Оглавление

Моей маме и бабушке
К. Д. М.

Аринн, Виктории и Дэвиду, Шелдону, Винсенту
и Елене Роуз и в особенности Шарлотте
У. Л. С.

Предисловие

Впервые я встретил Кевина Митника в 2001 году, во время съемок документального фильма «История хакинга» для канала Discovery. На этом наше общение не закончилось. Через два года я прилетел в Питтсбург и предложил ему прочитать лекцию в Университете Карнеги — Меллона. Его выступление я прослушал на одном дыхании и был ошеломлен биографией хакера, которой он поделился. Гений взламывал корпоративные компьютеры, но не портил файлы, не использовал и не продавал те номера кредитных карточек, к которым имел доступ. Он брал программы, но никогда не торговал ими, так как делал это для удовольствия и самоутверждения.

В лекции Кевин подробно рассказал невероятную историю о том, как взломал дело, которое завело на него ФБР. Митник досконально изучил все материалы и обнаружил, что его новый приятель-хакер — шпион. Кевин узнал имена, домашние адреса всех агентов ФБР, которые занимались его делом, даже прослушал телефонные звонки и голосовую почту сыщиков, пытавшихся собрать против него улики. Специально устроенная система сигнализации предупреждала Кевина о том, когда именно ФБР готовило на него облаву.

Как-то продюсеры телешоу *Screen Savers* пригласили меня и Кевина выступить в одной программе. Они попросили продемонстрировать новое электронное устройство, которое тогда только появилось на потребительском рынке, — GPS. Мы договорились, что я стану ездить неподалеку на автомобиле, а они будут отслеживать мою машину по навигатору. В эфире маршрут показался на первый взгляд случайным, хотя на самом деле линии пути складывались в два слова:

СВОБОДУ КЕВИНУ.

С Кевином нам довелось выступать и в 2006 году, в то время Митник был постоянным гостем ток-шоу Арта Белла *Coast to Coast AM*. Он предложил мне стать его собеседником в эфире. К тому времени я в подробностях знал его историю. В тот вечер я давал ему интервью, рассказывал о себе, мы много смеялись — нам всегда было весело вдвоем.

Кевин изменил мою жизнь. Однажды я осознал, что он не раз звонил мне, когда был за тридевять земель: Митник ездил в Россию, где читал лекцию, в Испанию, где консультировал одну компанию по вопросам безопасности, в Чили, где помогал банку справиться с недавним компьютерным взломом. Все это звучало потрясающе. Я почти десять лет не пользовался загранпаспортом, пока эти звонки не пробудили во мне жажду странствий. Кевин познакомил меня со своим агентом, который организовывал его лекции. Эта дама как-то сказала: «Если хотите, я могу и вам помочь устроить цикл лекций». Так, благодаря Кевину, я принялся путешествовать по миру.

Кевин стал одним из моих лучших друзей. Мне нравится проводить с ним время, слушать истории об эксплойтах и приключениях. Его молодость была не менее захватывающей и авантюрной, чем у корсара из приключенческого фильма.

Теперь и вы сможете узнать все те истории, которые я слышал одну за другой на протяжении многих лет. В известном смысле я немного завидую, ведь перед вами только открывается необычное путешествие. Вам предстоит узнать удивительную, даже невероятную биографию и хронику эксплойтов Кевина Митника.

Стив Возняк,
соучредитель Apple Inc.

Пролог

Физический доступ — это проникновение в здание интересующей вас компании. Мне это никогда не нравилось. Слишком рискованно. Пишу об этом — и меня уже пробивает холодный пот.

Как-то мне довелось испытать, что такое физический доступ. Невероятное чувство охватывает, когда в теплый весенний вечер прячешься на темной парковке компании, которая ворочает миллиардами долларов, и выбираешь тот самый нужный момент. За неделю до этого я посетил здание средь бела дня. Пришел под предлогом того, что нужно оставить письмо для одного сотрудника. На самом деле, войдя в здание, я смог разузнать, как в этой компании выглядит пропуск. Итак, фотография сотрудника крупным планом размещается в левом верхнем углу. Прямо под ней — имя и фамилия, сначала идет последняя, большими печатными буквами. В нижней части карточки — название компании, крупным красным шрифтом.

Я сходил в интернет-клуб и посмотрел сайт компании. На нем можно было скачать и скопировать изображение логотипа этой фирмы. Проработав около 20 минут в Photoshop с логотипом и отсканированной фотографией на документы, я сделал вполне убедительное факсимиле идентификационной карточки. Результат творения я аккуратно вставил в копеечный бейджик. Еще один фальшивый пропуск смастерил для друга, который согласился подсобить, если понадобится его помощь.

Оказалось, что без этой маскировки можно было обойтись. В 99% случаев на пропуск практически не смотрят. Если основные элементы карточки расположены правильно и выглядят примерно так, как и должны выглядеть, то вы спокойно попадете внутрь. Однако какой-нибудь чересчур ретивый охранник

или сотрудник, решивший поиграть в цербера, может попросить вас поднести карточку ближе. И если вы живете, как я, то такую опасность никогда нельзя списывать со счетов.

На парковке меня не видно. Я смотрю на огоньки сигарет той череды людей, которые выходят на улицу покурить. Наконец, замечаю группу из пяти-шести человек, возвращающихся в здание. Дверь черного хода — одна из тех, что открываются только тогда, когда кто-то из сотрудников подносит карточку к считывающему устройству. Я пользуюсь моментом и последним пристраиваюсь к этой группе. Парень передо мной переступает порог, замечает, что за ним кто-то идет, мельком меня оглядывает, видит бейдж, как и у всех сотрудников, и придерживает дверь, чтобы я вошел. Я благодарно киваю.

Такой прием называется «паровозик».

Внутри я сразу замечаю плакат, расположенный так, что его обязательно увидит каждый посетитель. Этот плакат, вывешенный ради дополнительной безопасности, предупреждает, что нельзя придерживать дверь перед кем-то, кто идет после вас: нужно, чтобы все заходили в здание по одному, поднося идентификационную карточку к считывающему устройству. Однако обычная вежливость, та самая минимальная любезность, которую каждый день оказываешь коллеге-товарищу, заставляет сотрудников с завидным постоянством игнорировать предупреждающий плакат.

Итак, я внутри. Я иду вперед по длинным коридорам широким шагом человека, который бежит решать важную задачу. На самом деле это исследовательское путешествие, и я ищу офис отдела информационных технологий (IT). Нахожу его минут через десять в другой части здания. Я хорошо подготовился к визиту и знаю имя одного системного администратора этой компании. Полагаю, у него самые широкие права доступа в корпоративную сеть.

Черт возьми! Когда я нахожу его рабочее место, оказывается, что это не обычная отгороженная кабинка типа «заходи кто хочет», а отдельный офис, где дверь закрыта на ключ. Однако такая проблема мгновенно решается. Подвесной потолок

выстлан белыми звуконепроницаемыми квадратами. Выше него часто оставляют технический этаж для труб, электропроводки, вентиляции и т.п.

Я звоню товарищу, говорю, что нужна его помощь, и возвращаюсь к черному ходу, чтобы впустить соучастника. Он, худой и высокий, сможет сделать то, чего не смог я. Возвращаемся в отдел информационных технологий, и мой подельник залезает на стол. Я хватаю его за ноги и поднимаю достаточно высоко. Ему удается приподнять звуконепроницаемую пластину. Я напрягаюсь, поднимаю его еще выше — он хватается за трубу и подтягивается. Не проходит и минуты, как я слышу, что он уже в офисе. Ручка двери поворачивается — и товарищ запускает меня в кабинет. Он весь в пыли, но улыбка его растянулась до самых ушей.

Я захожу и тихо закрываю дверь. Теперь мы в большей безопасности, и возможность, что нас заметят, очень мала. В офисе темно. Включать свет опасно, но он и не нужен: мне хватает монитора, чтобы увидеть все необходимое. Кроме того, риск гораздо меньше. Я быстро рассматриваю стол, проверяю, что лежит в верхнем ящике и под клавиатурой — вдруг администратор оставил шпаргалку, на которой записал пароль к компьютеру. Не нашел. Жаль, но это совсем не проблема.

Достаю из сумки загрузочный компакт-диск с операционной системой Linux, где также записан инструментарий хакера, и вставляю в дисковод. Один из инструментов позволяет изменить локальный пароль администратора. Я меняю его на тот, который мне известен и с помощью которого я смогу войти в систему. Затем убираю диск и перезагружаю компьютер. На этот раз уже вхожу в систему с правами администратора через локальную учетную запись.

Я работаю как можно быстрее. Устанавливаю троян удаленного доступа — особый вирус, который дает мне полный доступ к системе, — и теперь могу вести учет всех нажатий клавиш, собирать зашифрованные значения (хеши) паролей и даже приказывать веб-камере фотографировать человека, который работает за компьютером. Тот троян, что я установил

на машине, через каждые несколько минут будет подключаться через Интернет к другой системе. Я полностью контролирую это соединение и теперь могу делать в пораженной системе все, что захочу. Делаю последнюю операцию: захожу в реестр компьютера и указываю в качестве последнего пользователя, вошедшего в систему (last logged in user), логин ничего не подозревающего инженера. Так я стираю все следы того, что проникал в систему через локальную учетную запись администратора. Утром инженер придет на работу и заметит, что он зачем-то вышел из системы. Ничего страшного: как только он снова в нее войдет, все будет выглядеть именно так, как нужно.

Пора идти обратно. Мой товарищ уже заменил звуконепроницаемую плитку.

Уходя, я закрываю дверь на замок.

На следующий день в 08:30 системный администратор включает компьютер и устанавливает соединение с моим ноутбуком. Поскольку троян работает под его учетной записью, у меня есть все права администратора в этом домене. Всего за несколько секунд я нахожу контроллер, который содержит пароли от всех учетных записей сотрудников этой компании. Хакерский инструмент fgdump позволяет мне собрать в отдельном файле хешированные, то есть зашифрованные пароли каждого пользователя.

За несколько часов я прогоняю список хешей через «радужные таблицы» — огромную базу данных, содержащую заранее вычисленные хеши, — и восстанавливаю пароли большинства сотрудников этой компании. В конце концов я нахожу внутренний сервер, который обрабатывает пользовательские транзакции, но понимаю, что номера кредитных карточек зашифрованы. Однако это совсем не проблема. Оказывается, ключ, используемый для шифрования номеров, спрятан в хранимой процедуре внутри базы данных на компьютере SQL-сервер. Доступ на этот компьютер открыт для любого администратора базы данных.

Несколько миллионов номеров кредитных карточек. Я могу покупать все, что захочу, каждый раз пользоваться другой карточкой, а главное — они никогда не закончатся.

Поверьте, я не собираюсь ничего покупать. Эта правдивая история не очередная попытка хакинга, из-за которого я нажил себе уйму неприятностей. Меня *наняли* для того, чтобы я совершил это проникновение.

Мы сокращенно называем такую операцию пен-тестом. «Пен» означает пенетрацию, то есть проникновение. Это значительная часть той жизни, которой я теперь живу. Я проскальзывал в здания крупнейших мировых компаний, взламывал самые неприступные компьютерные системы, которые когда-либо разрабатывались. Все это происходило по поручению самих этих компаний. Такие тесты помогали им совершенствовать меры безопасности, чтобы компания не стала жертвой настоящего хакера. Я самоучка и потратил немало лет на изучение методов, тактики и стратегии, позволяющих преодолевать защиту компьютерных систем. Попутно я все лучше узнавал, как работают компьютерные и телекоммуникационные системы.

Страсть к технике и увлеченность ею толкнули меня на скользкую дорожку. Хакерские атаки стоили мне более пяти лет за решеткой, а моим близким и любимым людям — невероятной душевной боли.

В этой книге — моя история, настолько подробная и точная, насколько я могу ее припомнить. Здесь мои личные записи, протоколы судебных заседаний, документы, полученные по Закону о свободном доступе к информации, перехват телефонных разговоров из ФБР и записи, сделанные на скрытые диктофоны, многочасовые показания и беседы с двумя правительственными информаторами.

Это история о том, как я стал самым разыскиваемым и востребованным хакером в мире.

Имена Бетти, Дэвид Биллингсли, Джерри Коверт, Кумамото, Скотт Лайонз, Мими, Джон Нортон, Сара и Эд Уолш вымышлены. Под ними выступают реальные люди, с которыми мне доводилось сталкиваться. Я воспользовался этими псевдонимами, потому что хоть и умею хорошо запоминать числа и ситуации, но настоящие имена иногда забываю.

Часть I
Рождение хакера

Глава 1
Жесткий старт

Yjcv ku vjg pcog qh vjg uauvgo wugf da jco qrgtcvqtu vq octg htgg rjqpg ecnnu?[1]

Мой инстинкт, который помогал обходить преграды и пробираться незамеченным мимо охранников, проявился очень рано. Когда мне было полтора года, я сумел выбраться из кроватки, доползти до дверцы и сообразить, как она открывается. Для моей мамы это был первый звоночек, предвещавший будущие невероятные события.

Я рос единственным ребенком в семье. После того как от нас ушел отец (мне было три года), мама Шелли и я жили в симпатичных недорогих квартирках в спокойных районах долины Сан-Фернандо, а прямо за близлежащим холмом начинался Лос-Анджелес. Мама зарабатывала на хлеб, работая официанткой то в одной, то в другой забегаловке, которые были разбросаны вдоль бульвара Вентура, что протянулся с востока на запад по всей долине. Отец жил в другом штате. Хотя он не забывал обо мне, от случая к случаю появляясь в моей жизни на протяжении всего детства. Когда он перебрался в Лос-Анджелес, мне было уже тринадцать.

---

[1] Так называется система, используемая операторами любительского радио для бесплатных звонков по телефону. Здесь и далее — расшифровки эпиграфов по сайту http://fabiensanglard.net/Ghost_in_the_Wires/index.php) — *Здесь и далее примечания переводчика.*

Мы с мамой переезжали слишком часто, поэтому мне было сложно заводить друзей. Мое детство в основном прошло за уединенными и спокойными занятиями. Когда я пошел в школу, учителя часто говорили маме, что у меня удивительные способности к математике и правописанию, и я на несколько лет опережаю свой возраст. Однако я был неугомонным мальчишкой, и мне было сложно сидеть на месте.

Пока я рос, мама трижды выходила замуж и сменила еще несколько мужчин. Один из них меня обижал, другой, работавший в какой-то правоохранительной организации, пытался совратить. Мама, в отличие от других матерей, о которых мне доводилось читать, никогда не закрывала на это глаза. Как только она узнавала, что меня обижают или даже грубо разговаривают, любовники собирали манатки и исчезали. Я не требую ни от кого извинений, а просто пытаюсь понять, оказали ли эти жестокие мужчины какое-то влияние на мою взрослую жизнь, через которую красной нитью прошло неповиновение авторитетам.

Моей любимой порой года было лето, особенно если мама не работала в обед и у нее находилось свободное время в середине дня. Мне очень нравилось ходить с ней на чудесный пляж Санта-Моника. Мама любила лежать на песке, загорать, расслабляться и смотреть, как я плескался в прибое: волна сшибала меня, а я выныривал с хохотом из воды. Плавать я научился в лагере YMCA (Христианской ассоциации молодых людей), где несколько лет отдыхал летом. На самом деле меня раздражало там абсолютно все, кроме прогулок на пляж.

В детстве у меня не было проблем с физкультурой, я с удовольствием играл в Малой лиге[1]. Увлекался этим спортом достаточно серьезно и с удовольствием проводил свободное время на тренировках. Однако страсть, которая определила ход моей жизни, началась лет в десять. У наших соседей была дочка примерно моего возраста. Она мне очень нравилась и отвечала взаимностью. Признаюсь, она даже танцевала

[1] Бейсбольная лига для мальчиков и девочек 8–12 лет.

передо мной голышом. Однако в те годы меня интересовала не ее прелесть, а то, что мог мне дать ее отец, — волшебство.

Несколько недель я ходил в вечернюю школу. Там вдумчиво изучал схемы и нормы любительского радио, чтобы сдать письменный экзамен.

Этот дядя был чародеем. Его фокусы с картами или монетами и другие по-настоящему серьезные штуки страшно занимали меня. В этих представлениях я открыл главный секрет: зрители — то один, то трое, то вся компания — получали удовольствие от того, что их обманывают. Тогда эта мысль не была осознанной. Однако позже я понял, насколько людям нравится покупаться на фокусы. Это ошеломляющее открытие изменило всю мою жизнь.

Лавка волшебника, расположенная от нас на расстоянии всего лишь краткой велосипедной прогулки, стала моим прибежищем, где я проводил все свободное время. Именно магия научила меня обманывать людей.

Иногда я ездил туда не на велосипеде, а на автобусе. Както раз, примерно через два года после того, как начались эти поездки, Боб Аркоу, водитель автобуса, заметил, что я надел футболку с надписью CBers Do It on the Air. Он рассказал мне, что недавно нашел полицейскую рацию фирмы Motorola.

Я предположил, что через нее Боб теперь может прослушивать переговоры на закрытых полицейских частотах, а это, конечно же, было очень круто. Оказалось, водитель просто пошутил. Однако он был заядлым радиолюбителем и своим энтузиазмом заразил меня. Боб научил, как, используя радиочастоты, бесплатно звонить по телефону с помощью службы, которая называлась «автопатч». Поддерживали ее такие же любители, как он сам. Бесплатные телефонные звонки! Невозможно передать, как это меня впечатлило. Я просто подсел на радиосвязь.

Несколько недель я ходил в вечернюю школу. Там вдумчиво изучал схемы и нормы любительского радио, чтобы сдать письменный экзамен. Кроме того, я освоил азбуку Морзе

и получил первую в жизни квалификацию. Вскоре почтальон принес конверт из Федеральной комиссии по связи. Там лежала моя лицензия на любительские занятия радиосвязью. Немногие дети в 12 лет могли похвастаться таким документом. Меня охватило чувство огромного удовлетворения.

Обманывать людей, показывая фокусы, было очень интересно. Однако разбираться в том, как работают телефонные системы, оказалось гораздо круче. В начальной и средней школе, где-то до седьмого класса, я учился очень хорошо. Примерно в восьмом или девятом классе начал прогуливать уроки и зависать в Henry Radio — любительском радиомагазине на западе Лос-Анджелеса. Я часами читал книги по теории радиосвязи. Для меня наведаться в этот магазин было намного интереснее, чем съездить в Диснейленд. Кроме того, мне казалось, что любительское радио приносит пользу людям. Какое-то время я подрабатывал по выходным и осуществлял техническую поддержку радиосвязи в местном отделении Красного Креста. Однажды летом я целую неделю занимался подобной работой на олимпиаде для спортсменов с особенностями развития.

Поездка на автобусе была для меня чем-то вроде выходного дня. Я рассматривал городские достопримечательности, хотя они все давно были мне знакомы. Это было в Южной Калифорнии. Погода там практически всегда великолепная, если, конечно, не висит смог. В те годы ситуация со смогом была гораздо хуже, чем сейчас. Билет на автобус стоил 25 центов, еще 10 центов приходилось платить за пересадку. На летних каникулах, пока мама работала, я иногда катался на автобусе целыми днями. Мне тогда было 12, но я уже любил серьезно мыслить. В один прекрасный день я осознал, что *если бы мог сам компостировать пересадочные талоны, то поездки на автобусе стали бы бесплатными*[1].

[1] Эта мысль будет понятнее, если представлять себе принцип использования пересадочных билетов, которые применялись в то время. Вот что рассказывает об этих билетах сам Митник в первой главе книги «Искусство обмана»: «Под термином „билет с пересадкой“ подразумевается возможность для человека

Мой отец и дяди были бизнесменами и занимались торговлей. Все они умели убеждать. Думаю, я унаследовал это качество от них. С самого раннего детства мне удавалось уговаривать людей делать что-либо за меня. Вот и в тот день, когда мне пришла в голову эта гениальная идея, я прошел в начало автобуса и сел поближе к водителю. Когда он остановился на светофоре, я сказал: «Знаете, мне тут в школе дали творческое задание. Мне нужен дырокол, чтобы пробивать им на картоне разные узоры. Вот бы мне такой дырокол, как тот, которым вы компостируете пересадочные билеты. Не подскажете, его можно где-нибудь купить?»

Мой отец и дяди были бизнесменами и занимались торговлей. Все они умели убеждать. Думаю, я унаследовал это качество от них.

Я и не думал, что водитель поверит в такую чушь — слишком уж неправдоподобно звучала моя история. Думаю, у него даже не возникло мысли о том, что такой пацан, как я, может им манипулировать. Он сказал мне название магазина, я позвонил туда и узнал, что они действительно продают дыроколы по 15 долларов за штуку. Когда вам было 12, вы могли придумать для матери убедительную причину, почему вам вдруг понадобились 15 долларов? У меня все прошло как по маслу. Уже на следующий день я купил

сменить автобусные маршруты и продолжить поездку к месту назначения, но я придумал, как использовать „билеты с пересадкой“ для бесплатных путешествий туда, куда мне хотелось. Добыть их можно было, прогуливаясь по парку: мусорные корзины на автобусных станциях были всегда заполнены только частично использованными билетами, которые выбрасывали сами водители перед сменой маршрутов. С пачкой пустых листов и дыроколом я мог отмечать только мои поездки и путешествовать везде, где ходили автобусы Луизианы. По прошествии времени я имел все расписания маршрутов для всей системы, к тому же заученные наизусть. Это ранний пример моей удивительной памяти на определенные типы информации, и даже сейчас я могу вспомнить телефонные номера, пароли и другие заметки, начиная с раннего детства».