Wpa Psp Ключ

Это как черный ход для любого роутера Оказалось, что если в точке доступа активирован WPS (который, на минуточку, включен в большинстве роутеров по умолчанию), то подобрать PIN для подключения и извлечь ключ для подключения можно за считанные часы! Как работает WPS? Задумка создателей WPS хороша.. Надо указывать имя реального интерфейса, например, wlan0.. Запускаем брутфорс Теперь можно приступать непосредственно к перебору PIN'a.. Будем надеяться, к моменту публикации статьи эту ошибку исправят.. В этом случае Reaver приостанавливает свою деятельность, причем время паузы может быть задано с помощью опции '—fail-wait': # reaver -i mon0 -b 00:01:02:03:04:05 --fail-wait=360 Рисунок 6.. HOW-TO Как и для любой другой атаки на беспроводную сеть, нам понадобится Linux.. Пример работы брутфорса Reaver Можно ли защититься? Защититься от атаки можно пока одним способом — отключить нафиг WPS в настройках роутера.

Чтобы лучше понять, как это будет работать, посмотри на схему.. Есть один неприятный баг в Reaver версии 1 3, из-за которого не определяются снятия подобных блокировок.. Поэтому чем сложней пароль, тем меньше шансов у злоумышленников.. Это, в общем, самый универсальный способ установки (для любого дистрибутива).. Лучший способ — свериться со списком поддерживаемого оборудования на сайте проекта.. Зачем шифровать? Кому я нужен? Мне нечего скрывать Не так страшно если украдут пин-код с кредитной карты и снимут с нее все деньги.. Самое большее, что они могут сейчас сделать, – это максимально противодействовать брутфорсу.. Также можно использовать опцию '-f' и скормить утилите cap-файл, созданный, например, тем же airodump-ng.

Дело в том, что последняя цифра PIN-кода представляет собой некую контрольную сумму, которая высчитывается на основании семи первых цифр.. Утилита использовала библиотеку Scapy, позволяющую инъектировать произвольные сетевые пакеты.. Тем более, если кто-то будет сидеть за ваш счет в интернете, зная Wi-Fi пароль.. Кажется, что скоро их можно будет занести в Красную книгу.. Практика показывает, что для успешного результата обычно достаточно перебрать лишь половину всех вариантов, и в среднем брутфорс занимает всего от четырех до десяти часов.. Куда обидней когда злоумышленники проникнут в ваш компьютер и удалят фотографии как Вы забирали сына из роддома, как он сделал первые шаги и пошел в первый класс.

Он делится на две равные части, и каждая часть проверяется отдельно!Посмотрим на схему: • Если после отсылки сообщения M4 атакующий получил в ответ EAP-NACK, то он может быть уверен, что первая часть PIN-кода неправильная.. Далее запускаем эмулятор терминала, где загружаем последнюю версию утилиты через репозиторий: # apt-get update # apt-get install reaver Тут надо сказать, что в репозитории находится версия 1.. Например, если блокировать WPS на один час после пяти неудачных попыток ввода PIN-кода, то перебор займет уже около 90 дней.. Поскольку уязвимость существует не на уровне реализации, а на уровне протокола, ждать от производителей скорого патча, который решил бы все проблемы, не стоит.. /wash -i mon0 В качестве параметра задается имя интерфейса, переведенного в режим мониторинга.. 1 октября 2013 76754 Сегодня у многих есть дома Wi-Fi маршрутизатор.. Для старта Reaver в самом простом случае нужно немного.. Нас интересуют точки с шифрованием WPA/WPA2 и аутентификацией по ключу PSK.

По непонятной причине в пакет Reaver в BackTrack не включили утилиту wash.. Правда, как оказалось, сделать это возможно далеко не всегда.. 3, которая лично у меня заработала неправильно.. USB'шные донглы легко найти в интернете за 20$.. Это можно сделать при помощи утилиты wash: запусти её и проверь, что твоя цель находится в списке.. Более того гостевая зона в маршрутизаторах изолирована от основной сети.. Кроме того, точка доступа может на время заблокировать использование WPS.. И он (маршрутизатор) по сути — врата в информационную вселенную.. Безопасность Wi-Fi от такого упрощения не страдает.. Поискав информацию о проблеме, я нашел пост автора, который

рекомендует обновиться до максимально возможной версии, скомпилировав исходники, взятые из SVN.. Также важно помнить, что если твой беспроводной адаптер видит точку доступа, то это ещё не значит, что и точка доступа видит тебя.. Оказывается, проверка PIN-кода осуществляется в два этапа.. Основными инструментами здесь служат снифер airodump-ng для сбора пакетов и утилита aircrack-ng, используемая непосредственно для взлома ключа.. Она также может быть настроена: # reaver -i mon0 -b 00:01:02:03:04:05 -d 0 • Некоторые точки доступа могут блокировать WPS на определенное время, заподозрив, что их пытаются поиметь.. Если же встанет вопрос о том, какой беспроводной модуль купить, то начать можно с любого адаптера на чипсете RTL8187L.. В СССР на железнодорожных вокзалах получили широкое распространение автоматические камеры хранения.. Reaver Pro — железка от создателей Reaver FAQ Вопрос: Какой беспроводной адаптер нужен для взлома? Ответ: Перед тем как экспериментировать, нужно убедиться, что беспроводной адаптер может работать в режиме мониторинга.. Пользователь нажимает специальную кнопку на роутере (хардварную) и на компьютере (софтварную), тем самым активируя процесс настройки.. Цена упрощений Открытых точек доступа, к которым вообще не надо вводить ключ для подключения, становится все меньше и меньше.. При соединении с роутером можно открыть специальную сессию WPS, в рамках которой настроить роутер или получить уже имеющиеся настройки, если правильно ввести PIN-код.. Сценарий можно запустить только под Linux-системой, предварительно переведя беспроводной интерфейс в режим мониторинга.. Лучше выбирать одну из первых в списке, так как для проведения атаки желательна хорошая связь с точкой.. В качестве воркэраунда предлагают использовать опцию '—ignore-locks' или скачать последнюю версию из SVN.. В качестве кодовой комбинации замка использовались одна буква и три цифры.. В итоге получаем уже 10^7 (10 000 000) вариантов Но и это еще не все! Далее внимательно смотрим на устройство протокола аутентификации WPS (рисунок 3).. Установка Reaver Чтобы загрузить Reaver, нам понадобится интернет.. Reaver v1 4 WiFi Protected Setup Attack Tool Copyright (c) 2011, Tactical Network Solutions, Craig Heffner [+] Waiting for beacon from 00:21:29:74:67:50 [+] Associated with 00:21:29:74:67:50 (ESSID: linksys) [+] Trying pin 63979978 Если программа последовательно отправляет PIN'ы точке доступа, значит, все завелось хорошо, и остается тупо ждать.. С одной стороны все упрощается, нет необходимости создавать и сопровождать базу пользователей, с другой стороны все заходят под одним паролем.. Но другой вопрос, насколько быстро можно накатить такой патч на миллионы устройств, которые работают по всему миру? Прокачиваем Reaver В HOWTO мы показали самый простой и наиболее универсальный способ использования утилиты Reaver.. Reaver эту ситуацию замечает и делает паузу в переборе на 315 секунд по умолчанию, длительность этой паузы можно менять: # reaver -i mon0 -b 00:01:02:03:04:05 --lock-delay=250 • Некоторые реализации протокола WPS разрывают соединение при неправильном PIN-коде, хотя по спецификации должны возвращать особое сообщение.. Оказавшись в консоли, можно смело стартовать «иксы» (есть отдельные сборки BackTrack — как с GNOME, так и с KDE): # startx Шаг 2.. Вход в систему Логин и пароль для входа по умолчанию – root:toor.. Взломать ее можно буквально за несколько минут, используя слабости применяемого в ней шифра RC4.. В домашних условиях целесообразней использовать WPA2-PSK, то есть упрощенный режим стандарта WPA.. А это значит, что в качестве пароля нельзя использовать даты рождения, ваши имена, номера машин, телефонов и т.. Механизм автоматически задает имя сети и шифрование.. Поэтому только современные методы шифрования и сложный пароль.. Однако количество вариантов можно существенно сократить.. Затраченное на это время можно уменьшить, выбрав на стороне клиента простой секретный ключ, который в дальнейшем упростит расчеты других ключей.. Читай входная дверь И от этой двери зависит зайдет ли к вам незваный гость без вашего разрешения.. Брутфорс может затянуться на дни, месяцы и годы.. С учетом современных вычислительных мощностей вскрытие ключей такого размера занимает буквально несколько минут.. Вопрос: Можно ли одновременно запустить два и более экземпляров Reaver для ускорения атаки? Ответ: Теоретически можно, но если они будут долбить одну и ту же точку доступа, то скорость перебора едва ли увеличится, так как в данном случае она ограничивается слабым железом точки доступа, которое уже при одном атакующем загружается по полной.. В частности если у Вас на компьютере установлена Windows XP без 3-го сервис пака, то WPA2 работать не будет.. • Ввод PIN-кода на компьютере пользователя (рисунок 2).. В декабре сразу два исследователя рассказали о серьезных фундаментальных прорехах в протоколе WPS.. • Можно задать номер канала и SSID точки доступа: # reaver -i mon0 -b 00:01:02:03:04:05 -c 11 -e linksys • Благотворно сказывается на скорости брутфорса опция '—dh-small', которая задает небольшое значение секретного ключа, тем самым облегчая расчеты на стороне точки доступа: # reaver -i mon0 -b 00:01:02:03:04:05 -vv --dh-small • Таймаут ожидания ответа по умолчанию равен пяти секундам.. Непременным условием аутентификации является предъявление пользователем свидетельства (иначе называют мандатом), подтверждающего его право на доступ в сеть.. • Если же он получил EAP-NACK после отсылки M6, то, соответственно, вторая часть PIN-кода неверна.. Поэтому использовать мы будем именно его Готовим систему На официальном сайте BackTrack 5 R1 доступен для загрузки в виде виртуальной машины под VMware и загрузочного образа ISO.. Именно так и нужно стараться настраивать Wi-Fi.. Экспресс-курс по взлому Wi-Fi • WEP (Wired Equivalent Privacy) Самая первая технология для защиты беспроводной сети оказалась крайне слабой.. Упрощённый режим Pre-Shared Key (WPA-PSK, WPA2-PSK) позволяет использовать один пароль, который хранится непосредственно в маршрутизаторе.. Если точек много и список не умещается на экране, то можно

воспользоваться другой известной утилитой — kismet, там интерфейс более приспособлен в этом плане.. Тут надо сказать, что Reaver присутствует в репозитории всеми известного дистрибутива, в котором к тому же уже включены необходимые драйвера для беспроводных устройств.. Ведь по безпроводке куда проще подключить к интернету и ноутбук, и планшет, и смартфон, коих развелось в каждой семье больше чем людей.. Если раньше человек мог даже и не знать, что беспроводную сеть можно закрыть ключом, обезопасив себя от посторонних подключений, то теперь ему все чаще подсказывают о такой возможности.. • Важный момент — возможная скорость перебора.. Основное время при этом затрачивается на расчет открытого ключа по алгоритму Диффи-Хеллмана, он должен быть сгенерирован перед шагом M3.. Вопрос: Почему у меня возникают ошибки «timeout» и «out of order»? Ответ: Обычно это происходит из-за низкого уровня сигнала и плохой связи с точкой доступа.. В итоге имеем всего лишь 11 000 вариантов для полного перебора.. Ниже я приведу дополнительные опции, которые могут повысить скорость и эффективность перебора ключа.. Для этого в комплекте с Reaver (но только если брать его из SVN) идет утилита wash: #.. Поэтому подключаем патчкорд или настраиваем беспроводной адаптер (меню «Applications > Internet > Wicd Network Manager»).. • WPA/WPA2 (Wireless Protected Access) Перебор — это единственный способ подобрать ключ для закрытой WPA/WPA2 сети (да и то исключительно при наличии дампа так называемого WPA Handshake, который передается в эфир при подключении клиента к точке доступа).. Подготовка к брутфорсу Для использования Reaver необходимо проделать следующие вещи: • перевести беспроводной адаптер в режим мониторинга; • узнать имя беспроводного интерфейса; • узнать MAC-адрес точки доступа (BSSID); • убедиться, что на точке активирован WPS.. Также существует специальная тулза wesside-ng, которая вообще взламывает все близлежащие точки с WEP в автоматическом режиме.. Сетей в домашних условиях или небольших офисах обычно используется вариант протокола безопасности WPA на основе общих ключей – WPA-PSK (Pre Shared Key).. Для увеличения эффективности перебора сначала использовались специализированные словари, потом были сгенерированы радужные таблицы, позже появились утилиты, задействовавшие технологии NVIDIA CUDA и ATI Stream для аппаратного ускорения процесса за счет GPU.. Также эволюционировали и методы шифрования RC4, TKIP, AES.. Вопрос: Почему я постоянно получаю ошибки «rate limiting detected»?Ответ: Это происходит потому, что точка доступа заблокировала WPS. e10c415e6f