Роджер Граймс
Как противостоять хакерским атакам? Уроки экспертов по информационной безопасности

Я посвящаю эту книгу своей супруге Трише.

Во всех смыслах это женщина, стоящая за мужчиной

Roger A. Grimes

Hacking the Hacker: Learn From the Experts Who Take Down Hackers

БОМБОРА
ИЗДАТЕЛЬСТВО
Москва 2023

Об авторе

Роджер Граймс борется со злонамеренными компьютерными хакерами уже свыше трех десятилетий (с 1987 года). Он получил десятки сертификатов информационной безопасности (включая CISSP, CISA, MCSE, CEH и Security+), а также успешно сдал очень трудный экзамен дипломированных бухгалтеров (CPA), хотя это не имеет ничего общего с ИБ. Роджер создал и обновил курсы информационной безопасности, был инструктором и научил тысячи студентов, как взламывать и защищать. Он часто выступает на национальных конференциях по информационной безопасности. Граймсу платят как профессиональному пентестеру, чтобы он взламывал сети и веб-сайты компаний, и практически всегда он укладывается в пару-тройку часов. Ранее он написал (в том числе в соавторстве) восемь книг по информационной безопасности и около тысячи статей. С августа 2005 года Роджер пишет статьи про ИБ на сайте CSO Online (**https://www.csoonline.com/author/Roger-A.-Grimes/**), а также работает штатным консультантом более 20 лет. Роджер консультирует крупный и малый бизнес по всему миру по вопросам предотвращения хакерских и вредоносных атак. Опыт показал ему, что большинство злонамеренных хакеров не так умны, как многие считают, и они определенно проигрывают специалистам в области ИБ.

Благодарности

Я хотел бы поблагодарить Джима Минателa, давшего зеленый свет книге, которую я обдумывал на протяжении 10 лет, и Келли Тэлбот, лучшего редактора, с которой я сотрудничал на протяжении 15 лет. Келли отлично справляется с проблемами, не повышая голоса. Я хочу поблагодарить компанию Microsoft, моего лучшего работодателя за последние 10 лет. Спасибо Брюсу Шнайеру за его негласное покровительство надо мной и всеми в этой отрасли. Мое почтение Брайану Кребсу за его большое расследование и за то, что он приоткрыл завесу тайны крупного бизнеса, каковым уже стала киберпреступность. Спасибо Россу Гринбергу, Биллу Чесвику и другим авторам, которые настолько интересно писали об информационной безопасности, что я решил построить на этом карьеру. Наконец, я не был бы тем, кто есть сегодня, без моего брата-близнеца Ричарда Граймса, лучшего писателя, подтолкнувшего меня к написанию книги более 20 лет назад. Всем специалистам по ИБ респект за помощь от имени всех нас.

Предисловие

Роджер Граймс работает в сфере информационной безопасности почти три десятилетия, и я, к моему удовольствию, знаком с ним 15 лет. Это один из немногих избранных профессионалов среди моих знакомых, у кого безопасность в крови – интуитивное понимание предмета, которое в сочетании с колоссальным опытом поимки плохих парней и устранения уязвимостей в системах безопасности превращает его в идеального автора этой книги. Роджер впервые начал писать в журнал InfoWorld в 2005 году, когда по электронной почте раскритиковал автора статей по безопасности, причем настолько убедительно, что мы сразу же попросили его внести свой вклад в публикацию. С тех пор он написал сотни статей в InfoWorld, каждая из которых демонстрирует любовь к теме, а также понимание с точки зрения психологии как злонамеренных хакеров, так и людей, которые противостоят им. В своей еженедельной журнальной колонке «советника по безопасности» Роджер демонстрирует уникальный талант сосредоточиваться на значимых вопросах, а не преследовать эфемерные угрозы или новые технологии. У него было стойкое стремление к убеждению специалистов по информационной безопасности и их руководителей уделять ей больше внимания, несмотря на склонность многих организаций пренебрегать основами и переключаться на последние технологичные решения. В этой книге Роджер описывает этичных хакеров в сфере ИБ, которые повлияли на ситуацию. Их неустанные усилия помогают удерживать линию обороны против растущей армии злоумышленников, чьи цели с годами сместились от деструктивных воздействий в сторону кражи ценной интеллектуальной собственности и миллионов долларов у финансовых учреждений и их клиентов. Мы в неоплатном долгу перед ними. Упоминая о таких людях, как Брайан Кребс, Дороти Деннинг и Брюс Шнайер, Роджер отдает должное потраченным ими усилиям, формируя увлекательный сборник, который и развлекает, и информирует одновременно. Эту книгу важно прочесть всем, кто интересуется информационной безопасностью, и людям, которые стремятся нас обезопасить.

Эрик Кнорр, главный редактор журнала InfoWorld

Введение

Цель этой книги – раскрыть мир специалистов по информационной безопасности (ИБ), некоторых из лучших хакеров, защитников конфиденциальных данных, преподавателей и писателей. Я надеюсь, что вы прочитаете ее с большим удовольствием от осознания усилий, которые потребовались, чтобы реализовать фантастический мир компьютеров, в котором мы живем сегодня. Без добрых людей на светлой стороне, воюющих против злоумышленников, компьютеры, Интернет и все, что с ними связано, были бы невозможны. Эта книга – ода специалистам по ИБ.

Я хочу призвать всех, кто собирается сделать карьеру в области информационных технологий, подумать о карьере в сфере информационной безопасности. Я также хочу призвать всех начинающих хакеров, особенно тех, кто переживает насчет этичности применения своих знаний, сделать карьеру в

этой области. Я противостоял вредоносным хакерам и их творениям. Я смог исследовать каждый интерес в области хакинга, который у меня был, этичным и законопослушным способом. И десятки тысяч других. Информационная безопасность – одна из самых востребованных и высокооплачиваемых отраслей в любой стране. Это стало моим призванием и может стать вашим.

Книга разделена на главы, в которых кратко описывается реализация определенного способа атаки, а затем приводится один или два профиля специалистов по ИБ, преуспевших в этой области. Я попытался выбрать лучших из множества легенд, светил и даже некоторых относительно скромных специалистов, которые достигли блестящих успехов, даже если они не очень известны обывателям. Я попытался сформировать сочетание опыта ученых, разработчиков, преподавателей, лидеров, писателей и частных практиков, живущих в Соединенных Штатах и во всем мире. Я надеюсь, что читатели, заинтересованные в карьере специалиста ИБ, смогут так же мотивировать себя, как и я, чтобы сделать сферу ИТ значительно безопаснее для всех нас.

Да пребудет с вами сила!

1. Что ты за хакер?

Много лет назад я переехал в дом с прекрасным гаражом. В нем было очень удобно парковаться и даже хранить лодку и небольшой фургон. Сооружение было построено из отличных прочных досок. Электрику провели профессионалы, а качественные окна выдерживали порывы ветра скоростью 70 метров в секунду. Большую часть интерьера создал профессиональный плотник из ароматного красного кедра. Я неспособен и гвоздь забить, не то что собрать мебель, но даже мне было понятно, что он знает свое дело, думает о качестве и уделяет внимание деталям.

Через несколько недель после новоселья пришел чиновник и сказал, что гараж, построенный много лет назад, не имеет нужных документов, и придется снести незаконную постройку, иначе мне грозят крупные штрафы за каждый день просрочки исполнения постановления. Я позвонил в ведомство, чтобы утрясти вопрос, ведь гараж возвели задолго до моего переезда, и продавался он как часть недвижимости. Безрезультатно. Его нужно было немедленно снести. Штрафные санкции за один день превышали сумму, которую я мог выручить за отделку, если бы аккуратно ее снял. Проще говоря, в целях экономии, чем быстрее я демонтирую гараж, тем лучше.

Я достал кувалду и за несколько часов превратил сооружение в груду деревянных обломков и прочего мусора. В процессе я думал о том, что строителю, вероятно, потребовались недели, если не месяцы, чтобы возвести гараж, а я уничтожил его творение своими варварскими руками гораздо быстрее.

Вопреки распространенному мнению, злонамеренный взлом – это скорее кувалда стропальщика, чем тонкий инструмент ремесленника.

Если вы уверены, что сможете стать хакером, вам придется решить, будете вы стремиться к защите общего блага или довольствоваться низменными целями. Вы хотите быть скрывающимся, преступным хакером или праведным, опытным специалистом по ИБ? Эта книга – доказательство, что лучшие хакеры работают во благо. Они практикуются, развиваются интеллектуально, и им не нужно скрываться от правоохранительных органов. Они могут работать в центре сферы информационной безопасности, приводить в восхищение коллег и получать хорошие деньги. Эта книга о порой невоспетых героях, которые делают нашу невероятную цифровую жизнь возможной.

Примечание. Хотя термины «хакер» или «взлом» могут означать человека или деятельность как с хорошими, так и с плохими намерениями, в основном их используют в негативном ключе. Я понимаю, что хакеры могут быть разными, но во имя экономии бумаги впредь буду использовать эти слова без оговорок, подразумевая либо отрицательный, либо положительный их оттенок. Вникайте в смысл текста, чтобы понимать намерения, в связи с которыми упоминаются термины.

Большинство хакеров отнюдь не гении

К сожалению, почти каждый, кто пишет о «злых» хакерах, не имея реального опыта, романтизирует их как умные, богоподобные, мифические фигуры. Они могут подобрать любой пароль менее чем за минуту (особенно под прицелом пистолета, если верить Голливуду), взломать любую систему и секретный шифр. Они работают в основном по ночам и пьют много энергетических напитков, а их рабочее место завалено упаковками от чипсов и фастфуда. Школьник крадет пароль учителя, чтобы изменить свои оценки, и СМИ подлизываются к нему, как к потенциальному Биллу Гейтсу или Марку Цукербергу.

Хакеры необязательно гениальны. Я – живое тому доказательство. Несмотря на то, что я вламывался в системы всех компаний, в которых меня когда-либо нанимали для проверки систем защиты, я никогда полностью не понимал квантовую физику или теорию относительности Эйнштейна. Я дважды провалил экзамен по родному языку в средней школе, никогда не получал оценки выше тройки с плюсом по математике, а мой средний балл в первом семестре колледжа составил 0,62. Я получил пять двоек и одну пятерку. Одинокая пятерка была по курсу безопасности на водах, потому что я на тот момент пять лет работал пляжным спасателем. Плохие оценки были не только следствием того, что я не учился. Я просто не был достаточно умен и не пытался с этим справиться. Позже я узнал, что учеба и усердная работа часто более ценны, чем врожденный высокий уровень интеллекта. Я окончил университет и преуспел в мире информационной безопасности.

Тем не менее, даже когда писатели не называют «злых» хакеров сверхумными, читатели частенько предполагают, что они именно таковы, потому что, похоже, практикуют какую-то передовую черную магию, о которой остальной мир не подозревает. Коллективный всемирный разум считает, что «злой хакер» и «суперинтеллект» должны идти рука об руку. Это неправда. Некоторые из них умные, большинство средние, а остальные вообще бестолковы, как и многие другие люди. Просто хакерам известно о сведениях и процессах, которые незнакомы людям других профессий, например плотникам, сантехникам и электрикам.

Специалисты по ИБ – продвинутые хакеры

Если проводить интеллектуальное сравнение, то специалист по ИБ в среднем умнее хакера. Он должен знать все, на что способен злоумышленник, а также уметь остановить атаку. Защита не сработает, если нет участия конечного пользователя, работает скрытно и справляется идеально (или почти идеально) все время. Покажите мне «злого» хакера с определенной техникой, и я покажу вам много специалистов по ИБ, которые умнее и лучше его. Однако атакующим обычно уделяется больше внимания. И моя книга призвана исправить ситуацию.

Хакеры особенны

Несмотря на то, что я не разделяю хакеров на гениальных, хороших и плохих, все они имеют несколько общих черт. Одна из них – широкое интеллектуальное любопытство и готовность пробовать новое за пределами данных интерфейсов или границ. Они не боятся идти своим путем. Компьютерные хакеры, как правило, таковы и по жизни, взломщики всевозможного за пределами компьютеров. Они относятся к тому типу людей, которые, столкнувшись с системой безопасности в аэропорту, размышляют о том, как пронести оружие, которого у них нет, мимо детекторов. Они выясняют, можно ли подделать дорогие билеты на концерт, даже если не собираются посещать его. А покупая телевизор, задаются вопросом, можно ли получить доступ к его операционной системе, чтобы что-нибудь там изменить. Покажите мне хакера, и я покажу вам того, кто постоянно ставит под сомнение статус-кво и все исследует.

Примечание. В какой-то момент моя собственная гипотетическая схема пронесения оружия через охрану аэропорта строилась на использовании инвалидных колясок с оружием или взрывчаткой, спрятанными внутри металлического каркаса. Инвалидные кресла часто провозят мимо охраны аэропорта, не подвергая тщательному досмотру.

Хакеры настойчивы

Следующее после любопытства важное качество хакера – настойчивость. Каждый хакер – и хороший, и плохой – проходил через пытку, когда ты долгими часами пытаешься снова и снова заставить что-то работать.

Злоумышленники ищут бреши в защите. Одна ошибка специалиста по ИБ, по сути, сводит на нет всю защиту. Специалист по ИБ должен быть идеальным. Все компьютеры и программное обеспечение должны быть пропатчены, каждая конфигурация проверена на отсутствие уязвимостей, и каждый конечный пользователь отлично обучен. По крайней мере, в идеальном мире. Специалисты по ИБ знают, что применяемые средства защиты не всегда работают или применяются в соответствии с инструкциями, поэтому выстраивают уровни «глубокоэшелонированной обороны». И злоумышленники, и специалисты по ИБ ищут слабые места, только с противоположных сторон баррикад. Обе стороны участвуют в непрерывной войне со многими столкновениями, победами и поражениями. Самые стойкие выходят победителями.

Шляпных дел мастера

Я всю свою жизнь был хакером. Мне платили за то, чтобы я вламывался куда-либо (на что у меня были юридические полномочия). Я взламывал пароли, сети, писал вредоносные программы и при этом ни разу не нарушил закон и не преступил границ этики. Это не значит, что никто из знакомых не пытался меня на это соблазнить. На протяжении многих лет друзья просили меня взломать мобильный телефон супруга, уличенного в измене; заместители хотели получить доступ к электронной почте начальства; а также люди без ордера требовали «вскрыть» компьютер одного злого хакера, чтобы предотвратить его дальнейшие взломы. На ранней стадии вы должны решить, кто вы и какова ваша этика. Я решил, что буду хорошим хакером («в белой шляпе»), а «белые шляпы» не совершают незаконных или неэтичных действий.

Хакеры, которые участвуют в незаконной и неэтичной деятельности, называются «черными шляпами». Хакеры, которые зарабатывают на жизнь законным образом в сфере ИБ, но в духе «Бойцовского клуба» тайно промышляют взломами, известны как «серые шляпы». Мое представление о кодексе чести предусматривает лишь два варианта. Для меня «серых шляп» не существует. Ты либо делаешь незаконные вещи, либо нет. Ограбь банк, и я назову тебя грабителем, каковой бы ни была твоя цель.

Однако «черные шляпы» могут стать «белыми». Это происходит сплошь и рядом. Вопрос в том, станет ли хакер «белым», прежде чем ему придется сесть за решетку. Кевин Митник – один из самых известных арестованных хакеров в истории (см. главу 5), который после выхода из тюрьмы начал карьеру в сфере ИБ на всеобщее благо. Роберт Т. Моррис, написавший и выпустивший первого компьютерного червя, чуть не уничтожившего Интернет **(https://ru.wikipedia.org/wiki/Червь_Морриса)**, в итоге стал членом Ассоциации вычислительной техники (**https://awards.acm.org/award_winners/morris_4169967.cfm**) за «вклад в компьютерные сети, распределенные и операционные системы».

Раньше грань между легальным и нелегальным взломом была не столь четкой. Более того, многие ранние «злые» хакеры получили статус супергероев. Даже я не мог открещиваться от некоторых из них. Джон Дрейпер (ник Capitan Crunch)

свистел в игрушечный свисток, обнаруженный им в коробке кукурузных хлопьев Cap'n Crunch, чтобы сымитировать тон частотой 2600 Гц. Таким образом он мог бесплатно звонить по межгороду. Многие хакеры, которые публиковали приватную информацию «во имя общественного блага», часто становились известными. Но, за некоторыми исключениями, я никогда не придерживался чрезмерно идеализированного взгляда на хакеров-злоумышленников. У меня была довольно четкая позиция, что люди, которые делают несанкционированные вещи с чужими компьютерами и данными, совершают преступление.

Много лет назад, впервые заинтересовавшись компьютерами, я прочитал книгу Стивена Леви «Хакеры: герои компьютерной революции»[1]. На заре эры персональных компьютеров Леви написал занимательную историю о хакерах, хороших и плохих, воплощающих хакерский идеал. Бóльшая часть книги посвящена людям, которые улучшили мир с помощью компьютеров, но в ней также упоминаются и те, кто сегодня был бы арестован за свою деятельность. Некоторые из этих хакеров полагали, что цель оправдывает средства, и следовали свободе морали, воплощенной, по словам Леви, «хакерской этикой». Главным среди этих верований была философия о том, что каждый компьютер может быть доступен по любой законной причине, что вся информация должна быть свободной, и не следует доверять властям. Это был романтический взгляд на хакерство, хотя он не скрывал сомнительных этических и юридических вопросов. На самом деле все вокруг вновь расширили границы.

Ради автографа я отправил Стивену Леви экземпляр его книги (мне тоже стали присылать мои книги на подпись после того, как я выпустил восемь предыдущих). Леви публиковал свои статьи и редактировал чужие в нескольких крупных журналах, включая Newsweek, Wired и Rolling Stone. Кроме того, он написал еще шесть книг по вопросам информационной безопасности. Леви пишет и по сей день. Его книга «Хакеры: герои компьютерной революции» открыла для меня поразительный мир хакерства.

Позже другие книги, такие как *Flu-Shot* Росса Гринберга (давно не издается) и *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System* Джона Макафи **(https://www.amazon.com/Computer-virusesdiddlers-programs-threats/dp/031202889X)** познакомили меня со стратегиями борьбы со злонамеренными хакерами. Я настолько ими впечатлился, что всерьез задумался о карьере борца с этими угрозами.

Позже я узнал, что специалисты по ИБ – самые умные хакеры. Я не хочу сводить всех злонамеренных хакеров под одну гребенку посредственности. Каждый год редкие гениальные хакеры обнаруживают что-то новое. Но подавляющее большинство «черных шляп» довольно посредственны и просто повторяют то, что работает уже на протяжении двадцати лет. Среднестатистический хакер-злоумышленник не имеет достаточного таланта в программировании, чтобы написать простое приложение типа «Блокнот», а тем более самостоятельно проникнуть куда-то, взломать ключи шифрования или самолично успешно подобрать пароли – без помощи других хакеров, которые реально талантливы и успешны на протяжении многих лет.

Ирония в том, что умные люди в компьютерном мире, о которых я знаю, – это не злые хакеры, а специалисты по ИБ. Они должны знать все, что делает хакер, предугадывать то, что он может совершить, и выстроить качественную оборону. Мир специалистов по ИБ полон кандидатов наук, магистрантов и успешных предпринимателей. Теперь хакеры редко меня впечатляют. А вот специалисты по ИБ – всегда.

Обычно специалисты по ИБ открывают для себя новый способ взлома, чтобы предотвратить атаки такого рода, и умалчивают о своем достижении. Это сродни министерству обороны, и предоставление злоумышленникам новых способов взлома до того, как оборона будет возведена, никому не облегчит жизнь. Это их образ жизни: выяснить новый способ взлома и помочь с латанием бреши, прежде чем она будет обнаружена кем-то еще. Такое случается гораздо чаще, чем обратное (например, злонамеренный хакер обнаруживает новую уязвимость).

Я был свидетелем тому, как специалисты по ИБ находят новый способ взлома, но из-за высоких затрат или недостатка времени уязвимость не закрывается немедленно, и какой-нибудь хакер получает звание «первооткрывателя». К сожалению, специалисты по ИБ не всегда получают славу и признание, когда выполняют свою повседневную работу.

Я тридцать лет изучал приемы работы как вредоносных хакеров, так и специалистов по ИБ, и мне стало ясно, что специалисты впечатляют сильнее. Вредоносные хакеры даже рядом не стояли. Если вы хотите показать всем, насколько хорошо разбираетесь в компьютерах, не раскрывайте новый способ взлома – лучше покажите новую стратегию обороны. Не требуется особого ума, чтобы что-то по-новому сломать. Это в основном требует лишь настойчивости. Но человек должен быть особенным и одаренным, чтобы построить то, что может выдержать непрерывные атаки в течение длительного времени.

Если вы хотите произвести впечатление на мир, не сносите гараж. Вместо этого создайте код, который сможет выдержать кувалду хакера-взломщика.

2. Как хакеры взламывают

Самый приятный аспект моей работы – это тестирование на проникновение (также известное как пентестирование). Пентестирование – это взлом в прямом смысле этого слова. Это битва интеллектов человека и машины. Человек – «атакующий» – может использовать собственную изобретательность и новые или существующие инструменты, когда исследует слабые стороны машин или людей. За все годы, что я занимался тестированием, хотя мне на это обычно дают недели, я успешно взламывал цель примерно за час. Самый долгий взлом, помню, продолжался три часа. Это касается любого банка, медицинского, правительственного или корпоративного учреждения, который когда-либо нанимал меня для тестирования на проникновение.

При этом я не могу назвать себя отличным пентестером. По шкале от 1 до 10, где 10 – высший балл, мои способности составляют примерно 6 или 7. С точки зрения специалиста по ИБ я чувствую себя лучшим в мире, но я весьма посредственный взломщик. Я был окружен потрясающими пентестерами, как мужчинами, так и женщинами, которые не помышляли о написании собственных инструментов пентестирования или не считали свои действия успешными, если не они привели к созданию хотя бы одного события с предупреждением в логах. Но даже люди, которых я оцениваю на 10 баллов, обычно считают себя середнячком и восхищаются другими пентестерами, которых, по их мнению, десятки. Насколько же хороши должны быть эти хакеры?

Вам не нужно быть исключительным, чтобы стать очень успешным хакером. Для начала карьеры даже не нужно успешно взламывать клиента, который вас нанял (я предполагаю, что вам платят за законные пентесты). На самом деле клиенты будут в абсолютном восторге, если вы *не* взломаете систему. Они смогут похвастаться, что наняли хакеров, а их сеть выдержала атаку. Это беспроигрышный вариант для всех участников. Вы получаете свои деньги, а они радуются, что атака отражена. На моей памяти это единственная работа, где не может быть плохого результата. К сожалению, я не знаком ни с одним пентестером, который когда-либо успешно взламывал *все* свои цели. Я уверен, что есть хакеры, которые терпят неудачу, но подавляющее большинство «сорвут свой куш».

Примечание. Если ваши тесты не обнаружили слабых мест, а клиент вскоре был скомпрометирован реальными злоумышленниками, это выставит вас не в лучшем свете. Если это произойдет несколько раз, дурная слава не обойдет вас стороной, и вы, вероятно, будет искать новую работу. Слабые места есть. Ищите их.

Обычно пентестеры делают что-то еще, чтобы произвести впечатление на своих клиентов. Например, удаленно снимают генерального директора за рабочим столом на веб-камеру или взламывают пароль к серверу и размещают «Веселого Роджера» на рабочем столе компьютера сетевого администратора. Это стоит тысячи слов. Не стоит недооценивать, насколько одна глупая картинка может повысить удовлетворенность клиентов вашей работой. Они будут вспоминать о ней (и хвастаться вами) спустя годы после того, как вы закончите работу. Если можете, всегда заканчивайте красивым жестом. Это мой «золотой совет».

Секрет взлома

Если у хакеров и есть секрет взлома, то он точно не в том, как ломать. Это процесс изучения правильных методов и использования верных инструментов, точно как у электриков, сантехников или строителей. Нет определенного способа взлома. Однако существует вполне конкретный набор шагов, которые объединяются в более крупные этапы; это процесс, который включает в себя все, что необходимо хакеру для выполнения задачи. Не каждый хакер проходит

все шаги. Некоторые вообще делают только один. Но в целом, если вы будете следовать этапам, то, скорее всего, придете к успеху. Вы можете пропустить один или несколько шагов и все равно быть успешным хакером. Вредоносные программы и другие инструменты взлома часто позволяют пропускать шаги, но по крайней мере один из них – первоначальное проникновение – требуется всегда. Независимо от желания сделать официальную карьеру хакера, если вы собираетесь бороться со злоумышленниками, нужно понимать методологию взлома. Модели могут различаться, включая количество шагов, их названия и конкретные детали, но все они содержат одни и те же основные компоненты.

Методология взлома

Методология взлома содержит следующие прогрессивные шаги.

1. Сбор информации.
2. Проникновение.
3. Упрощение доступа в будущем (необязательный).
4. Разведка системы.
5. Перемещение (необязательный).
6. Выполнение намеченного действия.
7. Заметание следов (необязательный).

Сбор информации

Как правило, если хакер не рассчитывает взламывать все потенциально уязвимые сайты, он придерживается конкретной цели. Проникая в конкретную компанию, первое, что он делает, это собирает о ней всю информацию, которая поможет проникнуть в систему. Это IP-адреса, адреса электронной почты и доменные имена. Хакер узнает, сколько потенциальных сайтов и сервисов, к которым он может получить доступ, подключены к компании. Используя средства массовой информации и публичные документы, он находит сведения о руководителях высшего звена и прочих сотрудниках для проведения атак средствами социальной инженерии. Хакер просматривает новости, чтобы узнать, какое крупное программное обеспечение недавно купил объект, какие происходили слияния или разделения (такие мероприятия часто сопровождаются ослаблением уровня безопасности), и даже с какими партнерами взаимодействует «жертва». Многие компании были скомпрометированы гораздо более слабым партнером.

В большинстве хакерских атак важнее всего выяснить, с какими цифровыми активами связана компания. Обычно идентифицируются не только основные (публичные) сайты и службы; чаще злоумышленнику полезнее обратить внимание на менее популярные, такие как ресурсы сотрудников и партнеров. Такие сайты и серверы, скорее всего, имеют более слабую систему безопасности, нежели крупные порталы компаний.

Затем толковый хакер начинает собирать сведения обо всем ПО и сервисах, доступных на каждом из этих сайтов. Это процесс, известный как сбор цифровых отпечатков. Очень важно узнать, какие операционные системы (ОС) и их версии используются. Версии ОС могут сказать хакеру об уровнях защиты системы и ошибках, которые могут или не могут присутствовать. Представим, что он встречает операционную систему Windows Server 2012 R2 или Linux Centos 7.3-1611. По той же причине он ищет программы и вариации версий программного обеспечения, работающие на каждой из этих ОС. Если это веб-сервер, он может встретить Internet Information Server 8.5 на Windows или Apache 2.4.25 на Linux. Он проводит инвентаризацию каждого устройства, операционной системы, приложений и версий, запущенных на каждом из целевых объектов. Всегда лучше провести тщательную инвентаризацию, чтобы получить полную картину, но в других случаях хакер может найти крупную уязвимость на ранней стадии и перейти к следующему шагу. Если отбросить этот быстрый способ, как правило, чем больше информации хакер соберет о том, что работает, тем лучше. Каждое дополнительное ПО и версия предоставляет дополнительные возможные векторы атаки.

Примечание. Некоторые хакеры называют общий нетехнический сбор информации поиском следов, а поиск информации об операционной системе и программном обеспечении – сбором цифровых отпечатков.

Порой, когда хакер подключается к сайту, тот услужливо отвечает очень подробной информацией о версиях программного обеспечения, поэтому не нужны никакие дополнительные инструменты. На случай, если этого не происходит, существует много инструментов, упрощающих сбор цифровых отпечатков. На сегодня первый инструмент, который использует хакер для сбора цифровых отпечатков, – это Nmap **(https://nmap.org/)**. Программа разработана в 1997 году. Она представлена в нескольких версиях, поддерживающих операционные системы Windows и Linux, и, по сути, представляет собой швейцарский армейский нож, только для хакера. Nmap может выполнять все виды сканирования и тестирования хоста, и это очень хороший способ сбора цифровых отпечатков. Для этого существуют и более мощные приложения, в частности сосредоточенные на сборе определенных данных, таких как информация о веб-серверах, базах данных или серверах электронной почты. Например, программа Nikto2 **(https://cirt.net/Nikto2)** не только эффективнее Nmap собирает цифровые отпечатки с веб-серверов, но и выполняет тысячи пентестов и позволяет выявить уязвимые места.

Проникновение

Это шаг, который позволяет хакеру получить первоначальный доступ. От его успешности зависит весь дальнейший процесс. Если хакер хорошо поработал на этапе снятия цифровых отпечатков, то проникновение будет действительно не

таким уж сложным. Честно говоря, я всегда его проходил. В сфере ИБ есть недостатки: используется старое программное обеспечение, остаются незакрытые уязвимости из-за игнорирования патчей и почти всегда что-то неправильно настроено в системе аутентификации.

Примечание. Один из моих любимых трюков – атаковать ПО и устройства, которые специалисты по ИБ используют для защиты своих сетей. Часто такое обеспечение и устройства проблематично пропатчить, и в них на многие годы остаются незалатанные уязвимости.

Если вдруг все ПО и устройства полностью защищены (а такого не бывает), то можно атаковать через человеческий фактор, который всегда оказывается самым слабым элементом системы уравнения. Но без первоначального проникновения для хакера все потеряно. К счастью для него, есть много способов проникнуть к жертве. Вот различные методы, которые хакер может для этого использовать:

• уязвимости нулевого дня (0day);

• непропатченное программное обеспечение;

• вредоносные программы;

• социальная инженерия;

• подбор паролей;

• перехват или атака посредника;

• утечка данных;

• неправильная конфигурация оборудования;

• отказ в обслуживании;

• участие инсайдеров, партнеров, консультантов, производителей и других третьих лиц;

• пользовательский фактор;

• физический доступ;

• повышение привилегий.

Уязвимости нулевого дня

Уязвимости нулевого дня (0day[2]) – это эксплойты (внедрения), которые встречаются реже, чем другие известные уязвимости, большинство которых производители давно закрыли патчами. Для его исправления еще не выпущен патч, и общественность (как, впрочем, и разработчик) не знает об этом. Любые компьютерные системы, на которых присутствует программное обеспечение с уязвимостями нулевого дня, подвержены взлому, если потенциальная жертва не удалит его или не использует инструмент для смягчения последствий

(например, брандмауэр, список контроля доступа, сегментация посредством виртуальных ЛВС, средства защиты от переполнения буфера и т. д.).

Уязвимости нулевого дня не так распространены, как другие эксплойты, поэтому не могут постоянно эксплуатироваться злоумышленником. Если хакер ими злоупотребляет, они будут обнаружены и исправлены специалистами по ИБ и добавлены в сигнатуры антивирусных программ. В большинстве таких ситуаций специалисты по ИБ могут исправлять новые эксплойты через нескольких часов, максимум дней после обнаружения. Когда в ход идут уязвимости нулевого дня, они либо используются очень широко против нескольких целей сразу для максимально возможного эффекта, либо применяются только в крайнем случае. Лучшие в мире профессиональные хакеры обычно имеют подборки уязвимостей нулевого дня, которые используют только тогда, когда все остальные подходы не удались. И даже в таких ситуациях они атакуют так, чтобы сохранять максимальную скрытность. Уязвимость нулевого дня может быть использована для получения первичного доступа к особенно устойчивой системе, а затем все ее следы удаляются и далее реализуются более традиционные методы взлома.

Непропатченное программное обеспечение

Вовремя непропатченное ПО – одна из главных причин, почему компьютером или устройством завладевает злоумышленник. Каждый год публикуются сведения о тысячах (обычно 5–6 тысяч, т. е. около 15 в день) новых обнаруженных уязвимостях в популярном программном обеспечении. (Познакомиться со списком можно на сайте службы безопасности Microsoft: **https://www.microsoft.com/ru-ru/security/business/security-intelligence-report**.) Разработчики, как правило, стараются писать более защищенный код и исправлять собственные ошибки, но число программ и миллиардов строк кода растет, поэтому общее количество ошибок остается относительно неизменным в течение последних двадцати лет. Большинство разработчиков своевременно выпускают патчи для своего ПО, и чаще всего происходит это после того, как уязвимость становится общеизвестной. К сожалению, пользователи их продукции, как известно, нерасторопно применяют эти патчи, нередко даже отключая процедуру автоматического обновления. Определенный процент пользователей и вовсе не патчит системы. Они либо игнорируют предупреждения и оповещения об обновлениях, либо раздражаются при их появлении, либо вообще не знают, зачем их применять (например, многие торговые системы не уведомляют кассиров о необходимости обновления). Большинство эксплойтов касаются программного обеспечения, которое не патчилось (т. е. не обновлялось) в течение многих лет. Даже если конкретная компания или пользователь исправляет критические уязвимости так же быстро, как они появляются, терпеливый хакер может ждать «дыру», которая будет обнаружена со временем, и запустит соответствующую атаку, прежде чем специалисты по ИБ успеют выявить ее и инициировать выпуск патча. (Хакеру относительно легко удается обратная разработка таких «брешей», и он узнает, как эксплуатировать ту или иную уязвимость.) Как уязвимость нулевого дня,

так и обычные уязвимости ПО сводятся к небезопасным методам, применяемым при разработке программного обеспечения. Мы рассмотрим их в главе 6.

Вредоносные программы

Вредоносные программы бывают разных видов. Наиболее известные из них – это вирусы, троянские программы и черви. При этом современные вредоносные программы часто представляют собой гибридную смесь нескольких типов. Вредоносное ПО позволяет хакеру реализовать метод эксплойта, чтобы было проще атаковать или чтобы быстрее охватить большее количество жертв. Когда обнаруживается новый эксплойт, специалисты по ИБ знают, что авторы вредоносных программ будут использовать автоматизированное вредоносное ПО для более быстрого распространения. Этот процесс известен как «вооружение». В то время как эксплойтов следует избегать, зачастую именно их эксплуатация создает наибольший риск для конечных пользователей и общественности. Без вредоносных программ злоумышленник был бы вынужден атаковать каждую жертву поочередно. С их помощью миллионы компьютеров могут подвергнуться взлому в течение нескольких минут. Мы познакомимся с вредоносными программами поближе в главе 9.

Социальная инженерия

Одна из самых успешных стратегий взлома – социальная инженерия. Независимо от того, осуществляется она вручную или автоматически, это хакерский трюк, обманывающий конечного пользователя, который наносит вред собственному компьютеру или безопасности. Это может быть электронное письмо, которое обманом принуждает перейти по вредоносной ссылке или открыть зараженное вложение. Хакер может заставить пользователя раскрыть свои персональные данные для авторизации (так называемый фишинг). Социальная инженерия уже давно находится на лидирующих позициях среди атак, реализуемых хакерами. Опытный хакер в «белой шляпе», Кевин Митник, – один из лучших примеров социальных инженеров-злоумышленников. Речь о нем пойдет в главе 5, а социальная инженерия более подробно рассматривается в главе 4.

Подбор паролей

Пароли или их деривации могут быть подобраны или украдены. Долгое время простой подбор паролей (или социальная инженерия) был одним из самых популярных способов получения начального доступа к компьютерной системе или сети и до сих пор таковым остается. Но кража учетных данных и так называемые атаки повторного воспроизведения (pass-the-hash), по существу, затмили атаки со взломом паролей в течение последних нескольких лет. При атаках с кражей учетных данных злоумышленник обычно получает административный доступ к компьютеру или устройству и перехватывает одну или несколько записей учетных данных, хранящихся в системе (в памяти или на

жестком диске). Украденные данные затем используются для доступа к другим системам. Почти каждая крупная корпоративная атака включала кражи учетных данных в качестве общего компонента эксплойта, так что традиционный подбор паролей уже не так популярен. Взломы паролей описаны в главе 21.

Перехват или атака посредника

Перехват и атака посредника (MITM-атака) ставят под угрозу легитимное сетевое подключение, позволяя получить доступ к нему или злонамеренно участвовать в коммуникациях. Большинство таких атак успешны из-за недостатков в сетевых или прикладных протоколах, но также могут быть результативны вследствие человеческого фактора. В наши дни самые большие атаки происходят в беспроводных сетях. Сетевые атаки будут рассмотрены в главе 33, а беспроводные – в главе 23.

Утечка данных

Утечка персональной информации может быть результатом одной из форм взлома, а также непреднамеренного или преднамеренного действия самого владельца данных. Большинство утечек происходят из-за непреднамеренной (и незащищенной) их публикации или потому, что некий хакер выяснил способ доступа к определенным персональным данным. Но инсайдерские атаки, когда сотрудник или контрагент намеренно крадет или использует персональную информацию, – не менее распространенная форма взлома. Некоторые главы этой книги посвящены предотвращению утечек данных.

Неправильная конфигурация оборудования

Неправильная настройка компьютеров также часто реализует очень слабые варианты защиты, иногда непреднамеренно. Я не смогу сосчитать, сколько раз заходил на общедоступный веб-сайт и видел, что его самые важные файлы непонятным образом доступны всем пользователям или даже всему миру. Когда вы сообщаете миру, что любой желающий может получить доступ к любому файлу, который им нравится, ваш сайт или файлы, хранящиеся на нем, недолго будут оставаться приватными. Безопасные операционные системы и конфигурации описаны в главе 30.

Отказ в обслуживании

Даже если владелец не совершил ни одной ошибки или строго ставил все патчи на программное обеспечение, с помощью Интернета все равно можно взломать почти любой сайт или компьютер. Даже если вы совершенны, компьютеры, которые вы используете, полагаются на одну или несколько неподконтрольных вам служб, которые потенциально уязвимы. Сегодня масштабные атаки отказа в обслуживании могут положить или значительно повлиять на работу почти любого сайта или компьютера, подключенного к Интернету. В процессе таких атак часто передаются миллиарды вредоносных пакетов в секунду, из-за

которых падает (становится недоступен) целевой сайт (или его вышестоящие/нижестоящие соседи). Существуют десятки коммерческих, в том числе незаконных служб, которые можно использовать как для создания, так и для защиты от мощных атак отказа в обслуживании. Рассмотрим их в главе 28.

Участие инсайдеров, партнеров, консультантов, производителей и других третьих лиц

Даже если ваша сеть и ее компьютеры совершенны (что едва ли возможно), вы можете быть скомпрометированы дефектом в системе подключенного партнера или инсайдером. Эта категория довольно широка и пересекается с рядом других хакерских методов.

Пользовательский фактор

Эта категория проникновения также пересекается с другими методами. Например, пользователь может случайно отправить персональные данные неавторизованному пользователю, указав в адресе электронной почты один неверно введенный символ. Пользователь может случайно пропустить критический патч для серверного ПО или установить неверное разрешение. Частая ошибка пользователя – отвечая на электронное письмо определенному человеку или группе людей, случайно разослать письмо всем или даже, по ошибке, отреагировать в негативном ключе. Я отдельно выделил пользовательские ошибки только потому, что человеческий фактор иногда срабатывает, и хакеры готовы этим воспользоваться.

Физический доступ

Общепринятое мнение гласит, что, если злоумышленник имеет физический доступ к устройству, он может просто украсть его (секунда – и ваш мобильный телефон благополучно уведен) и уничтожить или в итоге обойти все средства защиты для доступа к персональным данным. Этот метод остается довольно успешным до сих пор, даже против средств, явно предназначенных для защиты от физических атак. Например, многие программы шифрования диска могут быть взломаны с помощью электронного микроскопа для выявления защищенного секретного ключа путем идентификации отдельных электронов, составляющих ключ. Или оперативная память может быть заморожена баллончиком со сжатым воздухом, чтобы прочитать секретный ключ шифрования в открытом виде из-за ошибки в том, как она хранит данные.

Повышение привилегий

Каждый хакер использует один из методов проникновения, описанных в предыдущих разделах, чтобы получить доступ к целевой системе. Единственный вопрос – это тип доступа, который он получает. Если хакер использует программное обеспечение или службы, запущенные в собственном

контексте безопасности пользователя, он изначально имеет только те же права доступа и разрешения, что и авторизованный пользователь. Или он может открыть святой Грааль и получить полный доступ к административной системе. Если злоумышленник получает только обычные, непривилегированные разрешения доступа, то он обычно выполняет вторую атаку для эскалации привилегий, чтобы попытаться получить более высокий доступ. Атаки эскалации привилегий охватывают весь спектр, по существу, дублируя те же подходы, что и для проникновения, но они начинаются с более высокой начальной точки, уже имеющей некоторый доступ. Атаки с повышением привилегий обычно проще выполнить, чем первоначальные эксплойты. И поскольку начальные эксплойты почти всегда гарантированно будут успешными, эскалация привилегий намного проще.

Упрощение доступа в будущем

Затем, хотя это необязательно, после получения первоначального доступа, злоумышленник работает над реализацией дополнительного метода, чтобы убедиться, что сможет легко получить доступ к тому же ресурсу или ПО в следующий раз. Многие хакеры размещают «прослушивающий» бэкдор, с помощью которого можно подключиться вновь. В других случаях это означает взлом паролей или создание новых учетных записей. Злоумышленник всегда может использовать те же эксплойты, которые успешно отработали в прошлый раз, чтобы снова взломать систему, но обычно применяет другой метод, который будет работать, даже если жертва исправляет уязвимость.

Разведка системы

Чаще всего, как только хакер проник в систему, он начинает выполнять команды или программы, чтобы узнать больше о цели, к которой получен доступ, и о том, что с ней связано. Обычно это означает поиск в оперативной памяти, файлов на жестком диске, сетевых подключений, общих ресурсов, служб и программ. Эта информация используется для лучшего понимания цели, а также для планирования следующей атаки.

Перемещение

Это редкая разновидность атаки или вредоносного воздействия, применяемого для взлома определенной цели. Почти все хакеры и вредоносные программы хотят подчинить себе как можно больше. Как только они получают доступ к первоначальной цели, распространение их влияния в пределах одной сети или объекта упрощается. Методы проникновения хакеров, перечисленные в этой главе, суммируют различные способы, которыми они могут это сделать, но, сравнивая их с первоначальными усилиями, последующее перемещение облегчается. Если атакующий движется к другим подобным целям, это называется боковым перемещением. Если злоумышленник переходит с устройств с одной привилегией на более высокую или более низкую, это называется вертикальным перемещением.

Большинство атакующих переходят от низких уровней к высоким, используя методы вертикального перемещения (опять же, реализуя методы хакерского проникновения, с которыми мы познакомились). После проникновения они ищут пароли от учетной записи локального администратора. Затем, если эти учетные данные совместно используются несколькими компьютерами (что часто бывает), они перемещаются горизонтально и повторяют процесс, пока не смогут получить доступ к самым привилегированным учетным записям. Иногда это делается во время первого взлома, так как авторизованный пользователь или система уже имеет очень высокие привилегии. Затем они перемещаются на сервер аутентификации и считывают учетные данные каждого пользователя. Это стандартный алгоритм для большинства современных хакерских атак, и переход от первоначального взлома к полному овладению сетью может занять менее часа.

Как хакеру средней руки, мне обычно требуется около часа, чтобы проникнуть, и еще час, чтобы захватить централизованную базу данных аутентификации. Так что на захват сети компании в среднем уходит около двух часов. Самое долгое проникновение заняло у меня три часа.

Участие инсайдеров, партнеров, консультантов, производителей и других третьих лиц

Даже если ваша сеть и ее компьютеры совершенны (что едва ли возможно), вы можете быть скомпрометированы дефектом в системе подключенного партнера или инсайдером. Эта категория довольно широка и пересекается с рядом других хакерских методов.

Выполнение запланированного действия

После формирования лазеек и установки прав собственности на файлы хакеры выполняют то, что намеревались сделать (если только действие взлома не выявило новые задачи). У каждого хакера есть цель. Официальный пентестер заключает договор на выполнение одной или нескольких процедур. Злоумышленник может распространять вредоносное ПО, читать или красть конфиденциальную информацию, вносить вредоносные изменения и причинять иной вред. Цель хакера, желающего скомпрометировать одну или несколько систем, – что-то с ней сделать. Давным-давно (два или три десятилетия назад) целью хакеров было просто продемонстрировать, что они взломали систему. Сегодня 99 % взломов криминально мотивированы, и хакер собирается сделать что-то вредоносное для цели (даже если единственный ущерб, который он наносит, это скрытное проникновение для потенциальных действий). Несанкционированный доступ без прямого ущерба – это все равно ущерб.

Заметание следов

Некоторые хакеры пытаются замести следы. Раньше это делали почти все, но в наши дни компьютерные системы настолько сложны и присутствуют в таком количестве, что большинство владельцев данных не проверяют хакерские следы. Они не проверяют логи, не ищут НИКАКИХ признаков незаконного проникновения, если те не бросаются в глаза. Каждый год отчет компании Verizon о расследованиях случаев несанкционированного доступа к данным **(https://www.verizon.com/business/resources/reports/dbir/)** сообщает, что большинство атакующих остаются незамеченными в течение нескольких месяцев или даже лет, а более 80 % атак были бы замечены, если бы специалисты по ИБ потрудились над анализом. Из-за такой статистики большинство хакеров уже не утруждают себя заметанием следов.

Хакеры сегодня еще меньше стремятся к этому, потому что используют методы, которые невозможно обнаружить традиционными способами. Или действия хакера настолько распространены в среде жертвы, что практически нельзя отличить легитимную деятельность от незаконной. Например, после взлома хакер обычно выполняет действия в контексте безопасности законного пользователя, часто получая доступ к тем же серверам и службам, что и последний. И они используют те же инструменты (например, программное обеспечение удаленного доступа и сценарии), что и администраторы. Кто может определить, что злонамеренно, а что нет? Области обнаружения вторжений рассматриваются в главе 14.

Взлом скучно успешен

Если вы хотите знать, как хакеры взламывают, то обратились по адресу. Единственное, что осталось сделать, это добавить инструменты, любопытство и настойчивость. Процесс взлома настолько успешен, что многие пентестеры после первоначального восторга от профессионального хакинга через несколько лет впадают в уныние и меняют сферу деятельности. Понимаете, насколько хорошо отработан процесс? Вот почему специалистам по ИБ нужно бороться с хакерами.

Автоматизированная вредоносная программа как инструмент взлома

Вредоносная программа может выполнять один или несколько шагов в автоматическом режиме или передать хакеру управление, как только цель достигнута. Большинство хакерских групп сочетают социальную инженерию, автоматизированное вредоносное ПО и действия самих хакеров для достижения целей. В больших группах отдельным хакерам могут назначаться роли и должности. Вредоносная программа может выполнить один шаг проникновения и достигнуть успеха, не пытаясь осуществить любой из других шагов. Например, самая быстрая вредоносная программа в истории, SQL Slammer, имела размер всего 376 байт. Она выполняла задачу по переполнению буфера на UDP-порте SQL 1434 независимо от того, был ли на целевом устройстве

запущен SQL. Поскольку на большинстве компьютеров он не выполняется, можно подумать, что атака будет весьма неэффективна. Но нет, за 10 минут этот червь изменил мир. Ни одна вредоносная программа никогда даже не приближалась к заражению такого количества устройств за столь короткое время.

Примечание. Если я пропустил какой-то шаг в хакерской методологии или способ проникновения, прошу прощения. С другой стороны, я же предупреждал, что я ничем не примечательный хакер.

Этика взлома

Я хотел бы думать, что мои читатели – этичные хакеры, которые проводят взлом своих целей законным образом. Взлом сайта, на который у вас нет предопределенных и выраженных полномочий, неэтичен и часто незаконен. Также неэтично (и даже незаконно) взломать сайт и сообщить владельцам о найденной уязвимости бесплатно. Неэтично и часто незаконно найти уязвимость, а затем попросить владельцев сайта нанять вас в качестве пентестера. Последнее происходит сплошь и рядом. Если вы сообщите кому-то, что нашли способ взломать его сайты или серверы, и попросите работу, это будет рассматриваться как вымогательство. Могу вас уверить, что почти все владельцы сайтов, получающие такой непрошеный совет, не задумаются о вашей пользе и не захотят вас нанимать. Они увидят в вас врага и передадут дело адвокатам.

Остальная часть книги посвящена описанию конкретных типов взлома, методов проникновения и способов противостояния им со стороны специалистов по ИБ. Если вы хотите зарабатывать на жизнь хакерством или бороться с хакерами, следует понять их методологию. Люди, упомянутые здесь, – гиганты в своей области, и вы можете многому у них научиться. Думаю, лучше всего начать с Брюса Шнайера, речь о котором пойдет в следующей главе. Многие считают его отцом современной компьютерной криптографии.

3. Профиль: Брюс Шнайер

Брюс Шнайер обладает столь большим опытом и знаниями, что при его упоминании многие люди используют словосочетание «светило индустрии» или называют его «отцом современной компьютерной криптографии». Однако интерес Шнайера не ограничивается шифрами, он уже давно задается более глобальными вопросами о том, почему в сфере информационной безопасности за все эти десятилетия произошло так мало улучшений. Поскольку он имеет авторитетное мнение по широкому кругу вопросов, связанных с ИБ, его часто приглашают в качестве эксперта на национальные телевизионные шоу. Несколько раз он даже выступал перед Конгрессом Соединенных Штатов. Шнайер пишет книги и ведет блоги, и я всегда считал ознакомление с его

работами получением неофициальной степени магистра в области информационной безопасности. Я и наполовину не был бы тем специалистом по ИБ, которым стал, без знаний, которые почерпнул у него. Он мой неофициальный наставник.

Шнайер известен тем, что говорит обезоруживающе простые вещи, которые заставляют пересмотреть старые догмы. Например, возьмем его фразу: «Если вы сосредоточены на SSL-атаках, значит, вы превосходите всех остальных экспертов в области ИБ». Это означает, что существует очень много других, часто более успешно эксплуатируемых уязвимостей, о которых стоит задуматься, поэтому, если вы действительно беспокоитесь об относительно редко используемом SSL-эксплойте, значит, уже устранили остальные, более вероятные и важные угрозы. Другими словами, мы должны расставить акценты среди мер обеспечения информационной безопасности, а не реагировать на каждую анонсированную уязвимость (которая, возможно, никогда не будет эксплуатироваться).

Он также говорил о том, что специалисты по ИБ часто расстраиваются, если сотрудники не относятся к парольной защите достаточно серьезно, используют слабые пароли (если это допустимо), применяют один и тот же на многих несвязанных веб-сайтах (словно умоляя о том, чтобы их взломали) и часто передают его друзьям, коллегам и даже незнакомым людям. Мы расстраиваемся по этому поводу, поскольку в отличие от рядовых сотрудников представляем возможные последствия для бизнеса. Согласно Шнайеру, конечный пользователь оценивает сложность паролей, исходя из степени риска лично для себя. Сотрудников редко увольняют за использование недостаточно надежных паролей. Даже если хакер украл деньги с банковского счета вкладчика, эти средства, как правило, немедленно возмещаются. Шнайер учит нас тому, что именно профессионалы в сфере ИБ не вполне адекватно оценивают риски. И пока вред не будет причинен конечному пользователю, они не изменят свое поведение. Каково это, быть специалистом по вопросам ИБ, а потом осознать, что рядовой пользователь оценивает риски лучше вас?

Шнайер написал более десятка книг, включая *«Прикладную криптография. Протоколы, алгоритмы и исходный код на С»*, написанную в 1996 году и вышедшую на русском языке[3]. Создав еще несколько трудов на тему криптографии (в том числе вместе с Нильсом Фергюсоном), он начал интересоваться причинами, по которым в сфере ИБ не наступало значимых улучшений. Результатом этого стала серия книг, каждая из которых посвящена причинам нетехнического характера, связанным с доверием, экономикой, социологией и т. д. Они наполнены простой для понимания теорией и подкреплены реальными примерами. Вот мои любимые книги Шнайера:

• *Secrets and Lies: Digital Security in a Networked World*[4] (**https://www.amazon.com/Secrets-Lies-Digital-Security-Networked/dp/0471453803**);

• *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (**https://www.amazon.com/Beyond-Fear-Thinking-Sensibly-Uncertain/dp/0387026207**);

• *Liars and Outliers: Enabling the Trust that Society Needs to Thrive* (**https://www.amazon.com/Liars-Outliers-Enabling-Society-Thrive/dp/1118143302**);

• *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (**https://www.amazon.com/Data-Goliath-Battles-Collect-Control/dp/039335217X**).

Если вы действительно хотите разобраться в сфере ИБ и ее проблемах, вам следует их прочитать. Также подпишитесь на блог Шнайера **(https://www.schneier.com/)** и ежемесячную рассылку канала Crypto-Gram **(https://www.schneier.com/crypto-gram/)**. Существует заметная разница между теми, кто регулярно читает Шнайера, и теми, кто этого не делает. Его манера письма понятна и интересна, и он рьяно борется с теми, кто продвигает неработающие методы обеспечения информационной безопасности. То, как он разоблачает криптомошенников, само по себе можно считать уроками по кибербезопасности. Он регулярно освещает самые актуальные вопросы в этой области.

На протяжении многих лет я несколько раз брал у Шнайера интервью, и иногда мне бывало страшновато. Не потому что он сложный или высокомерный собеседник (это не так), а потому что он часто позволяет интервьюеру рассуждать, опираясь на собственные убеждения и предположения. Если вы чего-то не понимаете или не согласны с ним, он не сразу отвергает ваш аргумент. Вместо этого Брюс задает вопрос за вопросом, позволяя вам самому прийти к выводу. В ходе интервью Шнайер всегда обучает собеседника. В процессе разговора становится ясно, что он обдумывал эти вопросы намного дольше, чем вы. Теперь я пытаюсь заимствовать кое-что из его техники самодопроса, когда обдумываю собственные глубоко укорененные убеждения.

Я спросил Шнайера о том, когда он впервые заинтересовался темой информационной безопасности, на что он ответил: «Я всегда интересовался математикой и секретными кодами – криптографией. Свою первую книгу, “Прикладная криптография”, я бы с удовольствием сам прочитал в свое время. Однако я понял, что технологии – это не самая большая проблема. Проблема в людях или интерфейсе, с которыми они взаимодействуют. Самые сложные проблемы ИБ связаны не с технологиями, а с социологическими, политическими и экономическими аспектами их применения. Я провожу много времени, думая о пользователях, склонных к риску. У нас есть технологии, чтобы защитить их, но можем ли мы создать такие решения, которые не помешают им делать свою работу? В противном случае мы просто не сможем убедить их использовать эти продукты».

Я спросил Шнайера, что он думает о недавних утечках информации из некоторых американских спецслужб. Он сказал: «В этих данных практически не содержалось того, о чем не знали люди, внимательно следящие за

происходящим. Обнародованные сведения были скорее подтверждением. Удивили подробности. Удивила секретность. Я не думаю, что мы смогли бы как-то повлиять на методы спецслужб, если бы знали о них больше, потому что после событий 11 сентября 2001 года любые их методы были бы одобрены. Так что, к сожалению, это не привело к серьезным изменениям, по крайней мере, сразу. Был принят один незначительный закон [запрещающий АНБ собирать метаданные о телефонных переговорах американцев]. Однако утечка спровоцировала публичное обсуждение проблемы, связанной с правительственной слежкой, что привело к изменению общественного мнения. Теперь люди знают и беспокоятся об этом. Может потребоваться еще десять лет, чтобы ощутить все последствия, но в итоге ситуация улучшится».

Я спросил Шнайера, что он считает самой большой проблемой в сфере компьютерной безопасности, и он ответил: «Корпоративная слежка! Корпорации хотят шпионить за людьми даже больше, чем правительства. Facebook[5] и Google следят за пользователями, нарушая их интересы, а ФБР может получить доступ к собранным ими данным, хотят того корпорации или нет. Следящий капитализм – вот фундаментальная проблема».

Я спросил Шнайера, над какой книгой он работает (он постоянно что-то пишет). Он рассказал: «Я обдумываю новую книгу, посвященную проблемам кибербезопасности, например связанным с Интернетом вещей и с тем, как все меняется, когда компьютеры действительно становятся опасными. Одно дело, если скомпрометированной оказывается уязвимая электронная таблица, и совсем другое, если речь идет о вашем автомобиле. Прорехи в системе защиты могут привести к человеческим жертвам. Это все меняет! В прошлом месяце я выступал в Конгрессе с докладом на эту тему. Я сказал, что игры кончились, и настало время для серьезной работы. Необходим контроль. На карту поставлены жизни людей! Мы не можем больше мириться со слабо защищенным и полным ошибок программным обеспечением. Но индустрия не готова осознать всю серьезность угрозы, хотя и должна. Как могут люди, работающие над улучшением системы безопасности автомобилей, на самом деле решить эту задачу, если нам до сих пор так и не удалось остановить хакеров и исправить все уязвимости? Необходимы перемены. И они произойдут».

Брюс Шнайер на протяжении нескольких десятилетий является одним из лидеров в области ИБ и остается ключевым участником самых важных дискуссий. Если вас интересует тема информационной безопасности, выберите его в качестве своего неофициального наставника.

Информация о Брюсе Шнайере

Более подробную информацию о Брюсе Шнайере смотрите по ссылкам:

• блог Брюса Шнайера: **https://www.schneier.com**;

• рассылка Брюса Шнайера *Crypto-Gram newsletter*: **https://www.schneier.com/crypto-gram/**;

• книги Брюса Шнайера: **https://www.amazon.com/Bruce-Schneier/e/B000AP7EVS/**.

4. Социальная инженерия

В компьютерном мире социальная инженерия – это методы побудить человека сделать что-то нехорошее для себя или других людей. Это одна из наиболее распространенных форм взлома, потому что часто успешна. И самая неприятная для специалистов по ИБ, потому что ее нельзя предотвратить только с помощью технологий.

Методы социальной инженерии

Социальная инженерия может быть реализована многими способами, в том числе через Интернет, по телефону, лично или посредством традиционной почты. Ее разновидностей так много, что нередко в списках, претендующих на полноту их перечисления, некоторые из видов или способов отсутствуют. Социальная инженерия, реализуемая с помощью компьютера, использует электронную почту или Интернет, а также службы обмена мгновенными сообщениями и компьютерные программы практически любого типа.

Фишинг

Распространенная цель социальной инженерии – перехват учетных данных пользователя в процессе так называемого фишинга. Фишинговые сообщения электронной почты или веб-сайты пытаются обмануть пользователя и заставить его указать свои реальные учетные данные для авторизации, имитируя легитимный веб-сайт или администратора-отправителя, с которым конечный пользователь знаком. Наиболее распространенная фишинговая атака – это электронное письмо якобы от администратора сайта, утверждающего, что учетные данные пользователя должны быть проверены, иначе доступ к сайту будет прекращен.

Целевой фишинг — это тип фишинга, который нацелен против конкретного человека или группы людей с применением непубличной информации, которой владеет цель атаки. Например, отправка сотрудникам документа по электронной почте якобы от участника проекта: при его открытии файл выполняет вредоносные команды. Целевой фишинг часто упоминается во многих самых громких корпоративных скандалах.

Троянский конь

Другой популярный прием социальной инженерии используется, чтобы заставить ничего не подозревающего конечного пользователя выполнить программу троянского коня. Она может быть отправлена по электронной почте, в виде файлового вложения или скачиваться по указанному в письме URL-адресу. Такой вредоносный код часто выполняется и на веб-сайтах. Легитимные сайты могут быть скомпрометированы, и когда пользователь загружает страницу, он видит инструкции по загрузке и запуску файла. Файл может быть

«необходимым» сторонним дополнением, поддельным антивирусным приложением или «обязательным» патчем. Может быть скомпрометирован как непосредственно сам легитимный веб-сайт, так и независимый элемент на нем, например сторонний рекламный баннер. В любом случае, у пользователя, который доверяет сайту после многих лет его посещения, нет оснований подозревать, что он мог быть скомпрометирован.

По телефону

Мошенники также звонят пользователям, которым может понадобиться техническая поддержка, от имени популярного разработчика, из государственного учреждения или компании.

Одна из самых популярных афер по телефону – когда мошенник звонит якобы от лица техподдержки, утверждая, что на компьютере пользователя была обнаружена вредоносная программа. Затем он просит загрузить «антивирусную» программу, которая, что неудивительно, обнаруживает множество вредоносных объектов. Мошенник побуждает загрузить и выполнить программу удаленного доступа, которую затем использует для авторизации на компьютере жертвы, чтобы внедрить другое вредоносное ПО. Фиктивные программы технической поддержки достигают кульминации, когда жертва покупает поддельные программы защиты, используя номер своей банковской карты.

Телефонные мошенники также могут представляться сотрудниками налоговой службы, правоохранительных органов и прочих государственных структур, стремясь получить деньги за то, чтобы конечный пользователь избежал якобы наложенных на него жестких штрафов или тюрьмы.

Мошенничество

Мошенничество – еще одна очень популярная афера, которая осуществляется с людьми, покупающими или продающими товары на веб-сайтах, таких как аукционы или ресурсы, подобные Craigslist.

При мошеннической операции покупатель быстро отвечает, обычно предлагает оплатить полную стоимость покупки плюс доставку и просит продавца использовать своих «доверенных» эскроу-агентов (посредников). Затем они посылают жертве поддельный чек на бóльшую сумму, нежели та, что была оговорена, и жертва возмещает излишек на счет злоумышленников (к сожалению, банки принимают поддельные чеки, но в итоге жертва теряет деньги). Покупатель просит потерпевшего продавца вернуть уплаченный излишек грузоотправителю по договору или посреднику. Жертва мошенничества обычно теряет как минимум сумму излишка.

При мошеннической продаже потерпевший покупатель отправляет средства, но не получает товар[6]. В среднем в случае такой продажи жертвы теряют суммы в пределах тысячи долларов. В некоторых случаях сумма ущерба может достигать десятков тысяч.

Личное участие

Некоторые из самых известных афер социальной инженерии были выполнены хакерами лично. В следующей главе речь пойдет об известном хакере Кевине Митнике. Десятилетия назад он был одним из самых наглых социальных инженеров в «черной шляпе». Митник переодевался в мастера по ремонту телефонов или сервисного инженера, чтобы получить доступ в защищенное помещение. Такие мошенники известны походами в банки и установкой специальных устройств на терминалах сотрудников, выдавая себя за системных администраторов. Каким бы недоверчивым ни был человек, он обычно доверяет людям, осуществляющим ремонт оборудования, особенно если слышат фразу типа: «Я слышал, что ваш компьютер стал работать медленнее в последнее время». Кто может опровергнуть это утверждение? Человек, выполняющий ремонт, очевидно, знает о проблеме и, наконец, пришел ее исправить.

Кнут или пряник

Конечному пользователю часто угрожают штрафом за то, что он чего-то не сделает, или обещают вознаграждение за то, что он совершит некие действия. Хитрость начинается с принуждения жертвы, так как люди недостаточно тщательно взвешивают риск в стрессовой ситуации. Они должны либо заплатить штраф, либо сесть в тюрьму. Перед ними встает выбор – запустить программу или рисковать, что компьютер останется зараженным, а банковский счет опустеет; отправить деньги или некий честный человек останется в иностранной тюрьме; изменить пароль на компьютере начальника или быть уволенным.

Один из моих любимых приемов социальной инженерии в процессе тестирования системы – отправить письмо сотрудникам компании от имени генерального или финансового директора с объявлением о том, что компания сливается с конкурирующей организацией. Я предлагаю открыть вложенный документ, чтобы они увидели, как слияние повлияет на их работу. Или я отправляю письмо сотрудникам-мужчинам якобы от адвоката их бывшей жены с просьбой о дополнительных алиментах для ребенка. Вы будете поражены, насколько успешны эти трюки.

Защита от социальной инженерии

Защита от атак социальной инженерии требует сочетания обучения и технологий.

Обучение

Обучение противостоянию социальной инженерии – одно из лучших, наиболее важных средств защиты. Обучение должно включать примеры наиболее распространенных видов социальной инженерии и того, как потенциальные жертвы могут обнаружить признаки нелегитимности. В моей нынешней компании каждый сотрудник смотрит видеоролик о защите от социальной инженерии каждый год, а затем проходит короткий тест. Наиболее успешные тренинги посещали очень умные, надежные и хорошо зарекомендовавшие себя

сотрудники, которые делятся личным опытом применения методов социальной инженерии.

Я думаю, что в каждой компании должны имитироваться фишинговые атаки, в ходе которых работникам отправляются поддельные электронные письма с запросом ввода персональных данных. Сотрудники, предоставившие свои данные, должны пройти дополнительное обучение. Существуют различные ресурсы, как бесплатные, так и коммерческие, для проведения поддельных фишинговых кампаний. Платные, на мой взгляд, наиболее просты и удобны.

Все компьютерные пользователи должны быть обучены тактике защиты от социальной инженерии. Люди, покупающие и продающие товары в Интернете, должны быть осведомлены о мошенничествах в сфере торговли. Необходимо использовать только безопасные сделки и следовать всем рекомендациям проверенных сайтов.

Будьте осторожны при установке ПО со сторонних веб-сайтов

Пользователей следует научить никогда не устанавливать какое-либо программное обеспечение непосредственно с сайта, который они посещают, если это не сайт легитимного разработчика ПО. Если веб-сайт сообщает, что вам нужно установить какое-то программное обеспечение, чтобы продолжить просмотр ресурса, и вы думаете, что это законный запрос, покиньте его и перейдите на сайт разработчика стороннего программного обеспечения, чтобы наверняка установить корректное приложение. Никогда не устанавливайте ПО с чужого веб-сайта, а не с сайта непосредственного разработчика[7]. Программное обеспечение может оказаться легитимным, но риск слишком велик.

Цифровые сертификаты с расширенной проверкой

Веб-серферам следует научиться применять цифровые сертификаты с расширенной
проверкой **(https://ru.wikipedia.org/wiki/Сертификат_Extended_Validation)** на многих самых популярных сайтах. Веб-сайты с расширенной проверкой часто каким-либо образом выделяются (обычно это выделенное зеленым цветом доменное имя, значок в адресной строке или сама адресная строка), чтобы подтвердить пользователю, что URL-адрес и безопасность сайта были подтверждены доверенной третьей стороной. Для примера расширенной проверки перейдите на **https://www.bankofamerica.com/**.

Избавьтесь от паролей

Фишинг не сработает, если сотрудник не сможет предоставить свои учетные данные для авторизации. Простые логины с паролями уходят в прошлое с распространением двухфакторной аутентификации (2FA), цифровых сертификатов, устройств авторизации, аутентификации по внешнему каналу и других методов входа в систему, которые не подвержены фишингу.

Технологии против социальной инженерии

Большинство решений для защиты от вредоносных программ, веб-фильтров и антиспам-модулей пытаются свести к минимуму риск атаки компьютеров путем социальной инженерии. Антивирусное ПО предупреждает запуск вредоносных файлов. Веб-фильтр может определить вредоносные сайты и заблокировать их, если браузер посетителя пытается загрузить фишинговую страницу. А решения по борьбе со спамом по электронной почте отфильтровывают сообщения социальной инженерии. Однако технология никогда не будет эффективной на 100 %, поэтому обучение конечных пользователей и другие методы должны использоваться совместно.

Социальная инженерия – очень успешный метод взлома. Некоторые специалисты по ИБ скажут, что вы никогда не проведете обучение так, чтобы все сотрудники смогли ей противостоять. Они ошибаются. Сочетание полноценного обучения и правильных технологий может значительно снизить риск ущерба от методов социальной инженерии.

В следующей главе вы узнаете о специалисте по социальной инженерии Кевине Митнике. Его опыт в качестве хакера помог ему эффективно защищать своих клиентов на протяжении десятилетий.

5. Профиль: Кевин Митник

При разговоре о компьютерных хакерах большинство людей вспоминает Кевина Митника. В 1970-е, 1980-е и 1990-е годы он был *тем самым* хакером. Сочетая методы социальной инженерии с низкоуровневым анализом операционных систем, Митник проворачивал всевозможные возмутительные трюки, хотя причиненный им вред вряд ли может сравниться с масштабом ущерба, наносимого современными APT-атаками и программами-вымогателями.

Он и его «подвиги» были описаны в нескольких книгах, показаны в кино и даже породили своеобразную субкультуру приписывания ему всевозможных эксцентричных хакерских выходок, которых он никогда не совершал. Власти настолько боялись того, что одно слово Митника способно запустить ядерную ракету, что он стал единственным заключенным в США, которому пришлось отбывать наказание в одиночной камере без права доступа к телефону. Если вы когда-либо видели фильм, где главный герой говорит по телефону всего одно слово, которое запускает цепь ужасных киберсобытий, знайте, что эта сцена порождена паранойей, вызванной страхом перед Митником.

Я поместил историю о Кевине в начало этой книги, потому что после совершения множества киберпроступков он посвятил свою жизнь борьбе с компьютерными преступлениями и стал одним из немногих исправившихся «черных шляп», которым я полностью доверяю. Митник написал несколько книг по информационной безопасности **(https://www.amazon.com/Kevin-D-**

Mitnick/e/B001IO9WEW), работает с разными компаниями (в том числе с KnowBe4), управляет собственной консалтинговой фирмой (Mitnick Security Consulting) и стал самым востребованным из известных мне лекторов в сфере ИБ. Он также принимал участие в программе The Colbert Report и даже появлялся в телевизионном шоу Alias. Благодаря Митнику была осознана роль методов социальной инженерии в хакинге и важность защиты от них. В конце концов, если вы хотите остановить преступника, вам не помешает поучиться у того, кто когда-то им был.

Когда я спросил Митника о том, что вызвало у него интерес к хакерству, он сказал: «В детстве я любил магию. Один парень из моей школы показал мне разные трюки с телефоном, в частности, научил тому, как бесплатно звонить по межгороду, как узнать чей-то адрес при помощи одного лишь номера телефона, как переадресовывать звонки и т. д. Он заходил в телефонную будку, набирал номер [телефонной компании], представлялся кем-то другим – и происходило чудо. Тогда я впервые узнал о социальной инженерии, которая показалась мне настоящим волшебством. Я не знал, как это называется. Я знал лишь то, что это весело и интересно, и это захватывало меня все сильнее. Я тратил на это все свое время. Мне наскучила школа, и поскольку по ночам, вместо того чтобы спать, я занимался фрикингом, моя успеваемость начала стремительно ухудшаться».

Я спросил, что думали родители о его хакерских «подвигах». Он ответил: «Ну, поначалу они ничего не знали. Может быть, просто думали, что я вытворяю с телефоном что-то сомнительное. Но моя мать, должно быть, считала, что самое страшное, что можно сделать с телефоном, – это кого-нибудь разозлить. Однако они понятия не имели, чем именно я занимаюсь, пока мама не получила официальное письмо из компании AT&T, уведомляющее об отключении телефонной связи. Она была очень расстроена. Как вы понимаете, это было задолго до появления сотовых телефонов. Домашний стационарный телефон был единственным средством связи. Я попросил ее успокоиться и пообещал все исправить.

С помощью все той же социальной инженерии я восстановил дома телефонную связь. Мы жили в доме № 13. Я позвонил в отдел продаж телефонной компании, представившись жителем дома № 13 “Б”. После трехдневного ожидания, необходимого для регистрации нового адреса в системе, я позвонил в отдел технического обслуживания и попросил установить новый телефон в этом доме. Я даже сходил в магазин и купил там букву Б, чтобы повесить ее на дверь. В ходе телефонного разговора я выдал себя за нового клиента по имени Джим Бонд из Англии. Я сообщил настоящий номер телефона в Англии, который нашел вместе с другой личной информацией, потому что знал, что они не смогут проверить сведения об иностранце. Затем спросил, могу ли я выбрать “красивый номер”, мне дали добро, и я выбрал номер телефона, заканчивающийся на 007. В конце разговора я спросил, можно ли мне использовать сокращение Джим, или им необходимо мое полное имя. Они попросили назвать полное имя, и я сказал, что меня зовут Джеймс. Итак, я был зарегистрирован в AT&T как Джеймс Бонд с номером телефона,

заканчивающимся на 007, а у моей матери снова появилась телефонная связь. Представители компании AT&T были в бешенстве, когда моя схема была раскрыта».

В тот момент я понял, что за все интервью он ни разу не упомянул о взломе компьютерных систем. Он говорил только о злоупотреблении телефоном. Я спросил, что подвигло его заняться взломом компьютеров. Он ответил: «Один парень из моей школы узнал, что я занимаюсь телефонным фрикингом, и подумал, что меня заинтересует новый школьный факультатив с углубленным изучением компьютерных наук. Сначала я сказал, что это не мое, но он возразил: “Знаешь, я слышал, телефонные компании начинают использовать компьютеры”. Мне этого было достаточно. Я должен был разобраться в этой теме.

Пришлось пойти к преподавателю, мистеру Крису, и спросить его, могу ли я записаться на факультатив, потому что у меня не было необходимой подготовки (которая тогда предполагала углубленное изучение математики и физики). Кроме того, моя успеваемость ухудшилась из-за постоянного недосыпа. Мистер Крис не хотел меня принимать; тогда я продемонстрировал ему свои навыки фрикинга, назвав его телефонный номер, который не был указан в справочнике, а также номера его детей. Он сказал: “Это волшебство!” и принял меня в группу.

Нашей первой задачей было написание программы на языке Fortran для вычисления последовательности Фибоначчи, которая показалась мне слишком скучной. Я пошел в местный университет в Нортридже и попытался получить доступ к компьютеру. Там использовались те же компьютеры и операционная система, но мне не разрешали проводить за ними более пяти минут. Я попросил руководителя компьютерной лаборатории дать мне больше времени. Он сказал, что я не студент колледжа и вообще не должен там находиться, однако он видел мою заинтересованность в компьютерах, и, чтобы поощрить ее, дал мне для практики логин и пароль своей личной учетной записи. Представляете? Вот так в те дни обращались с компьютерами.

В итоге я узнал о низкоуровневых вызовах операционной системы. На школьном факультативе мы это не изучали. В школе мы все использовали один модем, подключенный к телефонной трубке и акустическому соединителю. Он работал постоянно, и все по очереди вводили свои логины и пароли для получения доступа к терминалу и модему. Я написал низкоуровневую программу, которая оставалась активной в фоновом режиме и записывала все нажатия клавиш.

Настал день, когда ученики мистера Криса должны были показать ему, сколько чисел Фибоначчи вычислили их программы; у меня не было ничего. Мистер Крис отчитал меня перед классом, напомнив о том, как он, на свой страх и риск, разрешил мне посещать занятия, а теперь я даже ничего не могу ему показать. Все присутствующие смотрели на меня. И тогда я сказал: “Вообще-то, я был слишком занят написанием программы для взлома паролей. Ваш пароль – johnco”. Он спросил: “Как ты это сделал?” Я объяснил ему, и он поздравил

меня, объявив всему классу о том, что я компьютерный гений. Он совсем не рассердился. Возможно, это был очень плохой урок для меня с точки зрения этики».

Я спросил Митника, что, по его мнению, стоит делать родителям, если они заметили признаки того, что их ребенок занимается вредоносным хакерством. Вот что он посоветовал: «Покажите им законные способы занятия хакерством. Направьте интерес на такие законные и этичные занятия, как посещение конференций по информационной безопасности и участие в конкурсах типа “захват флага”. Родителю стоит бросить ребенку вызов, сказав что-то вроде: “Итак, ты думаешь, что достаточно хорош, чтобы победить в соревновании по захвату флага?” Таким образом родитель применит к ребенку метод социальной инженерии, а тот получит удовольствие от хакерства, не нарушая при этом закон. Например, сегодня я легально взломал корпоративную сеть, и это показалось мне не менее захватывающим, чем те неэтичные и противозаконные вещи, которыми я когда-то занимался. Хотел бы я, чтобы в мое время существовали те законные способы взлома, которые есть сейчас. Жаль, что я не могу вернуться и все исправить. Знаете, чем отличается незаконный взлом от законного? Написанием отчета!»

Я спросил, как Митник, обладающий жизненным опытом «по обе стороны забора», относится к тому, что правительство считает себя вправе следить за частной жизнью граждан. Вот что он на это сказал: «Я думаю, мы все имеем право на частную жизнь. Моя последняя книга “*Искусство быть невидимым*” **(https://book24.ru/product/iskusstvo-byt-nevidimym-kak-sokhranit-privatnost-v-epokhu-big-data-5255267/)** как раз о том, как человек может сохранить тайну своей частной жизни. Я думаю, очень трудно сохранять приватность, если вами интересуется кто-то вроде АНБ или правительства, обладающих неограниченными средствами. Если они не могут взломать ваши зашифрованные сообщения, то могут просто использовать одну из многих известных им уязвимостей нулевого дня и взломать ваш компьютер, либо купить такую уязвимость. За 1,5 млн долларов можно купить уязвимость нулевого дня в системе Apple, за полмиллиона – брешь в системе Android и так далее. Если у вас есть средства и ресурсы, вы получите необходимую информацию. В той книге я написал, что владею способом, который позволяет защититься даже от них, но его сложно осуществить и он включает в себя много шагов. Однако я думаю, что это все-таки можно провернуть таким образом, что даже АНБ и любому правительству будет трудно до вас добраться. Я понимаю, что в определенных случаях правительство должно обладать информацией, например когда речь идет о терроризме, но они хотят видеть и слышать всех и вся. И если за вами наблюдают, вы меняете свое поведение, а это означает ограничение свободы. Я не думаю, что свобода возможна без конфиденциальности».

В конце интервью я напомнил Митнику о том, что мы уже встречались на конференции по вопросам ИБ много лет назад, где он собирался выступить в качестве главного докладчика. Проходя мимо, он сказал, что ему нужен USB-накопитель, чтобы перенести свою презентацию на компьютер, находящийся на

сцене. У меня был один в кармане, и я предложил его. Кевин уже собирался взять флешку, но, подумав пару секунд, отказался, заявив, что не доверяет чужим USB-ключам. Несколько человек, стоявших поблизости, посмеялись над его паранойей. В конце концов, USB-устройство не может быть вредоносным. Так, по крайней мере, все тогда считали.

Никто, правда, не знал, что я обнаружил способ автоматического запуска любой программы с любого портативного носителя (используя трюк со скрытым файлом *desktop.ini*, который позднее использовала вредоносная программа Stuxnet), и предложенный мною USB-накопитель как раз содержал демонстрационную версию этого эксплойта. Я не намеревался заражать систему Митника. Просто в то время этот эксплойт был на всех моих USB-накопителях, включая тот, который я предложил ему.

Паранойя Митника уберегла его от обнаруженной мною уязвимости нулевого дня. Этот пример также показывает, насколько трудно обмануть профессионального социального инженера, по-прежнему находящегося на пике формы.

Информация о Кевине Митнике

Более подробно познакомиться с историей Кевина Митника можно по ссылкам:

• официальный сайт Кевина Митника**: https://www.mitnicksecurity.com/**;

• *«Призрак в Сети. Мемуары величайшего хакера»:* **https://book24.ru/product/prizrak-v-seti-memuary-velichayshego-khakera-180793/**;

• *«Искусство быть невидимым»:* **https://book24.ru/product/iskusstvo-byt-nevidimym-kak-sokhranit-privatnost-v-epokhu-big-data-5255267/**;

• *The Art of Deception*: **https://www.amazon.com/Art-Deception-Controlling-Element-Security/dp/076454280X/**;

• *«Искусство вторжения»:* **https://www.amazon.com/Art-Intrusion-Exploits-Intruders-Deceivers/dp/0471782661/**;

• тренинг Кевина Митника, посвященный вопросам ИБ: **https://www.knowbe4.com/products/kevin-mitnick-security-awareness-training/**;

• интервью с Кевином Митником: **https://news.slashdot.org/story/11/09/12/1234252/Kevin-Mitnick-Answers**.

6. Уязвимости программного обеспечения

Уязвимости программного обеспечения – слабые места (т. е. ошибки), которые появляются из-за недостатков, внесенных разработчиком или присущих языку

программирования. Не каждый баг – это уязвимость. Ошибка должна быть доступна злоумышленнику, чтобы стать угрозой или риском. Большинство программных ошибок вызывают проблемы в работе (которые могут и не проявляться непосредственно у пользователя) или даже приводят к фатальному прерыванию работы, но не могут быть использованы злоумышленником для получения несанкционированного доступа к системе.

Уязвимые места в ПО ответственны за большой (если не подавляющий) процент взломов в настоящее время, несмотря на то что другие методы взлома (такие как троянские программы и социальная инженерия) зачастую весьма конкурентоспособны. Некоторые эксперты по ИБ считают, что большинство проблем исчезнут, если все программы будут написаны без ошибок. Тем не менее, даже если это не панацея, более надежный код с меньшим количеством уязвимостей сведет на нет значительную часть хакерских проблем и сделает компьютерную среду существенно безопаснее.

Количество уязвимостей программного обеспечения

Существует множество источников для отслеживания уязвимостей общедоступного ПО, хотя список ошибок для каждого из них может существенно отличаться. В среднем каждый год крупные разработчики программного обеспечения и баг-файндеры объявляют о 5–6 тысячах новых уязвимостей ПО, то есть около 15 находках ежедневно. Организация Common Vulnerabilities and Exposures **(https://cve.mitre.org/)** и публикуемая ею база данных общеизвестных уязвимостей информационной безопасности **(https://cve.mitre.org/data/downloads/index.html)** считаются инклюзивными, надежными и независимыми источниками и хорошо подходят для отчетности и отслеживания общедоступных уязвимостей. Многие другие разработчики отслеживают либо собственные уязвимости, либо все известные. Прочитайте отчет Microsoft Security Intelligence **(https://www.microsoft.com/ru-ru/security/business/security-intelligence-report)**, чтобы узнать последние цифры и результаты анализа.

Конечно, это всего лишь ошибки, о которых узнает общественность. Многие разработчики не объявляют о каждой из них. Многие не обнародуют ошибки, найденные внутренними ресурсами или исправленные в предрелизном программном обеспечении. Хотя невозможно это подтвердить, большинство экспертов считают, что реальное количество ошибок значительно выше, чем общеизвестные числа.

Примечание. Количество уязвимостей ПО – это только один из аспектов, а не полная картина безопасности программы или системы в целом. Единственное, что действительно имеет значение, – какой урон был нанесен уязвимостями программного обеспечения. Количество таких уязвимостей, вероятно, войдет в историю как объем ущерба, хотя в целом использовать более безопасные программы будет лучше для всех.

Почему уязвимости ПО – по-прежнему большая проблема?

В наши дни разработчики часто исправляют наиболее важные уязвимости в течение нескольких часов или дней. Почему же уязвимости программного обеспечения остаются существенной проблемой, особенно когда большинство приложений и устройств имеют механизмы автоматического обновления для более быстрого применения патчей? Дело в том, что большая часть компьютерных устройств патчится с сильным опозданием или, в значительной части случаев, не обновляется вообще. И каждая «дыра» способна привести к неожиданной проблеме в работе, иногда вызывая больше разочарования у конечного пользователя, чем сам факт наличия уязвимости.

Общее количество эксплойтов довольно велико и постоянно. Значительная часть ресурсов компьютерного администрирования тратится на исправление ошибок. Это невероятная трата времени, денег и других ресурсов, которые лучше пустить на более продуктивные вещи. Даже когда пользователи и администраторы исправляют ошибки, со временем, когда разработчик допускает новую, хакер может ею воспользоваться до того, как пользователь закроет ее патчем. Если я терпеливый и настойчивый хакер, преследующий определенные цели, то могу просто подождать, пока разработчик не оповестит о новой ошибке, и использовать ее для достижения своей цели.

Когда разработчики выпускают патчи, «белые шляпы» и «черные шляпы» немедленно анализируют их, чтобы найти целевую уязвимость. Затем они создают эксплойты, которые могут ее эксплуатировать. Существуют десятки коммерческих компаний, несколько бесплатных сервисов и неизвестное количество хакеров, которые делают это каждый день. Вы можете приобрести и/или загрузить сканеры уязвимостей, которые будут сканировать устройства и сообщать о незакрытых уязвимостях. Эти сканеры часто содержат тысячи и тысячи эксплойтов. Есть много хакерских веб-сайтов по всему миру с тысячами отдельных эксплойтов, которые вы можете скачать, чтобы эксплуатировать определенную уязвимость. Один из самых популярных бесплатных инструментов – это Metasploit **(https://www.metasploit.com/)**.

Защита от уязвимостей программного обеспечения

Защита от уязвимостей ПО номер один – это квалифицированные разработчики и более безопасные языки программирования.

Жизненный цикл безопасной разработки

Процесс, преследующий цель уменьшить число уязвимостей программного обеспечения, теперь широко известен как жизненный цикл безопасной разработки. Он сосредоточивается на каждом компоненте в жизненном цикле

программы ПО, от ее начального создания к исправлению недавно найденных уязвимостей, чтобы реализовать более безопасное программное обеспечение. Компания Microsoft Corporation, вероятно, лучше всего потрудилась в этой области и опубликовала больше свободно доступной информации и инструментов (**https://www.microsoft.com/en-us/securityengineering/sdl/)**, чем любой другой источник. Человеческий фактор гарантирует, что программный код всегда будет иметь эксплуатируемые ошибки, но, следуя жизненному циклу безопасной разработки, мы можем допускать меньше ошибок на то же количество строк кода.

Примечание. Доктор Даниэль Бернштейн **(https://en.wikipedia.org/wiki/Daniel_J._Bernstein**) – профессор в колледже, который пишет и продвигает невероятно безопасный код. Он создал несколько бесплатных и широко используемых программ, таких как dbjdns и qmail, в которых крайне мало ошибок. Он даже платит за найденные баги из собственного кармана. Даниэль верит, что разработчикам становится стыдно, когда он публично объявляет об ошибках, прежде чем предоставить разработчикам возможность анализировать и исправлять свои продукты.

Более безопасные языки программирования

Менее опасные программы не могут быть написаны без более безопасного языка программирования. На протяжении многих лет большинство разработчиков языков программирования стремились создать более безопасные версии с целью уменьшить или устранить распространенные причины ошибок. Несмотря на положительный результат, программы, написанные на них, значительно сложнее использовать, чем те, которые разработаны на небезопасных языках.

Анализ кода и программы

После разработки версии программы ее всегда следует анализировать на отсутствие известных и распознаваемых ошибок. Это можно сделать вручную или с помощью программных средств. Анализ вручную, как правило, наименее эффективен, так как обнаруживает наименьшее количество ошибок в час, но он чаще находит эксплуатируемые ошибки, которые нельзя отыскать с помощью программы. Программные средства поиска ошибок часто называют «статическими анализаторами» или инструментами «фаззинг-тестирования». Они проверяют исходный код (или программы) на наличие известных программных ошибок в самом коде. Фаззинг-анализаторы вводят случайные (или неправильные, неожиданные) данные и ищут уязвимости в программе во время выполнения. Многие печально известные специалисты, ищущие уязвимости ПО, включая Чарли Миллера, о котором мы поговорим в главе 36, полагались на фаззинг-тестирование во многих своих открытиях.

Более безопасные операционные системы

Большинство операционных систем не только создаются программистами с учетом жизненного цикла безопасной разработки и более безопасных языков

программирования, но и включают встроенные средства защиты от распространенных эксплойтов. Большинство современных популярных ОС включают специально разработанные средства защиты памяти и наиболее важных областей операционной системы. Некоторые из них даже включают встроенные инструменты для предотвращения переполнения буфера, защиты от вредоносных программ, каждый из которых помогает ограничить эксплуатируемые ошибки или уменьшить последующий ущерб.

Сторонние средства защиты и надстройки разработчиков

Существуют тысячи программ, которые могут защищать компьютерную систему от ранее неизвестных уязвимостей ПО, по крайней мере, с некоторым успехом. Определенные из них предлагаются в качестве бесплатных или платных дополнений самим разработчиком, а другие – независимыми третьими сторонами. Программы, которые обещают обнаружить и остановить новые эксплойты, очень распространены и могут значительно снизить риск реализации новых угроз, хотя их нельзя назвать совершенными. Один из моих любимых способов защиты ПО заключается в «контроле приложений» или формировании «белых списков» программ. Такой способ не закроет существующий эксплойт, но может предотвратить или уменьшить потенциальный ущерб от действий хакера или вредоносной программы.

Идеальное программное обеспечение не решит все проблемы

Никакая защита не сравнится с ПО, которое изначально разрабатывается с учетом средств защиты и исключением ошибок. Тем не менее идеальное, безошибочное программное обеспечение не решит все проблемы. К сожалению, его уязвимости не единственная наша проблема. Троянские программы срабатывают только потому, что их запускает сам пользователь. Многие хакеры и вредоносные программы используют типичные, часто легитимные возможности данных, языков программирования и других компонентов, чтобы совершать злодеяния. А социальная инженерия может сделать то, на что не способно программное обеспечение. Тем не менее никто не спорит, что более безопасные программы не могут быть панацеей.

В следующих главах мы поговорим о двух экспертах, посвятивших свою жизнь совершенствованию ПО. Глава 7 посвящена Майклу Ховарду, который популяризировал более безопасные методы разработки, а глава 8 фокусируется на Гари Макгроу, одном из лучших специалистов по поиску уязвимостей в истории.

7. Профиль: Майкл Ховард

Майкл Ховард – отличный педагог и энергичный оратор, который за 20 лет работы в сфере ИБ не утратил ни грамма энтузиазма, которым заражает всех, кто с ним сталкивается. Обычно пары минут общения с Майклом достаточно, чтобы собеседник загорелся желанием сделать мир более безопасным с помощью нескольких строк кода. Он получил всемирное признание, написав книгу *Writing Secure Code* **(https://www.amazon.com/Writing-Secure-Code-Michael-Howard/dp/0735615888)** вместе с Дэвидом Лебланом. Кроме того, он сделал очень много для того, чтобы компания Microsoft стала приверженцем идеи безопасного программирования. Ховард родом из Новой Зеландии, но сейчас живет в Остине, штат Техас. Он стал соавтором нескольких книг по безопасному программированию и ведет собственный блог.

Примечание. Дэвид Леблан, в соавторстве с которым Ховард написал книгу *Writing Secure Code*, – еще один прогрессивный специалист по ИБ. Он значительно обезопасил пакет Microsoft Office и создал более безопасную модель браузера, которая в настоящее время используется компаниями Google, Adobe и Microsoft.

Я спросил Ховарда, как он пришел в сферу ИБ. Вот что он ответил: «Я работал над ранними версиями Windows NT в компании Microsoft. Отвечал за такие низкоуровневые аспекты, как контроль доступа, криптография и графические интерфейсы GINA (которые раньше использовались для авторизации в операционной системе Microsoft Windows и других сервисах аутентификации). Это заставило меня задуматься о безопасности как о функции. Примерно в 2000 году стало ясно, что встроенные в продукт защитные функции не делают его по-настоящему безопасным, поэтому мы должны сосредоточиться на разработке безопасных функций, а это совершенно другая дисциплина».

На мой вопрос об истории возникновения концепции SDL в компании Microsoft он сказал: «Со временем различные практики обеспечения безопасности, изученные командами разработчиков. NET Framework, Windows, Office и SQL Server, а также других продуктов, превратились в концепцию SDL (Security Development Lifecycle, жизненный цикл безопасной разработки). Эта концепция помогла популяризировать идею безопасного программирования, и во многом именно благодаря ей компании стали гораздо лучше защищать свое ПО».

Я спросил Ховарда, стала ли концепция SDL результатом совершенствования уже существовавшего подхода или чем-то абсолютно новым, на что он ответил: «Мы все опираемся на работу других людей, однако бóльшая часть концепции SDL – это результат экспериментов. То, что работает, остается, а то, что не работает или оказывается нецелесообразным, отбрасывается. Иногда я задаюсь вопросом о том, были ли те или иные академические модели опробованы в производственной среде со всеми ее дедлайнами, требованиями к производительности, сроками вывода продукта на рынок, экономическими соображениями, обеспечением обратной совместимости и т. д.

В то время было принято считать, что улучшение качества кода автоматически делает его более безопасным. Но я не видел никаких эмпирических доказательств этой идеи. Вы можете создать функциональный SQL-код, который проходит все функциональные тесты, но он может оказаться уязвим к SQL-инъекциям. Если вы никогда не сталкивались с ними, вы увидите перед собой лишь идеальный код, который делает то, что от него требуется. Безопасная система делает только то, что должна, и не более того, – небезопасной ее делает “дополнительная функциональность”, связанная с уязвимостью к SQL-инъекциям».

Когда я спросил о его роли во внедрении компанией Microsoft концепции SDL, Ховард сказал: «Этому способствовало сочетание различных вещей, над которыми помимо меня работало множество людей. Все началось в конце 2001 года, когда команда разработчиков. NET провела мероприятие, где обсуждались текущие проблемы безопасности и потенциальные риски. Благодаря ему мы многому научились и добавили множество новых средств защиты. Я помню, что для этого мероприятия было заказано несколько футболок с нанесенной на них датой конференции, правда, из-за начавшейся снежной бури ее пришлось отложить… Так что по иронии судьбы на мероприятии, посвященном повышению безопасности кода, мы все ходили в футболках с неправильной датой. Однако уроки, полученные в ходе этой конференции, в итоге были положены в основу концепции SDL. Публикация нашей с Дэвидом книги заставила многих людей задуматься о безопасности кода. В 2001 году система компании Microsoft подверглась множеству атак со стороны хакеров и вредоносных программ. Особенно серьезный ущерб нанесли черви Code Red и Nimda. Билл Гейтс спросил нас о природе уязвимостей в ПО и о том, почему мы до сих пор их не устранили. Будучи частью команды, с которой он встретился, я вручил ему раннюю копию книги *Writing Secure Code*, и после встречи он написал свою знаменитую заметку «*Надежные вычисления*» **(https://www.wired.com/2002/01/bill-gates-trustworthy-computing/)**, в которой упомянул нашу книгу, благодаря чему ее продажи выросли в разы! В итоге я перешел на работу во вновь созданное подразделение надежных вычислений Microsoft. После этого был проведен ряд аналогичных мероприятий, посвященных проблемам безопасности ОС Windows, SQL Server и многих других продуктов Microsoft. Все это способствовало проработке концепции SDL, которая обновляется практически ежегодно».

Я спросил, действительно ли он и компания Microsoft предоставили больше информации и инструментов, связанных с безопасным программированием, чем любая другая организация. Он сказал: «Однозначно да! Но что еще более важно, все эти инструменты и методы мы используем в своей производственной среде, ежедневно применяя их к миллионам строк кода. Это не отвлеченная теория. Это то, чем занимается одна из крупнейших компаний в мире. И она охотно делится своим наработками».

Я спросил, почему количество публично анонсируемых уязвимостей не сокращается, несмотря на то, что программисты все больше узнают о проблемах информационной безопасности. Вот что сказал Ховард: «Отчасти это связано с

появлением все большего количества программ, содержащих множество строк кода. Однако главная проблема заключается в том, что программистов все еще не обучают методам безопасного программирования, и они плохо осознают основные угрозы. Большинство образовательных программ не отвечают современным потребностям. На днях, просматривая учебную программу по информационной безопасности одного университета, я обратил внимание на то, что почти половина занятий посвящена низкоуровневым сетевым угрозам. Я не обнаружил лекций по обеспечению безопасности облака или безопасному программированию. Наши колледжи все еще выпускают программистов, которые мало что знают об информационной безопасности и разработке безопасного ПО, что довольно странно, учитывая то, что этим выпускникам предстоит создавать критически важные системы, подключенные к Интернету. Я до сих пор нахожу примитивные ошибки в коде других людей. Когда я демонстрирую им весьма распространенную проблему, связанную с повреждением памяти, или уязвимость к SQL-инъекции, на меня смотрят так, будто я совершил нечто невероятное. Программисты, знакомые с основами информационной безопасности, встречаются так редко, что я радуюсь, если кандидат хотя бы проявляет интерес к этой теме. Если программист внимательно слушает, когда я говорю о проблемах ИБ, это делает меня счастливым. Если человек заинтересован, мы можем научить его всему остальному. Но вы даже не представляете, скольким людям нет до этого никакого дела, и одна из главных причин в том, что их этому до сих пор не учат. Или учат, но не тем вещам, делая акцент на сетевой безопасности или каких-нибудь мелочах. Студентам подробно описывают принцип работы алгоритма RSA, но не объясняют, почему он должен использоваться, какие проблемы он решает и для каких целей подходит лучше всего. Умение правильно использовать инструмент для решения реальных проблем безопасности гораздо важнее понимания принципа его работы. Любой человек может разобраться в работе протокола, однако нам нужны люди, осознающие риски и думающие о решениях. Правда, существуют некоторые преподаватели и колледжи, которые придерживаются правильного подхода, например Мэтт Бишоп из Калифорнийского университета в Дэвисе. Он и другие неравнодушные преподаватели – настоящие герои».

Я спросил, что может сделать сам программист, учитывая то, что большинство колледжей недостаточно хорошо готовят студентов в этом отношении. Он посоветовал: «Постоянно учитесь. Я ежедневно выделяю час на учебу. Я читаю, пишу код и экспериментирую с чем-то новым. И занимаюсь этим на протяжении всей своей карьеры. Кроме того, если в вашем учебном заведении нет формального курса по информационной безопасности, разработайте собственную обучающую программу. Перейдите на сайт **https://cve.mitre.org/cve/** и внимательно прочитайте о недавно обнаруженных уязвимостях. Затем напишите код, содержащий одну из них, и подумайте, что нужно было сделать для предотвращения ее появления как на техническом уровне, так и на уровне процессов. Выясните, откуда взялась эта уязвимость и как именно попала в код. А затем используйте извлеченные уроки, чтобы предотвратить появление подобных ошибок в вашем собственном коде».

На вопрос о том, что могут сделать компании для создания более безопасного кода, помимо следования текущим принципам SDL и использования доступных инструментов, он ответил: «Сделайте так, чтобы программисты не только понимали теоретические основы, но и осознавали реальные угрозы. Кроме того, вам следует встроить процесс обеспечения безопасности в сам конвейер разработки ПО, чтобы плохой и небезопасный код не мог в него попасть. В Microsoft мы используем так называемые ворота качества. Хороший (не связанный с безопасностью) пример – это написание кода, который предполагает, что все IP-адреса состоят из четырех октетов. Это означает, что такой код никогда не будет работать в чистой среде IPv6. Этот код даже не сможет пройти проверку, поскольку специальный инструмент, работающий в автоматическом режиме, выявит проблему и предотвратит его сохранение в системе. Вот что мы подразумеваем под термином “ворота качества”. В целях обеспечения безопасности этот же подход можно применить для выявления уязвимостей к SQL-инъекциям, угроз, связанных с безопасностью памяти, и всего того, что вы не хотите видеть в своем коде.

Если бы меня попросили назвать несколько основных практик, связанных с обеспечением безопасности, то я выбрал бы следующие:

• разработчики должны приучить себя с недоверием относиться к входным данным и проверять их корректность, желательно с помощью протестированной и проверенной библиотеки. Если длина ожидаемого значения составляет всего 20 байт, ограничьте величину входных данных 20 байтами. Если вы ожидаете получить число, то убедитесь, что входное значение является именно числом, и так далее;

• разработчикам/архитекторам/менеджерам, отвечающим за создание ПО, необходимо освоить методы моделирования угроз и убедиться в том, что их система предусматривает соответствующие средства защиты;

• наконец, тестировщики должны доказать неправоту разработчиков, создавая или приобретая инструменты, которые генерируют вредоносные и/или недействительные данные. Цель в том, чтобы выявить недочеты, допущенные разработчиками, если они есть.

Разумеется, это далеко не все, что требуется для обеспечения безопасности ПО, но, на мой взгляд, это те фундаментальные навыки, которыми должны обладать все инженеры-программисты».

Информация о Майкле Ховарде

Если вы хотите узнать больше о Майкле Ховарде, перейдите по следующим ссылкам:

• книги Майкла Ховарда: **https://www.amazon.com/Michael-Howard/e/B001H6GDPW/**;

• блог Майкла Ховарда: **https://michaelhowardsecure.blog/author/mikehow/**;

• Майкл Ховард в Twitter: **https://twitter.com/michael_howard**.

8. Профиль: Гари Макгроу

Когда я позвонил Гари Макгроу по поводу интервью, он сказал, что минуту назад беседовал с католическим монахом, который проходил мимо его дома на реке Шенандоа в Вирджинии. Спустя несколько секунд он переключился на обсуждение нюансов информационной безопасности. Такого рода парадоксы сопровождают Макгроу всю жизнь. Он начал программировать на своем первом компьютере, Apple II+, в 1981 году, в возрасте 16 лет. В колледже он изучал философию и параллельно получал классическое музыкальное образование. Он даже дважды выступал в Карнеги-холле. Сегодня, будучи одним из лучших в мире экспертов по ИБ, Макгроу с удовольствием готовит, ухаживает за садом и придумывает новые коктейли.

Я спросил Гари о том, как он заинтересовался темой информационной безопасности во время изучения философии в Университете Вирджинии. Он сказал, что интерес к философии сознания привел его на курс под названием «Компьютеры, сознание и мозг», который преподавал Пол Хамфрис. Гари считал идеи профессора Хамфриса ошибочными, но они заставили его глубже задуматься о философии сознания и проблеме искусственного интеллекта. В итоге в ходе занятий он начал применять идеи светила индустрии и обладателя Пулитцеровской премии доктора Дугласа Хофштадтера, что кардинально изменило его карьерный путь. Свой первый курс по информатике Макгроу прошел, уже будучи аспирантом, хотя увлекся программированием еще подростком. Под руководством Дугласа Хофштадтера в Университете Индианы он получил двойную докторскую степень в области когнитивных наук и информатики. Он даже написал десятую главу первой книги, проданной на Amazon. Это была книга Хофштадтера *Fluid Concepts and Creative Analogies: Computer Models of the Fundamental Mechanisms of Thought* (**https://www.amazon.com/Fluid-Concepts-Creative-Analogies-Fundamental/dp/0465024750**).

После колледжа Гари присоединился к компании из семи человек, которые в итоге основали Cigital **(www.cigital.com)**. Организация получила крупный грант от Управления перспективных исследовательских проектов Министерства обороны США (DARPA) на проведение исследования в области информационной безопасности, и Макгроу был нанят для работы над этим проектом. В итоге компания выросла до 500 сотрудников и в 2016 году ее приобрела компания Synopsys. В настоящее время в отделе обеспечения безопасности ПО работает около 1000 человек.

Мое первое значимое воспоминание о Макгроу связано с его работой по поиску уязвимостей в языке программирования Java, проделанной им совместно с Эдом Фелтеном, в соавторстве с которым он впоследствии написал книгу. То, что они обнаружили, слегка шокировало сообщество, учитывая то, что компания Sun Microsystems стремилась сделать Java максимально безопасным языком программирования, понимая, что он будет использоваться для разработки веб-

приложений, часто подвергающихся хакерским атакам. Релиз Java состоялся в 1995 году, и компания Sun с самого начала делала акцент на безопасности языка, ведь его разработкой занимались такие специалисты, как Гай Стил и Билл Джой. Большинство экспертов по ИБ сомневалось в его безопасности, считая заявление компании Sun очередным громким обещанием. И они оказались правы. Написанные на Java приложения содержали беспрецедентное количество багов. Макгроу был одним из лучших экспертов в деле обнаружения уязвимостей Java, и они с Фелтеном положили начало анализу этого языка на предмет наличия ошибок безопасности. Макгроу познакомился со своим будущим соавтором на конференции, и результатом этой встречи стала их первая книга **(https://www.amazon.com/GaryMcGraw/e/B000APFZ2S/)**. Многие книги Макгроу попадали в список бестселлеров сайта Amazon (одна из них, *Exploiting Software*, даже оказалась на 16-й строчке), что довольно впечатляюще для книг по компьютерной тематике, а тем более для книг, посвященных информационной безопасности.

Макгроу продолжал размышлять о безопасности ПО и о том, где можно научиться создавать более защищенные приложения. Он спрашивал себя, как остальные программисты могут разрабатывать безопасные программы, если это не удается даже таким специалистам, как Билл Джой и Гай Стил. Он пытался выяснить, что пошло не так в процессе их работы. Гари осознал, что программное обеспечение следует с самого начала разрабатывать с учетом требований безопасности. Примерно тогда он и придумал концепцию Trinity of Trouble («Троица проблем»), с помощью которой попытался объяснить, почему обеспечение безопасности ПО остается столь интересной и сложной задачей. В соответствии с этой концепцией сетевое, сложное и расширяемое приложение всегда будет представлять интерес с точки зрения безопасности, но обеспечить ее будет очень сложно. У Java, к сожалению, были сильно выражены все три аспекта, однако главная проблема, вероятно, заключалась в его сложности. После написания в соавторстве с Джоном Виегой книги *Building Secure Software* в 1999 году Макгроу посетил многие компании, включая Microsoft, где Майкл Ховард, речь о котором шла в предыдущей главе, работал вместе с Джейсоном Гармсом в новом подразделении Secure Windows Initiative. Он помнит, что на его выступлении присутствовали все менеджеры продуктов Microsoft и что компания явно была готова к внедрению практик, направленных на обеспечение безопасности ее ПО.

Потратив еще несколько лет на практику в сфере обеспечения безопасности ПО (предполагавшую разработку как сервисов, так и технологий), Макгроу стал одним из создателей модели BSIMM (Building Security In Maturity Model). В настоящее время этот инструмент применяет более ста крупных компаний для измерения, отслеживания и понимания своего прогресса в области обеспечения безопасности программного обеспечения.

На вопрос о том, чем именно модель BSIMM отличается от концепции SDL Майкла Ховарда, учитывая акцент обеих на повышении безопасности ПО, Макгроу сказал следующее: «SDL – это методология, а BSIMM – инструмент, позволяющий измерять и сравнивать различные SDL-подобные подходы.

Концепция SDL, формализованная и опубликованная компанией Microsoft, – это отличная методология, но далеко не единственная. Достижение Майкла Ховарда, которому я очень симпатизирую, в том, что он разработал формальный подход для огромной организации, где работают десятки тысяч программистов. Он показал, что обеспечением безопасности ПО можно заниматься в чрезвычайно больших масштабах, что очень важно».

Как и остальных людей, у которых я брал интервью для этой книги, я спросил Макгроу о том, что, по его мнению, является самой большой проблемой в сфере ИБ. Его ответ был созвучен мнению Майкла Ховарда, с которым я беседовал ранее. Вот что он сказал: «Несмотря на существование огромного количества информации, касающейся разработки более безопасных систем, относительно малое число программистов обладает достаточной компетентностью в этом вопросе. И хотя некоторые колледжи и коммерческие обучающие центры уже готовят хороших специалистов, абсолютное большинство образовательных учреждений этим практически не занимается».

По его мнению, сам предмет компьютерной безопасности еще недостаточно хорошо проработан. Его любимая книга по разработке безопасного ПО – *Security Engineering: A Guide to Building Dependable Distributed Systems* Росса Андерсона **(https://www.amazon.com/Security-EngineeringBuilding-Dependable-Distributed/dp/0471389226/)**. Макгроу сказал, что она нравится ему даже больше, чем 12 его собственных книг. По его мнению, «это лучшая книга по безопасности на всей планете».

Макгроу ведет ежемесячный подкаст, посвященный теме безопасности, *Silver Bullet Security Podcast* **(https://www.garymcgraw.com/technology/silver-bullet-podcast/)**, в рамках которого берет интервью у экспертов и светил индустрии. Недавно он отпраздновал десятилетие своего подкаста, опубликовав юбилейный, 120-й выпуск. В списке опрошенных им экспертов я увидел имена многих из тех людей, о которых написал в этой книге. Как и я, он проявляет неподдельный интерес к истории развития сферы ИБ, любит учиться и делиться знаниями. Когда наше интервью закончилось, я представил, как Макгроу, настоящий человек эпохи Возрождения, прогуливается со своей собакой вдоль реки, думая о новых типах брешей в системе безопасности ПО.

Информация о Гари Макгроу

Более подробно о Гари Макгроу можно узнать на следующих сайтах:

• книги Гари Макгроу: **https://www.amazon.com/GaryMcGraw/e/B000APFZ2S/**;

• веб-сайт Гари Макгроу: **https://www.garymcgraw.com**;

• подкаст Гари Макгроу: **https://www.garymcgraw.com/technology/silver-bullet-podcast/**.

9. Вредоносные программы

Когда я впервые начал работать в области ИБ еще в 1987 году, первым делом мое внимание привлекли вредоносные программы. Первые компьютерные вирусы (например, Elk Cloner для компьютеров компаний Apple и Pakistani Brain) только появились, хотя трояны и черви существовали и раньше. Компьютерные вирусы были настолько новы и редки, что популярные медиаэксперты объявили их мистификациями. Так было до тех пор, пока целые компании не подверглись заражению, и это было прежде, чем Интернет стал таким, каким мы знаем его сегодня. В то время компьютерные вредоносные программы распространялись по телефонным сетям и из рук в руки, когда люди копировали программное обеспечение друг у друга (как легально, так и нелегально). Вредоносные программы – по-прежнему один из самых популярных методов взлома.

Примечание. Первая вредоносная программа, которую я когда-либо видел, была бомба Ansi. Она загружалась на компьютер при содействии «помощника» – файла *ansi.sys*, так же, как в то время устанавливались многие программы и операционные системы, поэтому было сложно заподозрить с виду безопасную программу во вредоносности.

Типы вредоносных программ

Традиционные типы вредоносных программ – это вирус, червь и троянский конь. Компьютерный вирус – это самореплицирующаяся программа, которая при выполнении ищет другие программы (или иногда, как в случае с макровирусами, данные) для заражения. Компьютерный червь – это программа репликации, которая обычно не изменяет другие программы или данные. Он просто путешествует по устройствам и сетям, руководствуясь собственными закодированными инструкциями, часто эксплуатируя одну или несколько уязвимостей ПО. Троянский конь – программа, которая маскируется под легитимное приложение, обманом заставляя устройство или пользователя активировать ее. Современная вредоносная программа часто представляет собой сочетание двух или более традиционных типов. Например, она может быть первоначально распространена как троян, чтобы получить точку опоры, а затем использовать собственный код для дальнейшего распространения.

Вредоносные программы могут быть достаточно эффективными. Тысячи из них успешно заражают целые сети по всему миру за несколько часов. Сотни вредоносных программ за один день заражают значительную часть компьютеров, подключенных к Интернету. Первое место по скорости заражения по-прежнему принадлежит программе 2003 года SQL Slammer worm **(https://securelist.ru/slammer-vsyo/8976/)**, которая заразила большинство доступных в Интернете уязвимых SQL-серверов примерно за 10 минут. Соответствующий патч был выпущен спустя пять месяцев, но тогда почти никто не реагировал своевременно. Сегодня большинство вредоносных программ являются троянскими и требуют, чтобы конечный пользователь инициировал действие (например, открыл веб-ссылку или вложенный файл) для запуска вредоносного ПО, хотя вовлеченное устройство или пользователь,

возможно, не имели никакого отношения к выполнению программы. Это зависит от сценария вредоносного ПО и его распространения.

Количество вредоносных программ

Существуют сотни миллионов различных вредоносных программ и неизмеримое количество новых создается каждый год. Большинство из них – небольшие настраиваемые вариации, создаваемые из нескольких тысяч различных базовых вредоносных программ. Тем не менее каждая вариация должна обнаруживаться антивирусными программами, которые часто используют комбинацию цифровых сигнатур (уникальный набор байтов для каждой вредоносной программы или группы программ) и поведенческого обнаружения. Инструмент защиты от них должен быстро сканировать десятки миллионов файлов на предмет отсутствия кода сотен миллионов вредоносных программ и делать это без значительного замедления работы устройства, на котором он запущен. Реализовать это трудно, и даже если сделать это с максимальной степенью точности, защита может быть пробита одной новой вредоносной программой с единственным измененным байтом.

Примечание. Инструменты против вредоносных программ часто называют антивирусными приложениями, несмотря на то что они обнаруживают и удаляют вредоносные программы нескольких типов, поскольку большинство из них – компьютерные вирусы.

Программы криминального назначения

Одна из самых больших и тревожных тенденций вредоносных программ – это то, что они в основном используются в преступных целях. Примерно до 2005 года большинство из них было написано молодежью, стремившейся доказать, что может писать компьютерные вредоносные программы. Того, что такая программа функционировала и реплицировала, было достаточно. Конечно, было несколько вредоносных программ, которые намеренно причиняли непосредственный вред, но большинство из них оказывались скорее надоедливыми, чем опасными.

Теперь почти все вредоносные программы создаются в преступных целях. Большинство так или иначе нацелены на кражу денег, будь то прямая финансовая выгода, кража цифровой личности или паролей. В наши дни «вымогатель», то есть вредоносная программа, шифрующая данные и требующая выкуп, чтобы расшифровать их, очень популярен. Другие программы крадут игровые ресурсы, электронную валюту или совершают несанкционированные сделки с акциями. Некоторые проникают в ваш компьютер, чтобы отображать рекламу (или конкретные объявления), или тайно заставляют компьютер заходить на определенные веб-сайты, чтобы увеличить количество посетителей (трафик) для получения доходов от рекламы. Некоторые используются для взлома и кражи конфиденциальной информации. Другие могут применяться для массовых распределенных атак типа «отказа в обслуживании» (см. главу 28). Прошли времена, когда большинство

вредоносных программ было создано озорными детьми; эти программы печатали милые маленькие поговорки на экране, играли в Yankee Doodle Dandy на вашем компьютере или просили вас помочь «легализовать марихуану» (например, вирус Stoned boot). Сегодня вредоносное ПО стало профессиональным!

Вредоносные программы часто создаются одним человеком, а покупаются и продаются другими. Часто тысячи компьютеров, скомпрометированных определенной программой, собираются вместе в так называемые ботнеты. Эти «сети ботов» могут быть арендованы или куплены, а затем настроены атаковать определенный сайт или сайты. Вредоносная программа, которая изначально внедряется в конкретный компьютер, известна как «загрузчик». Он получает начальный доступ к системе и модифицирует ее, чтобы допустить успешную работу будущих вредоносных программ или хакеров. Затем загружает новую программу с новыми инструкциями. Этот процесс может повторяться десятки раз, пока не будут загружены и выполнены финальные программы и инструкции. Таким образом, большинство вредоносных программ поддерживаются в актуальном состоянии и остаются скрытыми от антивирусных продуктов. Они даже продаются с круглосуточной технической поддержкой и гарантиями от обнаружения, и их разработчики получают отзывы удовлетворенных клиентов.

Вредоносные программы ответственны за кражи или причинение ущерба в сотни миллионов долларов ежегодно. Каждый опытный человек в сфере ИБ, который борется с ними последние десять лет, предпочел бы иметь дело только с озорными детьми.

Защита от вредоносных программ

Существует много средств защиты от вредоносных программ, большинство из которых также хороши и против нескольких других форм взлома.

Вовремя пропатченное программное обеспечение

Полностью пропатченная система гораздо сложнее для проникновения вредоносных программ, чем устаревшая. В наши дни наборы эксплойтов размещаются на скомпрометированных веб-сайтах, и, когда пользователь их посещает, набор эксплойтов будет искать одну или несколько незакрытых уязвимостей, прежде чем пытаться обмануть пользователя и принудить запустить троянского коня. Если система не пропатчена, вредоносная программа может быть тайно выполнена без ведома пользователя.

Обучение

Полностью пропатченную систему трудно скомпрометировать без участия конечного пользователя. В тех случаях, когда вредоносное ПО или набор эксплойтов не находят незакрытую уязвимость, они обычно прибегают к какому-либо трюку социальной инженерии. Обычно он включает в себя

указание конечному пользователю, что ему нужно запустить или открыть что-то, чтобы получить некий полезный результат. Обучение пользователей противостоять распространенным методам социальной инженерии – отличный способ снизить шансы успеха вредоносных программ.

Антивирусные программы

Антивирусное ПО необходимо использовать практически в каждой компьютерной системе. Даже лучший антивирус может пропустить вредоносную программу, и ни одна программа не гарантирует 100 %-ную защиту от них, но запуск компьютерной системы без нее – это как езда на машине без тормозов. Вы можете работать в такой системе некоторое время, но в итоге катастрофа все-таки случится. В то же время никогда не верьте обещаниям разработчиков антивирусов о 100 %-ной защите. Это ложь.

Программы контроля запуска приложений

Программы контроля запуска приложений (также известные как программы «белых» или «черных» списков) отлично подходят для блокировки вредоносных программ при использовании в режиме «белого» списка. В этом режиме разрешен запуск только определенных и легитимных программ. Такой подход останавливает большинство вирусов, червей и троянов. Программы контроля запуска приложений могут быть трудны в реализации в оперативном плане, потому что по своей природе каждая программа и исполняемый файл должны быть предварительно одобрены для запуска. И не каждый тип вредоносных программ или действия хакера могут быть предотвращены, особенно те, которые используют встроенные легитимные программы и инструменты сценариев. Тем не менее программы контроля запуска приложений – эффективный инструмент, который постоянно совершенствуется. Лично я думаю, что любая система, которая считается достаточно безопасной, должна иметь активную и определенную программу «белых» списков.

Инструменты пограничной защиты

Брандмауэры и другие типы локальных и сетевых инструментов пограничной защиты (например, виртуальные ЛВС, маршрутизаторы и т. д.) хорошо защищают компьютерное устройство от вредоносного ПО. Большинство операционных систем имеют встроенные локальные брандмауэры, но многие из них не настроены и не включены по умолчанию. Внедрение брандмауэра может значительно снизить риск быть скомпрометированным, особенно при наличии незакрытой уязвимости. Мы рассмотрим их более подробно в главе 17.

Обнаружение вторжений

Сетевая (NID/P) и хостовая (HID/P) системы обнаружения/предотвращения вторжений в программное обеспечение и устройства могут использоваться для распознавания и остановки вредоносных программ в сети или на локальном хосте. Обнаружение вторжений описано в главе 14. Но, как и традиционные антивирусные программы, сетевые и хостовые системы не гарантируют 100 %-ную защиту, и не следует доверять только им.

Вредоносные программы уже давно стали частью угроз информационной безопасности и всегда будут оставаться главной из них. Еще в конце 1990-х годов, с развитием антивирусных технологий, я был уверен, что они уйдут в прошлое к 2010 году. В те времена у нас были лишь сотни вредоносных программ. Теперь, сталкиваясь с сотнями миллионов различных вариаций, я понимаю, как был наивен.

Главы 10 и 11 посвящены Сьюзен Брэдли и Марку Руссиновичу, которые успешно борются с вредоносными программами на протяжении десятилетий.

10. Профиль: Сьюзен Брэдли

Я познакомился со Сьюзен Брэдли более 15 лет назад, когда получил статус одного из наиболее ценных профессионалов Microsoft (MVP, Most Valuable Professionals). Как известно, этот статус присваивается независимым лидерам сообщества, которые демонстрируют совершенное владение одной или несколькими технологиями Microsoft и активно взаимодействуют с конечными пользователями, например ведут блог, рассылку или колонку в СМИ. С самого начала было ясно, что Брэдли – одна из лучших MVP-экспертов. Она очень умна, трудолюбива и всегда готова помочь не только конечным пользователям, но и другим MVP-экспертам (которые тоже являются конечными пользователями). Статус MVP был впервые присвоен Сьюзен в 2000 году в связи с выпускавшимся в то время продуктом Microsoft Small Business Server (SBS), однако ее глубокие технические знания этим не исчерпывались и охватывали в том числе систему Windows. С тех пор она продолжает получать статус MVP-эксперта каждый год **(https://mvp.microsoft.com/ru-ru/PublicProfile/7500?fullName%20=Susan%20Elise%20Bradley)**, но теперь этот статус относится к категории Cloud and Datacenter Management.

Если вы не знаете, что такое Small Business Server, просто возьмите самые главные и сложные продукты Microsoft (например, Active Directory, Exchange, SQL, Outlook и т. д.), объедините их в одну программу для малого бизнеса и скажите, что ее легко использовать. Я заработал кучу денег, консультируя клиентов, которые быстро поняли, что это совсем нелегко. Брэдли оказала мне техническую поддержку, когда я столкнулся с проблемой, которую не смог решить самостоятельно. Мы периодически встречались на национальных конференциях, посвященных ИБ, на которых выступали, и немного сблизились на почве общего бухгалтерского прошлого. Мы оба – сертифицированные бухгалтеры (CPA), правда в настоящее время я уже не работаю в этой области, а она остается партнером в бухгалтерской фирме. Брэдли имеет сертификат SANS Global Information Assurance Certification (GIAC), стала автором отдельных глав к нескольким книгам, а также соавтором рассылки *Windows Secrets* (**https://www.askwoody.com/author/sb/)**.

На мой вопрос о том, как она попала в сферу ИБ, Брэдли ответила: «Сфера бухгалтерского учета, в которой я начинала свою карьеру, по определению связана с деньгами и конфиденциальностью. А обеспечение безопасности транзакций, на которые мы полагаемся, имеет непосредственное отношение к

информационной безопасности. Мы должны убедиться в том, что данные, введенные с клавиатуры (а теперь еще и с помощью голосового ввода, точек данных, датчиков и т. д.), попадут в целевой репозиторий в неискаженном виде. Я начала обращаться к представителям малых предприятий и другим людям по вопросам установки патчей. У меня был серверный продукт, состоящий из различных программ, которые мне нужно было пропатчить, а простого способа сделать это тогда не существовало. В те времена люди практически не устанавливали исправления в свои продукты. Затем [в 2003 году] появился червь SQL Slammer, оказавший на мир огромное влияние. Самое интересное, что исправление для соответствующей уязвимости было выпущено за шесть месяцев до его появления. Но сам процесс установки патча был слишком сложным. Я научилась делать это в своих продуктах, а затем поняла, что мой опыт может оказаться полезным и другим предпринимателям. Так я пришла к тому, чем занимаюсь сейчас».

Брэдли по-прежнему взаимодействует с представителями малого бизнеса, а также помогает людям защищаться от программ-вымогателей и восстанавливаться после соответствующих атак. На мой вопрос о том, что именно она рекомендует своим клиентам, она ответила: «За несколько лет стало очевидно, что программы-вымогатели представляют собой большую проблему не только для потребителей, но и для малых предприятий. Учитывая то, насколько сложно бывает отыскать нужную информацию, три года назад мы с моей подругой и MVP-экспертом [с 2006 года] Эми Бабинчак создали набор Ransomware Prevention Kit **(https://www.thirdtier.net/product/ransomware-prevention-kit-policies/)**. Он содержит всю необходимую информацию и инструменты для защиты от программ-вымогателей, включая параметры групповой политики и скрипты, а теперь еще и видео. Это не бесплатно. Минимальная цена продукта составляет 25 долларов. Первоначально все полученные от продажи средства шли в женский стипендиальный фонд **(www.thirdtier.net/women-in-it-scholarship-program/)**. Тетя Эми одолжила ей необходимую сумму для получения первого сертификата, и Эми считает, что без этого столь необходимого кредита ей не удалось бы достичь успеха. Так она пытается вернуть долг. Стипендиальный фонд возмещает женщинам стоимость IT-экзаменов в случае их успешной сдачи. Изначально Эми поставила цель собрать для фонда 10 000 долларов, и они были собраны за девять месяцев. Сегодня в этот фонд поступает уже не все, а только часть средств от продажи набора Ransomware Prevention Kit. На обновление продукта уходит огромное количество времени, но Эми изо всех сил старается сделать так, чтобы по мере обновления каждый покупатель получал актуальную копию, а это требует огромных усилий».

Я спросил Брэдли о том, что, по ее мнению, является главной проблемой в сфере информационной безопасности, на что она ответила: «Мы отвлекаемся на следствия, вместо того чтобы докапываться до первопричин. Возьмем, к примеру, наблюдаемое сегодня безразличие к утечкам данных. Поскольку эти утечки не сильно затрагивают бизнес, мы полагаем, будто достаточно обеспечить соответствие стандартам PCI (см. главу 37 «Политики и стратегия»), и сосредоточиваем внимание на пунктах чек-листа, вместо того чтобы

задуматься о повышении безопасности потоков данных. Отчасти сложность заключается в том, что технологии постоянно меняются. Однако основополагающая проблема остается прежней. Когда-то (очень давно) мы использовали мейнфреймы, затем появились ПК, серверы и сети (распределенная модель ПК). В то время люди просто устанавливали серверы, не задумываясь об их защите. Сегодня мы переходим к использованию облачной модели. Практически все мигрируют в облако, но допускают при этом те же ошибки. Люди переносят туда свои серверы или используют облачные сервисы для ведения бизнеса, но не понимают, как все это защитить. Мы совершаем те же ошибки, только теперь все усложняется тем, что клиент не всегда может повлиять на безопасность, и расследовать преступления становится труднее. Иногда кажется, что мы стоим на месте. Нам следует сосредоточиться на решении основополагающих проблем, потому что технологии постоянно меняются». Если вы хотите в совершенстве освоить Microsoft Windows, обязательно прочитайте то, что пишет Сьюзен Брэдли.

Информация о Сьюзен Брэдли

Более подробную информацию о Сьюзен Брэдли смотрите по ссылкам:

• блог Сьюзен Брэдли на сайте Computer World: **https://www.computerworld.com/author/Susan-Bradley/**;

• блог Сьюзен Брэдли на сайте AskWoody: **https://www.askwoody.com/author/sb/**.

11. Профиль: Марк Руссинович

Никто не в состоянии изучить Microsoft Windows целиком. Это десятки миллионов строк кода. Но за два десятилетия Марку Руссиновичу, техническому директору Microsoft Azure, удалось приблизиться к этой цели. Руководители компаний (главный исполнительный директор, директор по информационным технологиям и т. д.) редко углубляются в технологические нюансы. Руссинович в этом отношении скорее исключение. Мало кто может сравниться с ним по широте знаний, касающихся той или иной функции. Анализ кода делает Марка по-настоящему счастливым. Я отметил это во время нашего интервью, и он сказал: «Технологические нюансы – это именно то, что мною движет!»

Я знаю Руссиновича уже почти 20 лет. Долгое время он руководил двумя компаниями, занимающимися разработкой программного обеспечения. Одной из них была коммерческая компания Winternals, а второй – некоммерческая Sysinternals, производившая бесплатное ПО. Продукты обеих компаний были очень популярны среди технарей. В конце концов, Microsoft приобрела их, и Марк стал работать в одном из подразделений корпорации. На сайте **https://docs.microsoft.com/ru-ru/sysinternals/** представлены интересные утилиты, которые он создал и которые компания Microsoft по-прежнему

поддерживает и обновляет. Руссинович всегда был технарем до мозга костей, не боящимся открытой полемики вокруг результатов своих технических расследований.

Я хорошо помню, как обедал с ним в ресторане в 2005 году (ни один из нас тогда не был сотрудником Microsoft), когда разгорелся скандал в связи с обнаруженным им руткитом Sony BMG. Руссинович выяснил, что при вставке музыкального компакт-диска Sony в дисковод компьютера под управлением ОС Windows тайно устанавливалось два программных решения для управления цифровыми правами (DRM). Это ПО было сложно удалить, и его частичная установка происходила даже в том случае, если пользователь не принимал условия лицензионного соглашения (EULA). Оно не только мешало системе Windows осуществлять операции с компактами-дисками, но и содержало уязвимости, которыми в итоге воспользовались вредоносные программы.

Руссинович наткнулся на программу Sony, когда тестировал свое приложение для поиска руткитов – Rootkitrevealer. Для сокрытия следов своего присутствия руткит определенным образом модифицирует операционную систему. Руссинович уподобил действия DRM-программы Sony действиям вредоносного руткита, что было весьма громким заявлением для того времени. По сути, он обвинил крупную компанию в неэтичном поведении. Его оригинальный пост можно найти по адресу: **https://techcommunity.microsoft.com/t5/windows-blog-archive/sony-rootkits-and-digital-rights-management-gone-too-far/ba-p/723442**.

Эта история облетела все СМИ, и репутация Sony была существенно подпорчена. Сначала представители компании заявляли, что ее действия были нормальными и приемлемыми, но после волны общественного возмущения они признали вину и предложили специальный инструмент для деинсталляции ПО. В конце концов, компания отозвала соответствующие компакт-диски и предложила компенсацию. К сожалению, и с деинсталятором возникли проблемы. За этим последовали коллективные иски и правительственные расследования. Подробнее об этом скандале можно прочитать по адресу **https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal**. Расследование Руссиновича, вызвавшее общественный резонанс, стало предупреждением для всех разработчиков ПО, что позволило минимизировать количество случаев установки программ без ведома пользователя.

И это только малая часть заслуг Руссиновича. Помимо всего прочего он занимается преподаванием и часто выступает на конференциях с лекциями, содержащими огромное количество технических подробностей. Те из выступающих, кому доводилось соревноваться с ним за признание публики, знают, что максимальный результат, на который они могут рассчитывать, – это второе место. Он стал автором и соавтором множества книг **(https://www.amazon.com/Mark-E.-Russinovich/e/B001IGNICC/)**, в том числе ставшего бестселлером триллера на тему кибербезопасности. Тот факт, что его истории о киберармагеддоне могут произойти в реальности или уже происходят, делает их не менее пугающими, чем романы Стивена Кинга. Руссинович получил докторскую степень в области компьютерной инженерии в

Университете Карнеги-Меллона в 1994 году, а в 1996 году начал работать в компании Microsoft.

В настоящее время Руссинович – одна из самых значимых фигур в Microsoft. Благодаря ему компания совершила множество технологических прорывов. Он сыграл важную роль в ускорении и обеспечении безопасности самых последних версий операционных систем Microsoft, и теперь отвечает за облачный сервис компании. Помимо того, что Марк стал техническим директором Microsoft Azure, он имеет звание Microsoft Technical Fellow, которое присуждается только людям, оказавшим значительное влияние на компанию Microsoft и мир в целом. По иронии судьбы более двадцати лет назад, в 1997 году, руководство Microsoft чуть не добилось увольнения Руссиновича из компании, в которой он в то время работал.

Будучи сотрудником компании Open Systems Resources, Руссинович работал над программным обеспечением для Windows NT 3.51. В процессе подробного изучения внутреннего устройства системы он обнаружил, что изменение одного ключа реестра позволяет превратить Windows NT из ОС для рабочей станции в серверную ОС. Он пояснил: «На самом деле там были две записи реестра: одна называлась ProductType, а вторая, закодированная, использовалась для обнаружения изменения первой. Эта запись реестра затрагивала 12 системных параметров, которые буквально превращали Windows в ОС для сервера или для рабочей станции. И я написал статью по этому поводу для журнала Windows IT Pro **(https://www.itprotoday.com/windows-78/inside-windows-nt-registry)»**. Ее краткое изложение можно найти по адресу: **http://www.landley.net/history/mirror/ms/differences_nt.html**.

Я хорошо помню эту статью. Тогда я только начинал профессионально писать, и один из редакторов журнала предложил мне выступить в качестве технического редактора этой статьи. Еще до ее публикации все понимали, что компания Microsoft, скорее всего, будет очень недовольна, потому что она позиционировала Windows NT Workstation и Windows NT Server как два совершенно разных, хоть и похожих продукта, причем последняя версия стоила значительно дороже.

Помню, что до меня доходили слухи об увольнении Руссиновича в связи с публикацией. Когда я спросил его, действительно ли Microsoft добилась своего, он сказал: «Они, конечно, не обрадовались, но никто меня не увольнял. Правда, Microsoft надавила на руководство Open System Resources, и из-за этого я был вынужден покинуть компанию. Я устроился в IBM Research, но у меня всегда были друзья в Microsoft, и со многими другими сотрудниками компании я поддерживал хорошие отношения. Меня по-прежнему приглашали рассказывать о внутреннем устройстве Microsoft Windows, и я продолжал писать книги на эту тему. Мне даже несколько раз предлагали работу в Microsoft. В конце концов, они приобрели меня вместе с компаниями Winternals и Sysinternals, в которых в то время работало по 85 сотрудников». Остальное уже история.

Сегодня Руссинович развивает технологическое направление Microsoft Azure, стараясь сделать платформу более функциональной, быстрой и безопасной. В

последнее время он много работает с контейнерами и микросервисами. Контейнеризация – это форма виртуализации, популяризованная проектом Docker **(www.docker.com)**. Контейнеры появились из ниоткуда, и кое-кто видел в них угрозу крупным поставщикам решений для виртуализации (например, Amazon, Google, Microsoft и VMware). Однако Microsoft приняла контейнерную технологию, и под руководством Руссиновича платформа Azure превратилась в один из крупнейших в мире сервисов контейнеризации.

На мой вопрос о том, способствуют ли контейнеры обеспечению информационной безопасности, он сказал: «Это зависит от того, что вы называете контейнером, и от сценария сборки его образа. В некоторых случаях контейнеры слегка облегчают процесс обеспечения информационной безопасности. Фактически они не имеют состояния, что мешает злоумышленнику закрепиться во взломанной системе. Но в то же время, если уязвимость, позволившая хакеру проникнуть в систему в первый раз, не была устранена, то он с легкостью сможет снова получить к ней доступ. А если в первый раз злоумышленник сумел взломать систему, сохраняющую состояния, например SQL-сервер, то его не остановит и перезагрузка контейнера. Один из недостатков контейнеров, особенно если речь идет о Docker-образах, – это наслаивание множества контейнеров при создании одного приложения или сервиса. И если вы захотите исправить или обновить код одного Docker-образа, то из-за существующих зависимостей вам придется пересобрать все остальные связанные с ним образы. Это многократно усложняет процесс исправления и пересборки, и именно в этой сложности заключается один из недостатков контейнеризации».

В завершение интервью я спросил Руссиновича, что бы он порекомендовал всем тем, кто задумывается о карьере в сфере ИБ. Опираясь на собственный опыт, он посоветовал: «Вы должны стать экспертом во всем, что касается систем, которые собираетесь защищать. Вы должны понимать их внутреннее устройство и принципы их взаимодействия, включая процедуры проверки подлинности, политики, мониторинг и сегментацию сети. Первым делом вам необходимо глубоко ознакомиться с программным обеспечением или самой платформой. После этого следует рассмотреть интересующую систему под разными углами. Каждая точка зрения раскрывает разные аспекты одного и того же предмета, что помогает гораздо лучше разобраться в том, что вам предстоит защищать».

Информация о Марке Руссиновиче

Более подробная информация о Марке Руссиновиче содержится на следующих ресурсах:

• Марк Руссинович в «Википедии»: **https://en.wikipedia.org/wiki/Mark_Russinovich**;

• книги Марка Руссиновича: **https://www.amazon.com/Mark-E.-Russinovich/e/B001IGNICC/**;

• веб-сайт Марка Руссиновича: **http://markrussinovich.com/**;

• Марк Руссинович в Twitter: **https://twitter.com/markrussinovich**;

• блог Марка Руссиновича на сайте Microsoft: **https://azure.microsoft.com/ru-ru/blog/author/markruss/**;

• крутые утилиты Марка Руссиновича: **https://docs.microsoft.com/en-us/sysinternals/**.

12. Криптография

Бóльшая часть технологий в сфере информационной безопасности касается криптографии. Криптография существует уже целую вечность и будет существовать еще долго после того, как мы покинем планету Земля в поисках других гостеприимных планет. Криптография – это отрасль ИБ, которая мне больше всего нравится, хотя после почти трех десятилетий увлечения ею я не считаю себя экспертом в этой области.

Что такое криптография?

В цифровом мире криптография – это использование последовательностей единиц и нулей для шифрования или верификации цифрового контента. Она включает в себя использование математических формул (называемыми *шифрами*) наряду с единицами и нулями (называемых *криптографическими ключами*) для предотвращения несанкционированного доступа людей к конфиденциальному контенту или для аутентификации другого человека или легитимного контента.

Самый простой пример шифрования, который я могу привести, – это когда некоторое незашифрованное содержимое преобразуется в зашифрованное представление перемещением букв алфавита на одну позицию (например, А становится Б, Б становится В, В становится Г и так далее, пока Я не станет А). Таким образом, МОЗГ становится НПИД-ом. Дешифровщик может повернуть процесс вспять и отобразить исходный открытый текст. В этом примере шифр – это математика, которая в данном случае касается операций сложения или вычитания, а ключом служит единица. Как бы прост ни был этот шифр, его использовали на протяжении многих лет, несмотря на то что его легко дешифровать.

В современном цифровом мире криптографические ключи обычно имеют размер не менее 128 бит, если не больше. В зависимости от шифра ключ может быть длиннее, хотя, если алгоритмы устойчивы к криптоатакам, обычно самые длинные из них составляют 4096 бит. Если вам встречаются ключи еще больше, это указывает на слабые алгоритмы или кого-то, кто не очень хорошо знает криптографию (или пытается продать эти коды людям, которые в этом не сильны).

Почему злоумышленники не могут просто подобрать все возможные ключи?

Люди, которые не знакомы с криптографией, не понимают, почему хакеры не пробуют все возможные комбинации единиц и нулей, которые могут быть применены в результате определенного размера ключа. Не мог ли кто-то с очень быстрым компьютером подобрать все возможные комбинации? Нет. Даже размер современного ключа в 2000 бит устойчив против «перебора грубой силой». Мало того что для этого не существует достаточно мощного компьютера, но даже если бы вы использовали все компьютеры в мире, которые уже изобрели или изобретут в будущем, им все равно не хватило бы мощности (по крайней мере, до тех пор, пока квантовые вычисления не станут реальностью). Следовательно, взлом криптографических средств связан с утечками или слабыми алгоритмами. Криптографические алгоритмы, мягко говоря, сложны, и то, что первоначально может выглядеть непобедимой математикой, часто оказывается полным недостатков, которые позволяют быстро взломать систему. Вот почему стандарты шифрования и размеры ключей постоянно меняются, поскольку старые шифры ослабевают, а новые, более устойчивые, появляются.

Симметричные и асимметричные ключи

Если ключ шифрования совпадает с тем, что используется для расшифровки в дальнейшем (например, в простом примере выше), то шифр называется симметричным. Если ключ, используемый для шифрования, отличается от ключа, используемого для расшифровки, шифр называется асимметричным. Асимметричные шифры также известны как шифрование с открытым ключом, когда шифрующая сторона имеет закрытый ключ, который знает только она, а расшифровывающая сторона – открытый, и до тех пор, пока посторонние не знают закрытый ключ, коммуникации защищены. Однако симметричное шифрование обычно выполняется быстрее и надежнее.

О криптографии популярно

В наши дни многие шифры хорошо известны и протестированы, чтобы стать отраслевыми, если не мировыми, стандартами.

Популярные симметричные ключи шифрования включают алгоритм для симметричного шифрования (DES), 3DES (тройной DES) и симметричный алгоритм блочного шифрования (AES). Первые два алгоритма устарели и больше не используются. Последний считается криптостойким и наиболее популярным симметричным шифром, используемым сегодня. Размеры ключей симметричных шифров обычно варьируются от 128 до 256 бит, но постепенно их размер увеличивается. Каждое увеличение, скажем, со 128 до 129 бит, обычно двукратно усиливает надежность ключа в пределах одного и того же шифра.

Популярные асимметричные шифры включают криптографический протокол Диффи – Хеллмана (о Мартине Хеллмане поговорим в следующей главе), протокол Ривеста – Шамира – Адлемана (RSA) и эллиптическую криптографию (ECC). Эллиптическая криптография – новая технология в этой сфере и только начинает использоваться. Размеры ключей асимметричных шифров обычно варьируются от 1024 до 4096 бит, хотя сегодня 2048 бит считается минимальным допустимым размером для протоколов Диффи – Хеллмана и RSA. Эллиптическая криптография использует меньшие размеры ключей, начиная с 256 бит. 384 бита считаются достаточно надежным вариантом. Как правило, асимметричные шифры используются для безопасной передачи симметричных ключей, которые выполняют бóльшую часть шифрования между отправителем и получателем.

Хэши

Криптография также используется для проверки содержимого. Для этого применяют алгоритмы шифрования, известные как криптографические хэши. При этом содержимое открытого текста, подлежащее проверке, математически соотносится с ключом (опять же только в серии единиц и нулей) для получения уникального результата, называемого результатом хэширования, или хэшем. Идентификационные данные или контент могут быть хэшированы в любой момент и вновь хэшированы позднее (например, на другом устройстве). Хэши можно сравнить, чтобы убедиться, что хэш содержимого не изменился с момента начального хэширования.

Распространенные хэш-алгоритмы – Secure Hash Algorithm 1 (SHA-1), SHA-2 и SHA-3. Было обнаружено, что SHA-1 имеет некоторые криптографические недостатки (также схожие с SHA-2), и поэтому его упразднили. SHA-2 становится самым популярным хэшем, но эксперты криптографии уже рекомендуют использовать SHA-3.

Большинство криптографических решений используют симметричные, асимметричные и хэширующие алгоритмы для достижения требуемой защиты. Во многих странах, в том числе и в США, существует особый орган по стандартизации, который анализирует и утверждает различные шифры для использования правительством. Официально одобренные шифры используются во всем мире. В США Национальный институт стандартов и технологий **(www.nist.gov)** совместно с Агентством национальной безопасности **(www.nsa.gov)** проводят публичные конкурсы, в которых криптографам по всему миру предлагается представить собственные шифры для анализа и отбора. Он проводится открыто, и зачастую даже проигравшие соглашаются с разработками победителя. К сожалению, Агентство национальной безопасности и Национальный институт стандартов и технологий (НИСТ) как минимум дважды были обвинены в преднамеренном ослаблении официальных стандартов (особенно с DES и Dual_EC_DRBG [алгоритм, основанный на эллиптических кривых]). Возникла некоторая напряженность, и

многие теперь не доверяют тому, что НИСТ и АНБ считают надежной криптографией.

Применение криптографии

Криптография лежит в основе бóльшей части цифрового мира в сети. Криптография защищает наши пароли и биометрические удостоверения и используется в цифровых сертификатах. Криптография применяется каждый раз, когда мы садимся за свой компьютер и подключаемся к защищенному веб-сайту через протокол HTTPS. Она нужна для проверки загруженного программного обеспечения, безопасности общения по электронной почте и сверки компьютеров. Шифрование используется для защиты жестких дисков и портативных носителей от несанкционированного доступа, предотвращения повреждения загрузочного сектора жесткого диска и защиты беспроводных сетей. Криптография применяется при разработке программ, скриптов и верстке документов. Она позволяет организовывать приватные соединения через публичный Интернет и стоит почти за всеми банковскими картами и транзакциями в мире. Надежная криптография – враг шпионов, тиранов и авторитарных режимов. Можно без преувеличения сказать, что без криптографии Интернет не был бы Интернетом и наши компьютеры никогда не были бы под нашим контролем.

Криптографические атаки

Существует множество криптографических атак. Мы рассмотрим некоторые из наиболее известных.

Математические атаки

Многие атаки основываются на слабостях алгоритмов. Без нее шифр может выдержать атаку грубой силы, равную количеству битов в ключе минус один. Таким образом, 128-битный шифр (2128), такой как SHA-1, должен выдержать в среднем 2127 попыток, прежде чем будет взломан. Злоумышленники нашли недостатки алгоритма SHA-1, существенно ослабив его стойкость примерно до 257 бит.

Хотя шифр 2127 считается стойким (по крайней мере на данный момент), 257 можно взломать уже сейчас или в ближайшем будущем, и хакеру не понадобятся для этого огромные вычислительные мощности.

Атака на основе доступной информации

Многие атаки успешны, потому что у хакеров есть подсказка (также известная как шпаргалка). Обычно она представлена в форме известного набора битов или байтов в зашифрованном тексте, содержимом незашифрованного текста или закрытом ключе. Подсказка уменьшает возможное количество битов в криптографическом ключе.

Атаки по сторонним каналам

Атаки по сторонним каналам часто подразумевают атаку на непредвиденные дефекты реализации, позволяющие выявить секретные ключи. Например, когда процессор компьютера изменяет звук работы или электромагнитное излучение при обработке 0 и 1. Таким образом, злоумышленник с очень чувствительным прослушивающим устройством может определить нули и единицы, когда компьютер обрабатывает закрытый ключ. Другой пример: злоумышленник может определить, какие клавиши клавиатуры вы нажимаете, записав звуки нажатия.

Небезопасные реализации

Подавляющее большинство успешных криптографических атак в реальном мире не связаны со взломом алгоритмов или криптографических ключей. Вместо этого злоумышленники ищут недостатки реализации, подобные ключу от входной двери под ковриком в реальной жизни. Даже самые сильные алгоритмы не спасут слабую реализацию.

Существует много других типов криптографических атак, хотя перечисленные выше наиболее распространены. Единственная защита от них – надежные, проверенные алгоритмы, безопасные реализации и невидимые или понятные только конечному пользователю интерфейсы. Все остальное неважно.

Глава 3 посвящена Брюсу Шнайеру, который считается отцом современной компьютерной криптографии. В главе 13 мы поговорим об одном из самых известных криптографов в мире, Мартине Хеллмане, а в главе 15 познакомимся с доктором Дороти Э. Деннинг, написавшей одну из первых книг по компьютерной криптографии.

13. Профиль: Мартин Хеллман

Общаясь с лучшими специалистами, я сделал вывод о том, что они, как правило, хорошо разбираются не только в своей основной сфере деятельности. Обычно они увлекаются многими вещами, решая проблемы, никак не связанные с их специализацией. Отличным примером может служить Мартин Хеллман, один из создателей криптографии с открытым ключом. Будучи одним из лучших криптографов в мире, занимающихся актуальными проблемами криптографии, он также любит парить на планерах, улучшать брачные отношения и предотвращать ядерные войны… Причем необязательно именно в этом порядке.

В 1976 году Хеллман и его коллеги Уитфилд Диффи и Ральф Меркл создали криптосистему с открытым ключом, которую описали в статье *New Directions in Cryptography*, опубликованной в ноябре того же года **(https://ee.stanford.edu/~hellman/publications/24.pdf**). Созданный ими протокол обмена ключами стал известен как *алгоритм Диффи – Хеллмана*, но Хеллман предпочитает называть его *алгоритмом Диффи – Хеллмана – Меркла*, что он и делал во время нашего интервью. Примерно через год после

публикации статьи, основываясь на работе Диффи и Хеллмана, Рональд Ривест, Ади Шамир и Леонард Адлеман из Массачусетского технологического института разработали алгоритм RSA, и благодаря маркетинговым усилиям основанной ими впоследствии компании криптография с открытым ключом завоевала весь мир, увековечив имена своих создателей.

На протяжении длительного времени я рассказывал историю о том, как Хеллман и его коллеги изобрели криптосистему с открытым ключом, не будучи уверенными в точности своей версии. Это невероятная история о трех людях, ни один из которых не получил официального образования в области криптографии и в идею которых не верил практически никто, кроме них самих. До внесения поправок в свою версию этой истории я рассказывал о том, как Диффи однажды представил идею криптосистемы с открытым ключом на неформальной встрече в IBM, которая не впечатлила ни одного из присутствовавших. Однако, покидая мероприятие, один из слушателей рассказал Диффи о другом «сумасшедшем парне» по имени Хеллман, который продвигал схожие идеи. Диффи бросил все свои дела и рванул на другой конец страны, чтобы встретиться с ним. Хеллмана сначала смутило появление незнакомца, проделавшего столь длинный путь ради встречи, но он быстро распознал в Диффи своего единомышленника, и они сформировали партнерство, вошедшее в историю.

На мой вопрос о том, насколько правдивой была моя версия, Хеллман ответил: «Появление Уита меня вовсе не смутило, на самом деле я был в восторге. Вот что произошло: я работал в IBM задолго до появления там Диффи, но ушел, чтобы преподавать в Массачусетском технологическом институте, а затем в Стэнфорде. В 1974 году я вернулся туда, чтобы рассказать о проблемах современной криптографии. В то время сотрудникам IBM это было не очень интересно. На тот момент я не знал, что незадолго до моего появления они изобрели так называемый алгоритм симметричного шифрования DES, который не смогли взломать. Руководство IBM посчитало, что все криптографические проблемы решены, и пришло время двигаться дальше. Уит, с которым я тогда еще не был знаком, пришел в IBM несколько месяцев спустя и выступил с аналогичным докладом. Его выступление завершилось так же, как и мое, за одним исключением. Алан Конхайм, возглавлявший в IBM отдел вычислений, предложил ему связаться со мной по возвращении в район залива [Сан-Франциско]. В то время Уит уже ездил по стране, общаясь со многими криптографами, включая Дэвида Кана, автора популярной книги по криптографии *The Codebreakers* **(https://www.amazon.com/CodebreakersComprehensive-History-Communication-Internet/dp/0684831309)**. Вернувшись в Сан-Франциско, Уит позвонил мне, и мы договорились о встрече. Изначально мы планировали поболтать часок, но в итоге проговорили гораздо дольше, и я даже пригласил его с супругой к себе домой, чтобы продолжить обсуждение и познакомить с семьей. В итоге мы разговаривали до 11 вечера. Это была осень 1974 года. До встречи с Уитом коллеги отговаривали меня от работы в области криптографии, ссылаясь на то, что у АНБ были огромные бюджеты и несколько десятилетий форы. Разве мог я надеяться обнаружить то, о чем они еще не знали? А если бы

мне и удалось достичь каких-нибудь успехов, это ведомство наверняка засекретило бы информацию. Оба аргумента казались весомыми, но, учитывая награду, которую мы в итоге получили, с нашей стороны было очень мудро сделать то, что все тогда считали глупостью. Вероятно, я продолжил бы развивать свою идею и в одиночку, однако встреча с Уитом дала мне дополнительную мотивацию. Кроме того, мы отлично ладили и работали вместе на протяжении последующих нескольких лет, в том числе над криптосистемой с открытым ключом».

Я спросил Хеллмана о том, кто именно был автором той или иной идеи. Мы знаем, что Меркл, будучи студентом Калифорнийского университета в Беркли, работая независимо от остальных, частично развил идею системы шифрования с открытым ключом, предполагающую обмен ключами по небезопасному каналу без предварительного согласования. Но что именно сделал Хеллман, а что Диффи? Мартин ответил: «Мне сложно точно определить вклад каждого. Мы работали над проектом вместе, обсуждая проблемы и делясь своими наработками. Однако Диффи определенно первым высказал идею криптосистемы с открытым ключом. К тому времени мы уже разработали идею криптосистемы с “потайным ходом”. Шифр такой системы имеет уязвимость (то есть потайной ход), которым могут воспользоваться только те, кто о нем знает. Диффи пошел еще дальше, разработав концепцию криптографии с открытым ключом и соответствующей криптосистемы, позволяющей не только обмениваться открытыми ключами, но и создавать цифровые подписи. Он сделал это в 1975 году. О том, что Меркл, независимо от нас, тоже размышлял об обмене открытыми ключами, мы узнали позднее. В 1976 году я разработал математическую реализацию этой идеи, которую теперь часто называют алгоритмом обмена ключами Диффи – Хеллмана, но поскольку эта реализация была гораздо ближе к идее Меркла, чем к нашей, я настаиваю на том, чтобы ее называли алгоритмом Диффи – Хеллмана – Меркла. Кстати, сейчас я сижу за тем же столом, где придумал этот алгоритм майской ночью 1976 года».

На вопрос о возникновении алгоритма RSA Хеллман сказал следующе: «Я прочитал лекцию в Массачусетском технологическом институте, и мы начали переписываться с Роном Ривестом. Незадолго до публичного представления алгоритма RSA он прислал мне его описание. Ознакомившись с ним, я подумал: “Мы это упустили!” Разработчики RSA сумели создать криптосистему с открытым ключом на основе факторизации больших простых чисел. Алгоритм Диффи – Хеллмана – Меркла использовал большие простые числа, но не их факторизацию. В статье, которую я написал совместно со своим студентом Стивом Полигом несколькими годами ранее, мы рассматривали RSA в качестве одного из вариантов, но в тот момент еще не думали о криптографии с открытым ключом, поэтому упустили этот момент».

Я спросил Хеллмана, что он чувствует в связи с тем, что алгоритм RSA обрел такую популярность и принес миллионы своим создателям, тогда как его команда практически ничего не получила за свой вклад. Вот что он ответил: «За многие годы меня не раз спрашивали об отношении к тому, что разработчики алгоритма RSA представили его вскоре после нашего открытия, упомянули нас

с Диффи в своей статье в качестве изобретателей криптосистемы с открытым ключом, но, организовав компанию RSA Data Security, отказались платить роялти. Мои чувства по этому поводу со временем изменились. Сначала я считал, что разработчики RSA не вполне адекватно подчеркнули связь между своими наработками и той работой, которую проделали мы со Стивом Полигом. Однако позже я стал смотреть на это иначе. Компания RSA настолько блестяще справилась с продвижением криптосистемы с открытым ключом, что создала совершенно новую индустрию. Я получил признание и возможности, которые, вероятно, никогда не открылись бы передо мной, если бы не разработчики RSA. Теперь я им благодарен. Я до сих пор дружу с Роном Ривестом. Честно говоря, я как раз хотел связаться с ним по телефону перед этим интервью».

Мне было интересно, насколько внимательно Хеллман следит за текущими тенденциями, и я спросил, что он думает о перспективах квантовой криптографии, на что он ответил: «Вы имеете в виду квантовую криптографию или квантовые вычисления? Я спрашиваю, потому что это две совершенно разные вещи. Квантовая криптография обеспечивает безопасную передачу ключей или информации с помощью квантовых эффектов. А квантовые компьютеры могут свести на нет надежность всех современных криптосистем с открытым ключом. Я не знаю, когда это произойдет и произойдет ли вообще. Это как с управляемым термоядерным синтезом. Ученые уже полвека говорят о том, что он станет возможным в ближайшие 20 лет. И все же такая вероятность существует. Но у меня есть несколько возможных решений этой проблемы. Нам нужно шифровать и подписывать данные двумя способами, чтобы в случае взлома одного, другой продолжал обеспечивать необходимую защиту. Например, у нас есть криптосистемы с открытым ключом и центры распределения ключей [KDC, которые используются в PGP-приложениях]. Людям следует шифровать свои ключи обоими способами, чтобы в случае взлома криптосистемы с открытым ключом с помощью квантовых вычислений защиту данных обеспечили KDC. Кроме того, для документов можно использовать не только традиционные подписи с открытым ключом, но и подписи Меркла **(https://en.wikipedia.org/wiki/Merkle_signature_scheme)**. Если вы серьезно относитесь к вопросам криптографической защиты и хотите предотвратить ее взлом в будущем, реализуйте систему двойной защиты. В АНБ этот принцип называется “ремень и подтяжки”. Если вы носите и то, и другое, то никогда не окажетесь со спущенными штанами, даже если один из аксессуаров перестанет их поддерживать». Полагаю, это и был ответ на мой вопрос.

Последняя часть нашего разговора была посвящена ядерному сдерживанию и улучшению отношений в браке. Хеллман и его жена написали замечательную книгу *A New Map for Relationships: Creating True Love at Home and Peace on the Planet* **(https://ee.stanford.edu/~hellman/publications/book3.pdf)**, которая освещает обе темы. Хеллман прислал мне экземпляр перед нашим интервью, чтобы узнать мое мнение, и, честно говоря, мне было слегка не по себе от мысли о том, что один из моих криптографических кумиров пытается соскочить с темы. Но книгу я все же прочитал. И она мне очень понравилась. Я подарил по экземпляру всем своим детям, которые уже состоят в браке. Хеллману каким-то

чудесным образом удалось вплести большую часть своего криптографического опыта в книгу об улучшении отношений и предотвращении ядерного апокалипсиса. В 2015 году Хеллман и Диффи получили премию Тьюринга **(https://amturing.acm.org/award_winners/hellman_4055781.cfm)**, своего рода Нобелевскую премию в области информатики. Хеллман и его жена решили потратить свою часть премии (500 000 долларов США) на то, чтобы снизить риски ядерной катастрофы, об угрозе которой вновь заговорили после президентских выборов в США в 2016 году. Браво!

Информация о Мартине Хеллмане

Более подробную информацию о Мартине Хеллмане вы можете получить по ссылкам:

• книга *A New Map for Relationships: Creating True Love at Home and Peace on the Planet*: **https://ee.stanford.edu/~hellman/publications/book3.pdf**;

• биография Мартина Хеллмана на сайте Стэнфордского университета: **https://ee.stanford.edu/~hellman/**;

• работы Мартина Хеллмана в области криптографии: **https://ee.stanford.edu/~hellman/publications.html**.

14. Обнаружение вторжений/угроз

Обнаружение вторжений – это искусство определения несанкционированной деятельности. В компьютерном мире это означает обнаружение несанкционированных подключений, авторизаций в системе и попыток доступа к ресурсам. Необходимость обнаружения вторжений – одна из причин, почему почти каждое компьютерное устройство имеет систему регистрации событий. Речь о них идет в работе Джеймса П. Андерсона 1980 года *Computer Security Threat Monitoring and Surveillance* (**https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf)**.

В то время как компьютерные системы хороши в генерации огромного количества событий, люди и их системы выявления угроз далеко не идеальны. Для большинства пользователей компьютеров журналы событий (логи) полны тысяч событий, которые затрудняют определение вторжений.

Лучший отчет о промежутках времени между неправомерной авторизацией в системе и обнаружением факта взлома публикуется компанией Verizon **(https://www.verizon.com/business/resources/reports/dbir/).** Отчет 2016 года **(https://enterprise.verizon.com/resources/reports/2016/DBIR_2016_Report.pdf)** показал следующие тревожные долгосрочные тенденции:

• среднее время от первоначального взлома хакером до утечки персональных или учетных данных обычно занимает от нескольких минут до нескольких дней;

• большинство злоумышленников (70–80 %) находятся в системе в течение длительного времени (месяцами) до обнаружения;

• обнаружение нарушений злоупотребления внутренними ресурсами происходит лишь в 10 % случаев.

И это несмотря на доказательства, что большинство нарушений регистрируются в логах и, вероятно, были бы обнаружены, если бы логи были просмотрены. Для ясности, я говорю о логах компьютерной системы, а также логах механизмов обеспечения информационной безопасности (например, брандмауэров, систем обнаружения вторжений и т. д.).

Характеристики эффективного предупреждения об инциденте

К сожалению, большинство средств системы безопасности генерируют в логах тысячи, если не миллионы сообщений о событиях, которые не относятся к злоупотреблениям. Или, если они указывают на фактическую вредоносность, документируются события, которые имеют очень и очень низкий риск для окружения (например, когда брандмауэр регистрирует заблокированный пакет). В результате большинство логов весьма «замусорены», т. е. содержат больше бесполезной информации, чем полезной. Имея это в виду, хорошее сообщение о событии системы безопасности должно иметь следующие характеристики:

• низкий уровень шума;

• низкий уровень ложных срабатываний и несрабатываний, т. е. появление предупреждения с высокой вероятностью указывает на реальный взлом;

• понятное описание события;

• глубокие подробности, которые могут быть полезны специалистам по ИБ;

• генерация события всегда инициирует расследование инцидента.

Вот это и есть святой Грааль обнаружения вторжений.

Развитые устойчивые угрозы

Развитые устойчивые угрозы (APT, Advanced Persistent Threats) – это атаки, которые проводятся профессиональными преступными группировками. В компрометации подавляющего большинства предприятий, военных систем и других субъектов в течение последнего десятилетия виновны атаки именно такого рода. На самом деле большинство экспертов по ИБ считают, что все подключенные к Интернету организации уже были успешно скомпрометированы или, в случае необходимости, могут быть скомпрометированы в любой момент. APT-атаки совершаются профессиональными хакерами, которые отличаются от обычных следующими особенностями:

• стараются сохранить присутствие в системе после первоначального взлома;

• не «убегают» в случае обнаружения;

• имеют десятки и даже сотни способов взлома и эксплойтов, которые могут использовать, включая уязвимости нулевого дня;

• всегда получают полный контроль над взломанной системой;

• ставят целью постоянную кражу интеллектуальной собственности;

• как правило, ведут атаки из «безопасной гавани» – страны, в которой их никогда не будут преследовать за их деятельность (все верно, во многих государствах хакерство часто спонсируется и поощряется).

APT-атаки намного сложнее выявить традиционными методами обнаружения вторжений. Это возможно, но очень непросто без внедрения и настройки систем обнаружения вторжений. Некоторые системы из числа рассмотренных в этой главе эффективно обнаруживают и предотвращают APT-атаки. Именно поэтому мы о них говорим.

Методы обнаружения вторжений

Существует два основных способа обнаружения вторжений: отслеживать подозрительное поведение и сканировать сигнатуры. Многие системы обнаружения вторжений включают оба перечисленных метода.

Обнаружение вторжений на основе поведения

Также известные как системы обнаружения аномалий, такие механизмы отслеживают подозрительное поведение, указывающее на злонамеренность. Примеры: копирование одного файла в другой (например, компьютерный вирус), внезапное перенаправление браузера на посторонний URL-адрес (например, рекламное ПО, атака посредника и т. д.), неожиданное соединение с ханипотом или копирование содержимого базы данных аутентификации (как в случае кражи учетных данных). Основная идея, лежащая в основе систем обнаружения вторжений на основе поведения, заключается в том, что существует слишком много способов взлома, чтобы их можно было определять по отдельности, поэтому вместо этого отслеживается подозрительное поведение. И в этом есть смысл. Например, существуют десятки миллионов компьютерных вирусов, большинство из которых могут таким образом быть обнаружены – все они копируют себя в новые файлы. Доктор Дороти Деннинг (речь о которой пойдет в главе 15), большой сторонник систем обнаружения вторжений, написала свой эпохальный труд по обнаружению аномалий **(http://users.ece.cmu.edu/~adrian/731-sp04/readings/denning-ids.pdf)** в 1986 году.

Обнаружение вторжений на основе сигнатур

В таких системах реализован противоположный подход. Считается, что вредоносное поведение меняется слишком часто или что легитимные программы могут вызывать ложные срабатывания. Антивирусные сканеры – прекрасный пример программ, анализирующих сигнатуры объектов. Они

содержат миллионы уникальных последовательностей байтов (сигнатур), которые при обнаружении будут указывать на вредоносность.

Инструменты и сервисы обнаружения вторжений

В целом любое аппаратное или программное защитное обеспечение, которое обнаруживает и оповещает о вредоносных действиях, – это программа обнаружения вторжений. К ним относятся брандмауэры, ханипоты, антивирусные программы и системы управления событиями. Некоторые эксперты используют только решения, в названии которых присутствует словосочетание «обнаружение вторжений».

Системы обнаружения/предотвращения вторжений

Системы обнаружения вторжений (IDS, Intrusion Detection System) специально созданы для обнаружения вредоносных действий и обычно используют комбинацию методов детектирования подозрительного поведения и анализа сигнатур. Системы предотвращения вторжений (IPS, Intrusion Prevention System) обнаруживают и препятствуют вредоносным действиям. Многие IDS также используют алгоритмы предотвращения вторжений в целях защиты, поэтому IDS может означать и IPS. Некоторые специалисты по ИБ не применяют автоматизированные алгоритмы предотвращения в IDS из-за частых ложных срабатываний, которыми грешат многие такие системы. Иногда, в случае IPS с низким риском ложного срабатывания, таких как решения для защиты от вредоносных программ, автоматическое предотвращение используется.

Различаются хостовые и сетевые IDS и IPS, в зависимости от того, будет ли осуществляться защита отдельных узлов системы или анализироваться пакеты в сети.

Первой широко популярной хостовой IDS, которую я помню, была Tripwire (**https://en.wikipedia.org/wiki/Tripwire_(company))** еще в 1992 году. Она основана студентом Университета Пердью Джином Кимом и его профессором, доктором Юджином Спаффордом. Это не случайно, что в Университете Пердью также преподавала Дороти Деннинг.

Первой суперпопулярной сетевой IDS на моей памяти была бесплатная Snort **(www.snort.org/)**. Мне повезло, меня научил ею пользоваться создатель, Мартин Рош, в начале 1990-х на тренинге в компании SANS Institute. Сейчас это все еще очень популярный коммерческий продукт, предлагаемый в бесплатной и платной версиях компанией Sourcefire.

Системы управления событиями

За каждым успешным решением по обнаружению вторжений или программой для управления логами стоит система, которая находит и собирает события от одного или нескольких «датчиков». На каждом предприятии с большим количеством компьютеров необходимо собрать и проанализировать эти события в целом, чтобы получить полную картину. Системы управления отвечают за их

сбор, анализ и создание оповещений. От того, насколько хорошо и точно системы выполняют свою работу, зависит общая эффективность. У каждой системы управления событиями множество компонентов и свои особенности. Специальная публикация NIST 800-92 *Guide to Computer Security Log Management* **(https://csrc.nist.gov/publications/detail/sp/800-92/final)** считается наиболее полным руководством по эффективному управлению событиями. Это трудный и ресурсоемкий процесс. Соответственно, существует множество компаний, готовых сделать всю сложную работу за вас. Это так называемые SIEM (Security information and event management) – компании или сервисы, управляющие информацией о безопасности и событиями безопасности.

Обнаружение сложных постоянных угроз (APT)

Профессиональные APT-хакеры умеют проникать в компании, практически не оставляя следов. В течение многих лет считалось трудным, если не невозможным, их обнаружить. Но в итоге методы обнаружения вторжений стали эффективнее, и теперь доступно несколько продуктов, сервисов и компаний, весьма успешных в поиске APT-атак и им подобных.

Производители операционных систем создают функции и службы, которые значительно лучше находят такого рода преступления. Примерами могут служить сервисы компании Microsoft Advanced Persistent Threat **(https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics)** и Advanced Threat Protection **(https://www.microsoft.com/en-us/WindowsForBusiness/windows-atp)**.

Многие компании теперь регулярно отслеживают поведение десятков APT-группировок, определяя, что и где они делают. Многие компании предлагают услуги по быстрому обнаружению APT-атак и оповещению об их присутствии. Вероятно, самая большая разница между традиционными и более новыми методами обнаружения вторжений заключается в возможности у последних сбора данных о многих компаниях в Интернете. В этой области наиболее известны компании CrowdStrike **(https://www.crowdstrike.com/)**, AT&T Cybersecurity **(https://cybersecurity.att.com/)** и давний игрок на рынке TrendMicro **(https://www.trendmicro.com/ru_ru/business.html)**. Хакерам становится все труднее скрыть свое вторжение.

Следующая глава повествует о пионере обнаружения вторжений, докторе Дороти Деннинг. В главе 16 речь пойдет о Михаиле Дубинском, менеджере по продукции одного из наиболее передовых сервисов обнаружения вторжений, доступных сегодня.

15. Профиль: доктор Дороти Деннинг

На протяжении нескольких десятилетий я думал, что один из моих особых талантов в области информационной безопасности – это умение обнаруживать признаки вредоносной хакерской активности. Я могу заметить потенциальную хакерскую угрозу и найти способы ее более раннего обнаружения и генерации оповещений. Я по-прежнему считаю, что у меня это получается лучше, чем у

кого бы то ни было, однако я взаправду считал, что мой подход к обнаружению вторжений/аномалий абсолютно оригинален. Даже слегка задавался по этому поводу. Но потом я узнал о выдающейся работе доктора Дороти Деннинг для IEEE (Института инженеров электротехники и электроники), посвященной экспертным системам обнаружения вторжений в реальном времени **(https://users.ece.cmu.edu/~adrian/731-sp04/readings/denning-ids.pdf)**. В ней было описано все то, что я считал своим «оригинальным» видением, правда доктор Деннинг написала свою работу в 1986 году, задолго до того, как я сделал свои «открытия».

Это был первый из тех многочисленных случаев, когда я осознавал, что мое «оригинальное» видение вовсе не было таковым. Все мы опираемся на открытия великих людей, а доктор Деннинг, безусловно, стала легендой и одним из первопроходцев в области информационной безопасности. Вот что она мне сказала: «Когда я начинала работу, такой отдельной сферы, как информационная безопасность, еще не существовало. Не было ни книг, ни журналов, ни конференций, посвященных этой теме. Нам были доступны лишь докторские диссертации и несколько статей, опубликованных в таких мультидисциплинарных журналах, как Communications of the ACM. Но мне повезло работать в Университете Пердью, одном из немногих, начавших работу в области информационной безопасности наряду с МТИ и другими».

В колледже доктор Деннинг увлекалась математикой и думала, что станет преподавать ее старшеклассникам. Но в процессе получения степени бакалавра математики в Мичиганском университете она работала под руководством директора радиоастрономической обсерватории, который порекомендовал ей освоить программирование для решения рабочих задач. На последнем году обучения она прошла один из немногих доступных в то время курсов по информатике. Позже, в Университете Рочестера, Дороти создала транслятор командного языка, чтобы упростить выполнение программ на мэйнфрейме IBM, а также разработала и преподавала курсы по языкам программирования и компиляторам. Любовь к преподаванию мотивировала ее на получение докторской степени в Университете Пердью, где она изучала курс по операционным системам, который читал ее будущий муж, Питер Деннинг. В рамках этого курса рассматривались принципы обеспечения информационной безопасности на уровне ОС. Это положило начало многолетнему увлечению темой информационной безопасности. Она даже преподавала один из первых в стране курсов по этому предмету.

Примечание. Транслятор, разработанный доктором Деннинг, переводил команды, написанные на языке Рочестерского университета Easy Control Language, на язык управления заданиями (Job Control Language) компании IBM, который пользователи считали слишком сложным.

Дороти Деннинг получила докторскую степень в 1975 году, создав решетчатую модель безопасности, которую можно представить в виде структуры классификации информации, образующей решетку таким образом, что

информация может проходить через нее лишь в одном направлении и только от низших к высшим или равным уровням классификации. Концепция однонаправленного информационного потока по-прежнему остается движущей силой «оригинальных» разработок в области ИБ. В основе двух недавних проектов, над которыми я работал в Microsoft, – защищенные администраторские рабочие станции (**https://msdn.microsoft.com/en-us/library/mt186538.aspx**) и улучшенная среда администратора безопасности (ESAE) (**https://technet.microsoft.com/windows-server-docs/ security/securing-privileged-access/securing-privileged-access-reference-material**), – лежит определенный информационный поток, подчиняющийся тем же правилам.

В своей работе доктор Деннинг описала метод использования решетчатой математической модели для защиты информации. Вот что она мне сказала: «Я много размышляла на тему классификации и защиты данных, и, когда разработала модель и ее математическое обоснование, подумала, что это может стать новым словом в области компьютерной безопасности. Я поделилась своими теоремами и доказательствами с мужем, и он сказал, что это называется *теорией решеток*, а также назвал имя эксперта [Гаррета Биркгофа], написавшего об этом книгу. До того момента я полагала, что разработала новую математическую теорию». История доктора Деннинг слегка утешила меня по поводу моих собственных «открытий».

Доктор Деннинг опубликовала статью *A Lattice Model of Secure Information Flow* (**http://faculty.nps.edu/dedennin/publications/lattice76.pdf**) в 1976 году, после чего теория решеток начала применяться в области защиты информации. Статья содержит множество простых объяснений и математических формул, но в ней не говорится о конкретном способе реализации модели в операционной системе. Несмотря на то что сама Деннинг модель не реализовывала, в ее диссертации и более поздней работе **(http://faculty.nps.edu/dedennin/publications/CertificationProgramsSecureInfoFlow.pdf)** описан способ модификации компилятора с целью проверки потоков выполнения программ, которым пользуются другие люди при реализации ее модели.

Одной из основных тем в работе доктора Деннинг была защита конфиденциальной информации, в том числе при ее программной обработке. «Я думаю, – сказала она, – что хороший пример в данном случае – отправка налоговой декларации в соответствующую программу или сервис для обработки. В идеале в ходе такой обработки ваша конфиденциальная информация не должна попасть в чужие руки».

Я спросил, как, по ее мнению, сегодня обрабатывается конфиденциальная информация, на что она ответила: «Вообще, ситуация выглядит не очень хорошо. Информация постоянно оказывается не в тех руках. Сейчас многие компании прикладывают недостаточно усилий для защиты информации».

В 1982 году доктор Деннинг написала учебник *Cryptography and Data Security* **(https://www.amazon.com/Cryptography-Security-DorothyElizabeth-Robling/dp/0201101505)**, оказавший значительное влияние на развитие отрасли.

Причина, по которой она написала эту книгу, заключалась в том, что она сама не смогла найти необходимое пособие для преподавания курса по этому предмету. Это была первая из ее книг. За свою карьеру она написала несколько книг и более 170 статей и технических документов. В 1983 году Дороти начала работать в SRI International, некоммерческом научно-исследовательском институте, основанном попечителями Стэнфордского университета. Там она разрабатывала систему обнаружения вторжений для ВМФ, результатом чего стала работа, посвященная экспертным системам, которую я упомянул в начале главы.

После этого Деннинг перешла в довольно успешную на тот момент компанию Digital Equipment Corporation (DEC), результатом работы которой были тысячи патентов в области компьютерных технологий. В процессе сотрудничества с DEC она провела множество интервью с компьютерными хакерами, чтобы понять их мотивы и психологию. В результате Дороти написала еще несколько статей. Интервьюирование хакеров и параллельная работа по предотвращению их незаконной деятельности вызвали неоднозначное отношение к ее методам. И хотя она не стремится к подобным противоречиям нарочно, совершенно очевидно, что они вовсе не мешают ей в поиске решений. Это еще одна тема, которая иногда проявляется в работе Дороти, когда она открывает новые горизонты и провоцирует дискуссии. В ходе другого интервью доктор Деннинг посетовала на то, что иногда эмоции других людей по поводу того или иного вопроса мешают его публичному обсуждению.

В 1991 году она покинула компанию DEC и вернулась в Джорджтаунский университет, чтобы преподавать курс по ведению информационных и кибервойн в качестве директора Джорджтаунского института информационной безопасности. В 2002 году она перешла в Высшую школу ВМФ США в качестве профессора на кафедру оборонной аналитики, где работает по сей день. В 1999 году, еще в Джорджтаунском университете, она написала свою последнюю книгу *Information Warfare and Security* **(www.amazon.com/Information-Warfare-Security-Dorothy-Denning/dp/0201433036/)**. По ее словам, после этого она уже не возвращалась к писательству, так как было слишком сложно идти в ногу со временем и не хотелось писать то, что оказалось бы устаревшим еще до публикации.

За свою карьеру доктор Деннинг получила множество наград, которыми мог бы гордиться любой специалист по информатике. Среди прочего она была удостоена премии Ады Лавлейс **(https://www.acsac.org/ncss-winners.html)** и национальной премии в области разработки информационных систем безопасности **(https://www.acsac.org/ncss-winners.html)**. В 1995 году она стала членом Ассоциации вычислительной техники **(http://awards.acm.org/award_winners/denning_1239516.cfm)**, а в 2012 году введена в Национальный зал славы кибербезопасности **(http://www.cybersecurityhalloffame.com)**.

В конце 2016 года доктор Деннинг официально ушла в отставку. На мой вопрос о том, собирается ли она продолжать работать над проблемами информационной безопасности, она сказала следующее: «Я и дальше буду

работать, но теперь, получив статус заслуженного профессора, я освободилась от ряда служебных обязанностей и могу сосредоточиться на том, что мне интересно. Я все еще активно работаю в нескольких направлениях и собираюсь кое-что написать. Но я также люблю ходить в походы, чтобы очистить разум». По-моему, любой профессионал хотел бы иметь столь же продолжительную карьеру и оказать на мир такое же влияние, как это сделала доктор Деннинг.

Информация о докторе Дороти Деннинг

Поближе познакомиться с личностью доктора Деннинг помогут следующие источники:

• интервью Гари Макгроу с доктором Дороти Деннинг для Silver Bullet Security Podcast: **https://www.cigital.com/podcasts/show-011/**;

• интервью Чарлза Бэббиджа из Университета Миннесоты с доктором Дороти Деннинг в 2012 году: **http://conservancy.umn.edu/bitstream/handle/11299/156519/oh424ded.pdf**.

16. Профиль: Михаил Дубинский

Я уже давно весьма критично отношусь к продуктам для обеспечения информационной безопасности. Это объясняется тем, что за два десятилетия вредоносное ПО и эксплойты стали гораздо проще в использовании, а антивирусные программы зачастую не соответствуют заявленным характеристикам эффективности. Я зарабатываю на жизнь, тестируя такие программы, и нередко получаю на проверку до двадцати новых продуктов в день. Если за год мне попадается хотя бы одно приложение, которое действительно способно делать то, что от него ожидается, и существенно снижает риск взлома, это вызывает у меня настоящий восторг. Зачастую достаточно эффективные приложения не попадаются мне годами. Нередко я критикую и продукты, выпускаемые компанией, в которой работаю сам.

Учитывая это, должен сказать, что я был поражен новым продуктом Microsoft Advanced Threat Analytics (ATA). Он понравился бы мне вне зависимости от того, кто именно его разработал. ATA использует по-настоящему передовые методы анализа событий и сетевого трафика для обнаружения активных угроз, в том числе таких сложно выявляемых атак, как Pass-the-hash **(https://en.wikipedia.org/wiki/Pass_the_hash)** и Golden Ticket **(www.infoworld.com/article/2608877/security/fear-the-golden-ticket-attack-.html)**. Понаблюдав за работой ATA, я подумал, что с радостью бросил бы то, чем занимаюсь сейчас, и занялся продвижением этой замечательной платформы. Это не преувеличение. Я охотно сменил бы работу, если бы мне представилась такая возможность. Это действительно отличный продукт.

Компания Microsoft приобрела израильский стартап Aorato, разработавший платформу ATA, в ноябре 2014 года. Ежегодно в сфере информационной

безопасности создаются тысячи стартапов. Если вам доводилось развивать стартап, вы знаете, что это предполагает длительную напряженную работу в кругу единомышленников. Я знаком со многими людьми, которые «выгорели» в ходе работы над проектом, который так и не стал успешным. Они рисковали всем, соглашаясь на маленькую зарплату и тяжелую работу, в итоге не получая того вознаграждения, на которое рассчитывали. Мой брат-близнец Ричард А. Граймс, развивавший несколько интернет-стартапов, однажды сказал: «Если еще один стартап предложит мне в качестве оплаты долю в будущей прибыли, я скажу, что купить продукты и оплатить счета за электричество ею не получится».

Израильтянину Михаилу Дубинскому повезло. Менее чем через полгода после его прихода в Aorato стартап был приобретен компанией Microsoft. Теперь Дубинский главный менеджер по продукту ATA. Он по-прежнему много работает, но в более комфортных условиях крупной корпорации.

Сложная обстановка, в которой существует Израиль и его жители, привела к тому, что в этой маленькой стране было разработано огромное количество продуктов, предназначенных для обеспечения информационной безопасности. Израильские компании постоянно создают новые и передовые средства компьютерной защиты. Несколько лет назад меня наняли для обучения использованию ханипотов солдат Армии обороны Израиля, в которой должен отслужить каждый израильтянин. Я сам применял ханипоты и обучал этому людей на протяжении всей своей карьеры и даже написал о них книгу. Но когда я начал работать с израильскими военными, оказалось, что они знали об этой технологии не меньше моего и уже использовали ханипоты, которые я собирался им продемонстрировать. Мне оставалось лишь помочь им сделать системы более привлекательными и реалистичными.

Позднее я узнал, что с подобным опытом сталкиваются очень многие иностранцы, приезжающие в Израиль для преподавания основ информационной безопасности. В отличие от жителей большинства других стран, израильтяне с детства вынуждены задумываться о средствах обороны. За неделю, пока я находился в Тель-Авиве, по городу было выпущено несколько ракет. На занятии присутствовало примерно 20 человек, и я спросил, кто из них видел ракету, выпущенную в нашу сторону, которая, скорее всего, приземлилась бы где-то поблизости, если бы не была перехвачена. Почти все присутствующие подняли руки. Жизнь в таких условиях существенно влияет на приоритеты и восприятие действительности. А также способствует созданию выдающихся продуктов для обеспечения информационной безопасности.

Я спросил Дубинского, прожил ли он всю свою жизнь в Израиле, на что он ответил: «Я родился в Латвии, которая находится в Балтийском регионе Северной Европы. После Второй мировой войны она была частью СССР, а в 1990 году провозгласила свою независимость. Примерно тогда же мы с родителями переехали в Израиль и поселились к югу от Тель-Авива».

На мой вопрос о том, как он попал в сферу информационной безопасности, Дубинский сказал: «Я интересуюсь компьютерами с детства. И мне очень помог

один мой сосед, который был инженером-программистом. Сначала я просто возился с компьютерами, программировал на языках BASIC и Pascal, а также учился использовать дизассемблеры. Затем я заинтересовался троянами удаленного доступа (RATs), вроде SubSeven **(https://en.wikipedia.org/wiki/Sub7)**, с помощью которых разыгрывал друзей. Используя методы социальной инженерии или фишинга, я побуждал их устанавливать троянские программы, а затем шутил над ними, например, открывая дисководы их компьютеров. Потом я решил украсть чьи-нибудь учетные данные для получения доступа к Интернету. Это были времена dial-up-модемов и дорогого Интернета. Используя те же хакерские навыки, с помощью которых разыгрывал друзей, я украл чужие учетные данные для подключения к Интернету, но меня поймали. Родители очень расстроились и лишили меня компьютера. Позднее, во время прохождения службы в армии Израиля, я занимался компьютерной безопасностью. Больше всего меня интересовала тема аутентификации и способы повышения ее надежности».

Я спросил Дубинского о том, как он попал в Aorato. Такой оказалась его история: «В 2014 году я стал тринадцатым сотрудником этой компании, созданной двумя годами ранее. Я сразу сосредоточился на инженерных проблемах и поиске новых рабочих способов обнаружения вредоносных программ. Моя деятельность велась в двух направлениях. Первым было нахождение новых способов обнаружения вредоносного ПО, а вторым – усовершенствование конечного продукта путем расширения его возможностей. Спустя полгода после моего прихода в компанию Aorato она была приобретена корпорацией Microsoft, которая выразила нам полное доверие и поддержку. Мы по-прежнему работаем с замечательными людьми и создаем продукт, который пользуется большим успехом». Когда я спросил Дубинского о том, что он считает самой большой проблемой в сфере информационной безопасности, он ответил: «Образование. Большинство людей так или иначе на что-то нажимают. Сколько бы технологий вы ни внедрили, кто-нибудь все равно на что-нибудь нажмет. Ключ к предотвращению атак – образование».

Информация о Михаиле Дубинском

Больше информации о Михаиле Дубинском вы найдете по ссылке:

• Михаил Дубинский в Twitter: **https://twitter.com/michaeldubinsky**.

17. Брандмауэры

Брандмауэры – отличный пример того, как технология становится жертвой собственного успеха. Они так хорошо защищали компьютеры в течение трех десятилетий, что угрозы, против которых были созданы, практически перестали существовать. Плохие парни сдаются! По крайней мере, в области определенных типов угроз. Некоторые эксперты даже утверждали, что брандмауэры больше не нужны, но большинство считают, что они, как и

сканеры вредоносного ПО, – необходимые элементы информационной безопасности в любой сфере.

Что такое брандмауэр?

Если вкратце, брандмауэры – это программный или аппаратный компонент, предназначенный для предотвращения несанкционированного доступа между двумя или более границами безопасности. Его работа традиционно основана на имени протокола или номера порта, а на сетевом уровне обычно происходит фильтрация пакетов. Многие брандмауэры также могут разрешать или запрещать трафик на основе имен пользователей, устройств, членства в группах и сведений, содержащихся на верхних уровнях трафика приложений. Они часто предлагают дополнительные расширенные функции, такие как анализ пакетов высокого уровня, обнаружение/предотвращение вторжений, обнаружение вредоносных программ и VPN. Большинство брандмауэров поставляются с подробными лог-файлами. После запуска любого брандмауэра его журнал тут же заполняется записями.

Происхождение брандмауэров

Начало тому, что эксперты по безопасности позже определят как ранний брандмауэр на уровне приложений, было положено в 1987 году администраторами компании AT&T Bell Labs Дейвом Пресотто и Говардом Трики на компьютере VAX под управлением BSD с двумя сетевыми интерфейсами для защиты внутренних пользователей и их компьютеров. ПО позволяло получать доступ к Интернету, но не допускало несанкционированных входящих подключений. Они применяли собственный шлюз сеансового уровня, который появился на семь лет раньше, чем в протоколе SOCKS-прокси. Уильям Чесвик в начале 1988 года использовал такой же шлюз.

Примечание. Слово «брандмауэр» использовалось в фильме «Хакеры» 1983 года, но его значение не было четко определено.

Первое упоминание о брандмауэрах в технической документации содержится в презентации 1987 года под названием *The Packet Filter: An Efficient Mechanism for User-level Network Code* Джеффри К. Могула (он был сотрудником компании ACM и теперь работает в Google **(https://research.google.com/pubs/JeffreyMogul.html**), Ричарда Ф. Рашида и Майкла Дж. Аксетты, на симпозиуме ACM, посвященном принципам операционных систем.

Защищенная брандмауэром сеть Чесвика подверглась атаке печально известного Червя Морриса в ноябре 1988 года **(https://en.wikipedia.org/wiki/Morris_worm)**. Благодаря изменению настроек и удачному стечению обстоятельств брандмауэр и компьютеры, находящиеся под его защитой, не пострадали, в то время как сотни других сетей и тысячи компьютеров были заражены. Это был один из первых случаев, когда брандмауэр доказал важность своей роли в общих аспектах ИБ. Чесвика беспокоило удачное стечение обстоятельств, он обновил

исходную конфигурацию брандмауэра, добавив еще одну границу безопасности между внутренним и внешним интерфейсом. В конце концов он назвал это «прокси», и именно тогда в первый раз это слово было использовано в таком контексте.

Чесвик описал брандмауэры в 1990-м в трудах USENIX, а в 1994 году вместе со Стивеном Белловиным написал оригинальную книгу *Firewalls and Internet Security: Repelling the Wily Hacker*. Чесвик вспоминает удивительную популярность книги: «Брандмауэр Checkpoint Firewall Zone 1, который позже был переименован в Checkpoint Firewall, впервые появился весной 1994 года, на конференции Interop, то есть примерно через неделю после публикации книги. Издатель ожидал, что тираж составит 8–12 тысяч копий. Первая партия в 10 000 была продана за неделю, и они так быстро выпустили второй тираж в 20 000, что мы не успели исправить недоработки. Всего было продано около 100 000 копий, переведенных на десяток языков».

Брайан Рид и другие сотрудники компании Digital Equipment Corporation (DEC) выполняли аналогичную работу над брандмауэрами, взаимодействуя через Интернет с помощью корпоративной сети. Тем не менее их брандмауэр был больше сосредоточен на блокировке исходящего доступа, так как DEC ранее потерял важное программное обеспечение из-за несанкционированной эксфильтрации данных.

Маркус Ранум написал первый крупный коммерческий продукт брандмауэра для DEC в 1990 году и другую его версию под названием Screening External Access Link (SEAL) вместе с Джеффом Маллиганом в 1991 году. В то же время Джеффри Могул выпустил screend, один из первых брандмауэров **(https://www.researchgate.net/publication/2443301_Using_screend_to_Implement_IPTCP_Security_Policies)**. Затем последовали другие коммерческие брандмауэры от разных поставщиков, включая Tis Gauntlet, Checkpoint и Dupont’S Raptor Eagle. Ранум создал инструментарий брандмауэра с открытым исходным кодом в 1993 году в рамках проекта для Управления перспективными исследовательскими проектами Министерства обороны США (спонсора ранней версии Интернета) и Белого дома США.

Кульминацией всех этих действий стали брандмауэры, которые стали важным компонентом любой популярной операционной системы. Компания Microsoft Windows создала брандмауэр Windows, впервые выпущенный в Windows XP в 2001 году. Второй пакет обновлений вышел в августе 2004 года и был включен по умолчанию. Это изменение непосредственно связано с огромным снижением опасности вредоносных программ на базе Windows, которые в противном случае могли бы быть успешными. Сегодня многие устройства, включая интернет-маршрутизатор, беспроводной маршрутизатор и кабельное/спутниковое телевидение, содержат настраиваемые пользователем брандмауэры.

Правила брандмауэра

Все брандмауэры имеют правила (или политики). Наиболее распространенное правило брандмауэра по умолчанию следующее: разрешать все выходы, но запрещать любые неопределенные входящие подключения, которые ранее не были созданы исходящим подключением. Самые безопасные брандмауэры также ограничивают любой ранее неопределенный исходящий трафик. К сожалению, когда применяются чрезмерно строгие правила, это часто приводит к слишком серьезному прерыванию работы или управления, и поэтому большинство разработчиков используют наиболее распространенное правило по умолчанию.

Размещение брандмауэров

Брандмауэры можно размещать на уровне сети или непосредственно на узлах компьютеров.

На уровне сети

Традиционно большинство брандмауэров расположены как сетевые устройства между двумя или более сегментами сети. Изменилось только то, что количество управляемых сегментов увеличилось до такой степени, что некоторые брандмауэры могут управлять десятками сегментов одновременно. Современные новые программно-определяемые сети (SDN) содержат некоторые компоненты пересылки пакетов, которые могут напрямую отследить их происхождение до традиционных брандмауэров.

На узлах компьютеров

Многие люди считают, что даже защищенной брандмауэром сети нельзя доверять. Чесвик сказал, что внутри периметра сетевого брандмауэра находится «мягкий центр». Он также говорил, что мы должны убедиться, что все наши хосты (узлы) надежно настроены и защищены, чтобы уберечь себя от вещей, которые проходят через периметр сетевого брандмауэра.

Брандмауэры в узлах могут с этим помочь. Обычно они работают на уровне сети и пакетов, но часто имеют дополнительные возможности, поскольку интегрированы с хостом и его операционной системой. Например, брандмауэр Windows можно легко настроить как для отдельных служб, так и для пользователей и групп. Windows поставляется со встроенными почти ста правилами брандмауэра, которые включены операционной системой, даже если вы отключите управляемое пользователем программное приложение.

Многие специалисты по ИБ полагают, что каждый хост должен быть в состоянии только связаться с другими четко определенными хостами, следуя, по существу, очень безопасным, строгим правилам брандмауэра, которые определяют точно, какой трафик существует между хостами. Этот вид ультрагранулированного управления считается святым Граалем брандмауэров. К сожалению, сложность и управление такими межсетевыми экранами делает

маловероятным их широкое масштабирование, выходящее за рамки некоторых небольших сверхбезопасных сценариев.

Повышенная безопасность

Расширенные брандмауэры существуют уже несколько десятилетий и обычно ссылаются на функции, которые традиционный брандмауэр для фильтрации пакетов не предлагает. Традиционный брандмауэр может блокировать по протоколу (по имени или номеру), но расширенный блокирует почти любой подробный индивидуальный компонент протокола (иногда называемый «глубокой проверкой пакетов»). Или может объединить несколько пакетов для идентификации определенных атак. Традиционный брандмауэр отбрасывает определенное количество пакетов, но только продвинутый вариант покажет, что вы находитесь под атакой отказа в обслуживании. Брандмауэры-приложения могут просматривать прикладные уровни сети и обнаруживать угрозу или предотвращать ее попадание на хост. Например, расширенный брандмауэр может удалить последовательность переполнения буфера из веб-сервера. Они настолько распространены, что большинство брандмауэров до некоторой степени расширены.

От чего защищают брандмауэры

Брандмауэры предотвращают вредоносные атаки, происходящие из несанкционированного сетевого трафика. Традиционно удаленные атаки переполнения буфера на уязвимые серверы были угрозой номер один, с которой брандмауэры справлялись. Но со временем серверы стали более надежными (в основном благодаря тому, что их базовые операционные системы стали более безопасными по умолчанию), а брандмауэры усложнили злоумышленникам успешное использование этих типов атак. Соответственно, немногие современные атаки будут предотвращены брандмауэром из-за их реализации. Например, если конечного пользователя можно обманом заставить запустить троянскую программу, приходящую по электронной почте, брандмауэр мало что может сделать, чтобы предотвратить последующую злонамеренность. Тем не менее, поскольку брандмауэры легкодоступны (часто бесплатны и реализуются по умолчанию) и могут остановить определенные типы атак, большинство людей считают, что они должны быть активированы на каждой сети и вычислительном устройстве. Вы можете выбрать, активировать его или нет. В любом случае, этот выбор, по существу, указывает на большой успех брандмауэров.

В главе 18 представлен профиль одного из первых создателей брандмауэров, Уильяма Чесвика.

18. Профиль: Уильям Чесвик

Как уже говорилось в предыдущей главе, Уильям Чесвик – один из создателей современного брандмауэра. Он взял на себя управление первым документированным брандмауэром, изобрел сетевой брандмауэр, и, если вы

используете слово «прокси» в своей работе в сфере ИБ, вам следует его поблагодарить. У Чесвика более десятка патентов. Кроме того, в соавторстве со Стивеном Белловиным, в 1994 году он выпустил первую книгу о брандмауэрах *Firewalls and Internet Security: Repelling the Wily Hacker* **(https://www.amazon.com/Firewalls-Internet-Security-RepellingHacker/dp/020163466X)**. Я работал с брандмауэрами и до прочтения этой книги, но она помогла мне узнать многое из того, что мне известно о брандмауэрах сейчас. Она стоит на моей книжной полке вот уже более двадцати лет.

Его знаменитая статья *An Evening with Berferd in which a Cracker Is Lured, Endured, and Studied* **(http://www.cheswick.com/ches/papers/berferd.pdf)** познакомила многих из нас с ханипотами. Благодаря Чесвику термин jail стал прямым командным словом в системе FreeBSD, а chroot jail – один из самых простых и популярных способов изоляции отдельных подсистем в Unix и Linux. Немногие люди оказали такое же большое влияние на границы ИБ. Он также один из самых оптимистичных экспертов в области ИБ, с которыми я встречался. При этом Уильям понимает, что многое еще нужно исправить.

Я спросил Чесвика, как он попал в Лабораторию Белла, где работает специалистом по ИБ. Он рассказал: «В 1968 году я был химиком, но увидел первые компьютеры и подумал, что в будущем они станут популярными, поэтому заинтересовался ими. В конце концов этот интерес победил химию. Я попал в консалтинговую компанию SET. Мы осуществляли техническую работу для других компаний. За девять лет работы я познакомился с некоторыми людьми из Лаборатории Белла. Они мне понравились, как и само место. Я был бы счастлив, даже если меня взяли бы туда уборщиком. В конце 1987 года я прошел собеседование. Люди, которые его проводили, были гигантами в этой области: например, Деннис Ричи (создатель языка программирования C) и Кен Томпсон (соавтор Unix вместе с Ричи). Я был счастлив просто поговорить с ними и не расстроился бы, даже если бы меня не взяли, но почему-то я им приглянулся и вскоре стал членом их команды. В один из первых дней я подошел к Дэйву Пресотто [создателю первого файервола] и вызвался взять на себя брандмауэр. Он согласился».

По моей просьбе Чесвик, создатель брандмауэра цепного уровня, объяснил, что это такое: «Он буквально воссоздает трафик, шаг за шагом, между двумя или более шагами брандмауэра. Каждый пакет реконструируется и изменяется, чтобы выглядеть так, как если бы каждый исходящий пакет шел от брандмауэра. Для всех за пределами брандмауэра он выглядит как инициатор трафика. Прежде любой посторонний видел, что пакеты исходят от компьютеров. Сегодня каждый брандмауэр делает это по умолчанию».

Я спросил Чесвика, как он познакомился со своим будущим соавтором Стивеном Белловином. «Стивен уже работал в Лаборатории Белла до моего прихода. Дэйв Пресотто учил меня в классе TCP/IP, который Стивен также посещал. Мы подружились и постоянно говорили о брандмауэрах и различных угрозах. В конце концов мы создали “пакетный телескоп” (ранний анализатор

пакетов). Мы получили большую сеть класса A в Лаборатории, и у нее было так много IP-адресов, что мы не могли с ними справиться. Подсети в такой большой сети не очень хорошо работали в то время. Поэтому я анонсировал “12 network” в Интернете, чтобы посмотреть, что произойдет. Довольно скоро мы стали получать 25 Мб данных ежедневно. Многое кончилось гибелью трафиков в зараженных компьютерах. Но это немалому нас научило. Стивен писал об этом в своей статье *There Be Dragons* (**https://academiccommons.columbia.edu/catalog/ac:126916)**. В итоге мы сделали первый DNS-прокси, опираясь на то, что узнали. Так и появилась наша книга. Она вышла в нужное время, потому что до этого о брандмауэрах не писали книг, а они тем временем стали очень популярны. Мы продали много копий и неплохо заработали».

Я спросил Чесвика о его патентах. Я сам работал над получением нескольких и знаю, как трудно их получить. Он поделился: «У меня было бы гораздо больше патентов, если бы я знал, что то, что мы делаем, можно запатентовать. Раньше все казалось “очевидным” (“очевидный” – это юридический термин, который означает “непатентоспособен”), по крайней мере, так я думал. То, что мы делали, казалось очевидным – здравым смыслом – для меня и 12 парней, с которыми мы это обсуждали. Меня даже посещали патентные юристы и спрашивали, можно ли патентовать то, над чем я работал в то время. Я сказал нет, потому что это очевидно. Если бы я тогда промолчал, у меня было бы гораздо больше патентов. Годы спустя кто-то другой получил патент на то, о чем мы думали и что делали задолго до него. У меня даже есть несколько патентов и авторских прав, которые часто игнорируются, например на мои интернет-карты **(http://cheswick.com/ches/map/)**. Они были поистине революционны для того времени. Мы даже основали картографическую компанию Lumeta. Теперь я вижу, что мои интернет-карты все на месте, а я почти никогда не указан в источниках. Недавно я был на конференции, и спикер выложил одну из моих интернет-карт, конечно, некредитированную, и около половины аудитории посмотрели на меня, потому что знали, кому она принадлежит. Другой пример – DNS-прокси. На него у меня есть патент, но существует много DNS-прокси, и никто не обращает внимания на авторство».

Я спросил Чесвика, что его больше всего беспокоит в сфере ИБ: «Старый материал, который продолжает работать. Почти ничего нового. Может быть, Stuxnet, но прежние задумки все равно остаются в строю. Как минимум с 1979 года нам известно, что пароли бесполезны, так почему мы все еще их используем? В настоящее время я работаю над некоторыми новыми идеями пароля и аутентификации. Или взять недавние DDoS-атаки DYN **(http://dyn.com/blog/dyn-analysis-summary-offriday-october-21-attack/)**. Это случилось из-за всех тех корневых паролей, заготовленных в прошивке устройств IoT. Я бы поставил студенту неудовлетворительную оценку за ввод жестко закодированных паролей».

Тем не менее Чесвик считает, что информационная безопасность значительно улучшится. Он сказал: «Я много выступаю по всему миру, и одна из моих речей называется “Интернет-безопасность: я думаю, что мы победим”

(**https://cacr.iu.edu/events/2016/bill-cheswickcomp-sec-we-can-win.php)**. Мы находимся на стадии модели T информационной безопасности. Сейчас мы не пытаемся это исправить, но будем работать над этим. Мы наблюдаем рыночный провал, но рынок с ним справится. В будущем у нас появится значительно лучшая интернет-безопасность. Многие не верят, когда я говорю об этом, но поверят позже. Другие отрасли промышленности имели те же проблемы на раннем этапе, но росли и улучшались. Интернет сделает то же самое».

Я спросил его, что будет одним из основных улучшений. Он рассказал: «Я удивлен, что нам все еще разрешено запускать произвольное программное обеспечение на компьютерах. Даже с антивирусной проверкой это выглядит как запуск проверки на бродяг в вашей ванной комнате. Операционные системы должны позволять выполнять только проверенный код, и мы к этому близки. ОС уже начинают лидировать в этом направлении».

Я спросил, почему его не беспокоит, что улучшение информационной безопасности занимает так много времени. «Есть много проблем, но один из главных вопросов – это поддержка. Это можно сравнить с моделью города. У всех городов есть проблемы, связанные с наследием прошлого развития, которые люди просто не могут игнорировать».

Я спросил Чесвика, о чем он думает в последнее время. Он сказал: «Одна из самых больших проблем заключается в том, как вы измеряете безопасность в ПО. Как выглядит точная система показателей? Один из простых примеров – измерение общего числа сетевых служб, каждая из которых – потенциальный вектор атаки, и их сокращение означает уменьшение риска. Но это слишком упрощенно. Другой несложной мерой могло бы стать измерение количества “демонов”, работающих с setuid root [это означает, что программа намеренно продвигается для запуска в качестве наиболее привилегированного контекста учетной записи безопасности]. Опять же, меньше, конечно, было бы лучше. Но и это слишком упрощенно. Еще один способ измерить безопасность, скажем, операционной системы или программного обеспечения – это стоимость эксплойта нулевого дня, который можно купить на открытом рынке. Журнал Forbes написал об этом статью в 2012 году **(http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-daysan-price-list-for-hackers-secret-software-exploits/#43f3035e6033)**. Стоимость эксплойта будет фактором того, насколько трудно взломать программу или операционную систему и насколько она популярна для взлома. Например, полный эксплойт ОС стоит 500 000 долларов, но взлом часто скомпрометированной программы составляет всего 50 000 долларов. Большая цена указывает, что вендор лучше справляется с безопасностью.

Каждый, как я уже говорил, хочет измерить уровень безопасности. Людям нужно число. Они хотят показать, что в прошлом году их уровень составлял 27 условных единиц, а в этом повысился до 63, и безопасность явно улучшилась. Более реалистичное измерение – определение всех возможных измерений и присвоение им веса, а затем объединение их в большую метрику. Этого хочет любой управляющий. Я много думал об этом в последнее время. В наши дни становится все труднее и труднее проникать в новое ПО. Даже жалобы ФБР на

то, что они не могут что-то взломать, – хороший знак. Безопасность становится все крепче и крепче».

Информация об Уильяме Чесвике

Более подробную информацию об Уильяме Чесвике вы можете узнать по ссылкам:

• веб-сайт Уильяма Чесвика: **http://www.cheswick.com/ches/index.html**;

• *Firewalls and Internet Security: Repelling the Wily Hacker* (в соавторстве со Стивеном Белловином): **https://www.amazon.com/Firewalls-Internet-Security-Repelling-Hacker/dp/020163466X**;

• доклад *An Evening with Berferd in which a Cracker Is Lured, Endured, and Studied*: **http://www.cheswick.com/ches/papers/berferd.pdf**.

19. Ханипоты

Я был заинтригован ханипотами с тех пор, как прочитал книгу Клиффорда Столла *The Cuckoo'S Egg* **(https://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787/)**, изданную в 1989 году, в которой рассказывалось о том, как он поймал иностранного шпиона. С тех пор я запускал до восьми различных ханипотов за раз, отслеживая вредоносные программы и поведение хакеров. Я часто участвую в профессиональных проектах ханипотов и даже написал книгу о них под названием *Honeypots for Windows* **(https://www.amazon.com/Honeypots-WindowsBooks-Professionals/dp/1590593359/)**. Мне кажется, что все компании должны включать один или несколько ханипотов в свою защиту.

Что такое ханипот?

Ханипот (ловушка) – это поддельная система, созданная с целью обнаружения несанкционированной деятельности. В качестве ханипота может выступать компьютерная система, устройство, сетевой маршрутизатор, беспроводная точка доступа, принтер – все, что угодно. А ханинет – это набор ханипотов, их сеть. Ханипот может быть создан путем развертывания реальной, но неиспользуемой системы или специализированного программного обеспечения ханипотов.

Эмуляция может быть в любом месте на уровнях модели Open Systems Interconnection (OSI): физическом, канальном, сетевом, транспортном, сеансовом, презентационном или прикладном, – или в любой комбинации этих уровней. Есть много вариантов ханипотов с открытым исходным кодом или коммерческих, каждая из которых предлагает различные функции. Покупатель должен остерегаться. Есть лишь некоторые ханипоты, которые смогут работать десятилетиями, но подавляющее большинство предложений рассчитано на краткосрочный период.

Взаимодействие

Насколько хорошо система ханипотов эмулирует или работает на определенном уровне, определяет ее взаимодействие. Ханипот с низким уровнем взаимодействия только имитирует очень упрощенные соединения портов и регистрирует их. Подключающемуся пользователю может быть предложен или не предложен вход в систему, но обычно успешный вход запрещен. Ханипоты среднего взаимодействия позволяют потребителю войти и предлагают дополнительные, но вместе с тем реалистичные действия. Если они эмулируют веб-сайт, то часто это приличный, но довольно статический веб-сайт. Если они делают эмуляцию FTP, узел позволяет вход в систему, где есть файлы, которые могут быть загружены, и позволяет многократное использование команд FTP. Ханипоты высокого взаимодействия имитируют реальную производственную систему до такой степени, что хакер, взаимодействующий с ней, будет не в состоянии отличить ее от реального производственного актива. Если она эмулирует веб-сайт, то он широкий и реалистичный, с часто обновляемым контентом. Ханипоты низкого взаимодействия намного легче поддерживать, но иногда их цель требует более высокого взаимодействия. Конечно, реальная система предлагает лучшую эмуляцию, но может быть более сложной в настройке и управлении в долгосрочной перспективе.

Зачем использовать ханипоты?

Есть много причин, по которым следует использовать ханипоты, в том числе:

• в качестве системы раннего предупреждения для обнаружения вредоносных программ и хакеров;

• для определения намерения хакера;

• для исследования хакеров и вредоносных программ;

• для анализа вредоносного ПО.

При соответствующей настройке ханипот невероятно малошумный (в плане логов) и ценный элемент, особенно для анализа журналов или генерации предупреждений. Например, журналы брандмауэра всегда полны десятков тысяч отброшенных пакетных событий каждый день, большинство из которых не имеют ничего общего со злонамеренностью. И даже если есть злонамеренный элемент, потребуется много труда, чтобы определить, что именно представляет угрозу.

Ханипот – это поддельная система, и по идее никто (или ничто) не сможет подключиться к ней. Вы должны потратить немного времени на фильтрацию обычного широкого трафика и законных попыток подключения (например, из ваших антивирусных программ обновления, управления патчами и других инструментов управления системой и т. д.). Но как только это будет сделано (что обычно занимает от двух часов до двух дней), любая другая попытка подключения по определению вредоносна.

Ханипот – это, несомненно, лучший способ поймать злоумышленника, который обошел другие защитные механизмы. Он тихонечко ждет любой внезапной

попытки подключения. Я отслеживал многих хакеров и тестировщиков за десятилетия своей работы, и один правдивый факт заключается в том, что они ищут и перемещаются по сети, как только получили первоначальный доступ. Не многие хакеры знают, какие системы являются ханипотами, а какие нет, и когда они перемещаются и просто «касаются» их, считайте, вы их поймали.

Пример: одна из наиболее распространенных проблем, связанных с атаками, – это расширенные постоянные угрозы (APT), описанные в главе 14. Они легко и обычно без обнаружения двигаются в стороны и по горизонтали. Но разместите парочку ханипотов в качестве поддельных веб-серверов, серверов баз данных и серверов приложений, и вы обнаружите APT без труда.

Конечно, есть хакеры, которые просто перейдут от своего первого внутреннего вторжения к конкретному активу или набору активов, но это случается редко. Обычно даже после компрометации предполагаемой основной цели они будут оглядываться. И когда они осматриваются и «дотрагиваются» до ханипотов… вы их ловите! Или, по крайней мере, узнаете о них. Я большой поклонник размещения ханипотов низкого или среднего взаимодействия, чтобы получить раннее предупреждение о вторжении.

Как я ловил русского шпиона

За эти годы я выстроил десятки систем ханипотов, но одна из моих любимых историй – это когда я разрабатывал их для подрядчика из министерства обороны. Он был обеспокоен внешним взломом, но наши ханипоты быстро обнаружили несанкционированную инсайдерскую атаку.

Мы отследили ее и пришли к сотруднице отдела заработной платы из России. Мы уже установили камеры в отделе, чтобы наблюдать за ее действиями. Она вставила несанкционированную беспроводную карту в свой компьютер, чтобы «соединить» две изолированные сети, и передавала большие объемы личных данных другому внешнему партнеру. После двух дней наблюдения и определения ее намерений (она определенно собирала данные для сверхсекретных проектов), мы со службой безопасности вошли в комнату, чтобы противостоять ей. Она сразу расплакалась и так талантливо играла свою роль невинной жертвы, что, если бы мы не следили за ней несколько дней, я бы ей поверил. Она была хакером, но сотрудники ее отдела думали, что она настолько не разбирается в компьютерах, что отправили на курсы, чтобы она научилась лучше печатать.

Она была лишь одним из многих российских сотрудников, нанятых по временному контракту. В конце концов выяснилось, что все они были шпионами.

Ресурсы для изучения ханипотов

Проект Honeynet Project **(http://www.honeynet.org)** – это лучший источник для изучения ханипотов. Honeywall CD-

ROM **(http://www.honeynet.org/project/HoneywallCDROM)** – отличное бесплатное ПО с ханипотами для пользователей, которые не боятся конфигурации Linux.

Honeyd **(http://www.honeyd.org)** – гибкий бесплатный ханипот с открытым исходным кодом, но он требует твердых знаний Linux и сетевых навыков для установки и работы. Она выполняет отличную широкую эмуляцию более чем ста операционных систем и может быть легко связана с другими продуктами и скриптами. С другой стороны, она не обновлялась годами. Я думаю, что это хороший вариант для тех, кто хочет увидеть все, что только можно.

Мой любимый ханипот – Kfsensor **(www.keyfocus.net)**. Это коммерческий продукт, который работает только на компьютерах с Windows, и он постоянно обновляется и улучшается. У Kfsensor есть свои недостатки, но у него также много различных функций и он довольно прост в настройке. У него есть сотни опций и настроек, а также он позволяет регистрировать и предупреждать различные базы данных и журналы. Доступны бесплатные пробные версии.

В мире существует множество (более ста) ханипотов. Каждый год в Интернете появляется несколько новых. Если вы заинтересованы в ханипотах, то опробуйте некоторые из них. Нет никаких сомнений в том, что каждый человек, заинтересованный в скорейшем предупреждении о возможно успешном хакере или проникновении вредоносных программ, должен запустить ханипот.

Глава 20 посвящена профилю Лэнса Спицнера, который, вероятно, сделал больше для исследования ханипотов, чем кто-либо другой.

20. Профиль: Лэнс Спицнер

Ничто не расстраивает меня больше, чем то, когда сотрудник безопасности говорит мне: «Вы не можете исправить глупость», – Лэнс Спицнер

В конце 1980-х я прочитал книгу Клиффорда Столла под названием *The Cuckoo's Egg*. Это история о том, как ошибка в 0,75 доллара привела американского астронома к раскрытию международной шпионской группировки. Главным инструментом Столла в расследовании был ханипот. Эта книга действительно пробудила мой интерес к информационной безопасности и борьбе с хакерами.

Прошло десять лет, прежде чем я встретился с другим великим человеком, Лэнсом Спицнером. Сегодня большинство людей считают его отцом современных компьютерных ханипотов. Он написал и опубликовал так много информации о них в начале 2000-х годов, включая книгу *Honeypots: Tracking Hackers* **(https://www.amazon.com/Honeypots-TrackingHackers-Lance-Spitzner/dp/0321108957)**, что даже сегодня, спустя десятилетие, никто не написал больше, чем он. Благодаря свежему взгляду Спицнера на ханипоты я тоже заинтересовался ими и даже написал книгу на эту тему **(https://www.amazon.com/Honeypots-Windows-Books-Professionals/dp/1590593359)**.

Спицнер заставил людей по-другому взглянуть на ханипоты, способствуя тем самым развитию киберразведки. Его основной интерес состоял в том, чтобы узнать, как и почему хакеры компрометировали организации; он называл это «Знай своего врага». Он также создал определения для описания различных стилей и классов ханипотов и помог выяснить, что в них работало, а что нет, фактически вывернув их наизнанку.

Также Спицнер – хороший пример того, как человек, не будучи компьютерным специалистом, смог сделать хорошую карьеру в области ИБ. В колледже Лэнс изучал историю. Затем он присоединился к Корпусу подготовки офицеров запаса, чтобы заплатить за свое обучение, и после окончания стал танкистом в армии, где прослужил четыре года.

Спицнер глубоко убежден, что для создания карьеры в области ИБ не обязательно быть компьютерным специалистом. Он сказал: «Вам не обязательно с самого начала изучать компьютеры, чтобы построить успешную карьеру в ИБ. 20–30 лет назад было легче, потому что не было стандартного карьерного пути, как сейчас. Теперь я обеспокоен тем, что поле информационной безопасности переполнено завышенными требованиями. Нам нужно больше специалистов с «гибкими навыками», а не только людей, которые понимают биты и байты. Многие из самых больших проблем безопасности нельзя решить исключительно техническим способом».

Должен быть кто-то и из танкистов в информационной безопасности, потому что я знаю многих из них, кто отлично справляется со своей работой. Я спросил об этом Спицнера. «В армии вас постоянно учат узнавать своего врага. Я учился не только управлению танком, но и действию танков противника, и тому, как они будут атаковать нашу технику. Я был удивлен, что в мире ИБ люди так мало знали о своих врагах. Тогда, в конце 90-х, никто не заботился об информационной безопасности».

Я попросил его рассказать, как он попал в сферу ИБ. Лэнс ответил: «Когда я учился на программе MBA в аспирантуре после армии, меня буквально засосало в этот мир. Я начал стажироваться в консалтинговой компании Unix. Нам прислали несколько брандмауэров, и, так как я был новичком, их свалили на меня. Мне понравилось. Я узнал о брандмауэрах, изучил их и научился останавливать злоумышленников. Было здорово. После этого я четыре года работал в отделе безопасности Sun Microsystems, защищая клиентов по всему миру».

Я спросил его, как он перешел с брандмауэров на ханипоты. Лэнс ответил: «Я прочитал три труда о ханипотах. Во-первых, статью доктора Фреда Коэна, который считается отцом защиты от компьютерных вирусов **(https://en.wikipedia.org/wiki/Fred_Cohen)**. Во-вторых, книгу *The Cuckoo’s Egg* Клиффорда Столла. И в-третьих, доклад Билла Чесвика *[An Evening with Berferd in Which a Cracker Is Lured, Endured, and Studied* **(http://www.cheswick.com/ches/papers/berferd.pdf)**]. Билл Чесвик [речь о котором шла в главе 18] был одним из первых компьютерных ученых, специализировавшихся на брандмауэрах, и также одним из первых стал

использовать ханипоты. Клиффорд Столл начал опыты с ханипотами в 1986 году. Билл Чесвик – в 1991-м. Долгое время эти два источника были всем, что большинство из нас знало о ханипотах.

Долгое время не было качественных ханипотов. Я не владел достаточно хорошими навыками программирования, поэтому не мог их создавать. Тогда я решил использовать их на реальных компьютерах. Я просто поставил брандмауэр, в котором хорошо разбирался, перед реальными системами. А все остальное взял из уроков, которые извлек из этого опыта».

Самая продуктивная работа Спицнера над ханипотами проводилась, когда он работал полный день над проектом Honeynet (2004–2009 гг.) **(http://www.honeynet.org)**. Проект спонсировался Национальным разведывательным советом США **(https://www.dni.gov/index.php/about/organization/national-intelligence-council-who-we-are)** и был создан в 1979 году в качестве центра стратегического анализа. Он сформировал команду из лучших умов академических кругов, правительства и частных хакеров. Совет уже давно предоставляет экспертные услуги и сотрудничает по вопросам разведки, а также возглавляет ряд важных проектов.

Все, кто интересовался ханипотами, знают, что большинство самой последней и актуальной информации и инструментов было размещено на сайте Национального разведывательного совета и до сих пор там находится. Совет работает и по сей день. Кроме того, можно заглянуть на веб-сайт проекта Honeynet. Именно во время работы над этим проектом Спицнер написал бóльшую часть своих трудов о ханипотах и помог всем, кто ими интересовался (включая меня).

К сожалению, Спицнер в конце концов покинул Honeynet и больше не занимается ханипотами. Я спросил его, почему так произошло, и он ответил: «Благодаря работе над проектом я очень хорошо узнал врага. Поскольку мы стали настолько эффективно использовать одни технологии для защиты других, я видел, как кибератакующие быстро адаптируются и нацеливаются на человеческий фактор. Сегодня хакеры часто используют социальную инженерию. Когда вы в последний раз видели большого червя, вроде Conficker [Conficker был очень популярен в 2009 году]? Есть причина, по которой мы больше их не встречаем. Технология по умолчанию стала намного лучше, и теперь атакующие преследуют самое слабое звено – человека. Я заметил эту тенденцию и сформировал собственную компанию по вопросам безопасности. Институт SANS **(http://www.sans.org)** в конце концов приобрел ее в 2010 году, и теперь она известна как SANS Securing the Human **(https://securingthehuman.sans.org/)**. У нас более 1000 клиентов, которым мы помогаем создавать эффективные программы повышения осведомленности о состоянии безопасности. Теперь я работаю с ними, а также веду курсы и посещаю конференции».

В заключение я спросил Спицнера о том, что его больше всего беспокоит в сфере ИБ сегодня. Он ответил: «Это связано с человеческой составляющей. По-

прежнему слишком много внимания уделяется технологии и отсутствует внимание к человеку. Вот почему я работаю над этим. Я люблю то, чем занимаюсь, и верю в это. Плохие парни стали настолько хороши в своем деле, что стало нечего обнаруживать: нет зараженного вложения, вредоносных программ, руткита. Они просто идентифицируют цель с кредитной задолженностью с помощью фишингового электронного письма или поддельного счета и таким образом взламывают жертву. Затем они используют законные средства, такие как PowerShell, чтобы перемещаться по сети и делать плохие вещи. Антивирус и другие технологии не собираются его обнаруживать. По иронии судьбы, безопасность человека часто ставится под угрозу из-за других специалистов по ИБ. Многие из них по-прежнему считают, что вопрос безопасности можно решить только с помощью битов и байтов. Ничто не расстраивает меня больше, чем когда сотрудник безопасности говорит: “Вы не можете исправить глупость”, что означает “Вы не можете исправить человека”. В результате мало что делается для его защиты, и все же мы обвиняем людей в том, что они – самое слабое звено. Это просто глупо».

Информация о Лэнсе Спицнере

Более подробную информацию о Лэнсе Спицнере вы можете найти по следующим ссылкам:

• *Honeypots: Tracking Hackers*: **https://www.amazon.com/Honeypots-Tracking-Hackers-Lance-Spitzner/dp/0321108957**;

• Лэнс Спицнер в Twitter: **https://twitter.com/lspitzner**;

• курсы Лэнса Спицнера в SANS: **https://www.sans.org/instructors/lance-spitzner**;

• доклад *Know Your Enemy*: **http://old.honeynet.org/papers/enemy/**;

• серия докладов *Know Your Enemy*: **http://www.honeynet.org/papers**.

21. Взлом паролей

Взлом паролей всегда был популярным видом деятельности кибератакующих, хотя новые методы эволюционировали из простого подбора паролей. В голливудском представлении хакер – это человек, который сидит перед монитором и подбирает правильный пароль, хотя в реальности такое случается довольно редко. Реальный взлом пароля обычно строится на догадках или их отсутствии.

Компоненты системы аутентификации

Чтобы понять принцип работы паролей, вы должны понимать аутентификацию системы в целом. Пользователь (или устройство), также известный как субъект безопасности, должен отправить что-то (например, текстовую метку,

сертификат и т. д.), однозначно идентифицирующее их и вход в систему службы аутентификации. Для большинства традиционных сценариев паролей это метка, известная как имя пользователя. Затем субъект должен быть в состоянии доказать право собственности, что обычно делается путем предоставления другой информации, которую знает только субъект и система аутентификации. Это то, что мы называем паролем. Когда пользователь вводит правильный пароль, соотносящийся с именем пользователя, это доказывает, что субъект контролирует имя пользователя, и система разрешает доступ (другими словами, аутентифицируется) и может отслеживать пользователя во время доступа к системе (что зовется учетом или аудитом). Большинство операционных систем также обеспечивает субъекту доступ к необходимым объектам (процесс, называемый контролем доступа). Таким образом, вы можете проследить весь процесс, известный как четыре аспекта – аутентификация, доступ, аудит и учет. Они связаны, но обычно рассматриваются отдельно.

Пароли

Пароль может быть любым допустимым набором символов, который принимает система аутентификации. Например, в Microsoft Windows локальная база данных SAM или сетевая база данных NTDS могут принимать тысячи различных символов, для создания многих из которых требуются специальные комбинации клавиш (например, Alt+0128).

Базы данных проверки подлинности

Пароли хранятся в локальной и/или сетевой базе данных, известной как «база данных проверки подлинности». Обычно она защищена или зашифрована и редко доступна напрямую непривилегированным пользователям. Пароли также часто хранятся в локальной и/или удаленной памяти, когда пользователь или устройство активны.

Хэши паролей

Большинство введенных паролей преобразуются в какую-либо другую промежуточную форму по соображениям безопасности. В традиционных операционных системах пароли нередко преобразуются в криптографический хэш. Он может быть использован в самой последовательности аутентификации или просто сохранен для последующих входов. Общие хэши паролей в системах Windows – это LANManager (LM), NTLANManager (NT) и PBKDF2 для локального хранилища кэша паролей. Системы Linux часто используют MD5, Blowfish (созданный Брюсом Шнайером и описанный в главе 3), SHA-256 или SHA-512. Лучшие хэши создают и используют случайное значение во время создания и хранения хэша пароля. Это затрудняет хакеру его получение, чтобы преобразовать пароль обратно в исходное значение открытого текста.

Вызов-ответ

Это безопасный способ аутентификации, который не передает пароль или его хэш по сетевому соединению. Вместо этого выполняется вызов-ответ. Обычно удаленный сервер, который уже знает пароль клиента или хэш пароля, создает

случайное значение и выполняет криптографическую операцию, которую может также правильно выполнить только законный клиент с тем же самым законным паролем или хэшем. Сервер отправляет клиенту случайное значение, а тот использует пароль (или промежуточное представление) для выполнения ожидаемых вычислений и отправляет результат обратно на сервер. Сервер сравнивает результат, отправленный клиентом, с его собственным внутренне ожидаемым результатом, и, если они совпадают, клиент успешно аутентифицируется. Таким образом, если злоумышленник захватывает пакеты, используемые при сетевой аутентификации, у него не сразу будет пароль или хэш, хотя часто с помощью криптографического анализа можно вернуться к одному или другому с течением времени.

Факторы аутентификации

Поскольку пароли могут быть легко украдены (а иногда и подобраны), системы аутентификации все чаще запрашивают дополнительные «факторы» для субъекта, чтобы доказать право собственности на вход в систему. Существуют три основных типа факторов: то, что вы знаете (например, пароль, PIN-код или шаблон), то, что у вас есть (такие как маркер безопасности, мобильный телефон или смарт-карты), или информация о вас (биометрические данные, такие как отпечатки пальцев, сетчатки или геометрия руки). В общем, чем больше факторов требуется для аутентификации, тем лучше. Идея в том, что злоумышленнику труднее украсть два или более факторов, чем заполучить один. Использование двух факторов называется двухфакторной аутентификацией (или 2FA), а использование дополнительных факторов – многофакторной аутентификацией (или MFA). Использование двух или более одинаковых факторов не так сильно, как комбинирование различных типов.

Взлом паролей

Существует множество способов взлома паролей, включая методы, описанные в следующих разделах.

Подбор пароля

Как и показывают в кино, хакеры могут подобрать пароль. Если он прост и хакер что-то знает о человеке, он может попытаться подобрать пароль, исходя из его интересов. Хорошо известно, что юзеры часто используют в качестве пароля свое имя, имена своих близких или любимые хобби. Хакер может попытаться подобрать пароль вручную или использовать один из многих инструментов для автоматизации этого процесса. Если автоматический генератор паролей слепо пробует все возможные комбинации, это называется атакой «грубой силы». Если он использует предопределенный набор возможных значений пароля, который часто является набором слов, то такой инструмент называют «словарем». Большинство инструментов подбора паролей используют инструмент, который начинается с набора слов, а затем дополняет текстовые слова различными комбинациями цифр и специальных символов, чтобы

подобрать более сложные пароли.

Примечание. Однажды я случайно подобрал пароль пользователя, о котором ничего не знал, с первой попытки. Я как раз закончил смотреть знаменитый фильм Орсона Уэллса *«Гражданин Кейн»*, сюжет которого крутился вокруг словосочетания «бутон розы». Оно и оказалось паролем. Но со мной такое произошло только один раз.

Фишинг

Хакер также может использовать реалистичный, но мошеннический онлайн-запрос (через веб-сайт или электронную почту), чтобы обмануть пользователя и заставить его раскрыть свой пароль. Это называется фишинг. Если попытка фишинга использует то, что ранее было частной или внутренней информацией, это известно как spearphishing. Хакеры также могут использовать телефон или личный контакт, чтобы попытаться обмануть пользователей и узнать их пароли. Это работает гораздо чаще, чем вы думаете.

Кейлоггинг (запись нажатия клавиш)

Если хакер уже имеет повышенный доступ к компьютеру жертвы, он может установить программу под названием кейлоггер, которая фиксирует нажатия клавиш. Кейлоггеры отлично подходят для получения паролей, и им все равно, сложный он или простой, длинный или короткий.

Взлом хэша пароля

Если хакер может получить доступ к базе данных аутентификации жертвы, то может получить доступ к сохраненному паролю или, что более вероятно, к хэшам паролей. Сильные хэши криптографически устойчивы к обратному преобразованию в исходные текстовые формы. Более слабые и даже сильные хэши коротких паролей подвержены взлому. Взломщик хэша, используя методы грубой силы или словаря, пытается ввести все возможные пароли, преобразует их в хэш, а затем сравнивает вновь созданный хэш с украденным. Если они совпадают, то хакер теперь имеет пароль с открытым текстом. «Радужные таблицы» связаны с традиционными хэшами, только в их хэш-таблице хранится промежуточная форма, используемая для сравнения паролей или хэшей, что значительно ускоряет взлом. Есть много бесплатных программ для подбора и взлома паролей, доступных в Интернете. Если это вам интересно, обратитесь к открытому исходному коду John the Ripper **(http://www.openwall.com/john/)**.

Повторное использование учетных данных

Если у хакера есть повышенный доступ, он может украсть хэш пароля пользователя или другое представление учетных данных из памяти компьютера или сохраненной базы данных аутентификации, а затем воспроизвести его на других компьютерах, которые принимают аутентификацию с использованием украденных учетных данных. Этот тип атаки, в частности известный как Pass-the-Hash (или PtH), стал довольно популярным за последнее десятилетие. В традиционном сценарии PtH злоумышленник сначала проникает на один или

несколько обычных компьютеров конечных пользователей, находит локальные хэши учетных записей с повышенными привилегиями, а затем использует их для доступа к хранилищу всех учетных данных компьютера или сети, что, по существу, ставит под угрозу всю систему. За последнее время почти каждая организация, подключенная к Интернету, подверглась этому типу атаки.

Взлом сервиса восстановления пароля

Часто самый быстрый способ внедриться в систему – это взлом сервисов восстановления паролей. Многие системы аутентификации, особенно крупные онлайн-системы, позволяющие конечному пользователю ответить на ряд стандартных вопросов, используются для сброса пароля. Хакеры обнаружили, что гораздо легче подобрать или ответ на вопросы сброса пароля конкретной жертвы (например, «Какова девичья фамилия вашей матери?», «В какую начальную школу вы ходили?», «Какой была ваша первая машина?», «Какой ваш любимый цвет?» и так далее), чем подобрать сам пароль. Многие знаменитости были взломаны именно таким способом.

Защита паролей

Существует столько же способов защиты паролей, сколько и способов их взлома.

Сложность и длина

Длинные и сложные пароли значительно усложняют работу инструментов подбора и взлома. Лучше использовать длинные пароли, чем сложные (если вы не можете получить истинную сильную энтропийную сложность). Сегодня большинство экспертов рекомендуют 12-значные или более длинные пароли, и это только для обычных пользователей. Учетные записи привилегированных юзеров должны содержать не менее 16 символов. Длина рекомендуемого минимального размера пароля со временем увеличивается. Однако это не влияет на атаки повторного использования учетных данных, такие как PtH-атаки.

Частые изменения без повторного использования

Для защиты рекомендуют (а в некоторых случаях и требуют) соблюдать сроки, в течение которых может использоваться конкретный пароль (обычно 90 дней или менее) без повторения. Смысл в том, что, как правило, необходимо много времени, чтобы подобрать длинный и сложный пароль, но в итоге это может быть сделано благодаря вычислительной мощности. Периодическое изменение паролей снижает риск того, что хакер добьется успеха, прежде чем будет использован новый пароль.

Примечание. В некоторых недавних документах, посвященных паролям, ставится под сомнение, действительно ли традиционная защита длинным, сложным и меняющимся паролем эффективна. Хотя эти средства защиты могут показаться на первый взгляд хорошими, исследования показывают обратное.

Ознакомьтесь с документом Microsoft Research *Password Guidance* Робина Хикока (**https://www.microsoft.com/en-us/research/publication/passwordguidance/**) и документами доктора Кормака Херли, о котором мы поговорим в следующей главе, подвергающими сомнению традиционные рекомендации по паролям.

Разные пароли в разных системах

Это одна из лучших защит, но реализовать ее очень трудно (если не невозможно). Пользователи не должны использовать один и тот же пароль в разных системах. Повторное использование учетных данных повышает риск того, что хакер взломает одну из систем, захватит ваши общие учетные данные, а затем использует их для атаки на другую систему.

Блокировка аккаунта

Это распространенная защита от подбора пароля. Там, где хакеры пытаются его подобрать (например, в интерактивном режиме), система аутентификации блокирует или замораживает учетную запись после заданного числа неправильных попыток. Блокировка может быть временной или потребовать, чтобы конечный пользователь позвонил в службу поддержки, чтобы повторно активировать учетную запись или сбросить ее на портале сброса пароля. Эта защитная мера побеждает многих хакеров и инструменты для подбора паролей, но имеет свои риски, поскольку функция блокировки может быть использована хакером для создания широко распространенной атаки с отказом в обслуживании.

Устойчивые хэш-функции

Уязвимые хэш-функции не должны использоваться в системах аутентификации. Многие операционные системы по умолчанию используют устойчивые хэши, однако в целях обратной совместимости могут допускать использование менее стойких алгоритмов. В Windows хэши LM считаются уязвимыми и не должны использоваться. В Linux это хэши MD5 и SHA-1.

Не используйте пароли

Требования к паролям становятся настолько длинными и сложными, что большинству пользователей может быть проще вообще его не использовать. Вместо этого следует прибегнуть к 2FA, биометрическим данным, маркерам безопасности, цифровым сертификатам – чему угодно, только не простому имени пользователя и паролю. Такая рекомендация существовала и раньше, но сейчас это особенно актуально. Если веб-сайт позволяет использовать что-то лучшее, чем пароль, не отказывайтесь.

Примечание.. Работа альянса FIDO **(https://fidoalliance.org/)** по избавлению от паролей через Интернет набирает обороты в отличие от многих предыдущих безуспешных попыток сделать то же самое. Проверьте сами.

Защита от кражи учетных данных

Поскольку кража учетных данных с помощью таких атак, как PtH, стала настолько популярной в последнее время, многие операционные системы оснащены встроенными средствами защиты. Большинство из них сосредоточено на том, чтобы убедиться, что пароли/хэши недоступны в памяти для легкой кражи, или они не разделяют пароль и хэш через сетевые подключения.

Защита сервисов восстановления пароля

Сервисы восстановления пароля – самые слабые звенья в системе аутентификации. Они должны всегда позволять пользователям создавать собственные уникальные и трудоемкие/исследовательские вопросы и ответы. Если они этого не делают, пользователи должны дать трудоемкие ответы на вопросы и надежно сохранить их для последующего использования. Например, на вопрос «Какая девичья фамилия вашей матери?» ответом может быть giraffedogfish. По сути, вы превращаете ответ на вопрос о сбросе пароля в другой альтернативный пароль.

Глава 22 посвящена доктору Кормаку Херли, чьи исследования паролей бросают вызов общепринятым убеждениям.

22. Профиль: доктор Кормак Херли

Доктор Кормак Херли – своего рода разрушитель. Он говорит вещи, которые бросают вызов давним догмам; не все хотят это слышать, особенно если вложили миллионы долларов и долгие годы в то, чтобы делать прямо противоположное. Доктор Херли в поисках истины использует анализ данных. Он хорошо понимает, что некоторые из его теорий, подкрепленные данными, просуществуют десятилетия, прежде чем будут приняты людьми.

Например, исследование компьютерных паролей. Общепринятое мнение в том, что пароли должны быть длинными, сложными, а также часто меняющимися. Исследования доктора Херли **(https://www.microsoft.com/enus/research/wpcontent/uploads/2016/09/pushingOnString.pdf)** показали, что суждения о безопасности, которых придерживается почти каждый специалист по ИБ, не всегда правильны и могут даже усугубить проблему. Исследование доктора Херли показало, что длинные и мудреные пароли не усложняют большинство взломов в наши дни и часто приводят к более высокому риску из-за проблем конечных пользователей (таких как запись паролей или повторное использование на разных сайтах). Он даже осмелился сказать, что «большая часть информационной безопасности – это пустая трата времени» (**https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SoLongAndNoThanks.pdf**), и сам же это доказывает. Доктор Херли мне очень симпатичен.

Кормак Херли получил докторскую степень в Колумбийском университете, степень магистра в Университете Джорджии, а также учился в колледже Корк, Ирландия. В настоящее время он работает главным исследователем отдела

машинного обучения Microsoft Research в Редмонде. И хотя доктор Херли работает в мире ИБ всего 10 лет, он написал тонну исследовательских работ, а многие крупные СМИ цитируют его или проводят с ним интервью (включая New York Times, The Wall Street Journal, Bloomberg и NPR).

Я спросил Кормака, как он очутился в сфере ИБ. «Я думаю, этому поспособствовала моя прозорливость, а также опыт в обработке аудио- и видеосигналов и цифровой фотографии. Это поле очень ориентировано на данные. Вы должны собрать много данных, проанализировать их, получить статистику и выяснить правду. Это действительно хорошо подготовило меня к работе в области ИБ, хотя я удивлен, что большинство специалистов этого не делают. Думаю, я очутился в сфере ИБ, когда кто-то прислал мне новую защиту от фишинга, основанную на анализе логотипов. Я увидел в ней много недостатков. Она была не слишком прочной. В итоге я занялся паролями и информационной безопасностью. Я видел много декларативных заявлений о паролях, но не было никаких доказательств того, что какие-либо из рекомендованных способов защиты действительно работали. Мне показалось странным, исходя из прошлого опыта, что никто не делал того, что я ожидал, – не собирал данные, не проводил эксперименты с использованием двух разных групп [включая контрольную группу] и не изучал результаты. Вместо этого люди делали декларативные заявления, которые даже после десятилетий использования не получили доказательств своей эффективности. Несмотря на то что в области ИБ данные могут быть скудны, именно они – моя основная правда.

Мы имеем определенные рамки для защиты ценных активов, ради которых должны делать все возможное. Но как насчет обычных бизнес-активов? Ясно, что следует расставить акценты. Мы не можем делать все сразу – это было бы до смешного трудно. Но скажите мне, какими из них я могу пренебречь? Ранжируйте список или предоставьте какой-то принцип ранжирования».

В мире ИБ много людей, которые либо игнорируют работу доктора Херли, либо обеспокоены ею. Об этом мы тоже поговорили, и вот что он сказал: «Я пришел в мир ИБ не для того, чтобы преднамеренно антагонизировать кого-либо. Но поскольку я только недавно начал работать в этой сфере, у меня не было устоявшихся культурных предубеждений, которые есть у многих. У меня был другой фон, обусловленный данными и необходимостью искать вспомогательные данные. Когда я не владел нужной информацией, я задавал фундаментальные вопросы о вещах, которые культура уже давно приняла. Я хотел получить данные, проверить и сделать эмпирический анализ… То есть заняться математикой. Это не только хороший, но и необходимый метод. Возможно, вы разработали модель того, как поведут себя 2 миллиарда пользователей, но они будут реагировать так, как захотят, независимо от вашей модели. Можно понадеяться, что произойдет, как вы задумывали, но я бы на вашем месте хотел понять, какова реальность, чтобы увидеть, есть ли между ней и моделью сходство. И если ваша модель неверна, измените ее».

Исследование паролей доктора Херли действительно перевернуло догму индустрии ИБ. Мне было интересно, как он относится к вероятности того, что

его исследования и предложения относительно паролей могут просуществовать десятилетия, прежде чем станут общепринятыми. Он сказал: «Мне позвонили из Национального института стандартов и технологий **[www.nist.org]** с просьбой дать некоторые рекомендации касательно их паролей; я написал ответ, и они пытаются следовать советам. Я понимаю, почему мои слова расстраивают людей и организации информационной безопасности. Им говорили что-то, что было правдой на протяжении трех десятилетий, а затем появляется небольшая группа людей, которая утверждает, что их правда была на самом деле ложью. Есть тысяча других людей, которые утверждают обратное, и даже если некоторые из их суждений лучше подкреплены данными, я вижу, как это было бы неприятно, особенно для сотрудников безопасности и ИТ-директоров. У меня была возможность сесть и провести исследование, собрать данные и рассмотреть альтернативы. Но сотрудники безопасности и ИТ-директора не могут позволить себе роскошь исследовать только одну проблему. Они видят кучу противоречивых сообщений и пытаются определить, на какие из них нужно обратить внимание. Они должны сделать все возможное и использовать свою мудрость в отношении того, что происходит».

Я спросил доктора Херли, что, по его мнению, можно назвать самой большой проблемой в сфере ИБ. Он ответил: «Мы знаем, как идеально защитить ценные активы, такие как коды ядерных ракет. Компрометация недопустима, и поэтому мы делаем все возможное, чтобы защитить их. В отношении всего остального нужно расставить акценты: что делать, а что нет. У нас нет действительно качественных инструментов и данных, чтобы определить их заранее. Хороший эффект заключается в том, что люди делают все возможное, путаясь, по существу, случайным образом принимая решения, которые, им сказали, они должны сделать. С ценными активами проще. Не так сложно определить риск, количественно оценить его и создать правильную политику. Когда речь идет не о ценных активах, мы делаем в основном не то, что эффективнее, а то, что легче. Например, я не уверен, что суперсильный пароль так уж необходим, однако ему продолжают уделять огромную долю внимания и ресурсов. И в конце концов это касается всех нас».

Информация о докторе Кормаке Херли

Более подробно о докторе Кормаке Херли вы можете узнать по следующим ссылкам:

• веб-сайт доктора Кормака Херли: **http://cormac.herley.org/**;

• доктор Кормак Херли в Twitter: **https://twitter.com/cormacherley**;

• профиль доктора Кормака Херли на Microsoft: **https://www.microsoft.com/en-us/research/people/cormac/**;

• цитаты доктора Кормака Херли на Академии Google: **https://scholar.google.com/citations?user=1FwhEVYAAAAJ&hl=en&oi=ao**.

23. Взлом беспроводной сети

Современный компьютерный мир работает в области беспроводных сетей. Теперь редко встречаешь тех, кто подключает сетевой кабель к настольному или портативному компьютеру, и тем более никто так не делает со своими сотовыми телефонами и другими вычислительными устройствами, хотя проводной мир быстрее и безопаснее. Беспроводной мир – мир, который постоянно атакуют хакеры.

Беспроводной мир

Беспроводной мир велик и широк. Это сеть, которая есть на наших домашних точках доступа к сети стандарта 802.11 Wi-Fi, но термин «беспроводной» охватывает огромную полосу электромагнитного спектра, который включает в себя рентгеновские лучи, свет, радио и другие формы беспроводной энергии. Идентификация и распределение части беспроводного спектра определены числом волн в секунду (частотой) и расстоянием длины волны. 802.11 – это стандарт беспроводной связи между 900 МГц и 2.4, 3.6, 5.0, 5.8 и 60 ГГц частоты. Компьютеры в нашей жизни используют много различных беспроводных технологий, включая магнетизм, свет, спутник, наземное радио, Bluetooth, связь ближнего поля (NFC), RFID и микроволновую печь. Большая часть беспроводного спектра контролируется законами и регулирующими органами, что хорошо, потому что без них он был бы непригодным и небезопасным.

Типы взлома беспроводных сетей

Каждая часть беспроводного спектра и различные стандарты связи для него определяют типы взлома, которые, вероятно, будут выполняться, хотя само количество атак на спектр Wi-Fi – хорошее представление того, что может произойти в них всех. В целом большинство беспроводных взломов делается либо для подслушивания, сбора информации, несанкционированного обмена широковещательным спектром беспроводной связи, либо с целью вызвать отказ в обслуживании, контролировать обслуживание или атаковать подключенных клиентов.

Атака точки доступа

У каждой беспроводной технологии есть одна или несколько точек доступа (APs), позволяющих передавать и/или получать данные. Обычно они подключены к наземным или другим типам систем связи. Хакеры могут напрямую атаковать точки доступа и нарушить беспроводную связь. Они могут взломать пароль администратора AP, изменить его операции, провести подслушивание или обмануть жертву путем подключения к постороннему AP.

Отказ в обслуживании

Самая простая форма беспроводного взлома – это грубое прерывание или подавление сигнала связи, также известного как «заклинивание» или

«затопление». Хакер может даже захватить канал. Если затопление сделано правильно, AP может случайно повторно соединиться с другим, незаконным ресурсом.

Подбор пароля беспроводной сети

Некоторые беспроводные технологии требуют пароля (или других доказательств аутентификации) клиента для присоединения к беспроводному спектру, предоставленному участвующим AP. Редко делают AP, блокирующие устройства после определенного количества неправильных догадок. Таким образом, беспроводные устройства взлома могут подобрать правильный пароль.

Перехват сессии

Конечная цель многих атак – захватить сессию связи жертвы. Это часто делается путем затопления беспроводной сети, что вызывает нарушение, а затем обманом заставляет клиента позволить хакеру изменить сеанс несанкционированным способом или подключиться к вредоносному AP. Эти типы атак стали очень популярными, особенно среди хакеров, пытающихся украсть HTML-файлы cookies с веб-сайта через общие беспроводные сети, находящиеся в общественных местах (таких как кафе, аэропорты и так далее).

Кража информации

Кража информации – это скорее результат беспроводного взлома, но я рассматриваю ее отдельно, потому что часто именно она становится целью всей сессии взлома. Так обстоит дело со взломом RFID. Кредитные карты позволяют держателю делать покупки бесконтактным способом. Хакеры с RFID-сканерами могут получить информацию о кредитной карте, используя устройство для тайного включения передатчика RFID. Он также используется на других устройствах и документах, таких как сотовые телефоны и паспорта.

Примечание. Подслушивание с помощью электромагнита используется против устройств, которые намеренно не поддерживают беспроводную связь. Все электронные устройства излучают электромагнитное поле, которое может быть прочитано, иногда издалека, с помощью правильного чувствительного прослушивающего устройства.

Обнаружение местонахождения пользователя

Многие хакеры, а часто и правоохранительные органы, используют особенности и слабые стороны конкретной беспроводной технологии для обнаружения подключенных клиентов и их устройств. Правоохранительные органы любят применять устройства stingray, которые создают поддельные AP, чтобы физически определить местоположение целевых объектов по их мобильному телефону. Читайте
статью **https://en.wikipedia.org/wiki/Stingray_phone_tracker**, чтобы узнать больше об этих увлекательных устройствах и их сомнительной законности.

Некоторые инструменты для взлома беспроводных сетей

Есть десятки, если не сотни, хакерских инструментов, которые могут быть использованы для беспроводного взлома. Это, например, любая общецелевая программа захвата протокола, такая как Wireshark (**http://www.wireshark.com/**) или Ethereal **(https://sourceforge.net/projects/ethereal/)**, но большинство хакеров используют программы, специализирующиеся на ИТ. Эти инструменты – отличный способ узнать о беспроводных технологиях и взломе.

Aircrack-Ng

Самый популярный инструмент беспроводного взлома 802.11 – Aircrack-Ng. Выпущенный в 2005 году в качестве инструмента беспроводного аудита с открытым исходным кодом, этот часто обновляемый инструмент стал как атакующим, так и защищающим. О его создателе, Томасе д'Отрепп де Буветте, мы поговорим в следующей главе.

Kismet

Kismet **(https://www.kismetwireless.net/)** – еще один хакерский инструмент. Он может помочь кому-то проникнуть в беспроводную сеть или предупредить, если кто-то другой пытается сделать это с вами.

Fern Wi-Fi Hacker

Программное обеспечение Fern Wi-Fi Hacker **(https://github.com/savio-code/fern-wifi-cracker)** помогает хакерам со многими из методов взлома, которые я упоминал выше.

Firesheep

Сходите в кафе и опробуйте Firesheep **(http://codebutler.com/firesheep)**. Он будет искать и красть любые HTML-файлы cookie, которые сможет найти на общих беспроводных носителях. Кража HTML cookies была возможна и до появления Firesheep, но он сделал это таким же простым, как запуск браузера. Firesheep стал инструментом, который заставил экспертов всерьез задуматься о безопасности беспроводных сетей.

Защита беспроводных сетей от взлома

Способов защиты существует столько же, сколько способов атак.

«Прыгающие частоты»

Частоты – одна из самых больших ранних проблем с любой беспроводной технологией, которая заключается в том, что кто угодно может их заглушить. Известная голливудская актриса Хеди Ламарр (и ее партнер, композитор Джордж Антей) создала и запатентовала беспроводную технологию «частотного скачкообразного спектра» во время Второй мировой войны. Скачкообразная перестройка частоты работает как защита, потому что легитимный сигнал очень

быстро передается по другим частотам, о которых отправитель и получатель договорились заранее. Любой, кто хочет нарушить сигнал, должен заглушить широкий спектр. Без этой защиты большая часть того, что мы сегодня используем в качестве беспроводной связи, была бы невозможна. Почитайте об открытии Ламарр. Моя любимая книга на эту тему – *Hedy's Folly* Ричарда Родса.

Предопределенная идентификация клиента

Многие беспроводные технологии имеют защиту, которая позволяет подключаться только предопределенным клиентам. В спектре 802.11 многие AP разрешают доступ лишь устройствам с предопределенными MAC-адресами. AP может также принять цифровые сертификаты от предопределенных доверенных центров сертификации или посмотреть на уникальный адрес устройства. Можно использовать любой идентификационный параметр.

Устойчивые протоколы

Никакая защита не сравнится с сильными протоколами. 802.11 начался с проводной эквивалентной конфиденциальности (WEP), которая позже была признана непоправимо уязвимой. Она была заменена на Wi-Fi Protected Access (WPA), который с тех пор оказался удивительно устойчивым к атакам. WPA можно использовать с паролями, цифровыми сертификатами или другими методами корпоративной аутентификации. Было несколько успешных атак против различных версий WPA, но гораздо меньше, чем предсказывало большинство экспертов, и многие из них могут быть исправлены путем перехода на другую версию WPA.

Длинные пароли

Если беспроводной точке доступа требуется пароль для соединения, убедитесь, что он достаточно длинный (30 символов или больше). Кроме того, стоит быть уверенным, что пароль администратора AP был изменен от значения по умолчанию и он также длинный и сложный.

Установка патчей точек доступа

Точки доступа часто имеют уязвимости, поэтому необходимо вовремя установить патчи от производителя.

Электромагнитное экранирование

В случае дистанционных бесконтактных атак, вроде атак против RFID – кредитных карт, электромагнитная защита вокруг физического передатчика (или всего прибора) может предотвратить прослушивание. Некоторые электронные устройства, такие как сотовые телефоны, содержат встроенную защиту, но большинство людей, обеспокоенных прослушиванием через электромагнитные волны, покупают сторонние защитные чехлы. Экраны также используются в кабелях, например телевизионных, для предотвращения непреднамеренного прерывания сигнала.

Существует так много способов совершить беспроводной взлом и ничуть не меньше способов защиты от них, что невозможно поместить их все в короткую главу, хотя я, надеюсь, упомянул некоторые из основных.

Глава 24 посвящена Томасу д'Отрепп де Буветта, создателю популярного инструмента беспроводного взлома Aircrack-ng.

24. Профиль: Томас д'Отрепп де Буветт

В предыдущей главе мы познакомились со взломом беспроводных сетей, а в компьютерном сообществе, посвященном этой теме, едва ли кого-то уважают больше, чем бельгийца Томаса д'Отреппа де Буветта, создателя Aircrack-ng (**http://aircrackng.org/**). Это ПО состоит из 16 различных программ. Aircrack-ng – самый популярный, бесплатный и безопасный набор инструментов. Томас впервые выпустил его в феврале 2006 года. Сегодня каждый дистрибутив взлома Linux включает его по умолчанию, и, если вы хотите совершить беспроводной взлом или провести аудит, то, вероятно, либо используете Aircrack-ng, либо использовали его, прежде чем заплатить за какой-либо аналогичный коммерческий продукт. Aircrack-ng настолько популярен, что появляется в телешоу и фильмах **(http://aircrack-ng.org/movies.html)**, которые пытаются реалистично изобразить актера в образе суперкрутого хакера. Томас также создал и выпустил беспроводную программу обнаружения вторжений под названием OpenWIPS-ng **(http://www.openwips-ng.org/)**.

Мы поговорили о том, как он пришел в сферу ИБ. «Я начал заниматься компьютерами и программированием очень рано, лет в 6–8. Уже тогда я сумел создать крошечную игру. Как и любой ребенок, я играл в игры на компьютере, но потом они мне наскучили. Тогда я решил полистать книги, которые прилагались к компьютеру, и обнаружил, что могу запрограммировать его. Мой родной язык – французский, а руководства были на английском, поэтому оказалось нелегко понять, как попасть в режим «Программирование», который предлагал какой-то базовый язык. Кроме того, не было возможности сохранить свой код, поэтому я был вынужден записать его на бумаге. До сих пор помню, что это была за игра и как ее пройти.

В сфере ИБ я очутился с помощью программы Aircrack, которая изначально была создана Кристофом Дивайном. Я вносил свой вклад в виде небольших исправлений и разговаривал с разработчиком, когда внезапно в декабре 2005 года он перестал участвовать в проекте. Дивайн был единственным, кто занимался разработкой, и в то время программа воспринималась как инструмент для взлома соседского ключа WEP. Внезапно он исчез из IRC и больше не подключался. Затем слухи о том, что с ним случилось, начали просачиваться в IRC-канал. Я думаю, их распространяли его друзья. Для меня этого было достаточно, чтобы начать загрузку всех ресурсов, релизов и прочего, прежде чем через несколько дней сервер был полностью закрыт. В то время ходило много слухов о том, что же произошло. Позже я встречался с Дивайном несколько раз и узнал, что тогда он был слишком занят своей настоящей работой и встал перед выбором: либо потратить время на разработку Aircrack на

безвозмездной основе, либо сохранить свою работу. Но тогда его исчезновение было покрыто тайной.

После трех месяцев ожидания я решил создать собственную версию программы. Это было в декабре 2005 года. Я не получал с этого прибыли, но мне нравился проект, люди, которых я встречал, и путешествия. И хотя Aircrack-ng не принесла мне денег, благодаря ей я получил работу. Меня всегда привлекала задача взлома собственной сети, и я начал свой бизнес. Родители были против того, что я работал над Aircrack, говорили, что у меня будут проблемы (особенно, когда я только начинал). Но я рад, что не слушал их, так как работа над проектом – одна из лучших вещей, которые когда-либо со мной случались. Я встретил много удивительных людей, и большинство моих нынешних друзей – это люди, которые появились в моей жизни прямо или косвенно благодаря Aircrack».

Я спросил Томаса, не думает ли он, что безопасность беспроводных сетей улучшилась в последнее время, на что он сказал: «Да, определенно. Когда я начинал, большинство хакеров взламывали слабые WEP-ключи. Теперь WEP непопулярен и почти не используется. Сейчас беспроводная безопасность использует WPA и WPA2, а это довольно сильное шифрование. В наше время, чтобы взломать беспроводную сеть, нужно отыскать либо недостаток во встроенном беспроводном чипе (см. **https://www.youtube.com/watch?v=4WEQpiyfb50**, чтобы увидеть пример того, о чем я говорю), либо человеческую оплошность. У вас может быть лучшее шифрование в мире, но, если вендор или владелец использует восьмизначный пароль Wi-Fi, мы сможем его взломать.

Вот еще один пример: в последней квартире, которую я арендовал, использовали MAC-адрес точки доступа в качестве ключа и сказали, что мне нужно просто перевернуть его, чтобы узнать ключ. Это можно легко найти, если у вас есть сетевая карта, способная контролировать режим, и я, скорее всего, мог бы расшифровать трафик других клиентов, если бы захотел. Более того, арендодатель не позволил изменить его! Дело в том, что некоторые вендоры продают устройства с заранее сгенерированной парольной фразой, которая обычно является своего рода хэшем на основе MAC-адреса, смешанного различными способами. Например, кабельный модем пришел с WPA (или WPA2) с написанными шестнадцатизначными MAC-адресами. Это означает, что вам нужно всего лишь пройти 10 000 комбинаций, чтобы найти правильный ключ (что займет минуту или две)».

Я спросил, какая, на его взгляд, самая большая проблема в сфере ИБ. Томас сказал: «В сфере ИБ много крупных проблем, но их общий знаменатель – сами пользователи. Они хотят удобства и безопасности (например, конфиденциальность, шифрование данных). Тем не менее безопасность и удобство в значительной степени соперничают. Нельзя иметь и то и другое одновременно. Чем больше удобства, тем меньше безопасности. Очевидно, что бóльшая безопасность будет менее удобной».

Информация о Томасе д’Отреппе де Буветте

Больше информации о Томасе д’Отреппе де Буветте вы найдете по ссылкам:

• видео презентации Томаса д’Отреппе де Буветта и Рика Фарина о взломе беспроводных сетей: **https://www.youtube.com/watch?v=XqPPqqV_884**;

• презентация Томаса д’Отреппе де Буветта и Рика Фарина о взломе беспроводных сетей в формате PDF: **https://defcon.org/images/defcon-16/dc16-presentations/defcon-16-de_bouvette-farina.pdf**.

25. Тестирование на проникновение

В этой главе мы рассмотрим критерии, по которым можно определить, законна ли деятельность того или иного хакера. Также начинающие тестировщики на проникновение смогут извлечь для себя несколько полезных советов. Кроме того, я расскажу о наиболее востребованных сертификатах.

Самые запоминающиеся моменты в моей карьере пентестера

Несомненно, тестирование на проникновение было одним из самых приятных периодов моей карьеры. Взлом – это весело. Мне тяжело выделить несколько лучших проектов, поэтому я расскажу о наиболее запомнившихся.

Взлом всех телевизионных приставок в стране

Однажды нас наняли, чтобы посмотреть, сможем ли мы взломать новую кабельную приставку, которую планировала выпустить крупнейшая в мире кабельная компания. Я использовал сканер, чтобы вычислить все сетевые порты; нашлось около десятка открытых. Затем я использовал Nikto, инструмент сканирования веб-сервера, для сканирования всех портов в надежде, что у одного из них будет веб-интерфейс. Мои надежды оправдались. Nikto определил один из портов как неизвестную программу для веб-серверов, о которой я никогда не слышал, и сообщил, что у нее есть особая уязвимость. Когда я попытался ею воспользоваться, оказалось, что она недоступна. Но я знал, что программное обеспечение веб-сервера устарело, а это означало, что оно полно старых ошибок, которые давно исправили новые веб-серверы. Первое средство, которое я использовал, было известно как атака обхода каталога (по сути, я набрал http://..//..//..//), и это сработало. Так я стал администратором с полным контролем над кабельной приставкой.

Мы сообщили об уязвимости клиенту, и на следующий день все руководящее звено компании пришло на мою презентацию. Оказывается, именно эта уязвимость присутствовала на каждой кабельной приставке, а миллионы таких уже были распроданы по всей стране и все они были подключены к Интернету.

Одновременный взлом крупной телевизионной сети и кража порнографии

Та же кабельная компания наняла нас, чтобы проверить, можем ли мы украсть порнографию, которая была одним из главных источников ее дохода, а также посмотреть, получится ли украсть основные художественные фильмы. Мы сидели в одном из компьютерных залов с двумя кабельными приставками и двумя телевизорами, которые работали 24/7; один показывал порнографию, а другой – кино. Нетрудно представить, что просмотр порнографии в течение нескольких дней подряд быстро наскучил. Но это не помешало десяткам людей заходить, чтобы «проверять» нас каждый день. Забегая вперед, скажу, что мы смогли украсть как порнографию, так и полнометражные фильмы, а также доказать, что можем заполучить и номера кредитных карт клиентов.

Мы даже использовали межсайтовый скриптовый эксплойт, чтобы захватить всю кабельную компанию – из одной кабельной приставки. Мы обнаружили, что кабельный блок работает на веб-сервере и содержит журналы брандмауэра. Те в свою очередь содержали ошибку межсайтового скриптинга. Мы «атаковали» приставку таким образом, что знали, что вводили дополнительные хакерские атаки (в этом случае тот, который будет получать пароли администратора). Затем мы позвонили в компанию и попросили одного из технических специалистов проверить журналы брандмауэра, потому что нам было интересно, находится ли система под «хакерской атакой». Когда техник службы поддержки компании проверял журнал, пароль к его учетной записи появился на экране. Оказалось, на всем предприятии пароли использовались одинаковые.

Взлом сайта крупной платежной системы

В рамках тестирования компании нужно было взломать «тестовый» веб-сайт. Проводился конкурс, на котором оценивалось, за какой срок мы можем это сделать, сколько уязвимостей найдем и как ими воспользуемся. У нас было десять соперников. Победитель – команда, которая найдет больше всего уязвимостей, – получит сертификат и будет нанят для «сертификации» десятков тысяч других сайтов. Один из членов моей команды смог не только взломать веб-сайт, но и полностью завладеть производственной средой заказчика. Мы выиграли конкурс.

Создание «Камерного вируса»

Однажды я придумал, как получить свой «вредоносный» код для автоматической активизации с мультимедийной карты цифровой камеры. Я попробовал осуществить это, и у меня получилось! Я показал коллеге, и он понял, что это сработает с любой съемной медиакартой. При проверке выяснилось, что код работает с цифровыми камерами, музыкальными плеерами и сотовыми телефонами. Мой работодатель был в восторге. Мы решили, что я представлю свое изобретение на предстоящей конференции Black Hat. Я также сообщил о своих исследованиях соответствующему вендору. Они проверили их

и спросили, можем ли мы дать им несколько месяцев, чтобы создать патч для устранения проблемы.

И тут я столкнулся с дилеммой. Если пойду им навстречу, выступление на конференции Black Hat не будет столь интересным. Но, не дай я им времени, оставил бы вендора и его клиентов под угрозой, пока тот не сможет поспешно создать исправление. Помню, как тяжело мне далось это решение. В конце концов, я решил быть хорошим хакером; меня больше беспокоила безопасность в компьютерном мире, нежели собственное эго. Я дал вендору необходимое количество времени. Несколько месяцев спустя еще одно событие привело к открытию той же уязвимости, но вендор был готов к ней и тотчас выпустил исправление. Мое открытие не стало сенсацией, но в то же время оно не принесло большого ущерба, а это значит, что мы победили.

Как стать пентестером

Тестирование на проникновение (пентестирование) – это юридические взломы. Это сложнее, чем просто взломать сайт, хотя и начинается именно с проникновения.

Методология хакера

Для того чтобы быть успешным тестировщиком на проникновение, вам нужно следовать той же методологии взлома, которая была описана в главе 2.

1. Сбор информации.

2. Проникновение.

3. Гарантия более легкого последующего доступа (необязательно).

4. Внутренняя разведка.

5. Горизонтальное или вертикальное движение (необязательно).

6. Выполнение намеченного действия.

7. Заметание следов (необязательно).

Не будем снова вдаваться в подробности; достаточно сказать, что тестировщики на проникновение – это те же хакеры, и они следуют тем же шагам. Но быть юридически правомерным тестировщиком на проникновение сложнее.

Получение официального разрешения

Главное, что отличает незаконного хакера от законного тестировщика, – это разрешение атаковать/тестировать активы, которые вы исследуете. Вы должны иметь предварительное документированное подписанное разрешение от компании или лица, владеющего активами или имеющего юридические полномочия от владельца.

Искать и находить уязвимость на чьем-то веб-сайте, а затем просить владельцев взять вас на работу – неэтично. Многие начинающие тестировщики, которые

ищут свою первую профессиональную работу, пробуют эту тактику. Они думают, что компания найдет их открытие невероятно полезным и предложит им работу. Вместо этого их обычно воспринимают как потенциальную угрозу, независимо от истинных намерений горе-хакеров. Если вы действительно случайно столкнулись с уязвимостью во время работы в Интернете, конфиденциально сообщите об этом владельцу/вендору и помогите, если у них возникнут вопросы. В таком случае вы куда вероятнее сможете получить работу, но не стоит просить об этом напрямую.

Оформление контракта

Тестировщики на проникновение всегда подписывают контракт. В нем должны быть указаны имена договаривающихся сторон, объем обязательств (какие цели и даты проекта, что будет сделано и так далее), соглашение о неразглашении для защиты обеих сторон, какие инструменты и методы будут использоваться и предупреждение об отказе от возмещения ущерба при возможном прерывании работы системы. Если у вас нет каких-либо шаблонов контрактов, обратитесь к юристу и/или поищите примеры в Интернете.

Отчеты

Высшая степень профессионализма – это хорошо написанный подробный отчет. Для начала следует создать краткое резюме, а после более подробно описать проект, сферы охвата, проделанную работу и выводы. Последние лучше включить в качестве отдельных приложений. Многие консультанты считают, что чем больше отчет, тем лучше. Лично я думаю, что более короткие отчеты с достаточной детализацией для резервного копирования результатов оцениваются клиентами выше. Но всегда имейте в запасе более подробное описание, которым сможете поделиться при необходимости.

Сертификация

Получите сертификат. Это не залог того, что вы умнее тех, у кого сертификатов нет, но они могут стать вашим преимуществом при получении работы. Сертификаты – это простые заявления о минимальном уровне знаний и опыта человека. В следующих разделах я познакомлю вас с сертификатами, которые рекомендую получить.

Институт SANS

Я огромный поклонник всех проектов Института SANS **(http://www.sans.org)**, будь то обучение, исследования, образование, книги или сертификаты. Я описываю его соучредителя, Стивена Норткатта, в главе 42. Если вы заинтересованы в том, чтобы быть уважаемым техническим экспертом, этот сертификат вам необходим. Институт даже предлагает два уровня магистров аккредитованных степеней под своим брендом. SANS имеет множество сертификатов, начиная от узкоспециализированных тем безопасности (таких как анализ вредоносных программ, брандмауэры, безопасность хоста и элементы управления безопасностью) до чрезвычайно уважаемого сертификата эксперта

по безопасности (GIAC) **(http://www.giac.org/certifications/get-certified/roadmap)**. Последние классифицируются по следующим предметным областям:

• кибер-безопасность;

• тестирование на проникновение;

• цифровая криминалистика и реагирование на инциденты;

• разработчик;

• управление и руководство;

• эксперт по безопасности.

Некоторые из самых популярных экзаменов GIAC – это экзамен профессионала в области ИБ (**http://www.giac.org/certification/gisp**), экзамен разработчика (**http://www.giac.org/certification/gcih**) и экзамен на противостояние вредоносным программам (**http://www.giac.org/certification/grem**). Но они также охватывают деятельность Windows, веб-серверов, тестирование на проникновение, Unix и безопасность беспроводных сетей, программирование, руководство и управление программой. Тестирование GIAC проводится после посещения тренинга SANS, который обычно длится неделю. Если тест GIAC проводится после обучения, его стоимость составляет 659 долларов. Но вы можете бросить вызов (не проходя официальную подготовку) любому тесту за 1149 долларов.

Если вы заинтересованы в Unix и сертификации Linux, SANS предлагает GIAC сертификат администратора безопасности Unix (GCUX) (**http://www.giac.org/certification/certified-unix-security-administrator-gcux**).

Сертификат нравственности хакера (CEH)

Сертификат нравственности хакера (CEH) от международного совета EC–Council (**https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/**) очень уважаем и, по существу, учит вас, как быть хакером «в белой шляпе» (или профессиональным тестером на проникновение). CEH познакомил меня с некоторыми интересными инструментами взлома, которые я до сих пор использую. Экзамен длится максимум четыре часа и состоит из 125 вопросов с несколькими вариантами ответов. Стоимость участия – 100 долларов.

Совет EC–Council проводит множество других полезных экзаменов, в том числе экзамен на судебное следствие компьютерного взлома (**https://cert.eccouncil.org/computer-hackingforensic-investigator.html**), лицензированного тестера проникания (**https://cert.eccouncil.org/licensed-penetration-tester.html**), сертифицированного исследователя инцидентов (**https://cert.eccouncil.org/ec-council-certified-incidenthandler.html**) и сертифицированного профессионального аварийного восстановителя программ (**https://cert.eccouncil.org/ec-council-disaster-recovery-professional.html**). У них даже есть экзамен для руководителей служб информационной безопасности (**https://cert.eccouncil.org/certified-chief-information-security-officer.html**).

CompTIA Security+

Ассоциация индустрии компьютерных технологий (CompTIA) (**https://certification.comptia.org/**) предлагает комплексные экзамены начального уровня в сфере ИТ-поддержки инфраструктуры (A+) (**https://certification.comptia.org/certifications/a**), сетей (Network+) (**https://certification.comptia.org/certifications/network**) и безопасности (Security+) (**https://certification.comptia.org/certifications/security**). Поскольку для людей, недавно работающих в сфере ИБ, эти экзамены зачастую первые, они получили репутацию базовых и потому легких. Это не соответствует действительности. Экзамены очень всесторонние, и вы должны упорно учиться, чтобы быть уверенным в их успешном прохождении. Экзамен на получение сертификата CompTIA Security+ охватывает сетевую безопасность, криптографию, идентификацию, угрозы и узел защиты, а также другие темы. У вас будет 90 минут, чтобы ответить на 90 вопросов, а цена составляет 311 долларов.

ISACA

ISACA – международная профессиональная ассоциация, ориентированная на управление ИТ (**https://www.isaca.org**), – предлагает целый ряд профессионально-уважаемых экзаменов на аудит и менеджмент. Сертификаты включают в себя сертификат аудитора информационных систем (CISA) (**http://www.isaca.org/Certification/CISA-CertifiedInformation-Systems-Auditor/Pages/default.aspx**), сертификат менеджера по информационной безопасности (CISM) (**http://www.isaca.org/Certification/CISMCertified-Information-Security-Manager/Pages/default.aspx**), сертификат в области управления ИТ (CGEIT) (**http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Pages/default.aspx**) и сертификат профессионала в области управления ИТ-рисками (CRISC) (**http://www.isaca.org/Certification/CRISC–Certified-inRisk-and-Information-Systems-Control/Pages/default.aspx**). Если вы бухгалтер или аудитор, эти экзамены могут подтвердить ваши навыки, связанные с компьютерами и ИБ.

Сертификаты производителей

Многие компании, такие как Microsoft, Cisco и RedHat, предлагают свои экзамены по информационной безопасности.

Несколько лет назад Microsoft провела специальные экзамены по безопасности, например MCSE: Security. Но поскольку безопасность стала общей заботой для всех платформ и технологий, компания начала создавать собственные вопросы безопасности и включать их в свои экзамены. Эта тенденция в настоящее время несколько обращена вспять объявлением Microsoft о разработке нового экзамена обеспечения безопасности Windows Server 2016

(**https://www.microsoft.com/en-us/learning/exam-70744.aspx**). Он выходит далеко за рамки ее технической безопасности. Экзамен охватывает проектирование красного/зеленого леса, своевременное администрирование, достаточное администрирование и новейшие технологии безопасности Microsoft, такие как Advanced Threat Analytics (ATA). Тест Microsoft (**https://www.microsoft.com/en-us/learning/exam-98-367.aspx**) стоит 127 долларов.

Сертификационные экзамены Cisco всегда имели репутацию сложных. Экзамен на получение Certified Internetwork Expert (CCIE) (**http://www.cisco.com/c/en/us/trainingevents/trainingcertifications/certifications/expert/ccie-program.html**) известен как самый непростой в этой отрасли. По данным Cisco, менее 3 % студентов получат его, даже заплатив тысячи долларов, создав домашние лаборатории и потратив в среднем 18 месяцев на обучение. Сертификат специалиста безопасности сетей Cisco's Certified Network Associate (CCNA) Security certification (**http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html**) получить легче, но его также очень уважают. Сначала необходимо пройти любую другую допустимую сертификацию Cisco для прохождения CCNA. После ее получения (или любой другой сертификации CCIE), можно пройти Cisco Certified Network Professional (CCNP) – экзамен по безопасности (**http://www.cisco.com/c/en/us/training-events/trainingcertifications/certifications/professional/ccnp-security.html**). Но этот экзамен (**http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccie-security.html**) является экзаменом по безопасности Mack daddy Cisco. Он состоит из двухчасового письменного экзамена (который должен быть сдан первым) и восьмичасовой лабораторной части. Все сертификационные экзамены Cisco трудны, но если вы получите сертификацию безопасности CCIE, то сможете получить прекрасную работу почти в любой точке мира.

Компания RedHat проводит десятки сертификационных экзаменов (**https://www.redhat.com/en/services/all-certifications-exams**) и, как и другие крупные вендоры, предлагает по крайней мере один экзамен специалиста безопасности. Экзамен RedHat по безопасности называется RedHat Certificate of Expertise in Server Hardening (**https://www.redhat.com/en/services/certification/rhcoe-server-hardening**). Помимо обычной информации об усилении защиты сервера Linux, успешные кандидаты должны быть готовы к работе с отчетами об общих уязвимостях (CVE) и RedHat Security Advisory (RHSA). Цена – 600 долларов.

Профессиональный институт Linux (**https://www.lpi.org/**) предлагает экзамен безопасности LPIC-3 Exam (**https://www.lpi.org/study-resources/lpic-3-303-exam-objectives/**). Он охватывает множество тем безопасности, и кандидаты должны успешно пройти четыре предыдущих экзамена LPI более низкого уровня. Стоят они около 188 долларов.

Как я уже упоминал, SANS предлагает сертификат безопасности GIAC Certified Unix Security Administrator (GCUX) certification (**http://www.giac.org/certification/certified-unix-security-administrator-gcux**).

У компании Apple, кажется, нет определенных экзаменов в области безопасности, но обычные экзамены ОС, такие как Apple El Capitan (**http://training.apple.com/pdf/elcapitan101.pdf**) и основы интеграции с Mac (**http://training.apple.com/pdf/mac_integration_basics_1010.pdf**), имеют некоторые компоненты безопасности.

Каждая сертификация, которую я проходил, улучшила мои навыки. Получение сертификата может помочь вашим знаниям, карьере и способствовать получению работы.

Соблюдайте этику

Будьте этичным профессионалом. Никогда не предпринимайте несанкционированных действий и не стремитесь улучшить личную позицию в отношении обязательств и потребностей клиента. Если вы задаетесь вопросом, этично ли это, то, скорее всего, это не так.

Глава 50 посвящена Кодексу чести хакеров.

Минимизация возможных сбоев в работе

Старайтесь не допускать перерывов в работе клиентов. Многие инструменты тестирования на проникновение имеют «режимы безопасности», которые устраняют элементы с более высоким риском. Всегда начинайте с тщательного тестирования своих инструментов и методологий, прежде чем их использовать. Я всего лишь раз вызвал массовые сбои в работе, но это до сих пор меня преследует. Так произошло, потому что я не уделил достаточно внимания тестированию перед широкомасштабным применением.

Если вы будете следовать всем шагам, описанным в этой главе, то станете успешным и вас будут регулярно приглашать на новые проекты.

Глава 26 рассказывает про Аарона Хигби, одного из лучших тестеров на проникновение, которых я когда-либо знал, а в главе 27 представлен профиль Бенилда Джозефа, специалиста по тестированию на проникновение, эксперта по кибербезопасности и известного этичного хакера.

26. Профиль: Аарон Хигби

Поездка в машине Аарона Хигби – это опыт, знакомый только автомеханикам и инженерам. К процессору и двигателю его автомобиля подключено столько внешнего компьютерного оборудования и датчиков, что машину вполне можно принять за «Делориан» из фильма «Назад в будущее». Те из нас, кто знает Аарона уже несколько лет, ничему не удивляются. Хигби редко делает что-то наполовину. Он либо полностью погружен в работу, либо не заинтересован ею.

Очевидно, что девиз «Играй жестко или иди домой» имеет огромную роль в его жизни.

Сначала я работал с Хигби над проектом по проникновению, где мы были в команде, нанятой для взлома одного из крупнейших в мире провайдеров кабельного телевидения. Я осветил эту работу в последней главе о тестировании на проникновение, но пропустил часть истории. Мы успешно скомпрометировали не только предполагаемую цель кабельной телевизионной компании, телевизионную приставку, но и всю ее кабельную сеть. И это только за первый день! Хигби стало скучно, поэтому он начал искать слабые места оборудования от вендора. Он манипулировал оборудованием клиента, переключая провода, меняя местами перемычки материнской платы и устанавливая электрические кабели. Аарон продолжал пробовать различные хакнутые конфигурации, и в какой-то момент буквально поджег устройство. Дым повалил из блока, мы поспешили отключить электричество и потушить небольшой пожар. Пришлось подождать несколько минут, пока дым рассеется, чтобы увидеть, выпустят ли пожарные детекторы компьютерного зала токсичный газ и заставят ли нас эвакуироваться.

После того как дым рассеялся, Хигби вернулся и продолжил свой аппаратный взлом, что немало нас удивило. Никто из команды не смог его остановить. В конце концов он случайно спровоцировал пожар в аппаратном блоке, который мы потушить не смогли. Пока мы убегали, он посмеивался и, без моего ведома, снимал все происходящее на мобильный телефон. Через несколько минут видео появилось в Интернете.

Эта история – не пример для подражания. Неразумно делать что-то, что имело хотя бы малейшую возможность вызвать пожар. Но этот анекдот дает вам представление о том, каково было работать с Хигби. Большинство его друзей и коллег запросто могут поделиться с вами похожими историями о нем.

Помимо того, что с Аароном можно интересно и весело поболтать, он стал одним из лучших и преданных тестировщиков на проникновение, которого вы когда-либо встретите. Он вырос в довольно религиозной семье со строгими правилами. Я думаю, что такое воспитание и стало причиной его страсти к жизни и способности заставить всех, включая себя, смеяться. Сегодня он намного более профессионален и по-прежнему вносит свой уникальный вклад в опыт борьбы с хакерами и спамерами.

Позже мы оба покинули ту компанию. Я пошел работать в Microsoft, а Хигби стал соучредителем собственной невероятно успешной фирмы под названием PhishMe (**https://phishme.com/**). PhishMe специализируется на обучении конечных пользователей противостоянию фишинговым атакам. В частности, она позволяет легко отправлять поддельные, но реалистичные атаки против ваших сотрудников, чтобы увидеть, кто из них может быть обманут в вопросе конфиденциальной информации. Попытки сделать это предпринимались и до создания PhishMe, но она стала одной из компаний, которые сделали это невероятно легким в исполнении. С годами PhishMe расширялась, и теперь там

350 сотрудников, а доход составляет 12 млн долларов. Хотя с финансами у меня все хорошо, у Хигби дела идут лучше.

Я спросил его, как он очутился в сфере ИБ. Он ответил: «Я сел за компьютеры в эпоху BBS [системы доски объявлений], и некоторые из BBS, которыми я хотел воспользоваться, были дорогими междугородними звонками. Так что я начал узнавать о телефонном фрикинге, чтобы совершать звонки бесплатно, и таким образом начал разбираться во взломе. Меня взяли на первую работу в области ИБ в компанию EarthLink. Я занимался электронной почтой. Что бы ни пришло на адрес компании, я это обрабатывал: боролся со спамом, мошенничеством с кредитными картами, нарушением правовых норм и т. д. Мне так понравилось, что я бросил колледж. Родители посчитали, что я совершаю большую ошибку. Они думали, что Интернет был мимолетной причудой».

Я аплодировал Аарону и PhishMe, основанной на анти-фишинге. Многие из его конкурентов расширили сферу своей работы, но не компания Хигби. И это особое внимание к конкретному вопросу, похоже, приносит огромные дивиденды PhishMe и его клиентам. Он заявил: «Некоторые люди не понимают, что PhishMe делает. Они думают, что это пустая трата времени и что вместо того, чтобы пытаться помочь людям справиться с электронной почтой и проблемой фишинга, как это происходит сегодня, мы должны пытаться пропатчить саму электронную почту. Должны попытаться сделать вычисления совершенно безопасными для людей по умолчанию. Идея замечательная, но это своего рода журавль в небе.

Я увидел свое первое фишинговое письмо в 1997 году на EarthLink. Если бы вы сказали мне, что это все равно останется огромной проблемой, что я до сих пор буду зарабатывать на жизнь, борясь с этим, я бы никогда не поверил. Общая проблема заключается в том, что протокол электронной почты сломан, и не похоже, что это будет исправлено в ближайшее время. Через десять лет ее все равно будут взламывать. Многие люди на протяжении долгих лет пытались улучшить систему, но ни одно из дополнений не прижилось. И я не понимаю этого, потому что мы исправили другие протоколы и избавились от некоторых, таких как Telnet. Никто больше его не использует. Вместо этого мы обратились к SSH. Но по какой-то причине сломанный протокол электронной почты продолжает жить, несмотря на огромные проблемы, и до тех пор, пока это так, я хочу помогать компаниям обезопасить себя».

Я поделился своим недоумением по поводу того, что множество организаций не делает больше антифишингового тестирования и обучения, хотя это, вероятно, номер один или два в списке лучших вещей, которые они могут сделать, чтобы уменьшить риск взлома. Хигби сказал: «Часть проблемы в том, что некоторые из людей, проводящих фишинговые тесты, идут во всеоружии и в итоге провоцируют проблемы. Мы не просто проводим тест PhishMe. Мы говорим людям, чтобы они общались со всеми сотрудниками и руководством, и пусть они знают, что мы будем проводить фишинговые тесты в течение следующего года. Нужно меньше тестов и больше образования. Часть того, что мы делаем, – это обучение клиентов тому, как решать проблемы, чтобы все были в плюсе».

Вероятно, лучшее в моем интервью с Хигби – что он кажется таким же радостным и счастливым, как и когда я работал с ним более 10 лет назад. Он сказал, что создание и ведение бизнеса было невероятно напряженным, но он справился и смог сохранить жизнерадостность. Видимо, так же поступают и его сотрудники. Компания PhishMe совсем недавно была признана одним из лучших мест для работы по версии журнала Washington Business Journal и провела ежегодную встречу в Канкуне. И почему я не мог придумать антифишинговую компанию 10 лет назад?..

Информация об Аароне Хигби

Больше информации об Аароне Хигби вы найдете по ссылкам:

• Аарон Хигби в Twitter: **https://twitter.com/higbee**;

• профиль Аарона Хигби на LinkedIn: **https://www.linkedin.com/in/aaron-higbee-6098781**;

• блог Аарона Хиги на PhishMe: **https://phishme.com/author/aaronh/**.

27. Профиль: Бенилд Джозеф

В свои 25 лет Бенилд Джозеф из Бангалора в Индии стал одним из самых молодых людей, о которых мы говорим в этой книге. Но за свою недолгую карьеру, всего за восемь лет (на момент нашего интервью), он составил для себя неплохой послужной список и усердно работает над повышением информационной безопасности своей родины и региона. Он специализируется на безопасности веб-приложений и обнаружил критические уязвимости на многих популярных веб-сайтах, включая AT&T, Sony Music, BlackBerry и Deutsche Telekom. Сказать, что он яркая фигура, – ничего не сказать. В настоящее время он работает главным исполнительным директором проекта Th3 art of h@ckin9, являющегося частью международного проекта по ИТ-безопасности (инициатива при поддержке правительства Индии), а также членом правления Ассоциации по безопасности информационных систем родной страны. Он входит в топ-10 этичных хакеров Индии по версии социального форума Microsoft и был назван одним из восьми самых известных этичных хакеров Индии по версии журнала Silicon India. Джозеф часто пишет и преподает.

Индия – прекрасная развивающаяся страна со множеством ярких людей, но в то же время она только в последние десять или около того лет заметно вошла в эпоху Интернета. Бóльшая часть населения очень бедна. Зная это, я спросил Джозефа, как он очутился в сфере ИБ. Он сказал: «Я всегда увлекался хакерством, а вот информационная безопасность не была мне интересна. В то время это не было чем-то действительно известным или обсуждаемым в Индии. Мне просто нужно было взломать почтовый аккаунт друга. Я заинтересовался этичным хакерством, чтобы узнать больше о хакерстве в целом. Я даже сказал

преподавателю, что пришел на курс не для того, чтобы узнать об этичном хакерстве или информационной безопасности, а для того, чтобы взломать электронную почту моего друга. Я был уверен, что получение сертификатов – пустая трата времени. Но он увидел что-то во мне и научил первым вещам, которые я узнал об этичном взломе и информационной безопасности. Он стал моим наставником. Даже когда я узнал достаточно много об этичном хакерстве, он сказал, что мне предстоит долгий путь, чтобы стать профессионалом в области безопасности. Он бросил мне вызов, и я продолжил учиться».

В настоящее время Джозеф часто работает от имени агентств по борьбе с киберпреступностью и правительства Индии, включая проекты для Бюро по расследованию киберпреступлений (CCIB), Международной целевой группы по киберугрозам (ICTTF) и инициативы форума по кибербезопасности (CSFI). Он соавтор книги *CCI*, написанной для правоохранительных органов Индии. Бенилд специализируется на тестировании на проникновение веб-приложений и цифровой судебной экспертизе. Неплохо для парня, который просто хотел взломать почту своего друга!

Он продолжил: «Сейчас я работаю во многих компаниях и над многими проектами. Мои роли постоянно меняются. На данный момент я занимаюсь проектом для индийского правительства, cybersurveillance, цель которого – остановить злоумышленников. Я также много размышляю о кибервойне, которая часто ведется против Индии. Не только против государства и бизнеса, но и против граждан».

Я спросил его, с какой самой большой проблемой сталкивается его страна в области ИБ. Джозеф ответил: «Индия находится в первой десятке в области информационных технологий, но не в сфере информационной безопасности. Десять лет назад мы даже не слышали об этом. Этому не учили. Не было никаких вакансий для специалистов по ИБ. Моя страна долгое время не добивалась экономических успехов. Раньше, если кому-то нужно было воспользоваться компьютером, он шел в интернет-кафе. Теперь Интернет есть в каждом доме и даже в каждой руке (благодаря мобильным телефонам с выходом в Интернет). Можно сказать, что для нашей страны компьютеры и проблемы информационной безопасности стали чем-то новым. У нас есть много врачей, юристов, инженеров и других специалистов, но не так много специалистов по ИБ. Но ситуация постепенно меняется. Правительство и бизнес поняли, что нам нужны лучшие специалисты по информационной безопасности. Сегодня многие вузы предлагают магистерские программы по ИБ. Правительство понимает, насколько это важно, и начинает реализацию многих программ. Я провожу много времени, путешествуя по Индии и другим частям мира, преподавая курс по информационной безопасности. Индия сильно изменилась, и я помогаю ее улучшить».

Мы можем только надеяться, что в Индии и остальных странах мира достаточно таких ребят, как Бенилд Джозеф.

Информация о Бенилде Джозефе

Более подробную информацию о Бенилде Джозефе вы можете узнать по ссылкам:

• профиль Бенилда Джозефа на LinkedIn: **https://www.linkedin.com/in/benild**;

• профиль Бенилда Джозефа на Google+: **https://plus.google.com/107600097183424443393**;

• видео Бенилда Джозефа на YouTube о проектах Kaizen и Hacker5: **http://www.youtube.com/watch?v=BH_BNXfj0pQ**.

28. DDoS-атаки

Вам может казаться, что у вас лучшая информационная безопасность, но есть вещи, находящиеся вне вашего контроля. Добро пожаловать в мир атак отказа в обслуживании (DDoS). То, что начиналось с одного хакера, подавляющего сервер, отправляя больше трафика, чем тот мог принять, превратилось в эскалацию войны нескольких уровней и зависимостей, отправленных группами и профессиональными вендорами услуг. Сегодняшние массовые DDoS-атаки часто компрометируют подключенные к Интернету домашние устройства и отправляют сотни гигабит вредоносного трафика в секунду. DDoS-атаки совершаются по многим причинам, включая месть, увещевания, неуверенность, политические цели и даже игровые преимущества.

Типы DDoS-атак

Существует множество видов атак. В следующих разделах мы рассмотрим наиболее известные из них.

Отказ в обслуживании

Атаки отказа в обслуживании (DoS) – это когда один хост пытается скомпрометировать жертву при помощи чрезмерного трафика. Самыми простыми и ранними из них были «пинг-флуды». Их заменили потоками пакетов TCP, которые из-за полученного трехпакетного квитирования могли генерировать больше трафика. TCP-атаки были вытеснены UDP-атаками, так как состояние IP-адреса источника без установления соединения позволяет его подделать, что затрудняет отслеживание и остановку UDP-атак.

Простые типы атак уступили место массовым DDoS-атакам, где несколько хостов (иногда сотни тысяч) сосредоточены на одной цели. DoS-атака может посылать десятки мегабит вредоносного трафика в секунду, в то время как даже самая низкая DDoS-атака начинается с сотен мегабит в секунду. Каждый год ставится новый рекорд. Первая терабитная атака (1000 гигабит) может произойти к моменту публикации этой книги или вскоре после нее.

Прямые атаки

В прямой DoS-атаке вредоносный трафик генерируется единственным хостом. Злоумышленник может (случайным образом) изменить исходный IP-адрес в попытке скрыть его, но при прямых атаках только один отправитель создает трафик, который затем направляется непосредственно к цели без использования промежуточных узлов. Прямые атаки теряют свою популярность, потому что их легко обнаружить, смягчить и устранить.

Reflection-атаки

Reflection-атаки используют один или несколько промежуточных узлов для генерации DDoS-атак. Существует DDoS-бот вредоносных программ, ожидающих команд, которые будут проинструктированы атаковать конкретный хост. Как правило, сотни, десятки тысяч хостов используются против предполагаемой цели. Исходный сервер «Команда и контроль» (C&C) отправляет соответствующие инструкции ботам. Таким образом, несколько пакетов от сервера C&C могут оказаться миллионами пакетов в секунду.

Усиление

Усиленные DDoS-атаки используют «шумные» протоколы, которые отвечают более чем одним пакетом при получении одного пакета против намеченных целей. Например, злоумышленник DDoS может отправить неправильный запрос на веб-сервер с фальсифицированным IP-адресом источника, принадлежащим жертве. Промежуточный веб-сервер получает неправильный запрос и отправляет его обратно на исходный IP-адрес (целевой жертвы) с несколькими ответами или попытками исправления ошибок. Другая популярная DDoS-атака злоупотребляет DNS-серверами, запрашивая большее количество DNS-информации, на которую DNS-сервер отправляет несколько, если не десятки, пакетов в ответ. Вы можете узнать больше о DNS-атаках на сайте: **https://technet.microsoft.com/en-us/security/hh972393.aspx**. Чем больше усиление, тем успешнее DDoS-атакующий. Когда усиление координируется с десятками, сотнями тысяч ботов, могут быть выполнены огромные DDoS-атаки.

Применение на каждом уровне модели OSI

DoS/DDoS-атаки могут быть выполнены на каждом уровне модели OSI (физический, канал передачи данных, сеть, сеанс, транспорт, представление и применение). Физическая атака может быть выполнена путем физического уничтожения зависимости Центральной службы, такой как маршрутизатор, DNS-сервер или сетевая линия. Все остальные типы атак используют один или несколько протоколов на разных уровнях.

Усиливающиеся атаки

Сегодня наиболее успешные DDoS-хакеры атакуют цели с помощью широкого и разнообразного набора атак по модели OSI. Они могут начинаться с простого флуда в протоколе более низкого уровня и увеличивать трафик с течением времени с короткими паузами между ними. Вероятно, они начинают с простого

отражения, а затем переходят к методам усиления. Затем они переключают уровни атаки, продвигаясь вверх по модели OSI, и добавляют еще больше трафика. Злоумышленники часто используют уровень приложений, подделывая трафик, который изначально выглядит как законный, но занимает очень мало пропускной способности.

По мере того как жертва думает, что DDoS под контролем, он меняется и трансформируется. Жертва начинает думать, что поняла масштаб атаки и как ее победить, а атака уже изменилась. Это сбивает с толку жертву и специалиста по ИБ и заставляет дольше настраивать успешную смягчающую защиту. И каждый раз, когда жертва думает, что нашла решение, атака меняется снова, назад и вперед, назад и вперед, и продолжается борьба, пока у атакующего не появятся новые типы атак.

Атаки на исходящий и входящий каналы

На сайтах, ставших жертвами атак, часто реализуются методы и службы защиты от DDoS, и они нередко успешны. DDoS-атакующие перемещаются вверх или вниз «по течению» и ищут новую цель. Поставщик должен решить, стоит ли вредить всем своим клиентам, чтобы спасти одного. Если жертве повезет, специалист по ИБ успеет что-то предпринять до полного прекращения доступа. В других случаях жертва просто блокируется на несколько дней, если не дольше, пока массовые DDoS-атаки не ослабеют. Ежегодно встречаются случаи, когда жертве не удается реабилитироваться.

Подробнее о DDoS-атаках можно прочитать на сайтах: **https://www.incapsula.com/ddos/ddos-attacks**, **https://javapipe.com/ddos-types/** и **https://en.wikipedia.org/wiki/Denial-of-service_attack**.

Инструменты и сервисы для совершения DDoS-атак

Существует множество инструментов и вендоров услуг, чтобы помочь каждому осуществить DDoS-атаку.

Инструменты

Есть десятки инструментов и методов, доступных в Интернете, чтобы помочь любому выполнить DoS или DDoS-атаку. Просто введите «DDoS-инструменты» в интернет-браузере. Большинство из них действуют как законные тестеры. Некоторые примеры: Low Orbit Ion Cannon (**https://sourceforge.net/projects/loic0/**), DLR (**https://sourceforge.net/projects/dlr/**) и Hulk (**https://packetstormsecurity.com/files/112856/HULK-HttpUnbearable-Load-King.html**). Хакеры должны использовать эти инструменты только против сайтов, которые дали им на это разрешение. Многих начинающих хакеров

арестовывают, поэтому, чем быстрее вы присоединитесь к хакерам «в белой шляпе», тем лучше.

DDoS-сервисы

Есть даже десятки услуг, доступных в Интернете, с помощью которых вы можете запустить DDoS-услуги. Многие из них стоят не больше 100 долларов. Как и в случае с инструментами DDoS, большинство из них утверждают, что тестируют сервисы (которые просто не проверяют, чтобы убедиться, что у пользователя есть разрешение использовать их против конкретного сайта). К сожалению, некоторые услуги, которые заявляют, что они анти-DDoS-услуги, на самом деле были их частью. В отношении подобных служб ведется расследование, некоторые закрыты, а другие продолжают процветать. Следственный репортер Брайан Кребс написал несколько отличных статей на эту тему, в том числе и эту: **https://krebsonsecurity.com/2016/10/spreading-the-ddos-disease-and-selling-the-cure**.

Защита от DDoS-атак

Существует множество средств защиты, которые можно использовать для борьбы с DDoS-атаками.

Обучение

Все люди, участвующие в работе ваших сайтов и услуг, должны быть осведомлены о DDoS-атаках и способах их предотвращения. Образование – первый шаг на пути к их выявлению и профилактике.

Стресс-тестирование

Проводите стресс-тестирование ваших сайтов, потенциально используя некоторые из тех же инструментов, которые могут применить хакеры. Думайте как хакер и атакуйте все ссылки и уязвимые места, необходимые для взлома вашего сайта или сервиса. Узнайте, что нужно, чтобы «выбить себя из Интернета» и определить, какие у вас уязвимости. Как только вы их найдете, спроектируйте простые ссылки и определите соотношение затрат и выгод.

Соответствующая настройка сети

Убедитесь, что ваши сайты и службы защищены брандмауэрами и маршрутизаторами, которые способны обнаруживать и останавливать DDoS-атаки. Убедитесь, что все задействованные хосты настроены на защиту от них с минимальными сбоями. Кроме того, у многих компаний есть соглашения с другими вендорами и даже конкурентами, чтобы иметь возможность перемещать или заимствовать ресурсы, если они окажутся под угрозой DDoS-атаки. Некоторые из них связаны со свободными ресурсами или минимальной структурой возмещения расходов.

Исследование потенциально слабых мест

При создании услуг думайте обо всех потенциальных точках для DoS-атак. Например, в Microsoft поняли, что подключение удаленного рабочего стола (RDP) часто может быть сделано в Microsoft Windows с незащищенными соединениями и при этом эффективно использовать все имеющиеся ресурсы. Microsoft изменила RDP, чтобы авторизованный сеанс сначала использовал большое количество средств, и ограничили число попыток подключения, которые могут быть сделаны одновременно из всех источников. Эти новые функции делают его очень трудной мишенью для DoS-атаки.

Анти-DDoS-сервисы

Есть много премиум-анти-DDoS-сервисов, в том числе Imperva (**https://www.incapsula.com/**) и Prolexic/Akamai (**http://www.prolexic.com/**). Большинство защищают клиентов, используя многоуровневую комбинацию огромной, избыточной пропускной способности и средств защиты, специально предназначенных для смягчения DDoS-атак. Недостаток в том, что эти услуги довольно дорогостоящие, многие компании не могут позволить себе такие расходы. Тем более нападение может и не произойти. Если вы когда-нибудь решите использовать услуги защиты от DDoS-атак, внимательно изучите все варианты, чтобы убедиться, что вендор – не один из тех, кто их вызывает.

Так же, как DDoS-атакующих, в мире много «белых» специалистов по DDoS. При обдумывании и планировании DDoS-атаки могут быть менее разрушительными, чем без планирования и защиты.

В главе 29 представлен профиль Брайана Кребса, репортера информационной безопасности и исследователя, человека, наиболее выделяемого среди DDoS-атакующих.

29. Профиль: Брайан Кребс

Однажды, когда Брайан готовился к небольшому званому обеду у себя дома, в дверь позвонили. Это оказался отряд спецназа с черным тактическим снаряжением, штурмовыми винтовками и дробовиками, направленными на него. После того как спецназ задержал его, Кребс понял, что это обычный день в его жизни, ведь он борется с хакерами в качестве ведущего интернет-репортера и следователя. Он усердно препятствует спамерам, скиммерам и хакерам всех разновидностей уже более десяти лет. Он участвовал в нескольких расследованиях и рейдах, в результате которых те же самые хакеры потеряли миллионы долларов и были арестованы. В отместку хакеры отправляли ему все виды незаконной контрабанды, в том числе наркотики и поддельные валюты, наряду с многочисленными угрозами смерти ему и его семье. Истории, похожие на описанный инцидент, вы можете прочитать здесь: **http://arstechnica.com/security/2013/03/security-reporter-tells-ars-about-hacked-911-call-that-sent-swatteam-to-his-house/**.

Полиция приезжала в дом Кребса так часто, с тех пор как анонимный «добрый самаритянин» дал наводку, что местные правоохранительные органы в итоге стали получать как физические, так и электронные уведомления, чтобы не слишком реагировать на звонок. В итоге Кребс устал от преследований и решил на некоторое время отойти от дел. Он считал, что его семья заслуживает отдыха от постоянных угроз, впрочем, как и он сам. Но это не было победой хакеров. Кребс продолжает свои ежедневные расследования, чтобы одержать верх над теми, кто наносит вред другим.

Так было не всегда. В течение многих лет Кребс работал простым репортером в газете Washington Post. Но расследования компьютерных преступлений были настолько запутанными и подробными, что руководство газеты уволило его. Он сразу же создал свой блог (**https://krebsonsecurity.com/**) и продолжил исследования с еще большим рвением и вниманием. Его блог один из самых популярных в Интернете, он выпустил потрясающую книгу-бестселлер *Spam Nation* (**https://www.amazon.com/Spam-Nation-Organized-Cybercrime-Epidemic/dp/1492603236/**), а Голливуд даже подумывал снять о нем фильм.

Репортажи Брайана о расследованиях первоклассны. Когда Кребс решил, что лучшие в мире спам-компании расположены в России, он научился читать, писать и говорить по-русски, а затем отправился туда, чтобы взять интервью у богатых и влиятельных русских, стоящих за этими компаниями. После я разговаривал с ним и сказал, что не могу поверить, что он рискует жизнью, чтобы рассказать эту историю. Брайан ответил, что он, очевидно, так не считал, но несколько друзей сказали ему то же самое. Публичное разоблачение, сделанное Кребсом, лишало преступников десятков миллионов долларов, и теперь он посещает их на их родине, где у него очень мало прав. Многие из нас были готовы прочитать о безвременной кончине Кребса во время визита в Россию. Вместо этого он вернулся с достаточным количеством фактов, чтобы написать книгу (*Spam Nation*), а некоторые люди, с которыми он беседовал, попали в тюрьму.

Большинство журналистов по ИБ лишь повторяют факты, освещенные Кребсом. Кребс исследует и узнает новое. В своем блоге он говорил: «Я не писал об этих историях главным образом потому, что у меня не было оригиналов некоторых документов или другого фактического подтверждения моих слов. Поэтому я решил не писать просто занимательную историю, а сосредоточиться на киберпреступности и информационной безопасности».

Хотя Кребс расследует многие виды взлома, его основные направления – финансовые преступления, спамеры, скиммеры и отказ в обслуживании. Кребс с легкостью может отследить транзакции денег и данных. Он обнаружил людей, стоящих за многими из крупнейших в мире хакерских организаций и атак. Нередко случалось так, что после того как Кребс идентифицировал кого-то, его арестовывали и обвиняли в преступлениях. Кажется, будто правоохранительные органы читают его блог и ждут, когда он раскроет настоящую личность преступника, чтобы получить ордер. Я уверен, что это не совсем так, но очень на то похоже. Один из лучших показателей успеха Кребса – явление, которое последователи назвали «Циклом Кребса». Он часто узнает о взломах и утечках

данных за несколько дней до того, как это произойдет. Цикл Кребса – это промежуток времени между тем, когда он рассказывает миру правду о последнем взломе, и тем, когда вендор публично его признает.

Кребс не боится разоблачать организации, которые мы считали хорошими. Он обвинил компании кредитных карт и банки в том, что те помогают в совершении финансовых преступлений. Он обличил онлайн-налоговиков, помогающих облегчить преступникам подачу ложных налоговых деклараций. Он сделал прозрачно ясным, что крупные фармацевтические компании разрешают незаконную продажу лекарств, потому что не хотят признавать, что их оригинальные лекарства (а не подделки) продаются за меньшие деньги. Он доказал, что некоторые фирмы, которые утверждают, что защищают нас от хакеров, сами либо проводят хакерские атаки, либо защищают хакеров. Он обозначил интернет-провайдеров и пуленепробиваемые услуги хостинга для обслуживания хакеров в качестве бизнес-модели. Кребс следует за деньгами, куда бы они ни пошли.

По этой причине веб-сайт Кребса постоянно подвергается DDoS-атакам (см. предыдущую главу). DDoS-атакующие часто включают личные насмешки над Кребсом в свой вредоносный трафик и требуют, чтобы новые сотрудники проявляли себя, атакуя его сайты. Часто Кребс вычисляет преступника, и он попадает в тюрьму.

Брайан способен сделать то, чего многие другие люди и правоохранительные органы, похоже, не могут – идентифицирует хакера. Для его блога затишье в несколько недель не редкость, но когда Кребс снова начинает писать, он непременно выдает имя очередного злоумышленника. Он часто узнает их личность, следуя по цифровым «хлебным крошкам», которые связывают секретную личность хакера с его публичной онлайн-идентификацией. В итоге вы видите этого очень злого и неэтичного вредителя в отпуске со своей семьей, обнимающего жену и детей, и понимаете, что его беззаботные дни сочтены. Многие хакеры, которых Кребс разоблачил, стали международными беглецами, в то время как другие, похоже, пользуются коррумпированностью местных чиновников. В любом случае все они ненавидят Кребса, в то время как остальной мир любит его. Я думаю, Брайан Кребс настоящий американский герой!

Помимо выявления конкретных хакеров и сомнительных предприятий, труды Кребса позволяют читателям увидеть крупный бизнес «черных» хакеров. Мир хакерства – это не какой-то подросток, сидящей за компьютером с хлопьями в тарелке и колой в стакане; это огромный бизнес с различными отделами, генеральными директорами, а иногда и публично продаваемыми акциями. Порой это даже законный бизнес, которому мы доверяем. Мир взлома так же сложен, как и сама жизнь. Следственные отчеты Кребса пробудили мой личный интерес к этому вопросу. Эту «таблетку» трудно проглотить, но нам всем лучше от того, что мы ее приняли.

Информация о Брайане Кребсе

Более подробную информацию о Брайане Кребсе ищите по ссылкам:

• Брайан Кребс в Twitter: **https://twitter.com/briankrebs**;

• профиль Брайана Кребс на LinkedIn: **https://www.linkedin.com/in/bkrebs**.

30. Безопасность операционной системы

Вот одна из самых популярных шуток об информационной безопасности: «Если вы хотите безопасный компьютер, то:

• заприте его в шкафу, предварительно вынув сетевую карту;

• выбросите клавиатуру;

• избавьтесь от конечного пользователя».

Популярные компьютерные операционные системы стали более безопасными, чем когда-либо. Они поставляются с довольно безопасными настройками по умолчанию, требуют паролей, автоматически обновляются, шифруют данные и поставляются со множеством других функций. Это не означает, что все они имеют одинаковый уровень безопасности или успех. Тем не менее общий успех достиг того уровня, когда большинство хакеров и вредоносных программ прибегают к социальной инженерии или используют уязвимость, возникшую из-за того, что пользователь своевременно не применил патч.

Это произошло не случайно. Вендорам потребовались годы, если не десятилетия, опыта и анализа, чтобы найти приемлемую грань между слишком безопасной и слишком небезопасной системами. Конечные пользователи просто хотят, чтобы их ОС работали по назначению без особых помех. Если конечному пользователю будет слишком сложно работать с системой, он либо попытается обойти функцию безопасности, отключив ее, либо выберет совершенно другую операционную систему. Многие сотрудники безопасности заведомо уменьшают возможности любой операционной системы, которая принимает не самые надежные, но зато удобные для конечного пользователя, решения. С учетом сказанного, можно догадаться, что есть очень безопасные ОС.

Как защитить операционную систему

Существует три основных способа защиты ОС: изначально создать ее безопасной и сделать безопасные алгоритмы по умолчанию, повысить безопасность с помощью средств настройки безопасности или следовать рекомендациям по обеспечению безопасности. Большинство современных операционных систем используют все эти методы.

Создание безопасной операционной системы

Лучший, а по мнению некоторых, единственный способ получить безопасную операционную систему – создать ее. Она должна быть не только надежно спроектирована, но и иметь соответствующие функции безопасности с

настройками по умолчанию. Исследование за исследованием показывают, что большинство конечных пользователей принимают параметры безопасности по умолчанию, поэтому, если такое значение установлено неправильно, это подрывает безопасность.

Общие критерии

Международный стандарт оценки и ранжирования безопасности операционной системы известен как общий критерий оценки безопасности информационных технологий, хотя его часто называют единым критерием. Вендоры представляют свои ОС или приложения для оценки по общим критериям, надеясь получить сертификат как определенный уровень оценки гарантии и надежности, который варьируется с возрастающими сложностью и безопасностью от EAL1 до EAL7. Хотя кажется естественным предположить, что все вендоры операционных систем, которые заботятся о безопасности, хотели бы получить самый высокий рейтинг (EAL7), это не так. Уровни EAL5 и выше не только очень трудно заработать, но и, как правило, они требуют операционной системы, которая не всегда хорошо функционирует в реальном мире. Хотите подключиться к Интернету и скачать программу? Вероятно, вы не сделаете этого с системой уровня EAL5 или выше.

EAL5 и более высокие уровни обычно зарабатываются очень специфическими приложениями безопасности (например, смарт-картами, модулями аппаратного хранения и т. д.) или связанными с правительством ОС высокого риска, такими как ракетные системы. Большинство операционных систем, которые мы знаем и любим сегодня, включая конкретные версии Microsoft Windows, Linux, Solaris, AIX и BSD, имеют рейтинг EAL4 или EAL4+ (знак «плюс» указывает на то, что он чуть лучше, чем просто EAL4, но недотягивает до EAL5). Предпринимаются усилия для перехода от рейтингов EAL к так называемым профилям защиты (PP). Более подробную информацию можно найти по ссылке: **https://blogs.ca.com/2011/03/11/common-criteria-reforms-sink-or-swim-how-should-industry-handle-the-revolution-brewing-with-commoncriteria/**.

Примечание. Насколько мне известно, Apple iOS никогда не проходила традиционный процесс сертификации EAL.

Соответствие более высоким общим критериям EAL или PP не означает, что хакер не может успешно взломать рейтинговую систему, но говорит о сложности процесса. Это также не означает, что нерейтинговая операционная система небезопасна или не будет соответствовать той же сертификации, если пройдет ее.

Федеральные стандарты обработки информации

Соединенные Штаты имеют другой популярный стандарт под знаменем федеральных стандартов обработки информации (FIPS), по которому

операционные системы или их части могут быть оценены и сертифицированы. Хотя FIPS (**https://www.nist.gov/topics/federal-information-standards-fips**) официально относится только к правительству, связанному с компьютерными системами, это уважаемый мировой стандарт. Сертификаты FIPS известны по определенному номеру, например 199-3 или 140-2. FIPS 140-2 применяется к криптографическим процедурам, и представленные продукты могут быть сертифицированы как FIPS 140-2, уровня с 1 по 4, при этом 4 – показатель самой высокой безопасности.

Из-за потребительского спроса большинство вендоров операционных систем и приложений, которые получают общие критерии или сертификацию FIPS, обычно сей факт рекламируют. Некоторые клиенты требуют определенной оценки или рейтинга, прежде чем задумаются о покупке продукта.

История о двух безопасных операционных системах

В мире популярных ОС общего назначения есть две системы (обе с открытым исходным кодом), которые намерены быть более безопасными, чем среднестатистические: OpenBSD и Qubes OS.

OpenBSD (**www.openbsd.org**) была создана компанией Тео де Раадта как новый форк от NetBSD в 1995 году. Многие функции безопасности, необязательные в других операционных системах, включены в нее по умолчанию. Разработчики часто проводят аудит своего кода в поисках ошибок безопасности. OpenBSD особенно уважают за то, что она имеет наименьшее количество ошибок, найденных внешними сторонами, чем любая другая популярная операционная система.

Qubes (**https://www.qubes-os.org/**) была создана Варшавской лабораторией и ее основателем и генеральным директором Йоанной Рутковской (с ее профилем мы познакомимся в следующей главе) в 2012 году. Qubes использует изолированный гипервизор Xen, позволяющий дополнительной операционной системе и компонентам работать в дополнительных высокоизолированных средах виртуальных машин. Даже функциональность сети работает в своем собственном домене. Каждый домен может быть классифицирован в соответствии с потребностями безопасности и работать под управлением различных дополнительных ОС. Возможно, это опрометчиво, но даже основатели описывают Qubes как «достаточно безопасную операционную систему». Тем не менее другие тоже считают, что это самая безопасная популярная и доступная ОС, и она особенно любима многими экспертами по конфиденциальности и безопасности.

Не то чтобы это требовалось для разработки и ведения более безопасной ОС, но и де Раадт, и Рутковская известны своим интеллектом и случайной социальной абразивностью. Они не боятся задеть чувства других, когда отстаивают свою позицию или высказывают мнение, особенно когда сталкиваются с давней, но ошибочной догмой. Они применяют эту бескомпромиссность и к продуктам,

которые разрабатывают. Вам необязательно использовать OpenBSD или Qubes для обеспечения относительно безопасной ОС, но их использование, как правило, облегчает получение уровня безопасности выше среднего.

Рекомендации по обеспечению безопасности

Большинство популярных операционных систем имеют относительно надежные значения и параметры по умолчанию, но они не всегда соответствуют рекомендуемым лучшим параметрам безопасности. Например, Windows 10 поставляется с минимальным значением длины пароля всего 6 символов, хотя Microsoft и большая часть мира безопасности рекомендует минимум 12, а то и 16 символов. Проблема в том, что популярные операционные системы должны обращаться к широкому кругу людей и сценариев безопасности. Казалось бы, безвредные параметры безопасности, такие как минимальная длина пароля, если они включены в «рекомендуемых» настройках, могут вызвать проблемы в работе в большом количестве сред и даже потенциально привести к ухудшению безопасности. Поэтому большинство производителей ОС делают акцент на один параметр, хотя и рекомендуют использование дополнительной защиты.

Эти рекомендации можно загрузить у вендоров и некоторых сторонних организаций. Например, рекомендации корпорации Microsoft можно загрузить по ссылке **https://blogs.technet.microsoft.com/secguide/2016/07/28/security-compliance-manager-4-0-now-available-for-download/**, а рекомендации Apple – с **https://support.apple.com/en-gb/HT202739**. Центр стандартов интернет-безопасности (**https://benchmarks.cisecurity.org/downloads/**) – один из самых популярных источников для третьих сторон.

Средства конфигурации параметров безопасности

Вендоры ОС и третьи стороны предлагают средства и программы для безопасной настройки различных операционных систем и приложений. У Microsoft есть свои рекомендации по безопасности (ссылка представлена в предыдущем разделе). Многие дистрибутивы Linux начинаются с экрана настройки на основе графического интерфейса пользователя, который задает несколько общих вопросов безопасности во время установки, чтобы помочь вам настроить ОС. Центр стандартов интернет-безопасности также предлагает участникам коммерческие средства настройки. Есть без преувеличения сотни инструментов настройки безопасности. Все они призваны помочь конечному пользователю или администратору легче применять параметры безопасности и управлять ими.

Консорциумы по вопросам обеспечения безопасности

Мир ИБ полон надежных консорциумов промышленной безопасности, которые пытаются сделать вычисления более безопасными. Две группы, которые оказали большое влияние в последнее время, – это Группа надежных вычислений и Альянс FIDO.

Trusted Computing Group

Моя любимая отраслевая Группа надежных вычислений (**https://trustedcomputinggroup.org/**) работает над тем, чтобы придумывать и стандартизировать более безопасное оборудование и программное обеспечение. Она отвечает за многие из наиболее широко принятых, безопасных по умолчанию стандартов безопасности, таких как чип доверенного платформенного модуля и опаловые жесткие диски с самошифрованием. Если вы хотите узнать, что потребуется для создания действительно безопасных устройств и операционных систем, прочитайте все, что публикует эта Группа.

Альянс FIDO

FIDO (быстрая онлайн-идентификация) Альянс (**https://fidoalliance.org/**) специализируется на замене простого входа в систему аутентификации паролем с более сильной альтернативой. Основанная в 2012 году, FIDO ориентирована на более надежную аутентификацию через браузеры и устройства безопасности при доступе к веб-сайтам, веб-службам и облачным предложениям. В настоящее время все методы аутентификации FIDO используют криптографию с открытым/закрытым ключом, что делает их очень устойчивыми к традиционным фишинговым атакам и атакам «через промежуточное звено». Сегодня у FIDO есть два способа аутентификации: универсальная платформа аутентификации (UAF) без пароля и универсальный второй фактор (U2F), метод двухфакторной аутентификации (2FA). Последний может использовать даже несложный пароль, потому что дополнительный фактор гарантирует общую прочность. Аутентификация FIDO должна поддерживаться вашим устройством или браузером, а также сайтом или службой аутентификации. Аутентификация на основе FIDO только набирает популярность, но, я полагаю, достигнет больших высот в ближайшее время.

Ни одна операционная система не обладает совершенной безопасностью и не может бескомпромиссно противостоять атакам противника. Но многие из них могут быть относительно безопасными либо изначально, либо с применением рекомендаций по безопасности.

В главах 31 и 32 описаны профили Йоанны Рутковской и Аарона Маргосиса, двух выдающихся специалистов в области ИБ.

31. Профиль: Йоанна Рутковская

Уроженка Польши Йоанна Рутковская появилась на мировой сцене ИБ при драматических обстоятельствах. В 2006 году она объявила (**http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html**) руткит вредоносной программой. Руткит – это программа, которая изменяет операционную систему, чтобы лучше скрываться от нее и любой другой программы. Рутковская обнаружила метод, с помощью которого руткит может

скрыться таким образом, что будет обнаружена только с огромным трудом. Она назвала свою идею «синей таблеткой».

Аллегория синей таблетки происходит из знаменитого фильма «*Матрица*» (**http://www.imdb.com/title/tt0133093/**). Главному герою, Нео, предлагаются две таблетки: красная и синяя. Если он примет красную таблетку, то сможет остаться в реальном мире, а голубая вернет его в иллюзорный, более комфортный мир, который был Нео знаком. Каждый, кто смотрел этот фильм, знает, что герой выбрал красную таблетку и начал бороться за спасение мира.

Рутковская назвала свое открытие «синей таблеткой», потому что ее метод руткитов использует встроенные функции виртуализации современных процессоров для самореализации в качестве гипервизора виртуализации с неосведомленной операционной системой, работающей от него. Захваченная ОС думает, что работает без обременения, полностью контролируя себя, когда на самом деле находится под полным влиянием и потенциально неправильным направлением гипервизора.

Рутковская описала свое открытие так: «Идея “синей таблетки” проста: ваша операционная система проглатывает ее и просыпается внутри Матрицы, контролируемой ультратонким гипервизором. Все это происходит на лету (т. е. без перезагрузки системы), не сопровождается снижением производительности, а все устройства, такие как видеокарта, полностью доступны для операционной системы, которая теперь выполняется внутри виртуальной машины».

Ее заявление было революционным для того времени. Гипервизоры и виртуализация только начинали набирать популярность. Большинство людей, включая экспертов по безопасности, недостаточно хорошо понимали технологию, а тем более последствия. И тут Рутковская заявила, что эта новая технология может быть использована для обхода любого метода обнаружения. Это создало своего рода экзистенциальный кризис в мире безопасности. Некоторое время были опасения, что авторы вредоносных программ начнут производить программы по типу синей таблетки и антивирусу будет трудно выявлять и устранять их.

В то время я вел колонку в журнале InfoWorld, пытаясь развеять чрезмерные страхи людей. Хотя я согласился с тем, что предложила Рутковская, я чувствовал, что возникшая сложность, вероятно, затруднит использование разработчиками вредоносных программ. Я заявил, что до тех пор, пока простые принципы вредоносных программ работают эффективно, их создатели вряд ли перейдут к новым, более трудным методам; но даже если такое произойдет, я был уверен, что создатели операционных систем и сотрудники безопасности смогут адекватно на них среагировать. Спустя десять лет мое решение (не слишком беспокоиться об угрозах «синих таблеток») оказалось правильным. Тем не менее Рутковская показала, что не только умна и нестандартно мыслит, но и бросает вызов тому, могут ли традиционные методы, используемые миром ИБ, обеспечить надежные, безопасные системы.

С момента появления «синей таблетки» в 2006 году, Рутковская стала очень популярным спикером на конференциях и продолжает задавать хорошие вопросы и предлагать интересные решения в области безопасности. Она публикует свои идеи на сайте Лаборатории Invisible Things (**http://invisiblethingslab.com/**) и в своем блоге (**https://blog.invisiblethings.org/**), хотя сейчас большая часть ее внимания направлена на другие проекты. Совсем недавно она посвятила много времени проекту Qubes, упомянутому в предыдущей главе.

Рутковская всегда изучала реальные и искусственные границы безопасности в операционных системах. Она обнаружила неприемлемую уязвимость безопасности почти в каждом дистрибутиве Linux по умолчанию, которая позволяла одной программе получить доступ к любой другой в той же ОС, если они использовали один и тот же рабочий стол (**http://theinvisiblethings.blogspot.com/2011/04/linux-security-circus-on-gui-isolation.html**). Это распространенный тип уязвимости, который есть в большинстве ОС. В то время как многие вендоры операционных систем и эксперты по безопасности считают, что это приемлемый риск, потому что вы должны работать на том же рабочем столе на той же ОС, Рутковская полагает, что этого недостаточно. Тем более что такие простые действия, как просмотр веб-страниц, могут привести к полной компрометации всей системы и критически важных доверенных приложений.

По этим и другим причинам в 2010 году она разработала Qubes. Как мы уже говорили, это операционная система с поддержкой гипервизора с акцентом на изоляцию безопасности. Она может запускать другие операционные системы, каждую в своем экземпляре виртуальной машины, а также серверную часть администрирования и сеть, выполняемую на своих изолированных виртуальных машинах. Qubes – это административный центр, который позволяет создавать, управлять и легко взаимодействовать со всеми виртуальными объектами. Каждый из них может отображаться смешанным в рабочем столе графического интерфейса пользователя, хотя они полностью разделены границами безопасности гипервизора. Как и любое программное обеспечение, оно имеет свои уязвимости и подвержено влиянию других, находящихся вне его контроля (например, в программе гипервизора Xen). Хотя Рутковская называет Qubes лишь «достаточно безопасной» операционной системой, на самом деле она наиболее ориентирована на безопасность из всех ОС общего назначения, которую вы можете скачать и использовать бесплатно. Также Рутковская продолжает исследовать другие проблемы безопасности, такие как слабые места PDF-файлов и уязвимости USB. Она активный сторонник реальной информационной безопасности и продолжает бросать вызов остальному миру, чтобы он становился лучше.

Информация о Йоанне Рутковской

Больше информации о Йоанне Рутковской вы можете узнать по ссылкам:

• Йоанна Рутковская в Twitter: **https://twitter.com/rootkovska**;

• веб-сайт Йоанны Рутковской в Лаборатории Invisible Things: **http://invisiblethingslab.com/**;

• блог Йоанны Рутковской в Лаборатории Invisible Things: **https://blog.invisiblethings.org/**;

• веб-сайт проекта Qubes: **http://qubes-os.org/**.

32. Профиль: Аарон Маргосис

Один из печальных фактов мира ИБ заключается в том, что, хотя каждый действует так, будто безопасные и надежные вычисления – это самая важная базовая функция компьютера, на самом деле это не так. Пользователи гораздо больше заинтересованы в новейших крутых функциях, нежели в информационной безопасности! Вендоры и разработчики, которые тратили слишком много времени на безопасность, в итоге были побеждены на рынке конкурентами. Дизайнеры, которые создают свои устройства и приложения слишком безопасными, в итоге остаются без работы. Вы должны создать операционную систему, которая будет безопасной, но при этом легкой в использовании, а это сложно.

Следовательно, ни у кого нет самой безопасной ОС на планете. Подавляющее большинство работает с популярной, хорошо поддерживаемой, довольно безопасной операционной системой, но не с самой безопасной. Если бы конечные пользователи действительно заботились об этом, большинство бы использовало систему Qubes, созданную Йоанной Рутковской, речь о которой шла в предыдущей главе, или OpenBSD, о которой мы говорили в главе 30. Это самые безопасные ОС общего назначения, и они бесплатны, но большинство их не использует. Нельзя сказать, что это плохо, так как мы принимаем подобные решения в повседневной жизни постоянно. Безопасность редко становится первым или единственным фактором при принятии решения. Большинство стран мира, по крайней мере сейчас, работает под управлением Microsoft Windows, Apple iOS и Android.

К счастью, большинство современных операционных систем достаточно безопасны. Если вы будете следовать рекомендациям вендора ОС, быстро применять патчи и не поддадитесь социальной инженерии, вас будет сложнее скомпрометировать. Основная часть безопасности зависит от следования рекомендациям вендора. Если вы когда-либо задавались вопросом, как эти рекомендации были выбраны, то вот ответ: они основаны на накопленном опыте и уроках, извлеченных из истории, а также нескольких преданных людях, которые исследуют каждую рекомендуемую настройку и пытаются определить оптимальный баланс затрат/выгод для большинства клиентов.

Аарон Маргосис, один из моих давних друзей, – сотрудник компании Microsoft, который убедился, что Microsoft Windows надежно настроен. В настоящее время у Маргосиса прическа как у рок-звезды, и он так же взволнован аспектами ИБ, как и бейсболом. Он изучает тысячи параметров безопасности, создает

бесплатные средства настройки и публикует статьи о безопасных вычислениях в течение почти двух десятилетий. Он написал два из самых невероятных закулисных взгляда на то, как в действительности работает Windows, вместе с Марком Русиновичем (речь о нем идет в главе 11). Многие специалисты считают эти книги едва ли не Библией.

Почти каждый день Маргосис участвует в устранении неполадок, связанных с определенным параметром безопасности, или пытается выяснить, почему некая компания – Microsoft или другая – сделала это своей рекомендацией. За эти годы он нашел десятки очень плохих рекомендаций, многие из которых вызвали проблемы и трудноразрешимые кризисы. Маргосис сделал больше, чем кто-либо другой, кого я знаю, чтобы популяризировать рекомендации касательно безопасности в Интернете, например в Центре интернет-безопасности (**https://www.cisecurity.org/**). Сейчас он работает с функциями Microsoft AppLocker и Device Guard, которые стремятся остановить вредоносные программы. Это естественное продолжение того, что он делал на протяжении всей своей карьеры.

Я начал наше интервью с вопроса о том, как он очутился в сфере ИБ. Он ответил: «Я получил степень бакалавра психологии в Университете Вирджинии, но у меня всегда был интерес к вычислительной технике. Я начал программировать на BASIC в 1970-е, когда мне было 12 лет. Я взял несколько факультативов по ИБ, когда был студентом Амстердамского университета, но не специализировался на компьютерах, потому что это означало бы изменение моей специальности на инженерию. Позже, после того как я начал работать в области компьютеров, я вернулся в Амстердамский университет и получил степень магистра в области компьютерных наук.

После колледжа я работал в разных компаниях, в том числе в двух, которые производили оборудование для проверки слуха, в компании по бухгалтерскому ПО, а также в фирме, занимающейся мобильными телефонами. Кроме того, я работал в компании Maynard Electronics, которая создала программу резервного копирования NT, поставляемую с первой версией Windows NT, и продукт Backup Exec (в настоящее время Symantec). Меня беспокоило то, как оградить свой компьютер от посторонних (например, моих коллег), и поэтому я заинтересовался сферой ИБ. Я попал в Microsoft в 1999 году и до сих пор там работаю».

Маргосис был одним из первых, кто посоветовал людям не работать в качестве администратора все время. Такой способ становится довольно популярным на Linux и Unix, но он не применяется в мире Windows. Фактически почти каждый разработчик ожидал, что конечный пользователь будет иметь полный контроль над своей системой, чтобы программное обеспечение работало правильно. Microsoft, под большим неформальным влиянием Маргосиса, наконец, решила, что Windows Vista (выпущенная в 2006 году) будет версией, которая, «подведет черту». Она представила функцию под названием “контроль учетных записей пользователей” (UAC), которая заставила всех пользователей работать не от имени администратора, а в качестве обычных пользователей по умолчанию. Последовали десятки тысяч сломанных программ. Попытка заставить вендоров

и разработчиков изменить свое мышление в то время была огромной задачей. Люди думали, что изменение учетной записи будет означать конец Microsoft Windows. Все это выглядело очень противоречиво.

Я спросил Маргосиса, в чем заключался его вклад. Он ответил: «В то время Microsoft в целом не думала, что переход от постоянного администратора к стандартным пользователям – это правильный путь. Но некоторые люди были сторонниками этого метода, например Майкл Ховард [профиль в главе 7]. Он говорил об этом и вдохновил меня попробовать работать от лица обычного пользователя. Я последовал его совету, работая с бета-версией Windows XP, и многие вещи оказались совершенно другими. Это был восхитительный вызов. Я начал думать о том, как оставаться продуктивным не как админ, и поэтому начал придумывать рабочие инструменты и методы и поделился ими со всем миром. Моя первая публичная презентация на конференции в Microsoft TechEd состоялась в 2005 году, на ней присутствовало более 1500 участников; выступление было посвящено изменению учетной записи Windows XP по умолчанию. Мои блоги и беседы оказали большое влияние на группу разработчиков Windows Vista. В то время шла борьба, и было неясно, выиграет ли работа в системе в качестве пользователя, но Джим Олчин и команда контроля учетных записей отстояли ее. Я рад, что был частью этого. Это принесло пользу всей клиентской базе».

Я спросил Маргосиса, как он стал работать над своей выдающейся бесплатной безопасной диагностикой и настройкой инструментов. Он ответил: «Это началось с моей задумки по продвижению работы в качестве не-администратора. Правительство санкционировало Федеральную конфигурацию ядра рабочего стола (FDCC), которая включала большой набор параметров безопасности и требовала, чтобы конечные пользователи не подключались с правами администратора, что соответствовало тому, что я делал. Благодаря этому я узнал много нового о параметрах безопасности и групповой политике, а также разработал инструменты для автоматизации задач, которые не были достаточно освещены ранее. Получается, что приведение хорошо проработанных, испытанных и широко используемых базовых показателей – огромное преимущество для клиентов с точки зрения времени и качества. Если бы у нас их не было, каждый клиент в итоге должен был бы выполнять эту работу самостоятельно, что заняло бы много времени и, вероятно, привело бы к неоптимальным результатам. Легко ошибиться и сделать неправильные предположения».

Я спросил Маргосиса, над чем он работает сейчас, кроме базовых версий и конфигураций безопасности. «Я много работаю над белыми списками приложений, используя технологии AppLocker и Device Guard от Microsoft. Это будет мощная и необходимая для компаний защита от вымогателей и других видов вредоносных программ. Но для частных конечных пользователей реализовать ее будет сложно. На предприятии конечные пользователи не должны принимать решения о доверии, поэтому белый список возможен только в хорошо управляемой организации.

Я вижу сходство в том, что делаю сейчас в управлении приложениями и что делал со стандартными пользователями много лет назад. Обе вещи необходимы для лучшей информационной безопасности, и обе ломают программное обеспечение, потому что предположения, которые делали разработчики, больше неактуальны. Вендоры ПО должны перестать предполагать, что их программы могут хранить данные в каталоге программных файлов, и им придется перестать рассчитывать на то, что они смогут активироваться из профиля пользователя или других каталогов, доступных для записи. В то же время это будет интересная проблема совместимости приложений».

Я спросил, что ему было бы интересно узнать об информационной безопасности более подробно. Он колебался минуту, а затем сказал: «Я хотел бы знать, как убедить людей быстрее принимать правильные решения. Не думаю, что я сам научился делать это так хорошо, как мог бы. Я знаю, что поступаю правильно, но умение убедить людей поможет быстрее усовершенствовать безопасность».

Я думаю, что многие люди, описанные в этой книге, поймут боль Маргосиса.

Информация об Аароне Маргосисе

Более подробную информацию об Аароне Маргосисе вы можете найти по ссылкам:

• *Troubleshooting with the Windows Sysinternals Tools* (2-е издание): **https://www.amazon.com/Troubleshooting-Windows-SysinternalsTools-2nd/dp/0735684448**;

• *Windows Sysinternals Administrator's Reference*: **https://www.amazon.com/Windows-Sysinternals-Administrators-Reference-Margosis/dp/073565672X**;

• блог Аарона Маргосиса о работе не-администратора: **https://blogs.msdn.microsoft.com/Aaron_Margosis**;

• технический блог Аарона Маргосиса на US Government Configuration Baseline (USGCB): **https://blogs.technet.microsoft.com/fdcc**;

• блог Аарона Маргосиса на Microsoft Security Guidance: **https://blogs.technet.microsoft.com/SecGuide**.

33. Сетевые атаки

Во второй главе «Как хакеры взламывают» описывались различные способы, которыми злоумышленники пытаются использовать вычислительное устройство. Это физические нападения, уязвимости нулевого дня, устаревшие программы, социальная инженерия, пароли, проблемы, атака через посредника, утечка данных, DDoS-атаки, ошибки пользователей и вредоносные программы. Все эти атаки могут быть выполнены как на самом вычислительном устройстве, так и в сети, подключенной к вычислительному устройству.

Типы сетевых атак

Сетевые атаки могут произойти в любом месте модели Open Systems Interconnection (OSI) (**https://en.wikipedia.org/wiki/OSI_model**). Модель OSI – широко известная и используемая конструкция, показывающая различные уровни взаимодействия по сети и сетевому вычислительному устройству. У модели OSI есть семь уровней:

• физический;

• канальный;

• сетевой;

• транспортный;

• сеансовый;

• представительский;

• прикладной.

Взлом сети, а также устройств управления сетями может осуществляться на всех уровнях (сетевые устройства так же могут запускать приложения), при этом взлом компьютера в сети также может осуществляться на многих уровнях. Атака на физическом уровне осуществляется путем получения доступа, поломки или кражи сетевого оборудования. Для атак на канальном уровне используются сетевые мосты, коммутаторы, а также протоколы и стандарты этих уровней, например MAC-адрес устройства (**https://en.wikipedia.org/wiki/MAC_address**). Сетевой уровень отвечает за маршрутизацию, транспортный и сеансовый обеспечивают передачу данных на верхние уровни, а прикладной и представительский отвечают за отображение данных на устройстве или в приложении. Если в сетевой среде передачи данных работают несколько пользователей и нет дополнительной защиты, то всегда есть вероятность, что один узел сети может вмешиваться в работу других узлов. В следующих разделах описаны самые популярные виды сетевых атак.

Прослушка

Это несанкционированное прослушивание и/или запись приватного разговора, предназначенные для других целей. Несмотря на то что сейчас это не так успешно, много лет назад вы могли подключить приложение сетевого прослушивания к любой сети и видеть текстовые потоки разговоров и информацию об аутентификации. В Интернете есть множество бесплатных инструментов для захвата текстовых паролей. Есть и другие инструменты, которые позволяют захватывать файлы cookie. В большинстве случаев это не требует специальных знаний, необходимо лишь умение запускать программное обеспечение.

Атаки «через посредника»

Атаки «через посредника» (MitM) также могут быть выполнены на любом уровне модели OSI. Атака MitM врывается в несанкционированный поток связи

и притворяется уполномоченной стороной для всех других уполномоченных сторон. Большую часть времени вовлеченная оригинальная, законная сторона подвергается воздействию и часто выбивается из потока связи. MitM-атаки совершаются по тем же причинам, что и подслушивание, в том числе для просмотра и кражи личных данных. Тем не менее они также могут манипулировать коммуникационным потоком, чтобы изменить данные, например заменить «да» на «нет», когда кто-то задает вопрос или неправильно направляет одну или несколько прослушивающих сторон в несанкционированное место.

Сегодня у многих сетевых протоколов и приложений есть защита от атак MitM, но они не всегда включены по умолчанию, часто из-за проблем производительности или совместимости. Например, открытый стандарт DNSSEC был создан в 2004 году для предотвращения атак подмены DNS, но прошло уже более десяти лет, и менее 1 % DNS-серверов в мире используют его.

DDoS-атаки

Атаки типа «отказа в обслуживании» (DDoS), возможно, наиболее распространенные и легкодоступные атаки в Интернете. Ежедневно в Интернете отправляются терабайты данных для прерывания работы законных сайтов и служб. DDoS-атаки могут атаковать на любом уровне модели OSI.

Защита от сетевых атак

Существует множество средств защиты от сетевых атак, в том числе описанные в следующих разделах.

Изоляция домена

Изоляция домена означает создание безопасной границы между авторизованным и несанкционированным сетевым трафиком. Это можно сделать с помощью различных средств и методов, включая брандмауэры (как сетевые, так и на основе хостов), виртуальные частные сетевые подключения, IPSEC, маршрутизаторы, программно-определяемые сети и другие типы сетей. Если сетевая атака не может добраться до вашего устройства или сети, она, как правило, не сможет им навредить. Есть пограничные случаи, когда, например, DDoS-атака компрометирует зависимость восходящей или нисходящей сети, которая, в свою очередь, влияет на предполагаемую цель в любом случае. Но изоляция домена так или иначе защитит вас по крайней мере от части сетевых атак.

Виртуальные частные сети

Одна из лучших вещей, которую любое устройство может сделать, – это использовать частную сеть (VPN). VPN могут быть выполнены с помощью программного обеспечения, аппаратных средств или комбинации этих способов.

Виртуальные частные сети не идеальны. Например, DDoS-атака может их прервать.

Использование защищенных протоколов и приложений

Ничто не сравнится с безопасным протоколом и приложением, которое включает защиту от известных угроз. Люди должны использовать безопасные протоколы и приложения, если они прилагаются (например, SCP и SSH), и избегать сознательного использования небезопасных протоколов (таких как FTP и Telnet). Кроме того, ни одно приложение не должно хранить текстовые учетные данные на диске или в памяти или передавать их по сети.

Системы обнаружения вторжений

Заражения могут быть обнаружены сетевыми анализаторами (вручную) или автоматически по определенным шаблонам. При обнаружении вредоносности сети ее можно удалить или создать действенное предупреждение. Анализаторы сетевых протоколов – это отличный способ сбора и декодирования сетевых аномалий. Они позволяют осуществлять анализ как вручную, так и автоматически. Многие брандмауэры также содержат функции обнаружения сетевых вторжений.

Защита от DDoS-атак

Вы можете защититься от атак типа «отказа в обслуживании» (DDoS), укрепив сетевое оборудование, выделив больше пропускной способности и используя специализированные службы защиты от DDoS-атак. Существуют десятки анти-DDoS-сервисов, которые могут помочь защитить активы компании от очень крупных DDoS-атак. Единственная проблема в том, что они очень дорогие. К сожалению, есть ряд неэтичных конкурентов, которые сделают все, чтобы получить бизнес-клиента. Если вы планируете использовать службу защиты от DDoS, внимательно проанализируйте предложения, чтобы убедиться, что имеете дело с законной, бесспорно этичной фирмой.

Посещайте безопасные веб-сайты и используйте защищенные сервисы

Многие сетевые атаки, такие как простые кражи файлов cookie с веб-сайта, происходят только потому, что веб-сайт или служба не используют жизненный цикл безопасной разработки (SDL) в своем программировании. Правильно закодированный веб-сайт или служба с соответствующим моделированием угроз и использованием SDL для закрытия известных уязвимостей будут более устойчивы к сетевым атакам, чем те, которые этого не делают.

К сожалению, среднестатистическому пользователю трудно узнать, безопасен ли веб-сайт, который он посещает, или веб-сервис, который использует. Некоторые сайты содержат свидетельства безопасности от известных, надежных вендоров безопасности, и если они проверены как законные, то должны дать случайному пользователю дополнительный уровень комфорта.

Ежедневно кто-то подвергается сетевым атакам, и некоторые из них причинили огромный ущерб своим жертвам. Существует множество средств защиты, которыми могут воспользоваться компании, чтобы снизить риск атаки.

В следующей главе представлен профиль Лауры Чаппелл, одного из лучших в мире специалистов по сетевым анализаторам.

34. Профиль: Лаура Чаппелл

Ученые говорят, что если мы когда-нибудь встретим инопланетную цивилизацию, вероятным языком общения будет математика, потому что это единственный действительно универсальный язык, который, будет понят передовыми цивилизациями. Чтобы разобраться, что происходит с сетевым компьютером, необходимо хорошо изучить сеть. Никто не делает это лучше, чем Лаура Чаппелл. Она напоминает доктора Луизу Бэнкс (роль которой исполнила Эми Адамс) в фильме «Прибытие» 2016 года или доктора Элли Арроуэй (которую играет Джоди Фостер) в фильме «Контакт» 1997 года. Она очень умна, целеустремленна, добилась большого успеха в своей работе и заслужила уважение коллег.

На ее факультативах и презентациях всегда много народу. Я впервые встретил ее более 20 лет назад, когда она преподавала курс по сетевому снифферу в местной ИТ-группе в Вирджинии-Бич, штат Вирджиния. В то время сотрудники-женщины там были редкостью, и Чаппелл привыкла к тому, что парни приставали к ней, пытаясь показать, как много они знают о сетевых пакетах. Она закончила свою вступительную речь в нашей группе, сказав: «Если вы думаете, что произведете на меня впечатление, пытаясь выглядеть альфа-самцом благодаря своим знаниям сетей, не тратьте свое время. Я знаю больше вас». Публике это понравилось. Потом она доказала свою правоту, и мы стали ее фанатами на всю жизнь.

Она использовала большинство анализаторов сетевых пакетов, хотя ее нынешний фаворит – очень популярный Wireshark (**http://www.wireshark.com**), который поставляется как в бесплатной, так и в коммерческой версиях.

Я спросил Чаппелл, как она заинтересовалась анализом сетевых пакетов. Она ответила: «Еще в конце 1980-х и начале 1990-х я работала на Novell (электростанция в сетевых операционных системах в то время). Я была членом Технологического института Novell и работала в команде, которая исследовала, писала и читала лекции по всем горячим сетевым технологиям в то время. Когда Рэй Ноорда, генеральный директор[8] Novell, приобрел компанию Excelan Corporation в 1989 году, мне посчастливилось присутствовать на презентации Excelan LANalyzer. Наблюдая за этим ранним инструментом сетевого анализатора, я зашла на нашу сеть Novell и углубилась в запросы/ответы Novell, всплывающие имена пользователей и пароли… Я по-настоящему заинтересовалась этим и сказала себе (и всем, кто меня слушал): “Я хочу заниматься этим всю оставшуюся жизнь”. Боже… Итак, все эти годы спустя я все еще прослушиваю сетевые коммуникации!»

Я спросил Чаппелл, как она попала в сферу ИБ. «Я впервые вышла на арену сетевой криминалистики совершенно случайно. В 1993 году я основала свою компанию и большую часть времени проводила анализ различных корпоративных сетей. Тогда компании были заинтересованы только в устранении неполадок, оптимизации и планировании мощностей. Они никогда не вызывали меня, чтобы поговорить о “безопасности”. <…> Спустя много лет, однако, я подключилась к инфраструктуре компании, только чтобы найти огромные проблемы безопасности и объявить о них по всей сети. Выполняя заказы своих клиентов, я должна была начать поднимать вопрос безопасности для них. Я видела некоторые пакеты и сообщения, которых просто не должно быть в их сетях. Было довольно много случаев, когда я чувствовала, что плохая производительность сети – наименьшая из забот, ведь их грабили прямо под носом. Стало очевидно, что мне нужно вплести “анализ безопасности” в свои задачи сетевого анализа. Мир сетевой криминалистики вышел на первый план. Вот несколько примеров.

В разгар проведения анализа плохо функционирующей сети клиента я стала свидетелем внезапного потока быстрого трафика, направленного к точке выхода из сети. Он исходил из системы, которая должна была быть относительно тихой в то время, так как никто не был зарегистрирован на этом компьютере. Взглянув на поток трафика поближе, я заметила в нем много знаков долларов и долларовых сумм. После повторного анализа я поняла, что у меня в руках вся выручка компании.

Во время анализа в больнице оказалось, что студенты из крупного университета получают доступ к базе данных рецептов – системе, которая содержит не только имена, адреса и номера социального страхования пациентов, но и полную информацию о различных лекарствах, прописанных им. Эта программа была разработана как сеанс анализа в реальном времени для определения причины медленных процессов входа в систему. Как только подозрительный трафик был обнаружен, все изменилось. Это стало тренировкой по обнаружению вредоносного трафика. А остальное уже история».

Я спросил Чаппелл, что больше всего ее интересует в сфере ИБ. Она сказала: «Это большой вопрос. В сетевой криминалистике так много интересных областей. Две наиболее интересных для меня прямо сейчас: ловить автоматизированные фоновые процессы, поскольку они отправляют конфиденциальную и личную информацию незаметно для пользователей, и учить людей настраивать Wireshark, чтобы быстро обнаружить наиболее распространенные симптомы сетевой разведки и атаки. Проект настройки Wireshark – актуальная для меня тема. Создание профиля Wireshark, который может быстро предупредить эксперта об опасности, – отличная особенность. Обучать людей, как использовать его в качестве инструмента сетевой криминалистики, чрезвычайно интересно».

Я спросил Лауру, в чем, по ее мнению, самая большая проблема в сфере ИБ. «Исходя из точки зрения сетевой судебной экспертизы, я должна сказать, что недостаточно компаний понимают, как интегрировать безопасность в различные отделы организации. Я часто обнаруживаю, что людям, которые устанавливают

программное обеспечение клиентов, не рекомендуется изучать сетевую безопасность – они просто устанавливают его, и все. Они не делают базовую линию трафика к/от недавно отчеканенной системы. Они не понимают, что такое “нормальный” трафик, поэтому не могут обнаружить “ненормальный”. Им, конечно же, не предоставляется доступ к системе IDS для запуска файлов трассировки. Было бы просто великолепно, если бы сотрудники безопасности в компаниях провели внутреннее перекрестное обучение тому, как нарушаются системы и как предотвратить будущие проблемы. Я знаю, что эти люди заняты, но им нужно распространять знания на другие отделы».

Наконец, я узнал, что она порекомендовала бы людям, интересующимся сферой ИБ в качестве карьеры. «Во-первых, изучите Wireshark, конечно! Шучу… хотя, вообще-то, не шучу. Wireshark – идеальный инструмент понимания того, как работает сеть, к тому же он бесплатный! Он занимает первое место в инструментах безопасности sectools.org. Во-вторых, изучайте TCP/IP очень, очень, очень хорошо. Потратьте время, чтобы захватить свой собственный трафик при подключении к веб-серверу, отправлять электронную почту, загрузить файл через FTP, и т. д. Так вы узнаете, как работают протоколы, смотрите протоколы с помощью Wireshark. Наблюдайте за TCP-квитированием, характером запроса/ответа приложений, процессом разрыва соединения и т. д. В-третьих, создайте простую атакующую лабораторию. Вам не понадобятся какие-то особые компьютеры – просто свяжите некоторые из них вместе с коммутатором и воспользуйтесь бесплатными инструментами сканирования/тестирования на проникновение. Захватите и анализируйте трафик при запуске атак на другие системы. Большинство из нас учатся глазами – видеть ход сканирования гораздо интереснее, чем читать об этом. Сетевая безопасность похожа на двустороннюю монету – вам нужно почувствовать, как работают различные атаки, чтобы знать, как защититься от них.

Это всего лишь игра. Игры для решения проблем – отличный способ зарядить свой мозг для сетевого анализа и анализа безопасности».

Лаура Чаппелл – женщина, которая нашла свою нишу в мире сетевых пакетов, стала мировым экспертом и вот уже на протяжении 20 лет по-прежнему остается лучшей в своей области.

Информация о Лауре Чаппелл

Более подробную информацию о Лауре Чаппелл вы можете найти по следующим ссылкам:

• Университет Чаппелл: **https://www.chappellu.com/**;

• профиль Лауры Чаппелл на LinkedIn: **https://www.linkedin.com/in/chappelllaura**;

• Лаура Чаппелл в Twitter: **https://twitter.com/LauraChappell**;

• блог Лауры Чаппелл (датированный, но все еще актуальный материал): **http://laurachappell.blogspot.com/**.

35. Взлом IoT

Мир компьютеров не ограничивается только компьютерами. Это также автомобили, дома, телевизоры, холодильники, тостеры, очки, наручные часы, кроссовки, фары, детские мониторы, медицинские приборы и почти любой другой объект, который, по мнению некоторых производителей, понравится покупателям больше, если в нем есть компьютер или датчик. Большинство этих элементов подключены к Интернету и имеют IP-адрес. Они относятся к интернету вещей (Internet of Things, или IoT). К сожалению, многие, если не большинство IoT-устройств очень небезопасны и могут быть взломаны – некоторые довольно легко.

Как хакеры взламывают IoT?

IoT взламывается так же, как обычные компьютеры. Хакер выбирает одну или несколько уязвимостей на уровнях модели Open Systems Interconnection (OSI) (физический, канал передачи данных, сеть, транспорт, сеанс, презентация и приложение). Единственное отличие состоит в том, что они могут не использовать традиционное оборудование или хорошо известную операционную систему (или оно может вообще не иметь традиционной ОС). Хакеры должны узнать как можно больше об устройстве, исследовать его компоненты и операции, а также искать уязвимости.

Предположим, что хакер хочет проверить, сможет ли он взломать тостер. Первое, что нужно сделать, – это получить его и изучить сопроводительную документацию. Затем он пытается определить, как этот тостер подключается к сети и что по ней отправляет, включив сетевой анализатор и устройство. Вы можете узнать невероятное количество информации об устройстве, изучая, что оно делает или пытается сделать, когда запускается. Они могут сканировать порты, искать прослушиваемые порты и пытаться вычислить, какая операционная система и службы работают. Если есть консоль администратора, они пытаются подключиться к ней. Они могут выяснить, на каком языке был написан код устройства, и ищут интерфейсы прикладного программирования (API).

Физический взлом – также распространенный метод взлома подобных устройств. Хакеры разбирают устройство на части и видят, из чего оно состоит, отмечая отдельные чипы и их номера. Большинство устройств используют общие чипы, а они часто хорошо документированы. Иногда уязвимости чипа хорошо известны и могут быть аналогичным образом использованы на различных устройствах. Хакеры пересекают провода, присоединяются к чиповым контактам и даже создают собственные чипы, чтобы обойти блокировщиков аутентификации и контроля доступа к устройству. Они уделяют особое внимание поиску портов ввода и вывода и выясняют, можно ли подключить к устройству отладчик.

Они используют атаки «посредника» (MitM), чтобы попытаться увидеть передаваемую информацию то, и могут ли они ее изменить. Они часто

обмениваются информацией, делятся ею на соответствующих форумах. Они даже создают виртуальные группы, посвященные конкретному устройству, обобщающие опыт различных хакеров. Вот несколько примеров общедоступных IoT-хаков, интересных к прочтению:

• **https://blog.avast.com/2015/11/11/the-anatomy-of-an-iot-hack/**;

• **https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-BabyMonitor-Exposures-and-Vulnerabilities.pdf**;

• **https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/**;

• **http://resources.infosecinstitute.com/hardware-hacking-iot-devices-offensive-iot-exploitation/**.

В общем, если вы можете проникнуть на обычные компьютеры, то сможете и на IoT-устройства; однако иногда проникновение туда может оказаться сложнее, если вы незнакомы с их программным обеспечением или чипами. С другой стороны, это может быть легче, потому что большинство IoT-вендоров не понимают риска и не выделяют достаточное количество ресурсов на их защиту, по крайней мере, на данный момент.

Защита IoT-устройств

Похоже, люди не работают над улучшением безопасности IoT-устройств. Большинство вендоров думают, что они уделяют ей достаточно внимания. Работают десятки независимых групп, таких как IoT Village (**https://www.iotvillage.org/**), чтобы помочь им лучше защитить свои устройства. К сожалению, на хакерских форумах, таких как San Francisco IOT Hacking Meetup (**https://www.meetup.com/San-Francisco-IOT-hacking-Meetup/**), активно и успешно обдумывают атаки. Когда IoT-вендор утверждает, что его устройство безопасно, он, вероятно, сильно ошибается.

Так что же может сделать IoT-вендор, чтобы лучше защитить свою продукцию? Относитесь к этому так, как будто имеете дело с обычным компьютером. Убедитесь, что программирование включает в себя вопросы жизненного цикла безопасности (SDL). Вы должны быть уверены, что устройство использует самое современное ПО с новейшими патчами, и не забывать самостоятельно обновлять его. Удалите ненужное программное обеспечение, службы и сценарии. Закройте все лишние порты. Используйте хорошую криптографию надежным способом. Обеспечьте конфиденциальность клиентов. Не собирайте информацию, которая вам не нужна. Надежно храните информацию о клиентах, которая может пригодиться. Требуется строгая проверка на проникновение во время создания и бета-тестирования продукта. Предлагайте награды за ошибки. Не наказывайте хакеров за сообщения о них. Проще говоря, изучите все уроки информационной безопасности, извлеченные в мире компьютеров за несколько десятилетий, и примените их к устройствам IoT.

К сожалению, большинство IoT-вендоров этого не делают, и мы, вероятно, обречены еще десятилетия терпеть атаки на IoT-устройства.

Следующая глава рассказывает о Чарли Миллере, который считается одним из лучших в мире автомобильных хакеров.

36. Профиль: доктор Чарли Миллер

Большинство людей, знакомых с именем доктора Чарли Миллера и его работой, знают о нем как о члене хакерского дуэта, который может полностью дистанционно управлять вашим автомобилем, подобно детской игрушке. Если вы видели новостной репортаж о хакерах, удаленно заставляющих автомобиль внезапно ускориться или даже съехать с дороги, знайте, в этом участвовал доктор Миллер. Автор журнала *Wired* описал свой опыт общения (**https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway**) с доктором Миллером и его партнером Крисом Валасеком.

Миллер и Валасек написали подробный технический документ под названием *Adventures in Automotive Networks and Control Units* (**http://illmatics.com/car_hacking.pdf**), который описывает, сколько компонентов автомобиля – критических и некритических – можно контролировать, включая аварийный тормоз, кондиционер, индикаторные лампы, трансмиссию, развлекательные системы, тормоза и даже рулевое управление. Для многих из нас этот документ был самым глубоким анализом того, как работает и взаимодействует сеть компьютерных систем автомобиля. В более поздних итерациях они выяснили, как сделать это удаленно. Это был взлом автомобиля! Они даже выпустили собственные инструменты, чтобы упростить взлом для других.

Идея о том, что хакеры могут дистанционно управлять вашим автомобилем, не была сильно шокирующей, но, увидев, как два парня делают это со своего ноутбука на расстоянии 10 миль, люди осознали появление новой серьезной угрозы. Доктору Миллеру не нужно было активно продвигать идею о том, что эти методы в неправильных руках могут быть использованы для создания несчастных и смертельных случаев. До публичного разоблачения, сделанного доктором Миллером, компании не сильно беспокоились о безопасности автомобилей, которые выпускали (безопасность через безвестность была самой большой защитой). Исследования Миллера и Валасека это изменили. Производители автомобилей начали обращать внимание на негативную рекламу и стали относиться к информационной безопасности автомобиля более серьезно. Ходили даже слухи, что крупные компании могут подать в суд на тестировщиков, чтобы помешать дополнительным исследованиям и открытиям.

Когда я беседовал с доктором Миллером, он заверил меня, что на него и других, с кем он работал, никогда не подавали в суд, и даже не угрожали: «На любого можно подать в суд, но мы были очень профессиональны. Это честь и для них, и для нас. Они попросили не показывать некоторые детали в одной из наших будущих презентаций, но мы все равно это сделали, и никто не обратился в суд». Это не значит, что автомобильным компаниям понравилось то, что он

делал. Несмотря на то, что доктор Миллер проводит одни из лучших публичных исследований в области взлома автомобилей, его никогда не приглашали рассказать о своих выводах. И однажды во время конференции, когда он попросил автомобильные компании о большей прозрачности в будущем, чтобы помочь автомобильным хакерам найти и искоренить больше ошибок, ответом был отказ. По причинам, которые, к сожалению, имеют тенденцию повторяться снова и снова в разных отраслях, те самые компании, которые могли бы извлечь максимальную выгоду из этих исследований, просто видели в них раздражителей, если не прямых врагов. К счастью, времена изменились, и доктор Миллер работает на Uber. Компания считает, что он поможет лучше защитить будущие автономные беспилотные автомобили.

Я впервые встретил доктора Миллера почти десять лет назад, когда он пытался стать высокооплачиваемым профессиональным искателем ошибок. Он получил степень бакалавра математики в Северо-Восточном университете штата Миссури (ныне Университет штата Трумэн) и докторскую степень по математике в Университете Нотр-Дам. Вы можете встретить доктора Миллера на прогулке в солнцезащитных очках в стиле Элтона Джона, а при знакомстве он непременно пошутит и будет забавно жестикулировать. Если вы думали о том, как может выглядеть профессионал по угону автомобилей, кандидат наук, вы вряд ли представляли себе Чарли Миллера.

До своей нынешней работы он пять лет трудился в Агентстве национальной безопасности (**https://www.nsa.gov/**), три года в компании Twitter, а еще несколько лет в консалтинговых и других фирмах. Опыт доктора Миллера и любовь к математике заставили его заинтересоваться криптографией, а сочетание этих двух факторов сделало его интересным для АНБ. Для тех, кто не знает, АНБ – ведущее агентство США по шифрованию/дешифрованию, а возможно, даже и мировой лидер в этой области. Залы АНБ полны самых ярких криптографов, и доктор Миллер оказался среди них.

Я спросил Чарли, как он стал многопрофильным специалистом в сфере ИБ и профессиональным автомобильным хакером, и вот что он сказал: «До АНБ я никогда не думал, что смогу этим заниматься [информационной безопасностью]. Я ее не изучал. АНБ наняло меня криптографом, и я думал, что это моя специальность. Предполагается, что в АНБ вы будете каждые полгода переезжать в разные офисы (т. е. отделы), чтобы ознакомиться с широким спектром технологий, которые интересуют АНБ. Они думали, что я выберу разные темы, но я пошел на хитрость, чтобы они обучили меня только информационной безопасности, а не криптографии. Другие темы ИБ казались намного интереснее, чем криптографические. Я обманывал своих руководителей, думая, что каждый офис – это совершенно новая тема, но вместо этого они были сосредоточены на нескольких более узких сферах ИБ. Через три года я столкнулся со многими классными штуками. Мне повезло, что я оказался в месте, где должен был учиться и получать за это деньги».

Я спросил доктора Миллера, как он заинтересовался взломом машин. Он сказал: «Я долгое время взламывал телефоны и компьютеры. Но демонстрация этого не вызывала никакого беспокойства зрителей. Однако, когда рулевое колесо и

тормоз стали работать сами по себе, люди заволновались. Это был хак, который мне не пришлось рекламировать или продавать. Он продвигал сам себя и был доступен обычным людям. Мы не были первыми, кто взламывал машины. Мы построили свою работу на том, что обнаружили наши предшественники, чтобы использовать пределы того, куда это может нас привести».

На раннем этапе карьеры доктор Миллер сделал себе имя, выиграв не один хакерский конкурс Pwn2Own всего за несколько минут. Pwn2Own (**https://en.wikipedia.org/wiki/Pwn2Own**) – это конференция в Ванкувере, Канада. Его целью было предоставление денежных средств и других призов всем, кто мог взломать различные операционные системы и программное обеспечение, ошибки которых ранее не были публично известны. Каждый успешно продемонстрированный хак был новым «нулевым днем», который вожделен в хакерском мире и больше всего беспокоит вендоров.

На протяжении нескольких лет самым ярким событием конкурса Pwn2Own было участие доктора Миллера, который в течение менее чем нескольких минут использовал свои навыки, чтобы уйти с одним или несколькими крупными призами. Он делал это столько раз, что в конце концов конкурс стал известен как мероприятие, где каждый продукт будет взломан в течение пары минут после того, как доктор Миллер примется за работу. Несколько лет имя доктора Миллера было синонимом взлома автомобилей. Именно из-за его успеха во взломе некоторых из самых популярных операционных систем, браузеров и устройств люди обратили больше внимания, когда он начал говорить о взломе автомобилей. Его репутация опережала его. Не было сомнений, что он понимает, о чем говорит, и добьется успеха.

Секрет раннего успешного взлома доктора Миллера был связан с фаззингом. Существует множество способов поиска программных ошибок. Вы можете вручную испытать программное обеспечение путем анализа всей деятельности и вручную изменять входные сигналы для того, чтобы увидеть, к чему это приведет. Вы можете статически анализировать код, используя для проверки исходного кода ПО (или вручную просматривая его), которое ищет предопределенные ошибки кодирования. Или вы можете случайно наткнуться на ошибку при использовании программы в обычном режиме. На протяжении десятилетий эти три традиционных метода были способом обнаружения наиболее эксплуатируемых ошибок.

В конце 1990-х фаззинг стал невероятным источником ошибок, и любая программа разработчика программного обеспечения была обречена на несколько уязвимостей нулевого дня, если разработчики не тестировали собственные программы, прежде чем выпустить их. При тестировании другая программа (фаззер) автоматизирует процесс введения всех видов различных входных данных, обычно не ожидаемых программистом или языком программирования (например, очень длинных, содержащих случайные управляющие символы, «зарезервированные слова кодирования» и т. д.), в активную версию целевой программы, чтобы вызвать ошибку. Каждая найденная ошибка после этого проверяется программой фазз-испытания или вручную человеком, для того чтобы увидеть, можно ли использовать условие

ошибки для того, чтобы эксплуатировать программу или основную операционную систему.

Вот как Доктор Миллер описывает свои успехи в фаззинге: «Я узнал о фаззинге в АНБ. Он понравился мне, потому что находил ошибки быстро и очень легко. Я запускал программу, шел смотреть телевизор, потом засыпал, просыпался и смотрел на результаты. Примерно в 2010 году на конференции Blackhat (**http://blackhat.com/**) я использовал фаззинг на сцене против некоторых конкурентов, чтобы найти ошибки. Они при этом использовали статический анализатор. Мне потребовалось несколько минут, чтобы фаззинг сработал, а через час я выиграл».

Примечание. Если вы заинтересованы в использовании программного обеспечения для фаззинга, доступно множество бесплатных и коммерческих продуктов. Microsoft предлагает достойный фаззинг бесплатно по адресу: **https://www.microsoft.com/en-us/springfield/**.

Я спросил доктора Миллера, почему его первые исследования были направлены в основном на продукты Apple. Он сказал: «Тогда у Apple было немного средств информационной безопасности, особенно защиты памяти в коде. И они не проводили собственные тесты. Я сделал это для них и нашел много ошибок, которые мог бы использовать в Pwn2Own. Microsoft и Microsoft Windows провели тестовый фаззинг, и их программы теперь имеют встроенную защиту памяти. Я не был нацелен на Apple, просто их ошибки было очень легко найти, а мне нравится легкий взлом».

В 2007 году он стал человеком, удаленно взломавшим iPhone и телефон на платформе Android в тот же день, когда он вышел (в 2008 году). Позже в этом году доктор Миллер нашел уязвимость нулевого дня в браузере Safari MacBook Air и выиграл 10 000 долларов. В 2009 и 2010 годах он снова взломал браузер Safari от Apple и продолжил успешно взламывать iPhone. В 2011 году он обнаружил дыры в безопасности iOS на iPad и iPhone. По сути, он показал, как приложение Apple может злонамеренно украсть информацию или иным образом взломать владельцев устройств Apple. Он создал демонстрационную программу, которую разместил в Apple App Store.

Работа доктора Миллера по поиску ошибок вызвала у Apple гнев. Они обвинили его в нарушении условий соглашения с разработчиком (что, в сущности, было правдой) и отняли у него право разрабатывать и публиковать их ПО. Он рассказал мне об этом инциденте: «Они сказали, что забирают мой ID разработчика Apple на год. Когда я подал заявку на восстановление, его не вернули. У меня до сих пор нет ID разработчика Apple». Многие люди, наблюдавшие за этим, полагали, что Apple усвоила печальный урок и примет доктора Миллера обратно.

Когда я впервые встретил Чарли, он отчаянно пытался получить хорошо оплачиваемую работу, связанную с поиском ошибок. В то время очень немногие люди зарабатывали на жизнь таким образом. Большинство людей, как доктор

Миллер, вообще не получали зарплату. Было очень мало программ Bug bounty, предлагаемых вендорами публично, как сегодня. Единственные, кто получал большие деньги за новые уязвимости нулевого дня, были злонамеренные хакеры, часто спонсируемые плохими парнями и преступными группами. Иногда хакер «в белой шляпе» мог продать найденные ошибки законным компаниям, а затем перепродать их по самой высокой цене вендорам, чтобы они могли изучить ошибку и исправить ее. Это продолжается и сегодня.

Но доктор Миллер пытался попасть в Apple, Microsoft или другую компанию, где его энтузиазм и опыт были бы оценены по достоинству. По большей части этого не произошло, по крайней мере так, как он изначально надеялся. Но в итоге он получил работу в Twitter и Uber. Попутно Чарли выдвинул на первый план необходимость в том, чтобы профессиональные искатели ошибок получали возмещение за свои усилия. Он был если не ведущим инициатором, то как минимум очень важной частью этого процесса. Он даже начал кампанию «больше никаких бесплатных патчей». Сегодня почти у каждого крупного разработчика ПО есть платная программа для поиска ошибок, и хорошие искатели ошибок могут найти постоянную, хорошо оплачиваемую, законную работу.

Я спросил доктора Миллера о разочаровании тех дней, когда ему приходилось выполнять работу консультанта, вместо того чтобы найти постоянную работу, соответствующую его опыту и таланту. Он рассказал: «В итоге я стал консультантом-путешественником, а это неплохо для начала карьеры. Это помогает узнать множество компаний, их деятельность и культуру. Мне заплатили за поиск ошибки только один раз, в 2007 году. Это была ошибка, которую я нашел за пределами Pwn2Own. Я быстро обнаружил, что мне нравится выступать на конференциях даже больше, чем получать деньги. Для меня было важнее говорить об этом, делиться с людьми, чем молча зарабатывать».

Если вы посещали какие-либо из его презентаций или конференций, то знаете, что доктор Миллер любит веселить, развлекать и обучать аудиторию. Он сказал мне: «Как только я нахожу где-нибудь пять ошибок, то теряю интерес и двигаюсь дальше». Попутно он обнаружил другие уязвимости безопасности в таких областях, как Near Field Communication (NFC). Он также опубликовал три книги (**https://www.amazon.com/Charlie-Miller/e/B0085NZ1PS/**), которые охватывают взлом Mac, iOS и фаззинг.

Я закончил свое интервью с доктором Миллером последним вопросом: думает ли он, что автомобили станут достаточно безопасными в ближайшее время? Он ответил: «Автомобили ничем не отличаются от компьютеров, а мы до сих пор не знаем, как их полностью защитить. Автомобили больше похожи на атакуемые сети, поскольку содержат много компьютеров. Дело автомобилей – это особые вопросы физической безопасности. Ставки высоки. Я не могу уберечь вас от столкновений, но могу смягчить удары многими способами. Вы можете возиться с развлекательной системой, но, если мы сделаем все правильно, вам не придется разбираться с тормозами и другими крайне важными системами».

Верный своим ранним скрытным корням в АНБ, он не сказал мне, над чем работает в Uber, но я думаю, что компания и ее пользователи окажутся только в плюсе.

Информация о Чарли Миллере

Более подробную информацию о докторе Чарли Миллере вы можете найти на следующих ресурсах:

• доктор Чарли Миллер в Twitter: **https://twitter.com/0xcharlie**;

• книги доктора Чарли Миллера: **https://www.amazon.com/CharlieMiller/e/B0085NZ1PS/**;

• доклад *Adventures in Automotive Networks and Control Units*: **http://illmatics.com/car_hacking.pdf**;

• доклад *Car Hacking: For Poories*: **http://illmatics.com/car_hacking_poories.pdf**;

• доклад *A Survey of Remote Automotive Attack Surfaces*: **http://illmatics.com/remote%20attack%20surfaces.pdf**;

• доклад *Remote Exploitation of an Unaltered Passenger Vehicle*: **http://illmatics.com/Remote%2 °Car%20Hacking.pdf**;

• доклад *CAN Message Injection*: **http://illmatics.com/can%2message%20injection.pdf**.

37. Политики и стратегия

Я был тем, кто ненавидел политику и стратегию. Мне не нужны были документы. Они лишь замедляют работу. По крайней мере, я так думал.

Спустя десятилетия работы в качестве специалиста по ИБ я, наконец, понял, что без соответствующей политики и рамок ничего никогда не будет сделано. Любой может прекрасно обезопасить небольшое количество компьютеров и устройств. Но вы не сможете защитить больше, чем несколько персональных устройств, и, конечно, компьютеры всей компании, без «правильных» документов. Я изучал стандарты, политику, процедуры, рамки и тех, кто трудится, чтобы правильно определить их. Они действительно настоящие закулисные герои, и без них мы не смогли бы сделать компьютеры значительно более безопасными.

В этой главе я разбиваю документы, касающиеся информационной безопасности, на стандарты, политику, процедуры, рамки и законы.

Примечание. Вы также увидите часто используемые термины «рекомендации» и «практика», но я включил их черты в другие термины, представленные здесь.

Стандарты

Стандарты описаны минимальными нормами, конвенциями, протоколами и требованиями. В мире информационной безопасности стандарты часто передаются в виде утверждений, таких как:

• все критические данные будут зашифрованы во время передачи и хранения;

• минимальные размеры ключа открытого шифра – это 2048 битов для RSA и Diffie-Hellman и 384 бита для ECC;

• пароли должны быть длиной не менее двенадцати символов и содержать не менее двух неалфавитных символов;

• после введения трех неверных паролей в течение пяти минут учетная запись будет заблокирована до тех пор, пока ее не проверит администратор;

• все критические патчи должны быть применены в течение пяти рабочих дней после выпуска вендором;

• все компьютеры должны быть защищены брандмауэром на основе хоста с правилами запрета для входящих подключений.

Стандарт часто представляется в виде политики и далее поддерживается процедурами.

Иногда стандарты становятся правилами, законами или требованиями, которым должно следовать каждое управляемое устройство. В Соединенных Штатах один из крупнейших стандартов, которому должны следовать десятки миллионов компьютеров, – это Базовый уровень конфигурации правительства Соединенных Штатов (**https://usgcb.nist.gov/**). Стандарты также могут быть разработаны вендором, например базовые показатели Microsoft Security Compliance Manager (**https://technet.microsoft.com/en-us/library/cc677002.aspx**). Иногда стандарты становятся настолько уважаемыми и надежными, что превращаются в национальные или мировые. Отличный тому пример – почти все, что производит Национальный институт стандартов и технологий (**https://www.nist.gov/**). И многие компании тратят большое количество денег и ресурсов, пытаясь получить сертификат соответствия стандартам ISO/IEC 27001 (**http://www.iso.org/iso/home/standards/managementstandards/iso27001.htm**).

Политики

Политика подразумевает принципы принятия решений для достижения намеченных результатов. Часто это могут быть письменные объявления, которые не могут быть легко применены другими средствами. Пример: сотрудники не должны повторно использовать свой пароль в любой другой сети. Хотя компания не может гарантировать, что этого никогда не произойдет, просто написав и сообщив об этом сотрудникам, уменьшается вероятность того, что произойдет нарушение. Кроме того, если нарушение все же будет обнаружено, оно может легко привести к наказанию.

Процедуры

Процедуры – это документированная последовательность шагов, предназначенных для поддержки стандартов и политики, связанных с развертыванием и операциями. Соблюдение процедур обеспечит своевременное и удовлетворительное применение этих ранее заявленных стандартов и политики. Процедуры могут изменяться независимо от политики и стандартов, например если для новой программы требуются другие процедуры.

Фреймворки

Создание стандартов и политики для всего спектра аспектов информационной безопасности с нуля может быть очень сложным. Рамки помогают в этом, демонстрируя обычно поддерживаемые стандарты, политику, форматы и набор инклюзивных тем. Отличный пример рамочной кибербезопасности – NIST's Cybersecurity Framework (**https://www.nist.gov/cyberframework**).

Нормативные законы

Стандарты и политика могут быть кодифицированы в правовые нормы и законы. Например, компании, желающие обрабатывать многие распространенные типы кредитных карт, должны следовать стандартам, предусмотренным стандартом безопасности данных Совета по стандартам безопасности индустрии платежных карт (**https://www.pcisecuritystandards.org/**). Их несоблюдение может привести к приостановке использования кредитных карт или даже юридическим последствиям. Связанные со здравоохранением организации в Соединенных Штатах должны следовать рекомендациям закона о переносимости и подотчетности медицинского страхования (HIPAA). Все компании США должны следовать требованиям закона Сарбейнза-Оксли и так далее.

Глобальные проблемы

А для многонациональных компаний каждая страна может иметь собственный, иногда противоречивый, набор стандартов и политик. Некоторые страны высоко ценят личную жизнь, в то время как другие могут юридически не требовать гарантированной личной жизни. Одна страна может потребовать, чтобы компьютерные системы, популярные в другой стране, использовали меньшие стандарты (например, законы США о криптоэкспорте). Глобальные компании имеют экспоненциально больше вопросов соблюдения, о которых следует беспокоиться.

Поддержка систем

Многие компании сталкиваются с многочисленными, подчас противоречащими друг другу требованиями. Попытка соблюдать единый стандарт может быть очень трудной. По этой причине была создана целая система компаний и

инструментов для оказания помощи другим, пытающимся соблюдать один или несколько стандартов или правил. Компании, как правило, имеют отдельные команды и сотрудников, дорогое программное обеспечение и внимание генерального директора. Попытка своевременно соответствовать всем стандартам требует работы специального персонала, всей ИТ-команды и каждого сотрудника, работающего для достижения общих целей соответствия. Соответствие стандартам – это большой бизнес. Последствия несоблюдения могут привести к проблемам, судебным разбирательствам и использованию хакерами известных слабых мест.

Если вы прочитаете эту главу и захотите повернуть время вспять, потому что ваше внимание было усыплено, знайте, что я тоже через это прошел. Потребовались десятилетия, чтобы увидеть, как мои невероятно технические, требовательные рекомендации неправильно применяются и игнорируются, а без этого невозможно понять важность разработки политики и документации. Без документов соответствия не может быть настоящей информационной безопасности. Все просто.

Следующая глава посвящена Цзин де Йонг-Чен, чья работа сосредоточена на улучшении международных стандартов безопасности и глобального киберуправления.

38. Профиль: Цзин де Йонг-Чен

Как мы говорили в предыдущей главе, без правильных политики и стратегии невозможно обеспечить реальную долгосрочную безопасность компьютера. Некоторые из «невидимых» героев информационной безопасности – это люди, которые управляют корпоративными глобальными стратегиями информационной безопасности. Цзин де Йонг-Чен, партнер и CEO программы Глобальной стратегии безопасности отдела по корпоративным, внешним и правовым вопросам в Microsoft, посвятила свою жизнь продвижению лучших и более глобальных стандартов ИБ и гармонизации киберполитики. Также она вице-президент Trusted Computing Group (TCG), некоммерческой международной организации по отраслевым стандартам, специализирующейся на инновациях в области технологий безопасности. Она советник Исполнительного женского форума – организации, занимающейся продвижением женщин в сферах безопасности, конфиденциальности и управления рисками. Кроме того, де Йонг-Чен выступает в качестве советника по проекту Digital Futures Центра Вудро Вильсона, который отстаивает лидерство в области технологий для формирования государственной политики. В 2014 году она получила награду «Влиятельные женщины» от Форума исполнительных женщин за вклад в кибербезопасность. У Цзин есть степень магистра делового администрирования и степень бакалавра компьютерных наук.

Одна из вещей, которые я заметил сразу же, когда впервые брал у нее интервью, заключалась в том, насколько продуманными и полными были ее ответы. Она провела десятилетия, успешно борясь за улучшение глобальной

государственной политики и стандартов, и об этом говорят ее опыт и знания. Длительность ее опыта уникальна как для женщины, так и для азиатского профессионала, что она с готовностью признает, поскольку активно продвигает большее разнообразие инструментов в области ИБ.

Я спросил, как она впервые занялась информационной безопасностью. Она ответила: «Я начала работать в Microsoft в 1992 году, в частности, в области исследований и разработок для решения проблем производства азиатских версий Windows 3.1. В то время не было китайской версии Windows, а Китай стоял на пути к углублению своей экономической реформы и становлению важной частью мировой экономики. Мы успешно создали первые японские, корейские и китайские версии Windows 3.1, поддерживающие двухбайтовые символы. Для достижения нашего видения демократизации вычислений с компьютером на каждом столе и в каждом доме наши программы должны быть разработаны для пользователей во всем мире. Основываясь на проблемах, с которыми пришлось столкнуться при разработке Windows 3.1, мы поняли, что должны изменить наши способы создания программного обеспечения. Мы разработали подход, чтобы иметь единую кодовую базу и включить стандарт Unicode и отдельные ресурсы (языковые компоненты) из исходного кода.

Мы заметно опережали многие компании, когда выпустили по всему миру версию Windows 95 на многих языках. Мы отправили ее упрощенную версию на китайском языке в течение шести месяцев после выпуска в США. Это было большим достижением, учитывая локализацию. Чтобы выполнить это в соответствии со стандартом национального языка, мы включили 25 000 китайских упрощенных и традиционных характеристик. Как вы знаете, Китай гордится тем, что является родиной печатного станка, но до появления коммерческих операционных систем, таких как Windows 95, книгопечатание по-прежнему требовало ручного труда. С профессором Ваном Сюаньом, одним из основателей Founder Group (китайской компании информационных технологий), мы работали над усовершенствованием и популяризацией системы. Это было началом вступления Китая в эпоху электронных публикаций после тысячелетнего ручного труда. Это продемонстрировало ценность вычислений для значительного повышения производительности человека. Я получила от этого невероятное удовольствие.

Затем, в 1998 году, примерно в начале революции электронной коммерции, Microsoft начала проникать в интернет-пространство. Я стала частью нашего подразделения онлайн-сервисов, а невозможно быть частью интернет-сервисов и программного обеспечения без участия в безопасности. В течение нескольких лет мы сталкивались с довольно большими проблемами, так как хакеры начали использовать вирусы и вредоносные программы, чтобы испортить жизнь нашим клиентам и компаниям, например червь Code Red и SQL Slammer. Все в Microsoft пытались выяснить, как создать более безопасное и надежное ПО. В то же время последствия террористического акта 11 сентября показали, что отрасли, которые были более подготовлены к стихийным бедствиям, такие как финансовые услуги, восстанавливались быстрее. Некоторые уроки, извлеченные из предыдущих проектов по обеспечению готовности к 2000 году, для этих

компаний окупились. Я увидела, куда движется безопасность, и присоединилась к отделу передовой политики и стратегии Microsoft под руководством Крейга Манди. Я стала частью недавно сформированной компании Trustworthy Computing Group во главе со Скоттом Чарни, которая сосредоточилась на безопасности, конфиденциальности, надежности и целостности бизнеса. Мне очень повезло учиться у опытных лидеров в области кибербезопасности.

Я помню, что во время этих атак рынки таких стран, как Корея и Япония, сильно пострадали, потому что были ранними последователями нашей технологии и Интернета. Пострадали миллионы пользователей. Правительства были обеспокоены. Microsoft пришлось реагировать очень быстро. Я посвятила все свое время вопросам информационной безопасности и сотрудничеству с правительством. Я начала проводить информационно-разъяснительную работу и находить пути содействия созданию государственно-частных партнерств для минимизации рисков и комплексного решения проблем безопасности. Мы смогли поделиться своим опытом и разработать решения для оказания поддержки правительственным и промышленным партнерам в создании потенциала технического реагирования. Например, многие полицейские управления в разных странах не имели киберотдела и использовали устаревшие системы. Поскольку увеличилось количество киберпреступлений, правоохранительным органам требовалось больше экспертов, которые могли бы грамотно отреагировать на инциденты и провести судебный анализ. Корпорация Microsoft поддержала эти усилия, предоставив необходимую техническую поддержку, в том числе в таких регионах, как Юго-Восточная Азия.

Моя работа очень динамичная, и мне повезло работать с замечательными коллегами и учеными, которые многому меня научили. Microsoft стала чемпионом в области технологий и стратегии кибербезопасности. Мы начали с того, что заглянули внутрь и вовне и начали работать с партнерами. В некоторых странах в то время не было принято, чтобы конкуренты работали вместе, но мы считали, что кибербезопасность важнее, чем коммерческая конкуренция. Мы поделились конфиденциальной информацией о безопасности с вендорами антивирусного ПО и разработали государственную программу безопасности для поддержки усилий в области кибербезопасности как в развитых, так и в развивающихся странах. В конце концов я начала работать над техническими решениями безопасности в 2008 году и с тех пор продолжаю участвовать в Trusted Computing Group, где мне довелось работать со многими талантливыми людьми».

Мне было интересно, с какими проблемами она сталкивается в качестве вице-президента Trusted Computing Group. Она привела пример: «Вы знаете о микросхеме доверенного платформенного модуля (TPM) TCG, которая помогает защитить компьютеры от атак аппаратного уровня. Версия 1.2 доверенного платформенного модуля работала отлично, но ей не хватало гибкости, чтобы разрабатывать алгоритмы исправления, когда появлялись слабые места. В то же время страны начали настаивать на использовании собственных алгоритмов в своих продуктах безопасности. Доверенный платформенный модуль 1.2 не

может удовлетворить это требование, поскольку поддерживает только ограниченный набор алгоритмов.

Существовал риск конкуренции со стороны правительств на уровне стандартов до начала глобального принятия. Если страны пойдут по пути разработки несовместимых стандартов только из-за использования алгоритмов, общие преимущества безопасности для пользователей будут сокращены. С точки зрения принятия это, безусловно, вызов совместимости между микросхемами безопасности, которые основаны на международном стандарте, и микросхемами с локальным стандартом. TCG начала решать эту проблему "крипто-гибкости", среди прочих улучшений, с новой спецификацией TPM 2.0. При участии многих экспертов в области безопасности из разных стран стандарт TPM 2.0 был утвержден как ISO/IEC 11889:2015. Теперь это единый глобальный стандарт. Это было невероятно, поскольку требовало консенсуса между многими странами, включая США, Китай, Россию, Японию, Францию, Южную Африку, Малайзию и другие. Нам удалось сделать нечто особенное. Новый стандарт предлагает гораздо более широкую защиту не только для пользователей настольных ПК, но для облака и IoT-устройств».

Мне было ясно, что работа де Йонг-Чен несколько десятилетий назад в области глобализации Windows 95 окупилась, когда она помогала разрабатывать глобальные вычислительные стандарты. Я спросил, что, по ее мнению, является самым большим препятствием для значительного улучшения глобальной информационной безопасности. Она ответила: «Страны имеют очень разные системы убеждений, что нужно учитывать при продвижении международных стандартов безопасности. Есть вопросы, связанные с политикой и технологией. Естественно, технические специалисты хотят создать лучшую технологию, но это только часть задачи. Есть вопросы системы и киберуправления. Каждая страна беспокоится о защите своего киберсуверенитета, конкурируя за создание более сильного киберпотенциала. Вы не можете просто обратиться к технологии в одиночку или оставить кибербезопасность в руках политиков. Вы должны искать лучшее разрешение и требования к балансу через весь спектр забот. Это становится довольно сложной матрицей вещей, которые должны учитывать политики и лидеры отрасли, прежде чем принимать меры. Сюда входят: безопасность и конфиденциальность пользователей Интернета, защита критически важной инфраструктуры, социальная и экономическая стабильность, а также Глобальные коммуникации и торговля. По мере того как все больше стран выпускают все больше правил безопасности, стоимость предприятий, занимающихся бизнесом, будет расти. Любое соответствие включает в себя управление политическими последствиями, правовыми рисками, изменениями технического дизайна, а также изменениями бизнес- и операционной моделей. Есть проблемы и возможности, но вы не можете решить крупные, общие проблемы кибербезопасности, не понимая, как работают страны и как все взаимосвязано. Если мы сделаем все правильно, то, возможно, сможем достичь равновесия, необходимого для улучшения кибербезопасности и защиты глобальной кибернетической инфраструктуры, обеспечивая конфиденциальность пользователей, поддерживая справедливую конкуренцию

и постепенно снижая стоимость ведения бизнеса в поддержку глобальной торговли».

Я спросил об отсутствии женщин в ИТ-сфере. Де Йонг-Чен ответила: «В области ИТ в целом нечасто встретишь женщин, но еще реже они появляются в области ИБ. Я работала в большой интернет-компании, где активно нанимали женщин и видели в них потенциал своего роста. Несмотря на то что 54 % рабочей силы этой компании составляли женщины, я этого не понимала, когда общалась с их службой безопасности. Там была только одна женщина, и то не специалист по безопасности. Мы могли бы сделать эту отрасль лучше. Необходимо увеличить кадровый резерв в области кибербезопасности, а также найти пути привлечения и удержания женщин в сфере ИТ и поощрения разнообразия в области ИБ. Для этого нам нужна всеобщая поддержка».

Информация о Цзин де Йонг-Чен

Более подробную информацию о Цзин де Йонг-Чен вы можете найти по ссылкам:

• блог в Microsoft Цзин де Йонг-Чен: **http://blogs.microsoft.com/microsoftsecure/author/jingdejongchen/**;

• профиль Цзин де Йонг-Чен на LinkedIn: **https://www.linkedin.com/vsearch/p?orig=SEO_SN&firstName=Jing&lastName=Jong-Chen&trk=SEO_SN**;

• *Governments Recognize the Importance of TPM 2.0 through ISO Adoption* (пост в блоге Microsoft Secure): **http://blogs.microsoft.com/microsoftsecure/2015/06/29/governments-recognize-theimportance-of-tpm-2-0-through-iso-adoption/**;

• *U.S.-China Cybersecurity Relations: Understanding China's Current Environment* (Georgetown Journal of International Affairs): **http://journal.georgetown.edu/u-s-china-cybersecurity-relationsunderstanding-chinas-current-environment/**;

• *Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization* (Georgetown Journal of International Affairs): **http://journal.georgetown.edu/data-sovereignty-cybersecurity-andchallenges-for-globalization/**.

39. Моделирование угроз

Моделирование угроз – это процесс рассмотрения всех существенных и потенциальных угроз, ранжирования их возможного ущерба за определенный период времени и определения экономически эффективных способов их устранения с высокой степенью приоритетности. Моделирование угроз используется во всех отраслях промышленности и в нашем конкретном случае при планировании защиты. Оно используется в жизненном цикле безопасной

разработки (SDL) при программировании и проверке ПО, а также на всех компьютерных устройствах и в инфраструктуре. Только с помощью моделирования угроз специалист по ИБ может количественно оценить угрозы, риски и способы их устранения, а также сравнить реализованный план с реальностью происходящего.

Зачем нужно моделирование угроз?

Моделирование угроз снижает риск. По крайней мере, позволяет рассмотреть различные угрозы и риски. С его помощью можно сопоставлять многочисленные угрозы, разрабатывать и оценивать меры по смягчению их последствий и, как мы надеемся, осуществлять эффективные с точки зрения затрат и пользы меры по смягчению последствий. Мы точно знаем, что в долгосрочной перспективе ПО, запрограммированное с учетом моделирования угроз, имеет меньше ошибок и уязвимостей, чем ПО, которое не моделирует угрозы. Если в программном обеспечении впервые моделируется угроза, разработчики моделей могут обнаружить больше ошибок и уязвимостей, чем в предыдущем периоде, и их увеличение может продолжаться в течение некоторого периода, но в итоге количество вновь обнаруженных ошибок и уязвимостей должно снизиться. В конце концов, за время существования проекта или продукта общее количество ошибок и возможный ущерб, который они могут создать, должны быть уменьшены. В противном случае зачем его выполнять?

Моделирование угроз даже учитывает, достаточно ли смягчение экономически эффективно. Возможно, очень хорошее смягчение может быть настолько дорогостоящим (по стоимости, ресурсам, проблемам производительности и т. д.), что даже если оно компенсирует определенный риск, это экономически неэффективно. Например, предположим, что компьютерные вирусы ежегодно наносят компании ущерб в размере 100 000 долларов. Она не захочет тратить более 100 000 долларов на то, чтобы остановить компьютерные вирусы. Поэтому, вероятно, им будет выгоднее не использовать никаких средств защиты. Это хоть и глупый, зато наглядный пример.

Виды моделирования угроз

Существует почти столько же видов моделирования угроз, сколько и типов угроз. Обычно они известны под акронимами, такими как STRIDE, PASTA, VAST, TRIKE и OCTAVE. Есть много программных средств, которые имеют собственные модели или основываются на одной из существующих моделей. У каждой модели есть поклонники и критики. Для разработчиков и вендоров информационной безопасности гораздо важнее использовать любую модель угроз, чем не использовать ее, поскольку они не могут определить, какой из них отдать предпочтение. Простое моделирование угроз – это уже победа.

Каждая модель пытается охватить процессы понимания того, что представляет собой рассматриваемый проект в его совокупности. Обычно это делается с помощью мозгового штурма, блок-схем и подробного описания вовлеченных процессов. Затем рассматриваются все потенциальные угрозы проекту,

программе или сервису. Они ранжируются по вероятности потенциального ущерба. В первую очередь рассматриваются угрозы и риски, которые могут причинить наибольший ущерб. Затем разрабатываются и оцениваются меры по снижению рисков с точки зрения пригодности и экономической эффективности для каждой конкретной угрозы.

Все модели должны начинаться с концепции того, какой объем остаточного риска владелец готов или способен принять после применения всех согласованных мер по снижению риска. Например, моделирование угрозы наступательного или оборонительного военного оружия начинается с идеи о том, что существует очень мало приемлемого остаточного риска. Одна компания может позволить некоторому риску остаться, в то время как другая со строгими ограничениями ресурсов вынуждена сознательно принять многие крупные неразрешенные риски. Моделирование угроз помогает пользователям подготовиться к остаточному риску. Некоторые модели угроз даже напоминают пользователям, что не все риски когда-либо будут продуманы и смягчены.

Злоумышленники

Каждая модель должна также учитывать типы хакеров, которые могут атаковать ее. Существует большое количество злоумышленников, и у всех разная мотивация.

Государства

Большинство промышленно развитых стран теперь имеют команды ярких, способных и обеспеченных ресурсами хакеров, покорно и патриотически занимающихся взломом от имени правительства страны или военных. Они нападают на другие страны и ставят под угрозу их стратегии и цели, которые считаются необходимыми для успеха их страны. Кибервойна – огромная составляющая этого типа угрозы. Кибервойна пытается нанести вред способности противника вести войну или установить хорошую защиту, используя профессиональных хакеров и вредоносные программы. Отличный пример – червь Stuxnet, который уничтожил ядерное оборудование другой страны. Иные виды угроз могут приходить и уходить, но атаки на национальные государства будут всегда.

Промышленный шпионаж

Это хакеры, которые сосредоточиваются на краже секретов и интеллектуальной собственности других компаний, чтобы перепродать их или помочь другой компании или отрасли несправедливо конкурировать. Этот тип угрозы может атаковать от лица конкурирующей компании, от имени национального государства или независимо, как фрилансер.

Примечание. Как государства, так и промышленные хакеры известны как Advanced Persistent Threats (APTs). Это человеческие противники, которые

профессионально взламывают в рамках долгосрочных согласованных усилий против целевых противников. Они, как правило, имеют огромные ресурсы и легко добиваются успеха.

Финансовая преступность

Киберзлоумышленники представлены дистрибьютерами, отказом исполнителей услуг, производителями рекламы и хакерами, которые воруют электронные деньги, данные для аутентификации или совершают кражи. Деньги мотивировали преступников и до создания компьютеров, но нынешнее состояние информационной безопасности позволяет красть большие суммы легче и с гораздо меньшим риском, чем традиционные преступления, не связанные с компьютерами.

Хактивисты (хакеры-активисты)

Политически, морально и психологически мотивированные люди часто любят наносить ущерб финансам, репутации или ресурсам компаний и организаций, с которыми не согласны. Некоторые из крупнейших и наиболее разрушительных атак в истории были связаны с хактивистами.

Геймеры

Компьютерные игры и геймеры заставляют разработчиков программного и аппаратного обеспечения расширять технологические и эксплуатационные ограничения больше, чем любая другая группа. Сегодня люди не только платят, чтобы играть в игры, они платят и чтобы смотреть, как это делают другие. Геймеры заполняют концертные залы так же быстро, как вчерашние рок-звезды. Иногда кажется, что половина телевизионной рекламы во время самых популярных событий (таких как Суперкубок) – это реклама компьютерных игр. Сказать, что компьютерные игры очень популярны, – ничего не сказать. Некоторые хакеры существуют исключительно для того, чтобы их взламывать для увеличения своего выигрыша (что бы это ни значило), создания конкурентных преимуществ и нанесения вреда игровым сервисам, с которыми не согласны.

Инсайдеры

На повестке дня всегда стоял вопрос, насколько велика угроза, которую законные сотрудники представляют для компании, но ясно, что они составляют немалый процент всех атакующих. Некоторые инсайдеры крадут данные и иную интеллектуальную собственность, чтобы продать конкурентам или получить новую работу. Другие крадут деньги или информации, например кредитные карты клиентов (для личной финансовой выгоды). Инсайдеров, совершающих несанкционированные действия, очень трудно обнаружить и остановить, особенно при проведении операций с использованием законных полномочий. Это угроза, с которой индустрия ИБ все еще борется.

Обычные хакеры-одиночки или хакерские группы

Не будем забывать о традиционных хакерах, которые взламывают для собственных индивидуальных потребностей, будь то финансовая выгода или желание доказать, что они на это способны. Десять или более лет назад эта группа скомпрометировала почти все взломы. Хакерский мир не был заполнен профессиональными преступниками. Большинство довольствовались тем, что просто писали компьютерный вирус, который печатал забавную поговорку на компьютере или запускал игру Yankee Doodle Dandy в заданное время. Некоторые из них нанесли реальный ущерб, такие как загрузочный вирус Микеланджело, который отформатировал жесткие диски. Но большинство из них были просто чьим-то тщеславным проектом, способом сказать, что они достаточно умны, чтобы сделать это. Они не хотели причинить реальный, повсеместный вред.

Моделирование угроз – это то, что должны делать разработчики и каждый специалист по ИБ. Оно эффективно снижает риск путем ранжирования угроз на основе ущерба, который они могут причинить. Если у вас нет модели угроз, вы просто гадаете и блуждаете в чаще информационной безопасности.

Следующая глава посвящена профилю Адама Шостака, уважаемого специалиста по моделированию угроз.

40. Профиль: Адам Шостак

Одна из моих первых встреч с Адамом случилась в Microsoft, когда он изобретал новый способ решения проблемы. В данном случае речь шла о том, как победить червя Conficker (**https://en.wikipedia.org/wiki/Conficker**). Conficker был особенно неприятной вредоносной программой, которая появилась в конце 2008 года. У нее было несколько способов распространения (таких как «векторы»), включая взлом слабо защищенных паролем файловых ресурсов, исправление уязвимостей программного обеспечения, а также через USB-накопители с помощью встроенной функции автозапуска Windows. Conficker заражал миллионы машин в год и не проявлял никаких признаков ослабления. Вендоры антивирусных программ легко обнаруживали его, и Microsoft выпустила несколько статей о том, как остановить ее распространение, но она все равно делала свое дело.

Шостак предложил для изучения проблемы использовать анализ данных. Он совместно с Microsoft начал смотреть, какие векторы атаки позволяют Conficker распространяться больше всего. Первоначальное предположение состояло в том, что большинство пользователей инфицированных компьютеров не применяли доступный патч. И это действительно было одним из самых популярных векторов на раннем этапе. Но теперь, почти два года спустя, Шостак узнал, что в значительной степени это происходило из-за зараженных USB-ключей. Используя данные, которые собрал сам, он предложил Microsoft отключить функцию автозапуска, что было гениальным решением. Это означало изменение способа работы Windows, и Адам собирался заставить всех

пользователей совершать дополнительные действия для запуска файлов со съемных носителей. Автозапуска больше не было. Microsoft выдвинула обновление, которое отключило эту функцию. Так умер Conficker. Точнее, не совсем умер, но перестал быть огромной проблемой. С тех пор распространение вредоносных программ через USB-ключи перестало быть проблемой в целом.

Подход Шостака и Microsoft к использованию данных для управления безопасностью оказал на меня огромное влияние. Благодаря этому я написал то, что считаю самой важной своей работой, – *Implementing a Data-Driven Computer Security Defense* (**https://gallery.technet.microsoft.com/Fixing-the-1Problem-in-2e58ac4a**), которая с тех пор была рекомендована для чтения многими отраслевыми светилами и группами.

Позже я прочитал книгу Шостака *Threat Modeling: Designing for Security* (**https://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998**). Было ясно, что он действительно понимает моделирование угроз и ошибки в других моделях и реализациях. Это по-прежнему одна из лучших книг, которые я рекомендую людям, заинтересованным в моделировании угроз. Шостак работал в Microsoft, помогая с несколькими проектами, вроде отключения автозапуска, чтобы остановить вредоносные программы, такие как червь Conficker, инструмент моделирования угроз SDL (**https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx**) и повышение привилегий моделирования угрозы (**https://www.microsoft.com/en-us/sdl/adopt/eop.aspx**). Он стал соучредителем Симпозиума по технологиям повышения конфиденциальности и Международной ассоциации финансовой криптографии. Кроме того, он хороший писатель, блогер и спикер.

Я спросил Адама о приходе в сферу ИБ. Он рассказал: «Я работал системным администратором в медицинской исследовательской лаборатории, и безопасность была частью моих обязанностей. Это было в 1993–1994 годах. Я начал читать несколько ранних рассылок в Интернете, например про оригинальные брандмауэры и рассылки киберпанков. Среди них были разные интересные люди, которые говорили любопытные вещи. Я начал участвовать в этом и узнал, что могу внести свой вклад в обсуждение. Моя следующая работа была больше ориентирована на безопасность. Я стал консультантом в Бостоне. Это случилось в то время, когда произошел взлет Интернета. Таким образом, знания в области безопасности и возможность внести свой вклад в развитие интернет-безопасности действительно помогли. Я смог найти недостатки в нескольких продуктах, и это повысило мою репутацию».

Я попросил его рассказать об этом подробнее. «Я нашел уязвимость в ключе. Это был предшественник RSA Secure ID, прежде чем он был куплен RSA. Недостаток был в том, что информация из предыдущего сообщения использовалась для защиты следующего, что делало ключ, который связывал их, предсказуемым и легко подделываемым».

Я спросил, как он занялся общими уязвимостями и воздействием (CVE), словарем общеизвестных уязвимостей и воздействий информационной безопасности. Он ответил: «Одним из моих клиентов была компания Fidelity

Investments. Их код безопасности был таким, как в Microsoft 15 лет назад. Я все еще принимал активное участие в составлении интернет-рассылок, делился идеями и получал обратную связь. Я всегда буду благодарен, что руководители позволили мне это сделать, потому что не все начальники и компании разрешают своим сотрудникам использовать такой тип обмена информацией. В Fidelity я столкнулся с венчурным капиталистом, который владел частью компании по сканированию уязвимостей, и подумал, что это интересно, поэтому перешел туда. Мы были очень конкурентоспособны с тем, сколько уязвимостей могли обнаружить. Я работал над новой уязвимостью fingerd и не мог сказать, обнаружил ли один из продуктов нашего конкурента ту же уязвимость или нечто другое. В то время информация об уязвимостях была недоступна, как и поисковые системы. Найти информацию было не так легко, как сегодня. Я начал задаваться вопросом, как можно поговорить с другими пользователями ПО о том, какие уязвимости мы нашли или упустили, и эти размышления привели меня к мысли о том, как общаться с системными администраторами, чтобы они могли идентифицировать различные уязвимости и выяснить, исправили их или нет. Нам нужна была система, помогающая объединять разные типы людей, чтобы говорить об одних и тех же вещах на одном языке и понимать друг друга. Решением стал CVE».

Я спросил Шостака, чем он, в частности, способствовал моделированию угроз. Он немного поколебался, а затем ответил: «Я слушал людей, которые говорили мне, что что-то не работает. Некоторые пытаются объяснить, почему это не работает, но я считаю, что такие неполадки нужно менять. Например, если кто-то открывает электронное письмо и постоянно заражается, даже если вы просите не открывать ненадежные послания, проблема заключается в системе, а не в пользователе. Мы должны разработать системы, которые учитывают то, что делают люди, потому что они делают это правильно. Я читаю о системах безопасности самолетов, потому что в этой сфере, в отличие от ИБ, подробно анализируют неудачи. Даже если все, что у них есть, это инцидент с близким промахом, есть форма, которую любой пилот может заполнить и отправить в главный офис. Там их собирают и изучают. Управление может увидеть распространенные ошибки, даже если сначала те выглядят как человеческие оплошности. Они могут отправить рекомендацию производителю радио и рассказать, как исправить проблему, добавив, например, освещение, или поведать конкретному аэропорту (или группе аэропортов), как избежать проблемы с освещением взлетно-посадочной полосы. Это безупречный анализ первопричин. Поле ИБ не анализирует причины так же хорошо, поэтому мы в итоге повторяем одни и те же ошибки снова и снова, и для разработки лучших систем требуется больше времени».

Я закончил интервью, спросив, что бы он порекомендовал молодым специалистам в области ИБ. Он ответил: «Две вещи. Во-первых, я думаю, что студенты могут извлечь выгоду путем изучения гуманитарных дисциплин (психологии, философии и др.). В начале карьеры я изучал науку об окружающей среде. Я узнал, что на проблемы экологии влияют политические, правовые и экономические проблемы, и, если их не решить, невозможно помочь экологии. То же самое с ИБ. Конечно, есть технические вопросы, но вы должны

понимать политические, юридические и экономические аспекты, если хотите решить технический вопрос. Это не просто проблема с брандмауэром. Кроме того, научитесь писать. Во-вторых, приобретаемые вами технологические навыки не так важны, как умение думать. Технологические проблемы, с которыми я столкнулся, когда впервые вошел в это поле, даже не близки к современным. Мир ИТ постоянно меняется. Но подход, который я использую, остается прежним. Я стараюсь смотреть на крупные проблемы и спрашивать себя, почему они возникают. Я хочу найти проблему с широким диапазоном, но сузить фокус достаточно, чтобы ее решить. Вы не можете сразу справиться с крупными проблемами. Читатели должны выбрать правильные проблемы, значимые для них, задать правильные вопросы, а затем найти рычаги, которые могут использовать, чтобы повлиять на них».

Информация об Адаме Шостаке

Более подробную информацию об Адаме Шостаке смотрите по ссылкам:

• *Threat Modeling: Designing for Security*: **https://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998**;

• *The New School of Information Security* (в соавторстве с Эндрю Стюартом): **https://www.amazon.com/New-School-Information-Security/dp/0321814908**;

• веб-сайт Адама Шостака: **https://adam.shostack.org/**;

• Адам Шостак в Twitter: **http://twitter.com/adamshostack**;

• профиль Адама Шостака на LinkedIn: **http://www.linkedin.com/in/shostack/**.

41. Обучение информационной безопасности

Один совет, который дал почти каждый человек, о котором мы говорили, – это необходимость более качественного образования в области ИБ. Нет никакой уверенности в том, что некое совершенное технологическое решение, которое исключит необходимость рассказывать людям об угрозах ИБ и о том, как с ними обращаться, вскоре будет найдено. Некоторые «эксперты» по ИБ утверждают, что это пустая трата времени – пытаться обучить конечных пользователей, но большинство серьезных специалистов по безопасности знают, что образование для конечных пользователей и сотрудников принесет только пользу.

Мой нынешний работодатель, Microsoft, заставляет всех сотрудников проходить ежегодное обучение информационной безопасности по нескольким темам. Например, в течение года мы получали много электронной почты фишинга, и в конце нам показали обучающее видео с участием уважаемого сотрудника, обманутого таким способом. Он работал в области, которая требует обширных

знаний в сфере ИБ. Короче говоря, ему стоило быть более внимательным к социальной инженерии с помощью фишинговой электронной почты, но случилось то, что случилось. Он поделился своим опытом, в том числе тем, как попался на хорошо продуманную, целенаправленную попытку фишинга. Было интересно видеть, что один из наших технологических лидеров тоже совершает ошибки и рассказывает, как это произошло. Затем он рассказал, что, хотя и был смущен этой ситуацией, не стыдился сообщить об инциденте ради безопасности других. Это было чрезвычайно хорошо продуманное образовательное видео, которое привело к значительно меньшему количеству успешных фишинговых атак. Обучение оказалось настолько успешным, что к командам Microsoft IT security весь год приходили люди, чтобы узнать, не являются ли подозрительно выглядящие, но законные письма фишинговыми. Некоторые даже говорили, что этот случай был слишком показательным.

Другие образовательные видео в предыдущие годы охватывали тему получения паролей путем обмана. Образование может помочь значительно снизить угрозы информационной безопасности.

Темы обучения в сфере ИБ

Обучение в сфере ИБ поставляется во многих вариантах и подходах. В следующих разделах рассматриваются некоторые темы, которыми могут воспользоваться люди, заинтересованные в обучении в сфере ИБ.

Осведомленность в вопросах безопасности конечных пользователей (Security Awareness)

Этот тип обучения обычно готовит конечных пользователей к более безопасному использованию своих компьютеров и устройств. Специалист делится общими формами взлома, которым устройства могут подвергаться, и рассказывает, как обнаруживать и предотвращать атаки, а также сообщать о них. Каждый пользователь должен пройти такой курс, будь то дома, в школе или в офисе. Тренинг должен проводиться не реже одного раза в год и охватывать недавние и наиболее вероятные угрозы. Такого рода обучение обычно требует от 15 минут до нескольких часов в год.

Общие вопросы информационной безопасности

Полезно для специалистов в сфере ИБ и ИТ. Курс должен содержать общий обзор всех типов взлома и вредоносных программ и более подробно описывать самые распространенные и вероятные угрозы. Как правило, этот тип обучения проходит в течение многих дней или недель и может повторяться через какое-то время.

Реагирование на инциденты

Специалисты в сфере ИБ и, в частности, члены групп реагирования на инциденты должны быть обучены тому, как правильно реагировать на инциденты и управлять ими. Это должно быть обязательным обучением для

всех сотрудников, которые разделяют эти обязанности. Такого рода тренировки обычно длятся несколько дней и должны повторяться по мере необходимости.

Тренинги, специфичные для операционных систем и приложений

Многие популярные вендоры ОС и приложений предлагают общее и специфичное для продукта обучение безопасности. Обучение по конкретным продуктам может дополнить ваши общие знания в области безопасности, а если в конце выдается сертификат, он может подтвердить знания о конкретном продукте.

Технические навыки

Необходимо научить (и аттестовать) людей обеспечивать техническую безопасность. Это включает в себя обучение навыкам работы с определенными типами продуктов безопасности, такими как брандмауэры, обнаружение вторжений, анализ вредоносных программ, криптография, применение патчей, резервное копирование и т. д.

Сертификация

Существуют десятки сертификатов, связанных с информационной безопасностью. Каждая сертификация способствует общему образованию. Нет правильных или неправильных сертификатов. Тем не менее есть более уважаемые, чем другие. В целом любые сертификаты от следующих организаций широко популярны (в произвольном порядке):

• Международный совет по электронному коммерческому консультированию (EC–Council) (**https://www.eccouncil.org/**);

• Институт системных администраторов систем безопасности (SANS) (**http://www.sans.org**);

• Ассоциация вычислительных технологий промышленности (CompTIA) (**https://certification.comptia.org/**);

• Ассоциация информационных систем аудита и контроля (ISACA) (**https://www.isaca.org**).

Уважаемые сертификаты также предлагают компании Microsoft, Cisco и RedHat. Это не исчерпывающий список, и существует много других вендоров, которые предлагают отличные экзамены и курсы.

Дополнительные сведения смотрите в моей недавней колонке в *InfoWorld* по сертификации ИБ: **http://www.infoworld.com/article/3115344/security/essential-certifications-for-smart-security-pros.html**.

Методы обучения

Существуют десятки способов обучения. Рассмотрим некоторые из них.

Онлайн-обучение

Едва ли вы найдете тесты, сертификаты или темы, которые не сможете освоить с помощью онлайн-обучения. Онлайн-обучение может происходить посредством видео или при помощи комплекса, куда входят тексты, видео, обзоры глав и тестирование компетентности. На многих обучающих платформах есть онлайн-учителя, которым можно задать вопросы. Некоторые предпочитают личных преподавателей в реальном классе, но онлайн-обучение может дать вам почти такой же опыт, как правило, за гораздо более низкую цену.

Взлом сайтов

Существует масса сайтов по обучению безопасности, которые в первую очередь позволяют юридически законно проникнуть на их веб-сайт. Это отличный способ обучения и позволяет начинающему хакеру испытать острые ощущения от взлома чего-то без последствий. Один из моих любимых сайтов такого типа – **https://www.hackthissite.org/**.

Учебные заведения

Сегодня не так много крупных университетов, колледжей или официальных учебных заведений, где нет учебной программы по информационной безопасности. Хотя это, как правило, дороже, чем другие специальности, всё равно нужно убедиться, что вам будут предложены не пустые разговоры (дипломные заводы, которые на самом деле не готовят вас к хорошей работе). Хорошие образовательные организации часто могут дать очень подробное и всестороннее образование в области безопасности. Многие специалисты в сфере ИБ начинают в технических школах или местных колледжах, а затем в итоге прогрессируют до полных четырехлетних степеней университета или даже дальше.

Тренировочные лагеря

Лагеря boot camps – это места, которые предлагают ускоренную подготовку, обычно ориентированную на получение конкретной сертификации. Например, двухнедельный учебный лагерь может помочь вам получить те же сертификаты, которые вы могли бы получить в технической школе после обучения от одного до двух лет. Я люблю лагеря и в течение двух лет даже преподавал в некоторых. Посещая учебный лагерь, вы должны быть готовы к интенсивной учебе и освоению большого объема информации за короткий период. Для многих людей с насыщенной жизнью учебные лагеря – лучшая альтернатива. Просто убедитесь, что ваш boot camp предлагает гарантии возврата денег или несколько тестов при сертификации.

Корпоративное обучение

Как описано в разделе «Темы обучения в сфере ИБ» этой главы, многие организации предлагают и даже требуют обязательного обучения в сфере ИБ. Крупные компании предлагают частичные или полные программы возмещения

расходов на обучение и проводят групповые встречи с сотрудниками по конкретным темам безопасности. Сотрудники считают корпоративные образовательные льготы одним из лучших преимуществ работы в конкретной компании.

Книги

Конечно, глава об образовании не будет полной, если не упомянуть, что книги – отличный способ узнать о какой-либо теме в комфортном темпе и в любом месте. Книги, посвященные компьютерам, как правило, более инклюзивны по своей теме, предлагают обширные введения в новый материал и профессионально редактируются в области технических деталей и грамматики.

Непрерывное соответствующее образование необходимо как конечным пользователям, так и ИТ-персоналу и экспертам по ИБ. Одна из самых распространенных тем, о которой я узнал из интервью со всеми людьми, представленными в этой книге, заключается в том, что большинство из них не перестают учиться, и некоторые даже ежедневно выделяют определенное количество времени на изучение чего-то нового. Берите с них пример!

42. Профиль: Стивен Норткат

Я знаю Стивена почти 20 лет. Он не только жизненно важная часть невероятной организации, занимающейся обучением в сфере ИБ, Института системного администратора, сетей и безопасности (SANS), но и незаменимый человек, если вы пытаетесь отыскать специалиста в конкретной области. Я не вспомню, сколько раз за свою писательскую карьеру обращался к Норткату, когда испытывал сложности с поиском кого-то. Иногда кажется, что он не только знаком со всеми, но и всех удивляет.

Норткат – очень общительный, дружелюбный и при этом рассудительный человек. У него потрясающие идеи, и он умеет уговорить других осуществить их.

Некоторым людям присуща та особая харизма, которая притягивает остальных. Стивен как раз из таких, и я уверен, что именно поэтому SANS привлек его на раннем этапе, когда был еще маленькой организацией. Норткат также был ранним инвестором некоторых из самых прибыльных ИБ-компаний нашего времени, включая Tenable (**http://www.tenable.com**) и Sourcefire.

Институт SANS (**http://www.sans.org**) существует с 1989 года и с самого начала предлагал одни из лучших курсов в сфере ИБ. Их сертификаты стали цениться на уровне университетов. Они предлагают две магистерские программы (в области ИБ [MSISE] и управления информационной безопасностью [MSISM]) и три постбакалаврские программы (тестировщик на проникновение и этичность взлома, реагирование на происшествия и техническую кибербезопасность). Они обучили более 100 000 человек, ставших впоследствии одними из самых востребованных преподавателей, многие из которых публикуют книги-бестселлеры. Если вы, будучи работодателем, столкнетесь с тем, у кого есть

подобный сертификат, знайте, ваш работник – один из лучших. На мой взгляд, их онлайн-колонка (**https://www.sans.org/newsletters/**) обязательна к прочтению всем специалистами в области ИБ, а Internet Storm Center зачастую первым замечает новые угрозы.

Несмотря на то что мы знакомы с Норткатом почти два десятилетия, я никогда не спрашивал его о том, как он очутился в сфере ИБ, поэтому поинтересовался теперь. Он рассказал: «Я был сетевым проектировщиком в лаборатории BMC, работающей на станции Sun. Я ничего не знал об информационной безопасности. Однажды кто-то начал взламывать мой компьютер, и я вышел из себя. Сигнал шел из Австралии и компилировал на компьютере программу. Я не знал, что делать, поэтому выдернул шнур из розетки. Таков был мой ответ. Потом я почувствовал себя оскорбленным. Я начал изучать информационную безопасность и в конце концов получил финансирование. В то время, если у вас была хорошая идея, его было легко получить. Я много узнал об информационной безопасности и в конце концов получил второе место после Фреда Керби. [Фред Керби был менеджером по контролю информации, уже более 16 лет он работает инструктором SANS.]

Так я занялся обнаружением вторжений. Я написал теневую систему обнаружения вторжений, которая была очень хороша для своего времени. Я создал группу по обнаружению вторжений, и в итоге мы наблюдали за более чем 30 военными базами. [В итоге Стивен стал экспертом по информационной войне в организации противоракетной обороны.] Я совершил большую ошибку, согласившись на работу в Пентагоне. Моя работа состояла в том, чтобы ходить на собрания и подписывать бумаги, и я занимался этим в течение всего 1999 года».

Хотя Норткат не был одним из соучредителей SANS (ими были Мишель Гелл, доктор Юджин Шульц, Алан Паллер и доктор Мэтт Бишоп), он часто встречался с Аланом. Я спросил, как он связался с SANS. Стивен сказал: «Я был вовлечен в специальный проект в Пентагоне вокруг предприятия Y2K и опасался, что хакеры будут его использовать. Я создал отличную команду, включающую лучших технических аналитиков в мире, и это было здорово. Но мне не нравилось, что управление очень зависело от политики. Алан [Паллер] взял на себя ответственность за политические вопросы, в то время как я сосредоточился на технических. Я посещал и читал лекции на большой конференции SANS по обнаружению вторжений в декабре 1999 года и помню, что это понравилось мне гораздо больше, чем политика. Поэтому я отправился в свой офис в Пентагоне, собрал все вещи в чемодан и больше не возвращался.

Официально я начал работать в SANS 5 января 2000 года. В то время у них было только две встречи: весенняя и осенняя. Каждое мероприятие длилось четыре дня. Перед основной конференцией проводилось несколько учебных занятий, основная конференция длилась два дня, а за ней следовал еще день обучения. Было здорово, но я помню, как сказал Алану: “У нас слишком много всего, чтобы уместить это в двух мероприятиях в год”. Так их количество начало увеличиваться».

Я посещал некоторые ранние занятия SANS, без которых невозможно получить сертификат. Помню, что каждый из курсов был лучшим в своей области и остается таковым до сих пор. Помню, кто их вел и чему я научился. Я даже взял курс по инструментам обнаружения вторжений от его создателя Мартина Роеша еще в 1998 или 1999 году. Когда я сказал Норткату об этом, он ответил: «Помню, как Марти подошел ко мне – этот молодой парень – и сказал: “Я создал инструмент обнаружения вторжений, и он лучше, чем ваш [Shadow]”, и оказался прав. В итоге я стал одним из первых инвесторов в его коммерческое предприятие».

Sourcefire был настолько успешным, что позже его купил Cisco. Я спросил Нортката, когда появилась идея перехода от обучения к сертификации. Он сказал: «Это была идея Алана. Она заключалась в том, что компании хотят убедиться, не зря ли тратят деньги на обучение персонала, а сертификация – лучшее тому подтверждение. Я вспомнил об этом, когда еще работал в лаборатории BMC, и послал несколько человек на конференцию Unix LISA. Я и сам туда пришел, но не смог их найти. В конце концов, обнаружил ребят на байдарках в океане. Так я понял ценность сертификатов.

Идея сертификации появилась еще раньше. Алан пришел ко мне в лабораторию BMC в 1998 году и попросил классифицировать все работы в сфере ИБ. Их было немного: идентификаторы, брандмауэры, обнаружение вредоносных программ и парочка других. Поэтому, когда мы начали говорить о сертификации, оба думали, что образование и курсы, основанные на конкретных задачах, – лучший вариант. В конце концов мы сделали более целостную сертификацию Giac Security Essentials (GSEC), которая похожа на нашу версию CISSP. GSEC не очень технически сфокусирован. Он шириной в милю и глубиной в два дюйма. Но мы решили, что должны подготовить людей к безопасности в целом, прежде чем они начнут выполнять задачи, связанные с доменами, полные командных строк».

Когда мы закончили интервью, я вспомнил одну из наших первых встреч. У Нортката была отличная идея, он хотел побегать со мной около своего дома на Гавайях. Я сказал, что ближайшую неделю буду дописывать свою первую книгу (*Malicious Mobile Code* [**https://www.amazon.com/MaliciousMobile-Code-Protection-Windows/dp/156592682X**]). Я уже и так выбивался из всех сроков и должен был наконец отправить ее издателю. Но Стивен был настойчив. Помню наш разговор, как будто это было на днях. Он сказал: «Вы с женой любите подводное плавание, верно? Мой сосед со своим другом ныряют на Гавайях, и я возьму вас на погружение». Я еще раз поблагодарил, но сказал, что не успею. Тогда он решил зайти с другой стороны: «Как зовут вашу жену и какой у нее номер? Я озвучу ей свое предложение». Номер я ему не дал, на Гавайи не полетел, зато наконец закончил свою первую книгу. Но по сей день я жалею, что не принял его предложение. Вот он какой: даже те его предложения, которые вы отвергаете, запоминаются навсегда.

Информация о Стивене Норткате

Более подробную информацию о Стивене Норткате смотрите по ссылкам:

• профиль Стивена Нортката на LinkedIn: **https://www.linkedin.com/in/stephenraynorthcutt**;

• Стивен Норткат на SANS: **https://www.sans.org/instructors/stephen-northcutt**;

• *Network Intrusion Detection* (в соавторстве с Джоди Новаком): **https://www.amazon.com/Network-Intrusion-Detection-Stephen-Northcutt/dp/0735712654**.

43. Конфиденциальность

Многие люди, включая автора этой книги, считают, что право на личную жизнь, особенно в цифровую эпоху, должно быть гарантированным и неотъемлемым правом всех людей. К сожалению, большая часть нашей цифровой и финансовой конфиденциальности давно ушла. Интернет-поисковые системы, интернет-рекламодатели и вендоры программного обеспечения часто знают о вас больше, чем кто-либо другой, кроме вас самих, разумеется. Несколько лет назад разъяренный родитель пришел в Target, потому что отдел маркетинга магазина отправлял незапрошенную рекламу детских товаров его дочери-подростку. В конце концов отцу пришлось извиниться, когда он узнал, что магазин знает больше о его дочери, чем он сам (**http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-a-teen-girl-was-pregnant-before-her-fatherdid/#d84bcce34c62**).

В большинстве стран и, конечно, в Интернете ваша конфиденциальность исчезла. Ничто нельзя назвать действительно личным. Даже ультраконфиденциальные приложения, такие как Tor и darknet, которые утверждают, что предоставляют лучшую конфиденциальность, на самом деле недостаточно хорошо работают. Не верите? Спросите арестованных преступников, которые думали, что Tor или их служба анонимности обеспечивает абсолютную конфиденциальность. Есть много способов увеличить конфиденциальность, но пока отслеживание вас и вашей деятельности законно, компании и правоохранительные органы будут это делать.

Это не означает, что некоторые правительства и компании не пытаются дать людям разумный уровень конфиденциальности. Например, недавно принятое общее положение Европейского союза о защите данных (**https://en.wikipedia.org/wiki/General_Data_Protection_Regulation**) может накладывать штраф до 4 % доходов фирмы за нарушение закона. В большинстве стран существуют те или иные официальные правила (или свод правил), призванные защищать личные данные граждан.

К сожалению, большинство законов и правил – это усилия, которые появляются скорее для защиты правительства и предприятий, собирающих персональные данные, чем для защиты частной жизни граждан. И многие страны, особенно в

Азиатском регионе, прямо отвергают любое регулирование, которое помешало бы правительству осуществлять оптовый мониторинг граждан. В культурном отношении большая часть населения зачастую принимает его без жалоб. Оно отказывается от своей конфиденциальности ради предполагаемой безопасности.

Тем не менее нарушение законов о конфиденциальности страны может быть очень дорогим для нарушителей. Правительственные ведомства и целые правительства были признаны виновными в нарушении действующих законов о конфиденциальности (хотя они почти никогда не наказываются). Бизнесу, с другой стороны, гораздо проще попасть в неприятности. Все чаще корпорации имеют подразделения конфиденциальности и даже кого-то на уровне «С», чья работа заключается в защите конфиденциальности клиентов.

Организации, курирующие вопросы конфиденциальности

К счастью для мира, существует много организаций, которые борются за право каждого гражданина на неприкосновенность частной жизни. Среди них Фонд электронных границ (**https://www.eff.org/**) и Электронный информационный центр конфиденциальности (**https://epic.org/**).

Фонд электронных границ (The Electronic Frontier Foundation (EFF)) был основан в 1990 году для содействия прозрачности правительства, конфиденциальности и свободы слова во всем мире. Они делают это через сочетание судебных разбирательств, активизма, анализа политики, технических документов и создания технических инструментов. Они очень активны в нескольких судебных делах, в том числе в одном, где борются за право компаний повторно заполнять и продавать картриджи вендоров (**https://www.eff.org/cases/impression-products-inc-v-lexmark-international-inc**). Их инструменты конфиденциальности включают HTTPS Everywhere (**https://www.eff.org/https-everywhere**), который является расширением браузеров Firefox, Chrome и Opera для максимального использования HTTPS и Privacy Badger, блокирующим рекламу и другие инструменты отслеживания.

Электронный информационный центр конфиденциальности (The Electronic Privacy Information Center (EPIC)) – это общественный исследовательский центр, основанный в 1994 году, который специализируется на защите конфиденциальности, свободы слова, гражданских свобод и других демократических ценностей, в основном используя судебные разбирательства, публикации и другие средства защиты. Они используют судебную систему даже больше, чем EFF, и оба выступают за лучшую кибербезопасность, а также не позволяют кибербезопасности попирать другие цели. Список вопросов конфиденциальности, который они составили, огромен (**https://epic.org/privacy/**).

Информация о политических разбирательствах EFF или EPIC обычно шокирует большинство людей, ранее не разбиравшихся в этой теме. Удивительно, как много нашей личной жизни уже пропало. Почти ничего не осталось. Обе организации некоммерческие и зависят от пожертвований. Если вы заботитесь о

конфиденциальности и свободе слова, рассмотрите возможность поддержать подобную организацию.

Отдельное спасибо следует сказать Брюсу Шнайеру (**https://www.schneier.com/**) за его неустанные усилия по просвещению и защите нашей личной жизни. Шнайер публично выступал против эрозии конфиденциальности, и его книги, особенно *David and Goliath* (**https://www.amazon.com/Data-Goliath-Battles-Collect-Control/dp/039335217X/**), обязательны к прочтению всем, кто интересуется, что происходит сейчас с частной жизнью. Вы можете прочитать больше о Брюсе Шнайере в главе 3.

Приложения с обеспечением конфиденциальности

Ни одно из предыдущих страшных предупреждений о подрыве конфиденциальности не значит, что мы ничего не можем сделать для улучшения ситуации. Многие отличные, свободно доступные приложения предоставляют как можно больше индивидуальной конфиденциальности с минимальным дискомфортом. Почти каждый специалист по ИБ предложит использовать программное обеспечение с поддержкой Tor (**https://www.torproject.org/**), которое сделает вторжение в частную жизнь сложнее для всех, кроме тех, кто очень хорошо обеспечен ресурсами. Конфиденциальность, обеспечиваемая Tor, имеет свои недостатки, но это лучшее, что мы можем получить в ПО общего назначения. Многие специалисты любят использовать поисковую систему DuckDuckGo (**https://duckduckgo.com/**) вместо более известных аналогов, которые финансируются за счет вторжения в частную жизнь. Есть много вендоров программного обеспечения, конкурирующих за защиту конфиденциальности. Пожалуйста, прочитайте статью по ссылке **http://www.infoworld.com/article/3135324/security/17-essential-tools-to-protect-youronline-identity-and-privacy.html** для понимания лучшей безопасности системы.

Мы не можем иметь безопасность и свободу без личной жизни. Следующая глава посвящена Еве Гальперин, которая работает в Фонде электронных границ.

44. Профиль: Ева Гальперин

Вам наверняка понравится человек, который любит компьютеры и кибербезопасность и при этом проводит свободное время, занимаясь воздушной акробатикой. Будучи директором по кибербезопасности Фонда электронных границ (**https://www.eff.org**), Ева Гальперин именно такой человек. Работая в Фонде с 2007 года, она достигла своей должности в 2017 году. До этого Ева получила степень в области политологии и международных отношений в Государственном университете Сан-Франциско. Ее работа в первую очередь направлена на обеспечение конфиденциальности, свободы слова и безопасности

для всех по всему миру. Гальперин теперь известна во всем мире благодаря работе в этой области, трудам о вредоносных программах и выступлениям на конференциях по безопасности, таких как BlackHat (**https://www.blackhat.com/us-16/speakers/Eva-Galperin.html**).

Я спросил Еву, как она попала в сферу ИБ. Она ответила: «В компьютерной сфере я очутилась довольно рано. Мой отец работал в этой области, и я расспрашивала его о Prodigy [предшественнике AOL и других онлайн-сервисов]. А он взял и создал мне рабочий стол на своем компьютере Unix/Solaris. В 12 лет… на машине Unix, представляешь? Я участвовала в дискуссиях Usenet о научно-фантастических книгах, играла в интерактивные текстовые игры, а когда появился Интернет, начала создавать веб-страницы. Я училась в колледже на системного администратора Unix, а в то время быть им означало разбираться в информационной безопасности».

Я узнал, как она попала в EFF и занялась анализом вредоносных программ. «Я пришла в EFF в 2007 году. В итоге занималась исследованиями кибербезопасности, потому что никто другой в EFF этого не делал. Анализировать вредоносные программы я начала в 2011–2012 годах в Сирии. Тогда [президент Сирии Башар Хафез аль-]Асад был любимцем Запада. Он позиционировал себя как отца сирийского Интернета и открыл доступ к Facebook[9], который прежде был заблокирован. Все считали его великим. Западный народ думал, что разблокировка Facebook[10] стала признаком растущей открытости Асада к свободе слова. Как же сильно они заблуждались… Я работала над исследованием Интернета в Сирии, изучала вопросы свободы слова и цензуры, когда кто-то обнаружил вредоносное ПО, созданное проасадовскими хакерами, которое было нацелено на сторонников оппозиции. Это был Rat [Remote Access Trojan], установленный на их машинах для эксфильтрации данных, включая пароли и скриншоты, на сирийский IP-адрес. Вместе мы проанализировали его. В течение следующих двух лет я помогла написать около дюжины отчетов о двух проасадовских группах, пишущих такого рода вредоносные программы».

Я спросил Гальперин, что она считает самой большой проблемой в сфере ИБ. Она ответила: «Самая большая проблема в сфере ИБ – это не безопасность, а личное пространство. Многие компании отдают приоритет информационной безопасности, но не защищают конфиденциальность своих пользователей. Они монетизируют пользовательские данные, что стимулирует собирать как можно больше таких данных. Немало компаний имеют большое количество детализированных данных пользователей, а раз они есть, данные подлежат публикации. Даже если компания защищает свои данные от хакеров, им сложнее защитить их от правоохранительных органов и правительства. Часто они даже не думают о правительствах и правоохранительных органах как об атакующих. Я хочу прояснить, что не выступаю за то, чтобы компании не собирали информацию, но пользователи должны иметь власть над своими данными. Пользователь должен знать, когда они собираются, используются, как долго хранятся, как защищены и т. д. Выбор пользователя чрезвычайно важен».

Я поинтересовался, на сколько по десятибалльной шкале Соединенные Штаты по сравнению с другими странами защищают частную информацию своих граждан. Она сказала: «США, возможно, получит 4 или 5 баллов по защите конфиденциальности. Самые сильные цифровые защиты находятся в Европейском союзе. С другой стороны, США имеют гораздо более сильную защиту свободы слова, в то время как в ЕС она намного слабее».

Я спросил Еву, что она думает по поводу приватности и свободы слова в будущем: станет ли она лучше или хуже. Она ответила: «Было бы легко сказать, что все станет хуже. Многие так и делают, тем самым выставляя себя гениями, когда оказываются правы. Но я собираюсь использовать другую тактику. Я думаю, есть шанс, что со временем ситуация улучшится, но до тех пор, пока информация пользователя считается продуктом, а свободное ПО или услуга – это то, на что они его меняют, это будет очень трудно. Мы знаем, что пользователи ценят конфиденциальность и часто готовы платить за нее, если вы дадите им выбор. Но нужно предоставить им эту возможность, и я не уверена, что получится, поскольку крупные игроки становятся более мощными, и это несовместимо с текущей бизнес-моделью».

Наконец, я попросил Еву поделиться историей о том, как она увлеклась воздушной акробатикой: «Я занималась гимнастикой в средней школе. При школе был цирковой кружок, так что я занималась акробатикой, а не привычным спортом. После выпуска я занялась воздушной акробатикой. Это отличный вид спорта! К тому же когда вы на высоте 30 футов качаетесь в воздухе, то не думаете об Интернете».

Не знаю, как вы, но мне нравится, что одна из крупнейших защитниц конфиденциальности не боится рисковать ни на работе, ни в свободное время.

Информация о Еве Гальперин

Более подробную информацию о Еве Гальперин смотрите на следующих ресурсах:

• Ева Гальперин в Twitter: **https://twitter.com/evacide**;

• профиль Евы Гальперин на Electronic Frontier Foundation (EFF): **https://www.eff.org/about/staff/eva-galperi**.

45. Установка патчей

Каждый день миллионы веб-сайтов и электронных писем содержат ссылки на вредоносные программы, известные как «наборы эксплойтов». Злонамеренные программисты (или команды программистов) создают их, а затем используют или продают. Набор эксплойтов обычно содержит все, что может понадобиться хакеру в цикле эксплойтов, включая круглосуточную техническую поддержку и автоматическое обновление, чтобы не быть пойманным антивирусным сканером. Хороший набор эксплойтов даже найдет и злонамеренно изменит

совершенно сторонний веб-сайт, чтобы убедиться, что он выполняется всякий раз, когда посетители просматривают зараженный сайт. Все, что злоумышленник должен сделать, это купить комплект, запустить его и отправить на поиск жертв.

Наборы эксплойтов почти всегда содержат клиентскую часть (программы, функционирующие на рабочих столах конечных пользователей, и код, предназначенный для использования серверов), которая ищет отсутствующие патчи. Они могут проверить от нескольких единиц до десятков уязвимостей. Любой подверженный атаке компьютер сразу же взламывается (то, что также известно как атака drive-by download), в то время как полностью пропатченные веб-серферы обычно получают письмо социальной инженерии, чтобы установить программу троянского коня. Люди, использующие наборы эксплойтов, предпочли бы использовать непропатченные устройства, чем социальную инженерию, потому что не все конечные пользователи автоматически согласятся установить любую программу. Соответствующие уязвимости регулярно обновляются, чтобы набор эксплойтов был как можно более успешным. Большинство наборов эксплойтов даже содержат консоли централизованного управления, чтобы злоумышленники могли проверить, какие уязвимости работают и как заражены устройства.

Даже без использования наборов эксплойтов отсутствующие патчи – одна из самых больших проблем, которые позволяют злоумышленникам успешно эксплуатировать устройства. Это может измениться в один прекрасный день, но пока факт остается фактом на протяжении более трех десятилетий. Чтобы обеспечить себе или своим компьютерам наилучшую защиту от использования уязвимостей ПО, все, что вам нужно делать, это своевременно и последовательно устанавливать патчи. Звучит достаточно просто. Есть даже десятки инструментов, которые могут вам помочь.

К сожалению, эффективная установка патчей остается слишком сложным и трудоемким занятием. За всю свою карьеру, проверяя сотни и тысячи компьютеров, я не думаю, что когда-либо имел дело с устройством, на котором установлены все патчи. Если такое и случалось, то я не могу вспомнить. Это большая редкость.

Зачем устанавливать патчи

В следующих разделах мы рассмотрим некоторые очень важные факты, которые большинство людей упускают из виду.

Большинство эксплойтов вызваны старыми уязвимостями, для которых выпущены патчи

Большинство устройств эксплуатируются вредоносными программами, которые ищут уязвимости, исправленные год или более назад. Опросы показывают, что большая часть эксплуатации происходит от уязвимостей, которые вендор исправил пару лет назад. Некоторый немаловажный процент компьютеров никогда не исправляется. Если вы включите брандмауэр Интернета для

обнаружения и идентификации программ эксплуатации, пытающихся заразить ваш компьютер или сеть, то обнаружите попытки использования, которые возможны только с компьютеров, зараженных в течение 15 лет (например, Code Red, SQL Slammer и т. д.). Иногда бывают уязвимости нулевого дня (угрозы, использующие непропатченные уязвимости), но они очень редки и обычно составляют менее 1 % всех успешных атак в Интернете.

Большинство эксплойтов вызваны всего несколькими непропатченными программами

В среднем за год 5–6 тысяч различных уязвимостей находятся в сотнях разных программ. Но обычно только несколько программ отвечают за наиболее успешную эксплуатацию. Например, годовой отчет по безопасности Cisco 2014 года (**http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.htm**) гласил, что на непропатченные Oracle Java приходится 91 % всех успешных веб-эксплойтов. Если вы включите другие четыре лучшие программы, они покроют 100 % всех успешных веб-эксплойтов. Это значит, что любой мог исправить только пять программ и удалить большую часть риска эксплуатации рабочего стола в любой среде. Java больше не эксплуатируется по нескольким причинам (в том числе потому, что основные вендоры браузеров удалили Java по умолчанию из своих браузеров), но то, что стало номером один среди наиболее эксплуатируемых программ, всегда меняется с течением времени. Много лет назад это был DOS, затем Microsoft Windows, Microsoft Outlook или Microsoft Internet Explorer. Сегодня у наиболее эксплуатируемых программ, как правило, есть надстройки браузера, потому что они обычно существуют на нескольких компьютерных платформах. Наиболее эксплуатируемые программы могут измениться, но тот факт, что на горстку наиболее эксплуатируемых программ приходится большая часть риска, вероятно, в ближайшее время останется неизменным.

Самая непропатченная программа не всегда самая опасная

Существует огромная пропасть в риске использования самой непропатченной программы и наиболее вероятной эксплуатируемой непропатченной программы. Хороший специалист по ИБ понимает разницу и концентрируется на последних (самых опасных). Например, в течение многих лет одной из самых непропатченных программ была Microsoft Visual C++, установленная многими сторонними программами. Тем не менее она вряд ли когда-либо эксплуатировалась, потому что была установлена и использовалась по-разному тысячами различных программ, которые сделали ее трудной в обнаружении и злонамеренном использовании. Правозащитники должны сосредоточиться на латании критических дыр в системе безопасности наиболее часто используемых программ, которые при этом не всегда самые популярные и непропатченные.

Вам также нужно патчить аппаратное обеспечение

Само оборудование работает с помощью прошивки. Прошивка – это в основном программы, реализованные в кремниевых чипах, или, как я люблю говорить, «сложное для обновления программное обеспечение». Специалисты по ИБ должны следить за тем, чтобы их оборудование, прошивка, BIOSы и устройства были пропатчены вместе с ПО.

Основные проблемы, связанные с патчами

Если бы использовать патчи было легко, это не стало бы проблемой, каковой является сегодня. В следующих разделах мы познакомимся с некоторыми проблемами, связанными с патчами.

Не обнаруживаются отсутствующие патчи

Независимо от того, какую программу вы запускаете для проверки существующих патчей, она пропустит некоторый процент устройств. Это не всегда вина программы управления патчами. Компьютерные устройства представляют собой сложные машины с большим количеством проблемных частей, и любая из них может остановить верификацию патча. Кроме того, пользователи могут использовать устройства или версии, которые не поддерживаются программой проверки патчей или могут мешать границам сетевой безопасности. Есть еще немало причин, по которым статус проверки патчей может быть неточным, но достаточно сказать, что он никогда не бывает точным на 100 %. И если вы не в состоянии обнаружить патч, то не сможете применить его.

Вы не всегда можете применить патчи

Sun (и теперь Oracle) Java долгое время была самой взламываемой программой, и, к сожалению, ее оставляли без патчей в течение почти двух десятилетий. Программисты Java последовательно пишут свои программы (неправильно), полагаясь на определенные версии и функции Java, а обновление могло сломать программы, основанные на определенной версии. По этой причине большинство предприятий знали, что у них высокий процент незакрепленных программ Java и что Java больше остальных подвергалась успешным эксплойтам, но они все равно не были в состоянии выпустить патчи для Java.

Некоторые патчи не устанавливаются

Как и при проверке отсутствующих патчей, на некотором небольшом проценте компьютеров никогда не будут применены рекомендованные патчи. Опираясь на свой опыт, могу сказать, что это количество устройств составляет в среднем около 1–2 %, но иногда оно возрастает до 15–20 %, в зависимости от сложности патча и задействованных устройств. Отличный способ победить проблемы патчей – это уделять большое внимание компьютерам, которые с трудом ищут обновления.

Патчи могут приводить к проблемам эксплуатации

Вендоры изо всех сил стараются уменьшить количество операционных проблем, вызванных определенным патчем, но нельзя ожидать, что они будут тестировать его на каждой уникальной комбинации оборудования и программного обеспечения, к которым тот может быть применен. Иногда применение очень надежного и безопасного патча может быть отменено ранее не обнаруженным вредоносным ПО или непроверенной сторонней программой. Большинство компаний сломаны одним или несколькими патчами, что привело к значительному прерыванию работы, и впредь они станут избегать патчей, если, конечно, те не будут хорошо протестированы (на что у вендоров часто нет времени или ресурсов). Из-за страха перед непреднамеренными операционными проблемами, они либо никогда не применяют патчи, либо не используют их своевременно. Я понимаю этот страх, но риск несвоевременного применения критических патчей безопасности выше, чем возможные и менее вероятные операционные проблемы. Если вас беспокоят операционные вопросы, просто подождите несколько дней. Если у патча обнаружатся серьезные последствия, поставщик очень быстро исправит это, и вы сможете применить патч уже без риска.

Патч – оповещение об эксплойте на весь мир

Патч выпускается для того, чтобы закрыть уязвимость безопасности; если о ней еще не было публично известно, то с выпуском патча об этом узнают все. Авторы вредоносных программ быстро изучают любое вышедшее исправление (патч) и перепроектируют его, чтобы узнать, как использовать уязвимость. Так как требуется минимум несколько дней, чтобы все пропатчили уязвимость, каждый недавно выпущенный патч – еще один вероятный путь для эксплуатации.

Некоторые вендоры крадут патчи высокой критичности, которые устраняют другие проблемы и не объявляют об ошибке. Позже они официально рассказывают об уязвимости и выпускают патч. К тому времени, благодаря более раннему патчу, ошибка уже исправлена на большинстве компьютеров. Один очень популярный поставщик ОС однажды создал критическое исправление за несколько месяцев до других патчей. Для реверсивных инженеров это выглядело как необъяснимые сегменты кода, но как только трехмесячные патчи были применены, они закрыли огромную дыру, оставив клиентов счастливыми, а хакеров – разочарованными.

В конце концов, хорошее управление патчами означает одно: своевременное и последовательное исправление наиболее часто используемых программ. Это легко сказать, но трудно сделать. Мой совет – включить все автоматические патчи или использовать авторитетную программу управления ими, которая может обрабатывать все ваши потребности обновления ПО (и оборудования тоже, если это возможно); и пусть критические исправления безопасности будут применяться в течение нескольких дней. Если вы исправите уязвимость за пару дней, то станете одним из самых защищенных в Интернете. Идеальный патч может быть нелегким, но исправление критических уязвимостей наиболее часто

используемых программ необходимо на любом компьютере. Не делать этого значит буквально просить хакеров атаковать вас.

В следующей главе представлен профиль Уиндоу Снайдер, женщины, ответственной за помощь некоторым из крупнейших компаний в мире по исправлению уязвимостей.

46. Профиль: Уиндоу Снайдер

Вначале Уиндоу Снайдер работала директором по архитектуре безопасности в @Stake. Это была крупная компания, занимающаяся ИБ и поиском уязвимостей, которая создала или приобрела больше, чем множество компьютерных суперзвезд. Компания была приобретена Symantec в 2004 году. Снайдер начала работать в Microsoft в 2002 году и была старшим стратегом в области безопасности в группе безопасности и коммуникаций. Она внесла свой вклад в жизненный цикл разработки SDL и создала новую методологию программного обеспечения для моделирования угроз. Она также была лидером безопасности в Microsoft Windows Server 2003 и Windows XP Service Pack 2, которая была первой серьезной попыткой Microsoft создать по умолчанию безопасную операционную систему. Она координировала работу консалтинговых служб безопасности и отвечала за стратегию работы сообщества в сфере ИБ.

Она присоединилась к Mozilla в 2006 году и носила ироничный титул «начальник Службы безопасности того или другого» вместо более формального «главного сотрудника Службы безопасности (CSO)». Помню, многие из нас завидовали этому титулу. В конце концов, она стала работать старшим менеджером по продуктам безопасности в Apple, разрабатывая стратегию безопасности и конфиденциальности и функции для iOS и OS X. Сегодня она работает на Fastly (**https://www.fastly.com/**), сеть доставки контента, которая быстро расширяется на другие сферы, такие как информационная безопасность. Отец Снайдер – американец, а мать родом из Кении. Снайдер стала соавтором книги *Threat Modeling* (**https://www.amazon.com/Threat-Modeling-Microsoft-Professional-Swiderski/dp/0735619913/**) совместно с Франком Суидерски. Она единственный человек, которого я знаю лично, кто работал в трех из четырех крупнейших компаниях, предоставляющих очень популярные браузеры и программное обеспечение. Она, так сказать, стояла у истоков.

Я был обязан начать наше интервью с вопроса об ее имени. Она рассказала: «Я могу поделиться с вами историей о том, как работала в Microsoft. Тогда, по умолчанию, адреса электронной почты большинства людей начинались с их имени, за которым следовал последний инициал. Но большая группа рассылки, группа продуктов Windows, уже имела слово Windows в адресной строке (что было бы в адресе моей электронной почты, если бы я оставила ее по умолчанию). На протяжении долгих лет многие пытались отправить мне что-то личное или конфиденциальное… Возможно, речь шла о вредоносном ПО или новом отчете об уязвимости. Но вместо того чтобы отправить его мне, они

случайно посылали его в одну из наших крупнейших групп рассылки по электронной почты».

Потом я спросил ее, как она попала в сферу ИБ. Она сказала: «Я изучала информатику и заинтересовалась криптографией и криптоанализом. Я увлеклась идеей секретов, связанных сложностью математической задачи. Это было примерно в то же время, когда я впервые получила доступ к многопользовательским операционным системам. Я начала думать о границах безопасности между различными пользователями и процессами, а также о том, что препятствует им вмешиваться в чужую программу или ОС. Я обнаружила, что тогда в лучшем случае были полупроницаемые барьеры. Это было весело, как разбирать головоломку или машину и выяснять, как она работает. Захватывающая работа!»

Я знал, что Уиндоу участвовала в разработке жизненного цикла безопасности (SDL) в Microsoft. Меня интересовало, как это произошло и что именно она сделала. Она ответила: «Когда я впервые попала в Microsoft, эта тема не была хорошо продумана. Безопасностью занимались всего одиннадцать сотрудников. Я была двенадцатой, сосредоточившейся на безопасности Windows. И тогда мы в основном реагировали на те уязвимости, которые находили другие люди. Не было сильной внутренней программы. Затем появились SQL Slammer и Blaster. Я помогала в создании первых основных методологий моделирования угроз [и написала в соавторстве книгу на эту тему]. С моей помощью началось активное обнаружение ошибок и общение с пользователями. Когда я впервые попала в Microsoft, если кто-то извне обнаруживал ошибку безопасности, компания называла их хакерами. СМИ в то время смешивали хакеров всех мастей с преступниками. Но люди, сообщающие о проблемах в Microsoft, даже публично писавшие о них, не были преступниками. Я помогала продвигать информационные программы, чтобы сделать этих людей нашими союзниками, а не противниками. Одним из таких улучшений было назвать их исследователями безопасности, а не хакерами, чтобы сосредоточиться на том, что их работа оказалось ценным вкладом. Я также помогла создать программу, спонсировавшую множество небольших внешних хакерских конференций, таких как Hack-in-the-Box. Мы смогли в итоге изменить представление о том, что Microsoft не заботится о безопасности или не знает о ней, и стали вместе с этими исследователями командой.

Когда я попала в Microsoft, не было никого, кто занимался бы безопасностью продуктов Windows, поэтому я вмешалась. Я представляла безопасность на “военных собраниях” Windows, где общались спонсоры и заинтересованные стороны. Было огромное количество ошибок, которые мы решали в своего рода игровом стиле, и это было неэффективно. В рамках SDL мы начали рассматривать более глобальные причины ошибок, пытаясь найти более широкие категории, которые, если бы были исправлены, смягчили бы сразу много ошибок. Мы взяли уроки у сторонних хакеров и начали применять их в других продуктах, например в Microsoft Office».

Я попросил ее назвать еще один ценный урок, который она извлекла из этого опыта. Она поделилась: «За сегодняшним вредоносным ПО стоит целая

финансовая система. Есть одна команда людей, обнаруживающая уязвимости, и другая команда, которая превращает эту уязвимость в эксплойт или набор эксплойтов. Таким образом, есть люди, которые могут взломать множество сайтов, и те, кто может это исправить. Если вы можете сделать ключевые точки системы более трудными или дорогими для взлома, то и всю цепочку сложнее сломать. Microsoft и Windows недостаточно рано это поняли. Когда я присоединилась, они уже испытывали натиск вредоносных программ, червей и вирусов. Позже я начала работать на других платформах, включая iOS и OS X в Apple, и использовала свой опыт, чтобы успешно поставить препятствия, которые делали вредоносную систему менее действенной и прибыльной. Если вы можете подорвать экономику вредоносных программ, то можете выиграть и таким образом тоже».

Снайдер работала в некоторых из самых известных крупных компаний. Интересно, что общего она видит в корпорациях, которые так сильно отличаются? «Во всех компаниях вы должны заставить безопасность работать на конечных пользователей. Функции безопасности, которые стоят слишком дорого или сильно прерывают обычный рабочий процесс, не будут работать. Нам нужно реализовать большую и лучшую безопасность, но не мешать пользователю. Кроме того, не собирайте данные, которые вам не нужны. Если вы занимаетесь сбором, то должны защитить данные и предоставить пользователям контроль над ними. Самая большая проблема в сфере ИБ – это успешное выполнение того, что мы уже умеем делать».

Без сомнений, ее позицию можно считать экспертной.

Информация об Уиндоу Снайдер

Более подробную информацию об Уиндоу Снайдер смотрите по ссылкам:

• профиль Уиндоу Снайдер на LinkedIn: **https://www.linkedin.com/in/window**;

• Уиндоу Снайдер в Twitter: **https://twitter.com/window**.

47. Карьера писателя

Я дважды завалил английский в школе. В аспирантуре, во время стажировки в больнице, мой первый корпоративный отчет был настолько плох, что босс вслух разругал всю систему образования нашей страны. Когда я время от времени перечитываю его, чтобы напомнить себе, с чего начал, мне физически больно. Почти 30 лет спустя я стал автором или соавтором девяти книг и почти 1000 статей в национальных журналах по информационной безопасности, а также веду колонку, посвященную ИБ, в журнале *InfoWorld* вот уже 12 лет. Все благодаря моему брату (первому и лучшему настоящему писателю в семье), моей настойчивости и множеству хороших редакторов.

Хотя мне все еще непросто писать электронные письма без опечаток, мой навык письма улучшился настолько, что я очень хорошо зарабатываю этим на жизнь.

Я часто выполняю письменные задания, за которые могу заработать до 500–1000 долларов в час, и получаю за год больше, чем средний доход американской семьи, – и это только подработка. Несмотря на работу консультантом в сфере ИБ, я писал об информационной безопасности еще до этого. Это неплохой дополнительный доход, который я могу получить, записывая запасные циклы дома, во время полета, в гостиничных номерах. Некоторые люди смотрят телевизор ночью, а я обычно пишу, когда смотрю телевизор. Это хобби финансировало моей семье несколько грандиозных отпусков и позволяет мне тратить слишком много денег на другие любимые занятия. И я не один такой.

Сотни людей по всему миру зарабатывают на жизнь благодаря тому, что пишут об информационной безопасности. Даже находясь вне дома, с хорошим подключением к Интернету, они обеспечивают достойную жизнь для себя и своих семей. Некоторые работают на известных медиагигантов, а другие – фрилансеры, продающие статьи и услуги заинтересованным сторонам. Некоторые пишут книги, блоги и статьи. У них есть страсть к информационной безопасности, они не обращают внимания на рекламную шумиху вендора и раскрывают правду читателям более понятным языком.

Куда можно писать об информационной безопасности

Существует много способов написать об ИБ, в том числе описанные ниже.

Блоги

Большинство авторов книг по информационной безопасности ведут один или несколько блогов. По сути, это современная версия журнальных статей. Публикации в блогах могут быть платными или бесплатными, а также могут иметь или не иметь редактора, который поможет проверить и исправить содержимое перед публикацией. Личные блоги и посты очень легко начать, хотя самая большая проблема – это привлечение читателей и поддержание работы в долгосрочной перспективе. Подавляющее большинство блогов существует всего около года, если авторы либо не получают желаемой читательской аудитории, либо сказали все, что хотели. Ведение блога, как и написание журнальных статей, – тяжелая работа.

Если вы хотите вести блог и не знаете, с чего начать, ознакомьтесь с одним из многих популярных сайтов, из которых WordPress **(http://www.wordpress.com)** – неоспоримый лидер на данный момент. WordPress, созданный и поддерживаемый компанией Automattic, управляет 27 % всех интернет-сайтов и примерно 70 % всех сайтов блогов.

Социальные сети

Большинство людей, пишущих об информационной безопасности, также пишут посты в Twitter. У них могут быть профессиональные (и личные) сайты на LinkedIn или Google. Многие авторы пишут в сетях в дополнение к другим профессиональным местам публикации.

Статьи

Большинство профессиональных авторов по информационной безопасности пишут статьи, что обычно означает написание контента в диапазоне от нескольких сотен до многих тысяч слов. Средняя длина столбца составляет около 1000 слов. Статьи могут быть опубликованы в печатных журналах, в интернет-изданиях или на сайте блога. Темы статей могут быть в категориях новостей, мнений, учебных пособий или технических обзоров продуктов.

Если вам нравится писать и вам повезет, вы можете даже получить еженедельную или ежемесячную колонку. Хотя, прежде чем взять на себя регулярное письменное задание, убедитесь, что готовы к этому. Помню, как я был рад получить свою еженедельную колонку в журнале *InfoWorld* еще в августе 2005 года. Я не мог дождаться, чтобы рассказать миру все, что думал и чем был увлечен. Оказывается, поведать миру обо всем, чем вы действительно интересуетесь, можно примерно в 12 статьях. После этого придется читать о новых открытиях, явлениях и тенденциях перед написанием очередной статьи. Иногда я просыпаюсь в 4 утра и пишу три колонки, но порой изо всех сил пытаюсь придумать новую интересную тему или точку зрения, пока не наступит крайний срок. Большинство рутинных писателей сгорают, поэтому, если вы хотите сделать карьеру, придумайте творческую рутину, которая будет интересна вам и вашему работодателю.

Книги

Книги – это замечательный способ поделиться тем, что вы знаете, и даже подтвердить свои навыки писателя. Я до сих пор помню ту невероятную радость, когда получил первый контракт на книгу (после многих лет попыток и более 100 писем с отказом), и чувства, которые испытывал, держа ее в руках. Если вы стали автором книги, велик шанс, что в некрологе вас так и назовут. Этого у вас никто не отнимет.

Итак, если вы не найдете способ интересно писать на нестандартную тему, то вряд ли сделаете хорошую писательскую карьеру. Подавляющее большинство книг по информационной безопасности не приносят своим авторам больше 10 000 долларов. Так было не всегда, но все изменилось с тех пор, как поисковые интернет-системы стали популярными, и люди могут найти необходимую информацию бесплатно. Однако есть исключения. Я знаю некоторых авторов компьютерных книг, которые заработали сотни тысяч долларов и смогли купить яхты и пляжные домики. Просто не начинайте писать, если ваша цель – разбогатеть. Сделайте это, потому что у вас есть интересная идея, которая понравится десяткам тысяч читателей. Убедитесь, что действительно можете помочь сделать их жизнь и карьеру проще и приятнее.

Однако, хотя написание компьютерной книги может и не сделать среднестатистического автора богатым, это почти всегда приводит к более высокооплачиваемой работе. Если вы пишете книги, у вас такой же авторитет, как у доктора наук или человека с хорошим сертификатом, если не больше. Среднестатистический автор компьютерной книги зарабатывает гораздо больше, чем те, кто этого не делает. И опять же, всего за несколько часов

работы я могу заработать больше, чем другие получают за неделю или две. Неплохо для парня, который дважды завалил английский!

Самиздат или издатель?

Если вы собираетесь написать книгу, вам нужно решить, хотите ли вы самостоятельно опубликовать ее или отнести в издательство, предварительно выбрав его. Для начинающих авторов книг может быть трудно получить контракт на книгу, в котором есть гарантированные и текущие договоренности об оплате. Многие авторы, как в первый раз, так и в других случаях, решают опубликовать книгу самостоятельно отчасти потому, что хотят получить более высокую долю прибыли от каждой проданной книги. Чаще всего авторы решают публиковаться без помощи после того, как их не приняли в издательстве. Это может быть очень трудно.

Если авторы могут гарантированно получить более высокий процент прибыли от каждой самостоятельно опубликованной книги по сравнению с сотрудничеством с издательством, многие читатели зададутся вопросом, почему кто-то вообще решает обратиться в издательство. На самом деле по многим причинам. Среднестатистический автор тратит на написание книги примерно год – некоторые меньше, некоторые больше. Если вам не посчастливилось делать это на работе, значит, придется жертвовать каждым свободным моментом. В итоге вы пренебрегаете членами семьи, пропускаете веселые вечеринки и вообще застреваете перед компьютером дольше, чем длится ваша профессиональная деятельность в области ИБ. Несмотря на усилия, вы хотите, чтобы книга была хорошей. Книга, выпущенная издательством, с большей вероятностью будет таковой. Самостоятельно изданные книги редко продаются тиражом более нескольких десятков экземпляров (особенно в области ИБ) и обычно выглядят не так профессионально, как книги, выпущенные издательствами.

Работа с издательством сделает вашу книгу лучше. Кроме того, издательство возьмет на себя «неписаные» части книги, которые могут быть существенными. Прежде чем писать эту книгу, я задавался вопросом, должен ли самостоятельно опубликовать ее, но потом понял, что лучше написать главы и передать их в издательство, где за меня займутся редактированием, техническим редактированием, профессиональной графикой, маркетингом и продажей, а сэкономленное на этом время провести с семьей или за любимым хобби. Например, вместо того, чтобы создавать переднюю и заднюю обложки книг с нуля, редактор отправил несколько макетов, сделанных более профессионально и творчески, чем если бы этим занимался я. Я просто выбрал те, которые мне понравились. Это заняло буквально одну минуту вместо нескольких дней или недель работы, и вышло куда лучше. Кроме того, профессиональные редакторы, которые будут работать над вашей книгой в издательстве, вероятно, профессиональнее, чем любимый человек или друг, редактирующий вашу книгу безвозмездно.

Я думаю, что сотрудничество с профессиональным издательством сэкономит вам половину сил и имеет гораздо больше шансов сделать лучший продукт с большим количеством продаж, чем самиздат. С учетом сказанного, если вы преданный профессионал и не возражаете против дополнительных усилий, самиздат – хорошая альтернатива для тех, кто готов делать дополнительную работу. К сожалению, в книгах, выпущенным самостоятельно, зачастую присутствует множество опечаток. Это не значит, что в книгах издательства ошибок нет, но их определенно гораздо меньше.

Если вы заинтересованы в публикации книги профессиональным издательством, перейдите на их веб-сайт и найдите форму предложения книги. Не торопитесь при ее заполнении. Обычно это занимает несколько дней. Отправьте ее на свой адрес электронной почты. Если вы впервые пишете книгу и хотите, чтобы вас приняли быстрее, свяжитесь с книжным агентом, который специализируется на типах книг, которые вы хотите написать. Они помогут усовершенствовать вашу идею и предложение книги, и, скажу по собственному опыту, это поможет получению контракта. Я не всегда прибегал к услугам книжного агента, но когда обращался к ним (я использую StudioB [**http://www.studiob.com/**]), это стоило небольшого процента, который они берут из роялти.

Техническая редактура

Задолго до того, как стать автором опубликованной книги, я был техническим редактором, рецензирующим книги, направленные на публикацию. Я и сегодня продолжаю этим заниматься. Многие авторы книг по информационной безопасности с этого начинают. Это отличный шанс узнать, как работает процесс, что ожидается от авторов и как избежать распространенных ошибок, которые делают новички.

Новостные рассылки

Существуют десятки ежедневных, еженедельных и ежемесячных новостных рассылок по информационной безопасности, для которых вы можете писать. С популярными изданиями может быть трудно начать сотрудничать. Многие не принимают новичков. Однако другие, менее популярные, издания новостных рассылок ищут новых авторов на условиях бесплатного сотрудничества. Новостные информационные рассылки могут стать отличным местом для создания письменных работ и написания резюме, чтобы помочь вам получить другие более высокооплачиваемые контракты.

Подробные отчеты

По моему опыту, подробные отчеты, спонсируемые вендорами, часто могут принести большую сумму денег. Вендоры предлагают хороший гонорар за 5–10 страниц. Некоторые хорошо оплачиваемые отчеты я могу написать за несколько часов, другие требуют больше исследований и интервью и в итоге занимают много недель. Но в целом вы можете заработать те же деньги за несколько отчетов с гораздо меньшими усилиями, чем требует написание книги. Помните

об этичной стороне: если вы когда-либо получали оплату от вендора за отчеты, вы всегда должны раскрывать это в любом другом проекте с участием того же вендора или его конкурентов.

Технические обзоры

Самое сложное, что я когда-либо делал, – это технические обзоры продуктов. Вы просматриваете один или несколько продуктов, чтобы удалить постоянно присутствующую рекламу вендора и сообщить читателям о возможностях реального продукта. Обзоры занимают дни или недели и часто включают в себя тестовые лабораторные моделирования и интервью с реальными клиентами. За эти усилия обычно платят недостаточно много. Хороший технический обзор может быть гораздо более полезным и помочь большему количеству людей. Я стараюсь делать несколько обзоров каждый год, когда вижу перспективный продукт или чрезмерно раздутые проекты, которые интересуют читателей.

Конференции

Как только вы начнете писать для того, чтобы заработать на жизнь, вы можете начать участвовать в конференциях. Мне потребовалось два десятилетия, чтобы преодолеть страх сцены, но я могу серьезно сказать, что выступление на конференциях – одна из самых плодотворных работ, которые я когда-либо делал. Вы не только получите возможность поделиться своими идеями, но и встретите кучу единомышленников, получите дополнительные предложения о работе и узнаете что-нибудь новое. Конечно, выступление требует дополнительных навыков, таких как умение создавать хорошие слайд-шоу и презентации. Многие конференции проводят предварительные семинары, чтобы помочь как новым, так и опытным докладчикам улучшить свои презентационные и устные навыки.

Советы профессионального писателя

После почти тридцати лет писательства я могу дать читателям несколько советов, в том числе описанных в следующих разделах.

Самое сложное – начать

В течение многих лет ко мне приходили сотни людей и спрашивали, как профессионально писать. Я всегда даю им много информации и рекомендаций. За это время, возможно, лишь некоторые из них последовали моим советам и попытались что-то написать. Технология профессионального письма трудна по крайней мере до тех пор, пока вы не станете достаточно опытным. Самое сложное – начать. Если вы хотите быть профессиональным писателем, вам нужно начать писать и прикладывать усилия, необходимые для публикации. Конечно, вы должны уметь писать качественно и хорошо разбираться в том, о чем пишите, но, как я уже говорил, некоторые вещи можно узнать и после начала написания книги. Если вы не очень хорошо пишете, почитайте несколько книг по грамматике и письму.

Читайте иначе

Как профессиональный музыкант слушает музыку иначе, чем поклонник, писатели должны смотреть на другой стиль письма, чтобы подобрать идеи, подсказки и трюки. Начните читать статьи, обращая внимание на то, как писатель выразил свои мысли. Как он представил свою историю? Какое было первое предложение? Как он изложил материал? Интересно ли его читать? Использовал ли он картинки и, если да, в каких местах? Чем он закончил? Если вы собираетесь стать профессиональным писателем, начните замечать кирпичи в фундаменте дома. Кроме того, если вам нравится стиль письма конкретного автора, следите за его творчеством. Один из самых явных признаков того, что вы заинтересованы в конкретном стиле письма, это когда вы начинаете следовать своим любимым писателям, потому что знаете, что они лучше других выражают свои мысли.

Начинайте безвозмездно

Крайне мало писателей, которые получают деньги за свою первую работу. Большинству из нас приходится проводить время в окопах. Если вы надеетесь стать новым профессиональным автором, ищите информационные рассылки и блоги, чтобы узнать, будут ли они принимать ваши статьи и идеи. По мере того как вы наращиваете навыки письма и опыт, можете начать просить увеличить гонорар, хотя помните, что разные типы работ оплачиваются по-разному. Дело не всегда в деньгах. Каждый бит письма завоевывает доверие.

Будьте профи

И, наконец, само собой разумеется, что в профессиональной письменной индустрии будущий профессионал проходит долгий путь. Это означает готовность и осведомленность, а также соблюдение сроков. Каждый редактор и издатель сталкивался со страшилками о людях, с которыми подписали контракт, но те так и не закончили книгу или статью. На ранней стадии я сомневался в своей способности писать, и это привело к пропущенным срокам. Я узнал, что простое соблюдение сроков может дать вам много другой оплачиваемой работы. Часто, когда издатель или редактор встречает вас впервые, он пытается выяснить, будете ли вы надежным и профессиональным. Если вы можете доказать свою надежность, то можете стать и профессиональным писателем. Если вы будете делать это постоянно, от этого может зависеть ваша будущая карьера.

Продвигайте себя

Независимо от того, публикуете вы свою книгу сами или используете профессиональную организацию, вам нужно потратить как можно больше усилий на то, чтобы вашу работу увидели больше людей. Вот почему многие профессиональные писатели имеют страницы в социальных сетях. Чем больше людей о вас знают, тем больше шансов, что вы сможете зарабатывать на жизнь писательством.

Лучше один раз увидеть, чем сто раз услышать

Я благодарю своего старого друга и профессионального автора бестселлеров в области ИТ, Марка Минаси (**http://www.minasi.com**), за такой совет: постарайтесь, чтобы ваш профиль сопровождался вашей фотографией. Читателям легче вас запомнить, если вы поможете им связать изображение с вашим именем. На ранней стадии я говорил администраторам веб-сайтов, что напишу бесплатно (даже в том случае, когда они сами предлагали заплатить), если они разместят мою фотографию рядом со статьей. Это помогает читателям быстрее вас узнавать и способствует дальнейшему успеху. Побочный эффект «эгоизма» в том, что иногда совершенно незнакомые люди подходят к вам и говорят, что им нравится ваша работа. Мои книги никогда слишком не впечатляли моих дочерей, но иногда встречался случайный поклонник, который подходил к нам в ресторане или парке развлечений, узнавал и благодарил меня.

Я не только штатный консультант в сфере ИБ, но и писатель, что определенно сделало меня лучшим консультантом. Когда вы пишете, вы должны очень хорошо изучить свой предмет и стать мастером. Это заставляет вас учиться и тренировать свой мозг таким образом, как в противном случае вы бы не смогли. Мне нравится думать, что работа консультантом в сфере ИБ помогает мне быть лучшим писателем, а работа писателем – быть лучшим консультантом в сфере ИБ. По крайней мере, в моем случае это не случайно.

Следующая глава посвящена Фахмиде Я. Рашиде, писательнице и коллеге по журналу *InfoWorld*.

48. Профиль: Фахмида Я. Рашид

Я – журналист, пишущий об информационной безопасности уже почти 30 лет. Хотя я не лучший писатель, я считаю себя одним из лучших технических писателей, потому что живу и дышу своей темой. Читая работы других авторов по информационной безопасности, я не многому учусь. Но это изменилось, когда наш главный редактор Эрик Кнорр познакомил меня с новым журналистом InfoWorld. Эрик был очень рад ее нанять, и вскоре я понял почему. Как журналист в сфере ИБ Брайан Кребс (профиль в главе 29), Фахмида Я. Рашида – невероятный исследователь информационной безопасности. Я еще не прочитал ни одной ее статьи, из которой не узнал бы ничего нового. Она представляет свой предмет таким образом, что продолжает удивлять меня. Она действительно понимает технические детали и способна выведать информацию лучше, чем кто-либо другой. Иногда она задает мне технические вопросы о чем-то, чего не понимает, на что я почти всегда отвечаю «я тоже не знаю», но через несколько дней после дополнительных исследований она публикует простое для понимания объяснение. Она где-то находит ответы.

Фахмида опытный журналист по ИБ. Она работала в eWeek старшим техническим редактором испытательного центра, создающего сетевую инфраструктуру Forbes.com. Она была главным редактором конференции RSA и

писала для десятка авторитетных журналов и сайтов, включая: Dark Reading, PCMag.com, SecurityWeek, Tom’s Guide, InfoWorld, SCMagazine, Dice.com, BankInfoSecurity.com и GovInfoSecurity.com. В настоящее время она старший журналист в InfoWorld, а также работает в Pragmatic Bookshelf, помогая авторам в написании технических книг.

Я спросил Фахмиду, как она начала работать в сфере ИБ. Она ответила: «Я начинала как сетевой техник и сотрудник службы поддержки для студентов, преподавателей и администраторов в Большом городском университете. Я много узнала о защите сети, жонглируя вызовами BYOD еще до того, как аббревиатура стала модным словом безопасности. Я изучила администрирование веб-сервера трудным путем, работая в качестве разработчика ColdFusion для запуска dotcom, и кто-то взломал сервер IIS и удалил файлы. Я провела шесть лет в качестве консультанта по вопросам управления в различных фирмах финансовых услуг и фармацевтических компаниях, разрабатывая Java-приложения, создавая большие хранилища данных и манипулируя большими наборами данных. Наслаждаясь работой, я хотела сделать шаг назад, иметь более широкий взгляд на мир технологий, а не просто изучать сеть одной компании. Я присоединилась к миру журналистики в качестве репортера по корпоративным технологиям, пишущего о сетях, хранилищах и оборудовании. Весь мой технический опыт очень пригодился, потому что я действительно понимала технологию, о которой писала.

Безопасность стала логическим продолжением моей деятельности, потому что очень трудно писать о сети и не думать о безопасности. Примерно через пять лет я начала специализироваться на ИБ. Отчасти это была случайность, так как увеличение числа громких атак, утечек инсайдерской информации и рост мошенничества с онлайн-кредитными картами означали, что мне нужно тратить больше времени на безопасность. Я поняла сети, так что могла увидеть пробелы, которые сделали атаки возможными. Я начала изучать SQL-инъекции и XSS и действительно надеялась, что ни один из кодов, написанных мной, когда я была консультантом, не был в производстве, потому что я знаю, что не санировала никаких входов. Я писала как для деловой, так и для потребительской аудитории и узнала, что разные группы смотрят на безопасность по-разному. Но, спустя много лет, я рада видеть, что все больше и больше людей действительно думают о безопасности, а не отвергают ее как нечто, с чем имеют дело технари».

Я спросил Фахмиду, что, по ее мнению, можно назвать самой большой проблемой в сфере ИБ. Она ответила: «Я думаю, что самая большая проблема заключается в том, что трудно быть в безопасности. Это требует новых привычек, а у нас нет ни времени, ни терпения, чтобы развивать их. Это не должно быть легко или удобно, но когда безопасность сбивает с толку, преимущества не так очевидны, и есть люди, которые просто ищут обходные пути. Все, что мы знаем и имеем в области безопасности, сводится к тому, что трудно работать безопасно и намного проще держать все открытым и незащищенным. Некоторые примеры: шифрование имеет смысл, но его все еще слишком сложно использовать регулярно. WhatsApp заботится об этом

автоматически, поэтому теперь люди не против использовать зашифрованный чат. Но безопасный обмен файлами и зашифрованная электронная почта по-прежнему слишком сложны.

Мы не думаем дважды, прежде чем запереть двери наших домов, но, должно быть, было время, когда люди думали, что это безумие. Теперь люди так же думают о шагах безопасности, но это мнение постепенно меняется. Чтобы действительно изменить это, нам нужны лучшие инструменты. С другой стороны, я встретила немало людей с iPhone, которые до сих пор не используют TouchID для блокировки своих телефонов, поэтому не знаю, насколько дальше мы должны идти по простому для людей пути. Возможно, нужно добраться до точки, где iPhone автоматически записывает отпечатки пальцев пользователя, чтобы не настраивать TouchID вручную. Нам нужна безопасность по умолчанию, где двери запираются автоматически, без необходимости вставлять ключи в замочную скважину. Skynet может быть решением всех наших проблем с безопасностью».

Я спросил Фахмиду как успешного специалиста в сфере ИБ, что она порекомендует другим людям, рассматривающим карьеру писателя в области ИБ. Она сказала: «Хотя я не думаю, что вам обязательно иметь техническую подготовку, чтобы быть хорошим писателем, это помогает. Изучите основы того, как работают сети, как компьютеры и другие устройства взаимодействуют и что означают некоторые из распространенных терминов. Если вы собираетесь рассматривать атаки веб-приложений, имейте представление о том, как взаимодействуют веб-приложения, веб-серверы и базы данных на уровне блок-схемы. Если вы собираетесь писать о DDoS-атаках (или его младшем родственнике, DoS), нужно иметь базовое понимание того, как работает сеть. Вам не нужно знать математику, лежащую в основе криптографии, но необходимо понять разницу между различными реализациями и почему некоторые из них не должны использоваться. Читайте. Посмотрите на технологию. Не уклоняйтесь от понимания того, как она работает. Вы не можете объяснить людям, почему нужно увеличить безопасности цифровой жизни и защищать технологии, если вы их боитесь. Подумайте об этом так: не нужно быть пилотом, чтобы писать об авиационной промышленности, но если вы летали хотя бы на некоторых самолетах, вам это поможет.

Еще одна важная вещь, которую нужно помнить, – это то, что технология имеет тенденцию идти волнами. То, что раньше казалось старым, перестает таковым быть с настройкой или новой функцией. Количество молодых писателей, которые не знают о мейнфреймах или отвергают их потому, что “никто их больше не использует”, пугает, поскольку большая часть нашего мира все еще имеет мейнфреймы в основе. И каждый раз, когда я слышу, как люди говорят о мобильных устройствах и данных в облаке, я вспоминаю рассвет тонких клиентских вычислений. Знание истории важно, но это действительно имеет значение, когда вы смотрите на безопасность, потому что можете видеть шаблоны».

Я спросил Фахмиду, узнала ли она сейчас нечто новое, что могло бы помочь в ее карьере, узнай она об этом раньше. Она ответила: «Не бойтесь задавать

вопросы. У меня было такое чувство, что для того, чтобы исследователи и эксперты по безопасности воспринимали меня всерьез, я должна быть сведущей в основах, поэтому я потратила много времени, занимаясь самообразованием, чтобы попытаться добраться до сути. Потребовалось немало времени, чтобы понять, что эксперты хотят, чтобы им задавали вопросы и они могли похвастаться своими знаниями. Без базовых знаний никуда: не стоит спрашивать, что такое DDoS-атака, но можно узнать, какая разница между атакой DoS уровня 4 и уровня 7. Большую часть моих знаний основ безопасности я получила как самоучка, и если бы я попросила о помощи раньше, то могла бы узнать все гораздо более подробно, избавив себя от стресса. Кроме того, скептически относитесь к таким словам, как “инновационный”, “первый в истории” и “лидирующий на рынке”. Когда вы смотрите на объявления безопасности, мысленно вычеркивайте кричащие слова, чтобы увидеть главное».

Я спросил Фахмиду, почему ей нравится писать об ИБ. Она ответила: «Мне нравится информационная безопасность, потому что она заставляет меня продолжать учиться. Всегда есть новые исследования и новые способы решения проблем. Безопасность сочетает в себе творческое решение проблем, любопытство и готовность сломать что-то во имя улучшения. Это также касается эго. Профессионалы в области безопасности – это люди, которые каждое утро встают с намерением спасти мир.

И пусть не все могут заработать миллионы, как учредители Instagram[11], или получить такую славу, как Илон Маск, но люди, которые хранят данные в безопасности в корпоративных базах данных, убеждаются, что SSL-сертификат на веб-сайте актуален, так что финансовые данные могут надежно передаваться через Интернет, и проверяют код, чтобы убедиться, что в нем нет зияющей дыры, – современные герои. Мне нравится писать об информационной безопасности, потому что это ставит меня рядом с ними».

Информация о Фахмиде Я. Рашиде

Более подробную информацию о Фахмиде Я. Рашиде смотрите по ссылкам:

• профиль Фахмиды Я. Рашиде на LinkedIn: **www.linkedin.com/in/fyrashid**;

• публикации Фахмиды Я. Рашиде в журнале InfoWorld: **www.infoworld.com/author/Fahmida-Y.-Rashid/**.

49. Руководство для родителей юных хакеров

Примечание. Частично текст этой главы возник из статьи, которую я написал в 2016 году: «*11 признаков того, что ваш ребенок – хакер, и что с этим делать*»[12].

Как человеку, пишущему об информационной безопасности вот уже свыше 20 лет, несколько раз в год мне приходят письма от родителей, спрашивающих, как они могут узнать, что их ребенок – киберпреступник, и что они могут сделать, чтобы мотивировать его на многообещающую честную карьеру. Я знаю, о чем они говорят, потому что много лет назад такая же проблема возникла с моим сыном-подростком. Он начал заниматься не совсем легальным хакерством и несколько раз попадал в неприятности. К счастью, мы с женой успели вовремя вмешаться и, обзаведясь парой морщин, успешно поддержали его начинания в роли «белой шляпы».

Я думаю, что многие умные подростки, увлекающиеся компьютерами, могут связаться с «черными шляпами», если их не направлять должным образом. Часто они либо не преуспевают в школе, либо не получают удовлетворения от своих научных достижений. В школе и, вероятно, дома им говорят делать то, что они считают унылым и бесцельным, и чувствуют, что их осуждают за то, что они не раскрывают свой потенциал. В киберпространстве они ищут и находят восхищение и уважение коллег. Чувствуют себя могущественными и таинственными одновременно. Это опьяняет. Они привлекают внимание. Большинство этих детей имеют добрый умысел, и они переживут свое «вредное» хобби без особых последствий. Проблема в том, что вы не можете быть уверены, станет ли ваш ребенок этим заниматься, поэтому лучше вмешаться, прежде чем вам позвонят из полиции.

Как определить, что ваш ребенок – хакер

Прежде чем вы сможете посоветовать своему ребенку использовать навыки взлома только для этичных и добрых целей, сначала выясните, действительно ли его намерения вредны. Если вы исключили, что скрытность подростка связана только с порнографией или любовным интересом, обратите внимание на некоторые признаки того, что ваш ребенок участвует во вредоносном взломе.

Примечание. Очевидно, что существует много вещей, которые могут беспокоить родителей, когда они не знают, чем их ребенок занимается в Интернете: например, просмотр порнографии, посещение чатов, где сидят грабители, участие в других тревожных, опасных или незаконных мероприятиях. Каждая из этих проблем серьезна и может быть решена с помощью различных средств, но в этой главе мы сосредоточимся именно на опасностях взлома.

Он рассказывает о том, что ломает

Это довольно просто. Ваш ребенок рассказывает о том, как легко взломал что-либо. Я знаю, это звучит смешно, но некоторые родители слышат прямое утверждение и игнорируют его. Они либо не понимают, что на самом деле означает «взлом», или хотят верить, что их ребенок не делает ничего глупого или неправильного. К сожалению, иногда это так.

Чрезмерная секретность в Интернете

Каждый ребенок хочет 100 %-ной конфиденциальности. Дети, занимающиеся взломом, пойдут еще дальше, чтобы скрыть свою деятельность. Я говорю о полном удалении всего, что они делают в Интернете. Их история браузера всегда пуста, а лог-файлы чисты. Вы не сможете найти новые файлы или папки. Все скрыто. Отсутствие какой-либо активности – серьезный признак того, что они намеренно скрывают что-то, что может привести к большим неприятностям. Кроме того, очистка истории браузера может скрывать и другие виды деятельности.

Тайные аккаунты в соцсетях или адреса электронной почты

Обычно у детей есть несколько учетных записей электронной почты и социальных сетей. В данном случае важен вопрос доступности. Если у ребенка есть электронная почта и учетная запись в социальных сетях, которые они от вас не скрывают, но вы обнаруживаете признаки того, что есть и другие, которые они держат в секрете, то велика вероятность, что что-то происходит.

Вы нашли хакерские инструменты на его компьютере

Если вы найдете хакерские инструменты, вроде тех, что описаны в этой книге, или которые, как правило, используются для взлома веб-сайтов, то есть большой шанс, что ваш ребенок заинтересован во взломе.

Люди жалуются на взломы

Несколько раз в тот период, когда мой сын занимался хакерством, я получал электронные письма и звонки от незнакомых людей, и даже интернет-провайдер предупреждал, что если я продолжу свою деятельность, он отключит нам Интернет или даже заявит в полицию. Сначала я был в замешательстве: я-то никого не взламывал. Но оказалось, это делал мой сын.

Ребенок выключает экран, когда вы входите в комнату

Дети могут выключать экран, чтобы скрыть любую из многих вещей (например, порнографию или общение с подругой/парнем), но если такое происходит каждый раз, стоит обратить на это внимание.

Эти признаки могут быть нормальными

Тем не менее совершенно не обязательно, что эти признаки говорят о плохом. Ваш ребенок может не быть хакером, я лишь пытаюсь поделиться некоторыми из признаков, так что вы не будете пойманы врасплох, как мы с женой, как и многие из читателей, которые писали мне об этом. Осведомленность – это хорошо. Я не сомневаюсь, что многие читатели и их дети, прочитав об этом, скажут, что каждая из перечисленных выше вещей имеет место быть, но при этом никто не был вовлечен в незаконный или неэтичный взлом.

Клубы робототехники

Найдите любые местные клубы робототехники. Многие школы и вендоры компьютеров спонсируют клубы, специально предназначенные для молодых хакеров, и лидеры, как правило, на высшем уровне. Если вы не можете найти местный клуб, RoboRealm (**http://www.roborealm.com/clubs/list.php**) и Arrick (**http://arrickrobotics.com/clubs.html**) отлично подойдут для начала.

Примечание. Еще одно хобби и клуб для начинающих хакеров – клуб радиолюбителей. Многие мои друзья-хакеры – давние радиолюбители.

Конкурсы Capture the Flag

Многие школы, веб-сайты, группы и конференции по безопасности спонсируют конкурсы Capture the Flag, где отдельные хакеры или команды соревнуются, чтобы увидеть, кто может успешно взломать что-то первым и получить приз. Просто введите «конкурсы Capture the Flag» в любую поисковую систему в Интернете, и вы увидите десятки конкурсов, к которым вы или ваш ребенок можете присоединиться. Этот веб-сайт показывает много различных предстоящих конкурсов: **https://ctftime.org/**.

Обучение и сертификация

Прохождение обучения или получение сертификата – отличный способ направить юношеский хакерский потенциал в нужное русло. Бросьте вызов своему ребенку, чтобы доказать, насколько он хорош, получив сертификат информационной безопасности (некоторые из которых рассматриваются в главе 41). Получение авторитетного сертификата, например от EC–Council (**https://www.eccouncil.org/Certification/certified-ethical-hacker**), – это отличный способ узнать что-то новое и в итоге сделать на этом карьеру. За мои почти 30 лет взлома я узнавал новое и ценное из каждой сертификации, которую заработал, что сделало меня лучшим хакером.

Поиск хорошего наставника

Наконец, попробуйте свести ребенка с тем, кто прошел через тот же опыт и смог превратить новообретенное творчество в законную и прибыльную карьеру. Если вы больше никого не знаете, рассмотрите меня (**roger_grimes@infoworld.com**). Я буду счастлив добавить вашего ребенка в список людей, которых наставляю.

Обычно я даю те же рекомендации, что и здесь, но также могу познакомить их с умными, хорошими хакерами. Большинство детей ошибочно полагают, что хакеры «в черных шляпах» самые умные. Но каждый год в лучшем случае всего один плохой хакер делает что-то новое и интересное. Остальные просто следуют тому, что уже было придумано. Бесспорно, лучшие хакеры, которых я встречал, всегда были специалистами по ИБ.

Легко взять кувалду и уничтожить автомобиль, но гораздо сложнее построить его. Хотите впечатлить меня? Будьте человеком, который строит то, что может противостоять постоянным вызовам со стороны злонамеренных хакеров.

Если вы подозреваете, что ваш или чей-то еще ребенок может быть замешан в неэтичном или незаконном взломе, покажите им эту книгу. Подростков, которые любят взлом, всегда можно привлечь на хорошую сторону. Если уж на то пошло, то и взрослых тоже.

А мой сын-хакер? Он отлично справляется в жизни. Успешно работает с компьютерами, зарабатывая много денег. Он замечательный сын, отец и этичный человек. Я его очень люблю. Мы оглядываемся назад и смеемся над теми днями, когда были против него в цифровом мире. Он благодарит меня и маму за то, что мы вмешались и предоставили ему небольшое руководство, чтобы помочь отойти от темных аспектов взлома.

50. Кодекс чести хакера

Если вы будете искать в Интернете «кодекс этики хакеров», то, скорее всего, найдете гламурную версию так называемых «хакерских правил», которые позиционируют идею того, что хакеры могут делать все, что хотят, без ограничений, в погоне за тем, к чему стремятся. Стивен Леви, автор бестселлера *Hackers: Heroes of the Computer Revolution* (**https://www.amazon.com/HackersComputer-Revolution-Steven-Levy/dp/1449388396/**), представил миру одну из самых ранних версий хакерской этики (**https://en.wikipedia.org/wiki/Hacker_ethic**). В двух словах, почти слово в слово, он сказал следующее.

1. Доступ к компьютерам должен быть неограниченным и полным.

2. Вся информация должна быть бесплатной.

3. Недоверие к власти – содействие децентрализации.

4. Хакеры должны оцениваться по их взлому, а не по таким критериям, как степень, возраст, раса или положение в обществе.

5. Вы можете создавать искусство и красоту на компьютере.

6. Компьютеры могут изменить вашу жизнь к лучшему.

Леви делился тем, что многие хакеры чувствовали по поводу первых дней взлома. К сожалению, многие из них приняли этику Леви, чтобы обозначить, что цели оправдывают средства и даже незаконная деятельность в порядке вещей. Это все равно что сказать, что ограбить банк или забрать чужую собственность – нормально, если вы отдаете ее, чтобы изменить свою или чужую жизнь к лучшему. Взлом без морального компаса может привести к неэтичным ситуациям и незаконности. Но более того, это навредит всем нам.

Несмотря на то что заявления Леви были сделаны более чем за десять лет до того, как появилась информационная супермагистраль, даже он не способствовал откровенному беззаконию и неэтичной деятельности. Хотя

некоторые из людей в его книге делали этично сомнительные вещи, большинство этого избегали. Многие улучшили жизнь для себя и общества, не совершив ни одного незаконного поступка. Многие бескорыстно посвятили свою жизнь обогащению жизни других людей. Там, где одни хакеры видели этику Леви беззаконной и свободной для всех, большинство читателей и начинающих хакеров нашли красоту в этичном сотрудничестве. Хакеры в книге Леви, возможно, начинали как децентрализованные, не доверяющие свободным мыслителям, но в конце концов то, что они узнали, создали и изобрели, изменило мир к лучшему.

Если бы информация была по-настоящему бесплатной, это уничтожило бы стимул для лучших художников и писателей мира создавать замечательные вещи. Даже Стивен Леви хотел, чтобы ему заплатили за написание книги. Большинство вендоров оборудования и программного обеспечения не станут делать свою работу, не будучи в состоянии заработать на жизнь. Кто-то ведь должен оплачивать счета за работу, которая прокладывает информационную магистраль. Если бы создатели и владельцы не могли взимать плату за свою информацию и творения, у нас было бы гораздо меньше и того, и другого. Если бы мы взяли оригинальную хакерскую этику в ее самой строгой интерпретации, не рассматривая моральную этику, наше общество не было бы таким великим. На самом деле хакерство без этичных соображений общего блага просто очернит его.

Кульминация этой книги заключается в демонстрации того, что лучший взлом – это этичный и законный взлом. Все, кто описан в этой книге, использовали свои удивительные умственные способности на благо человечества.

Наиболее важный руководящий принцип для взлома – то, что вы не причините зла даже за хорошие деньги. Поставьте этику выше денег и славы. Это не означает, что вы не можете получить прибыль или известность, но сделать это нужно законным и этичным способом.

Сегодня многие организации, обучающие информационной безопасности, имеют этичный кодекс поведения, который вы должны соблюдать, чтобы быть сертифицированным ими. Самый популярный кодекс этики хакеров, который я могу найти в Интернете, – Кодекс этики EC–Council (**https://www.eccouncil.org/code-of-ethics/**). Это хороший пример, но слишком сосредоточенный на тестировании на проникновение. Поэтому я создал свой четкий, краткий кодекс этики для работы, как личной, так и профессиональной.

Кодекс чести хакера

Это мой личный Кодекс этики хакеров, которого я придерживался всю свою жизнь. И я думаю, что это хорошая отправная точка для любого хакера, ищущего этичного руководства.

Будьте этичным, прозрачным и честным

Само собой разумеется, что следование кодексу этики означает быть этичным. Этика подразумевает противостояние добра и зла, справедливости и несправедливости. Столкнувшись с дилеммой, делайте то, что принесет наибольшую пользу обществу. Будьте прозрачны в том, что вы делаете, будучи уверенными, что позволяете либо наблюдение, либо адекватное общение со всеми заинтересованными сторонами. Озвучьте, что вы будете делать, а затем сделайте это.

Не нарушайте закон

Следуйте законам, которые управляют вами и вашей деятельностью. Если этичный вопрос заставляет вас нарушить закон, убедитесь, что вы попробовали все методы и ваши действия, вероятно, будут рассматриваться как направленные на общее благо. Большинство незаконных ситуаций являются таковыми, потому что общество определило, что все работает лучше определенным образом, даже если вы считаете, что у вас есть веские основания для нарушения закона. Будьте готовы жить с последствиями нарушения этих законов, если вас поймают.

Получите разрешение

Всегда получайте предварительное документальное разрешение от владельца или законного представителя, прежде чем взломать актив. Без исключений.

Будьте конфиденциальны с защищенной информацией

Общество ломается без доверия. Часть доверия, помимо этичности, прозрачности и честности, означает неразглашение конфиденциальной информации без предварительного разрешения владельца, особенно если эта информация была предоставлена вам конфиденциально. В общем, чем меньше личной и конфиденциальной информации вы рассказываете, тем более надежным люди будут вас видеть. Я всегда получаю соглашение о неразглашении (NDA), подписываемое новыми клиентами. Это заставляет нас чувствовать себя увереннее. Если вы собираетесь сломать чье-то доверие, убедитесь, что это этично, законно и лучше для общества в целом.

Не причиняйте вреда

Клятва Гиппократа должна распространяться на общество в целом, а также на любые компании или клиентов, на которых вы работаете. Все хакеры должны ему следовать. Хакеры и профессиональные тестировщики на проникновение должны начинать каждое действие с оценки возможного ущерба. Минимизируйте сбои. Всегда начинайте любую операцию, которая может привести к сбою в среде, осторожно. Затем используйте наименее разрушительные настройки вашего программного обеспечения, если такие параметры существуют. Выполняя взлом, всегда предупреждайте клиентов (в письменной форме), что ваши действия могут нанести непреднамеренный вред их среде. Кроме того, не делайте публичного раскрытия уязвимостей ПО без

предварительного уведомления вендора и предоставления ему достаточного времени для создания исправления. Иначе вы можете навредить клиентам.

Ведите себя профессионально

Стремитесь быть профессионалом во всех видах деятельности. Это не означает, что вы должны носить костюм, но необходимо действовать таким образом, чтобы люди находили вас заслуживающим доверия. Это возвращает нас к этичности, честности и прозрачности. Хорошее общение – залог профессионализма. Это также означает использование настоящего имени (чтобы можно было легко вас идентифицировать).

Станьте примером для других

Наконец, будьте примером, ведя этичную хакерскую жизнь. Используйте свои силы во благо и для улучшения общества. Покажите другим, как ваша хакерская этика улучшает жизнь каждого.

Пусть ваше хакерское поведение определяется сочетанием «хакерской этики» Леви и истинно этичных принципов, предложенных в этой главе. Объявите себя этичным хакером и гордитесь этим. Как и все люди, описанные в этой книге, вы можете хорошо зарабатывать на жизнь и делать все необходимые взломы этичным и законным способом. Самые великие умы – это не злонамеренные хакеры, а специалисты по ИБ, которые взламывают хакеров.