0 для 104 бит.
* ****AUTH —****Используемый протокол аутентификации. Один из MGT (WPA/WPA2 используя отдельный сервер аутентификации), SKA (общий ключ для WEP), PSK (предварительно согласованный ключ для WPA/WPA2) или OPN (открытый для WEP).
* ****ESSID —****Так называемый SSID, который может быть пустым, если активировано сокрытие SSID. В этом случае airodump-ng попробует восстановить SSID из зондирующих запросов ассоциирования.
* ****STATION —****MAC адрес каждой ассоциированной клиента подключенного к точке доступа. Клиенты, в настоящий момент не ассоциированные с точкой доступа, имеют BSSID «(not associated)».

###### **Можете немного поиграться :**

###### ****airodump-ng***—manufacturer —uptime**—wps***wlan0mon****

Запускаем airodump-ng для беспроводного интерфейса ****wlan0mon****, кроме основной информации мы задаём отображать производителя *****(—manufacturer)*****, время работы *****(—uptime)***** и информацию о WPS *****(—wps)*****.

Теперь нам надо перехватить  ****handshake****какой либо точки доступа, желательно конечно к которой подключены клиенты ).

****airodump-ng -c 1 —bssid C0:4A:00:F0:F4:24  -w WPA wlan0mon****

****-c  <номер>**** номер канал.

****—bssid <MAC>**** мас адрес точки доступа

****-w <имя или путь/имя>**** файл в который будут сохранены все перехваченные пакты.

****wlan0mon**** Название беспроводного интерфейса интерфейса.

После удачного захвата рукопожатий в правом углу будет надпись WPA handshake

Кстати мы можем попытаться ускорить процесс , заставив клиента переподключиться к точки доступа :

****aireplay-ng —deauth 100 -a 00:11:22:33:44:55 -c AA:BB:CC:DD:EE:FF wlan0mon****

****—deauth <число сообщений>**** — отправка запроса  деаунтифицировать. (0 не ограниченное число пакетов)

****-a <MAC>**** — Мас адрес точки доступа.

****-с <MAC> —**** Мас адрес клиента.

****wlan0mon**** — интерфейс.

Другие виды атак :

       --fakeauth    задержка : фальшивая аутентификация с ТД (-1)

      --interactive       : интерактивный выбор фреймов (-2)

      --arpreplay         : стандартная повторная отправка запросов ARP (-3)

      --chopchop          : расшифровать/порубить WEP пакет (-4)

      --fragment          : сгенерировать валидный поток ключей   (-5)

      --caffe-latte       : запросить клиента на новые IVs  (-6)

      --cfrag             : фрагментирование в отношении клиента  (-7)

      --migmode           : атаки режим миграции WPA  (-8)

      --test              : тест возможности инжекта и качества соединения (-9).

[РЕКЛАМА](https://an.yandex.ru/count/WymejI_zO9O35Hu093HmAJO5Fqjz60K0bWGng-E7OW00000urkieG0n80c2C66W4SC3T_B-ko9-9w0600Sxd_mI80Q_ai0-G0SJsoQRQW8200fW1nFR9fbgm0QZIlAu8k07EqjZ89C010jW1nDMKfW7W0OZFomte0Q82-07219W2mCFY3w02m83Y2Ra2N8Jc4Qd1Ez_m0iICkvOBa0su1Fy1Y0MAEf05ztAm1U8Ek0MS7S05w5_81QuOq0MLIeUgSbqx9Kwf1mxi_9eJI_Sbk0U01GJG29gAW872a846u0YWWF44w0a7y0c07lW9y1202Wh92ZoUL2p1CVC_2AeB4AyLjRuEx0007cMw0NRVw0ltSl0B1eWCgCNUlW7e39y6c0sVd4dW3OA2WO60W808FygEgfNNwywIJg0Em8GzZjZpYRhYqlibk0yZW13huCCTa125tlsMc9_sbkwG9D0GzW6O4Scz8w4HPxJthRiCu16mkVi1w16Yde23fRt2s5Bf4WQu_0ZFTfG4y18AY1C1c1C8g1F3YkJfxT2cznRW4vmTW1IWW62859hhvwtiwlABf06W59mTg1JtSWUpmvwK1k0K0UWKZ0BG5RF3dfG6s1N1YlRieu-y_6Fmc1QGt_sJ1g0Ma8wOb0Qe5kW7i1Rx1iaMq1QenTw-0TWMWHUO5yM6cm-e5mcu5mZ05xQM0TWNm8Gzw1S1e1WBi1YhfP-K1hWO0T0O3_WOki6_pD68vC4yW1c7-TQxqDFPx1s96U_ge1cg0x0Pk1d0qXaIUM5YSrzpPN9sPN8lSZOsD2qqu1a1w1da1V0PWC83WHh__riewmOmw8WQm8Gza1g019WQyS2q0R0QvEU9YxZqhU1kzHe10000-1gVd4cO6_-XGx0RORWR1EaR0000OD3FXK7m6ut0vLNu6vAXmmA270rcE4CwSJ54Qdb7K5etwHm0y3-07Vz_cHq0y3-X7MvAw2ivSCm_g1q1u1t7aP47c1wJ-mse7W7G7iBoyy-oixkLr07O7hED7uWV_m6W7-BeiYEm7zG2o1_YgefJqXy6DJWpDpWrsHy0000WLJM5GU0V_TUrK-WVvzl30l0V0VWV0O0W0eWW0R0WW8200TWW_m7W804c8B44nXXZ110n2J5m0mKa1WXs2LAZqCwGtTP28G28OQbhC6ze602aLNnBA131coqlATf3Z-PyLzp9Ue_UyWtuC_8XtHuWH9K8FMlhg-_nBN4ML-QREexoVn10txq7oIttGyFcnbPt0l2v4Qxk47OE_2Ft50niEZ0xVEd3OmO0~1" \t "/home/dima/Документы\\x/_blank)

Теперь нам надо расшифровать его и узнать PSK:

****aircrack-ng -w wordlist.dic -b C0:4A:00:F0:F4:24  WPA.cap****

****-w <путь/файл словаря>**** — Указываем словарь для перебора паролей.

****-b <MAC>****  — Мас адрес точки доступа.

****WPA.cap**** — Файл с  handshake.

### **Создание своих словарей.**

При атаках типа брутфорс словари играют очень важную роль. Я думаю вы с легкость найдете в интернете куча всяких не понятных словарей. Но еще можно и нужно  делать самому.

Для этого в дистрибутиве Kali Linux есть интересная утилита, называется ****Crunch****. Синтаксис ее довольно прост:

* ****min =**** минимальная длина пароля;
* ****max =**** максимальная длина;
* ****characterset**** = символы, которые будут использоваться для генерации паролей;
* ****-t <pattern> =**** возможность создавать паттерны. Давай на примере. Скажем, ты знаешь, что у человека день рождения 28 июля и эти цифры есть в пароле вида 0728, но перед этим числом есть еще какие-то символы. Поэтому ты пишешь что-то вроде @@@@@@@0728, и получается, что лист будет сгенерирован на 11 -значный пароль. Семь символов, которые будут генериться, а четыре будут фиксированными. По мне, так весьма крутая и удобная фишка;
* ****-о <outputfile> =**** выходной файл для нашего листа.
* ****-p =**** перестановка.
* ****-d**** — ограничение числа последовательно одинаковых символов.

**crunch 4 8**

Как сам понимаешь, кранч будет генерить пароли от 4 до 8 символов. Как видишь, ничего сложного, теперь давай что-нибудь поинтереснее:

**crunch 6 8 1234567890 -о /гооt/wordlist.txt**

Здесь будет сгенерирован словарь от 6 до 8 символов, в пароле только цифры и зальются они во внешний файл, что мы указали. Остается только воспользоваться получившимся словарем.

****crunch 1 1 -p Alex Company Position****

Словарь состоит из всех возможных комбинаций слов Alex, Company и Position.

Для тега ****-t**** есть шаблоны :

* ^ — спецсимволы.
* @ — буквы в нижнем регистре.
* , — буквы в верхнем регистре.
* % — цифры.