Взламываем Хакера

Часть II

Учимся у экспертов борьбе с хакерами

Роджер А. Гримс

Перевод: @Samigg
http:\\skladchik.com

Глава 15. Профиль: Дороти Э. Деннинг

За десятилетия работы, я начал верить, что один из моих особых талантов в информационной безопасности - обнаружение киберпреступников и их действий. Я могу увидеть направление потенциальной хакерской угрозы и определить, каким способом можно быстро обнаружить эту угрозу и сгенерировать оповещения. Я все еще думаю, что у меня это получается лучше, чем у всех остальных, но было время, когда я думал, что у меня оригинальное представление об обнаружении вторжения/аномалии. Я даже возомнил себя особенным. Затем я узнал о выдающемся документе Доктора Дороти Э. Деннинг для IEEE (Института инженеров электротехники и электроники) по экспертным системам обнаружения вторжений в реальном времени (https://users.ece.cmu.edu/~adrian/731-sp04/readings/denning-ids.pdf). В нем было описано все, что я считал своим оригинальным представлением, но дело в том, что Доктор Деннинг написала этот документ в 1986-ом, задолго до моего собственного "открытия".

Это был первый из многих случаев, когда я узнал, что мое "оригинальное" представление, на самом деле, совсем не оригинальное. Мы все стоим на плечах гигантов, и Доктор Деннинг, определенно, является гигантом в информационной безопасности. Она была одним из первых пионеров в этой сфере. Она сказала: "Когда я начинала, не было сферы информационной безопасности. Не было ни книг, ни журналов, которые можно было прочитать, не было конференций, посвященных безопасности, на которые можно было бы прийти. Все, что мы могли прочитать - это докторские диссертации и несколько документов, опубликованных в журналах более широкой тематики, таких как *Communications of the ACM*. Но мне посчастливилось оказаться в Университете Пердью, одном из первых университетов, начавших работу в области информационной безопасности, наряду с Массачусетским технологическим институтом и некоторыми другими".

Когда Доктор Деннинг только начинала учиться в колледже, ей нравилась математика, и она видела себя преподавателем математики в старших классах. Когда она получала степень бакалавра по математике в Мичиганском университете, она стала работать на заведующего радиоастрономии, который вдохновил ее изучать программирование для решения некоторых задач. Позже, в Рочестерском университете, она создала транслятор командного языка, с помощью которого стало легче запускать программы на мейнфреймах IBM, она также разработала и преподавала курсы по языкам программирования и компиляторам. Ее любовь к преподаванию мотивировала ее на получение

докторской степени в Университете Пердью, где она брала курс по операционным систем у своего будущего мужа, Питера Деннинга. Этот курс включал принципы информационной безопасности на уровне ОС. Так зародилось ее пожизненное стремление к улучшению информационной безопасности. Она даже была одним из первых преподавателей курсов по информационной безопасности в стране.

ПРИМЕЧАНИЕ Транслятор Доктора Деннинг переводил команды Рочестерского языка Easy Control Language на язык IBM Job Control Language, с которым, по мнению пользователей, было сложно работать.

Доктор Деннинг получила свою докторскую степень в 1975-ом, создавая решеточную модель безопасности, которая, по сути, является структурой классификации информации, образующей решетку таким образом, что информация через эту решетку может идти только в одном направлении, и только от низших к высшим или равным классификациям. Сегодня, концепция одностороннего потока информации все еще остается ведущей для "оригинального" представления об информационной безопасности. В основе двух из последних проектов, над которыми я работал в Microsoft - защищенные администраторские рабочие станции (https://msdn.microsoft.com/en-us/library/mt186538.aspx) и проект «red forest» Enhanced Security Admin Environment (Усовершенствованная среда администратора безопасности) (https://technet.microsoft.com/windows-server-docs/security/securing-privileged-access/securing-privileged-accessreference-material) - лежит определенный поток информации, который следует тем же правилам.

Работа Доктора Деннинг позволила применить математическую решеточную модель в сфере защиты информации. Она говорила: "Я долго думала о классификации и защите данных, и, когда я придумала модель и объединила ее с математикой, я решила, что это довольно оригинально. Я поделилась своими теоремами и доказательствами с мужем, и он проинформировал меня, что это была *теория решеток* и сказал мне имя эксперта (Гаррет Биркгоф), который написал об этом книгу. До того момента, я была уверена, что придумала новую математическую теорию". После истории Доктора Деннинг мне стало легче, я понял, что я не единственный "первооткрыватель".

Доктор Деннинг опубликовала свой документ "Решеточная модель безопасного потока информации" (http://faculty.nps.edu/dedennin/publications/lattice76.pdf) в 1976 году. Так теория решеток стала применяться в сфере защиты информации. Весь ее документ состоит из простых объяснений и математических формул, хотя в нем нет точного способа непосредственного применения этой модели в операционной системе. Даже при том, что она сама никогда не применяла эту модель, ее тезис и последующий документ

(http://faculty.nps.edu/dedennin/publications/CertificationProgramsSecureInfoFlow.pdf) описывали способ изменения компилятора таким образом, чтобы определялись потоки программ. Разработчики использовали этот документ для реализации ее модели.

Одной из главных тем работы Доктора Деннинг была защита личной информации, несмотря на то, что последняя обрабатывалась на программном уровне. Она сказала: "Я думаю, что реальным примером может быть ситуация, когда вы отправляете налоговую декларацию в сервис по расчету налогов или используете ПО для обработки этих данных. ПО или сервис должны обработать декларацию, но при этом личная информация не должна попасть в руки посторонних".

Я спросил, как, по ее мнению, сегодня обращаются с личной информацией. Она ответила: "Ну, недостаточно хорошо. Посторонние люди постоянно крадут эту информацию и получают к ней доступ. В данный момент, многие компании не прикладывают достаточно усилий для защиты информации".

В 1982-ом Доктор Деннинг написала учебное пособие, оказавшее существенное влияние на индустрию *Cryptography and Data Security* (https://www.amazon.com/Cryptography-Security-Dorothy-Elizabeth-Robling/dp/0201101505). Настоящая причина, по которой она написала эту книгу, заключалась в том, что она не могла найти необходимую книгу, для преподавания курса по этому предмету. Это была первая из нескольких книг и из более, чем 170 статей, которые она написала за свою карьеру. В 1983-ем она начала работать в SRI International, некоммерческом исследовательском институте, основанном членами правления Стэнфордского университета. Она разрабатывала систему обнаружения вторжений для ВМФ, результатом чего стало учебное пособие по обнаружению вторжений, которое я упомянул в начале главы.

Затем она перешла в Digital Equipment Corporation (DEC), в которой в то время хотели работать многие специалисты компьютерной индустрии, результатом работы которой стали тысячи патентов в компьютерной сфере. В итоге, именно во время работы в DEC она брала интервью у группы хакеров, она хотела понять их мотивы и психологию. И в результате этой работы появилось огромное количество научных работ. Она брала у хакеров интервью и работая над предотвращением их нелегальной деятельности. В то время такой подход считался довольно спорным. Хотя поиск противоречий не был ее целью, очевидно, что она их не боится, когда ищет решения. Противоречия - это еще одна тема, которая периодически появляется в ее работе, когда она сдвигает границы и побуждает к дискуссии. В одном из давних интервью, Доктор Деннинг выразила сожаление, по поводу того, что иногда эмоции других людей относительно определенной проблемы, мешают так необходимому открытому обсуждению.

Она ушла из DEC в 1991-ом, чтобы вернуться в научное сообщество в Джорджтаунском университете, где она преподавала курс по информационной войне, будучи заведующим Georgetown Institute of Information Assurance (Института обеспечения доступности, целостности и безопасности информации). Затем, в 2002-ом, она ушла в Naval Postgraduate School (Высшая школа ВМС США), будучи профессором кафедры анализа защиты (Department of Defense Analysis), где и работает до сих пор. Свою последнюю книгу *Information Warfare and Security* она написала в Джорджтаунском университете, в 1999-ом, (https://www.amazon.com/Information-Warfare-Security-Dorothy-Denning/dp/0201433036/). Она сказала, что не написала после этого ни одной книги, потому что ей слишком сложно быть в курсе событий в этой сфере, и она не хотела писать книгу, которая устареет еще до публикации.

За свою карьеру, она получила множество наград, которыми гордился бы любой специалист по информатике, включая Ada Lovelace Award (http://awc-hq.org/ada-lovelace-awards.html) и National Information Systems Security Award (https://www.acsac.org/ncss-winners.html). В 1995-ом она стала лауреатом премии Ассоциации вычислительной техники (http://awards.acm.org/award_winners/denning_1239516.cfm), а в 2012-ом ее представили в зал славы национальной кибербезопасности (http://www.cybersecurityhalloffame.com).

Так как в конце 2016-го Доктор Деннинг официально вышла на пенсию, я спросил ее, будет ли она еще работать над проблемами информационной безопасности. Удается ли ей не работать после стольких лет работы? Она сказала: "Я оставлю себе офис и т.к. я эмерит – это значит, что я могу делать все, что захочу, не получая в нагрузку слишком большой ответственности. Я все еще активно работаю над несколькими проектами. Сейчас я готовлюсь что-нибудь написать. Но мне также нравится заниматься пешим туризмом. Это очищает разум". Я думаю, любой профессионал хотел бы иметь такую же продолжительную карьеру и оказать такое же влияние на мир, как Доктор Деннинг.

Подробнее о Докторе Дороти Э. Деннинг

Подробнее о Докторе Дороти Э. Деннинг вы можете найти на этих ресурсах:

- Подкаст Silver Bullet Гэри МакГроу, где он берет интервью у Доктора Дороти Э. Деннинг: https://www.cigital.com/podcasts/show-011/
- Транскрипция интервью с Доктором Деннинг Института Чарльза Бэббиджа: https://conservancy.umn.edu/bitstream/handle/11299/156519/oh424ded.pdf

Глава 16. Профиль: Майкл Дубинский

Я уже давно очень придирчиво отношусь к продуктам для обеспечения информационной безопасности. Сложно относиться к ним по-другому, зная, что за два десятилетия вредоносное ПО и эксплойты, судя по всему, стало проще применять, особенно, учитывая тот факт, что почти каждое новое средство, гарантирующее безопасность, на деле оказывается совсем не таким эффективным, как его позиционировали. Я зарабатываю тем, что проверяю такие средства, часто, мне дают на проверку по двадцать штук в день. Если за год попадается хотя бы одно, которое действительно умеет делать то, что обещает, и может значительно снизить риск взлома, я впадаю в экстаз. Я часто годами не вижу ничего стоящего. Также, моей критике нередко подвергаются продукты моих нанимателей.

В связи с этим, я действительно был потрясен новым средством Microsoft, которое называется «Advanced Threat Analytics (ATA)». Оно бы мне понравилось, даже, если бы его создали не Microsoft. ATA действительно использует расширенный анализ событий и сетевого трафика, что позволяет обнаружить активные угрозы, включая те угрозы, которые многие эксперты считают сложными для обнаружения, такие, как атаки Pass-the-hash (https://en.wikipedia.org/wiki/Pass_the_hash) или Golden Ticket (http://www.infoworld.com/article/2608877/security/fear-the-golden-ticket-attack-.html). После наблюдения за работой этой платформы, я понял, что она настолько хороша, что я хочу бросить то, чем занимаюсь, и работать только над продвижением ATA. И я не утрирую. Я бы действительно сменил работу, если бы мне предоставили возможность. Настолько хороша эта платформа.

ATA появилась в результате покупки Microsoft израильского стартапа Aorato, в ноябре 2014-го. Каждый год в сфере информационной безопасности появляются тысячи стартапов. Те, кто хоть раз работал над стартапом, знают, что это требует многих часов напряженной работы, иногда без выходных, в окружении коллег, которые также увлечены этим проектом. Я знаю многих людей, которые “перегорели”, работая над так и не вышедшим стартапом. Они рисковали всем, получая маленькую зарплату, вкладывая много сил, чтобы получить итоговое вознаграждение, которого так и не последовало. Мой двоюродный брат Ричард А. Граймс часто работал в ранних интернет-стартапах, и, однажды, он сказал мне: “Если еще один стартап предложит мне оплату с будущей прибыли, я скажу им, что покупать продукты и оплачивать счета за электричество нужно сейчас, а не с будущей прибыли”.

Израильтянину Майклу Дубинскому повезло. Через полгода, после того, как он пришел в компанию Aorato, ее купили Microsoft. Сейчас он главный руководитель производственного направления ATA. Он все также много работает, но теперь в комфортных условиях большой корпорации.

Из-за трудностей существования Израиля и израильтян, в маленькой стране появились невероятные средства информационной безопасности. Израильские компании всегда разрабатывают новые и продвинутые системы информационной безопасности. Несколько лет назад, меня наняли преподавать технологию работы honeypot для армии обороны Израиля (ЦАХАЛ), где должен отслужить каждый гражданин Израиля. Всю свою карьеру я использовал honeypot и преподавал принцип их работы, и даже написал про них книгу. Но когда я пришел, молодые парни и девушки из ЦАХАЛ меня поразили. Они уже знали почти все, что я знал, и уже использовали самые классные honeypot, которые я собирался им показать. Мне нужно было только помочь им сделать их honeypot еще более реалистичными и привлекательными.

Тогда я узнал, что мой опыт, такой же, как у других иностранцев, приезжающих в Израиль преподавать информационную безопасность. В Израиле о защите страны от киберугроз думают больше, чем где-либо еще. Во время моего визита, по Тель-Авиву было выпущено несколько ракет. В классе было 20 человек, и я спросил, сколько из них видели выпущенную по ним ракету, которая, скорее всего, приземлилась бы где-то рядом с ними, если бы ее не остановили. Практически все подняли руку. Жизнь в таких условиях меняет приоритеты и перспективы. Она также способствует созданию эффективных средств информационной безопасности.

Я спросил Дубинского, прожил ли он всю жизнь в Израиле. Он сказал: "Я родился в Латвии, это в Восточной Европе, Балтийский регион. После Второй Мировой этот регион был частью СССР, пока не провозгласил свою независимость в 1990 году. Примерно в то же время, мы с родителями переехали в Израиль. Я вырос в пригороде, на юге от Тель-Авива".

Я спросил Дубинского, как он попал в сферу информационной безопасности. Он ответил: "Меня с детства интересовали компьютеры, а один из моих соседей был инженером ПО, и он сильно мне помог. Я начал возиться с компьютерами, программировал на BASIC и Pascal, и изучал дизассемблеры. Позже я увлекся троянскими программами удаленного доступа (remote access Trojans, RAT), такими как SubSeven (https://en.wikipedia.org/wiki/Sub7). Это было действительно интересно, и я начал использовать эти программы для розыгрыша друзей. Используя социальную инженерию или фишинг, я делал так, чтобы мои друзья устанавливали их, а затем развлекался, открывая их CD-ROM. Позже, я перешел от розыгрыша друзей к краже чужих учетных данных для входа в интернет. Это было во времена dial-up модемов и дорогого интернета. Чтобы украсть чужие учетные данные для входа в интернет, я использовал те же хакерские навыки, которые применял для розыгрыша

друзей. Я добился цели, но, также, был пойман. Мои родители были очень расстроены и забрали у меня компьютер. Позже, когда я служил в армии Израиля, я работал над информационной безопасностью. Особенно, меня интересовала аутентификация, и то, как сделать ее максимально эффективной".

Я спросил, как он попал в Aorato. Он ответил: "В 2014 году я стал тринадцатым работником в компании, которой, на тот момент, было два года. Я сразу начал работать над инженерными проблемами, и выяснял, как можно увеличить процент обнаружения вредоносного ПО. В основе всегда было два направления деятельности. Для одного направления, целью было выявить новые способы обнаружения, для другого - улучшение конечного продукта, расширяя его возможности обнаружения. Я проработал в Aorato всего шесть месяцев, перед тем, как их купили Microsoft. Microsoft обеспечили нам 100% поддержки и доверия. Мы продолжаем работать с отличными людьми и делаем качественный продукт.

Я спросил Дубинского, что, по его мнению, является главной проблемой информационной безопасности. Он сказал: "Образование. В конечном счете, большинство людей на что-то нажимают. Неважно, какие технологии защиты применяются, люди все равно что-нибудь нажмут. Образование - ключ к предотвращению атак".

Подробнее о Майкле Дубинском

Подробнее о Майкле Дубинском:

- Твиттер Майкла Дубинского: https://twitter.com/michaeldubinsky

Глава 17. Файрволы

Файрволы - отличный пример технологий, которые стали жертвами своего же успеха. На протяжении трех десятилетий файрволы так хорошо справлялись со своей задачей, что угрозы, против которых они создавались, практически перестали существовать. Плохие парни сдаются! По крайней мере, в одном направлении. Некоторые эксперты даже утверждают, что файрволы больше не нужны, но большинство экспертов уверено, что файрволы, как и сканеры вредоносного ПО - это необходимый элемент для обеспечения информационной безопасности в любой системе.

Что такое файрвол?

Если кратко, то файрвол - это ПО или аппаратный компонент, созданный для предотвращения несанкционированного доступа между двумя или более границами безопасности. Традиционно, его работа основана на названии протокола или номере порта, а на сетевом уровне, как правило, используется фильтрация пакетов. Многие файрволы могут также разрешать или запрещать передачу трафика на основе имен пользователей, названии устройств, принадлежности к группе и информации, полученной из верхних уровней трафика приложений. Часто в файрволах есть расширенный функционал и дополнительные возможности, такие, как анализ пакетов высокого уровня, обнаружение/предотвращение вторжений, обнаружение вредоносного ПО, а также VPN. Во многих файрволах есть подробные лог-файлы. Как правило, после включения файрвола, его журнал событий тут же заполняется записями.

Ранняя история файрволов

Программа, которую впоследствии стали считать ранним файрволом на уровне приложений, была создана в 1987-ом, администраторами AT&T Bell Labs Дэйвом Пресотто и Говардом Трики на компьютере VAX, под управлением BSD, с двумя сетевыми интерфейсами. Она была необходима для того, чтобы защитить внутренних пользователей и компьютеры. Их программа позволяла внутренним пользователям получать доступ в интернет, но запрещала несанкционированные входящие подключения. Они использовали собственный шлюз сеансового уровня, который появился, примерно на семь лет раньше, чем в протоколе SOCKS-прокси, ставшем, в итоге, очень популярным. Позже, в начале 1988-го, Уильям Чесвик использовал такой же шлюз.

ПРИМЕЧАНИЕ Слово "файрвол" использовалось в фильме *Хакеры* 1983 года, однако в фильме не было четкого определения.

В технической документации файрвол впервые упоминался в 1987-ом, на презентации Джеффри Могула (лауреата премии Ассоциации вычислительной техники, который на данный момент работает в Google [https://research.google.com/pubs/JeffreyMogul.html]), Ричарда Ф. Рашида и Майкла Дж. Ачетта, которая называлась "The Packet Filter: An Efficient Mechanism for User-level Network Code (Фильтр пакетов: эффективный механизм регулирования сетевого кода на уровне пользователя) и прошла на симпозиуме ACM, посвященному основам операционных систем.

В ноябре 1988-го, сеть, защищенная файрволом Чесвика, подверглась атаке нашумевшего Червя Морриса (https://en.wikipedia.org/wiki/Morris_worm). Благодаря удачному стечению обстоятельств и предварительному изменению настроек, файрвол и компьютеры под его защитой, остались нетронутыми, в то время, как сотни других сетей и тысячи других компьютеров были заражены. Это был один из первых случаев, когда файрвол доказал свою ценность для информационной безопасности при реальном использовании. Чесвика беспокоил момент с удачным стечением обстоятельств, он обновил оригинальную конфигурацию файрвола, добавив еще одну границу зоны безопасности между внутренним и внешним интерфейсами. Впоследствии, он назвал эту конфигурацию прокси, и это был первый случай, когда слово "прокси" было использовано в таком контексте.

Чесвик описывал файрволы в трудах USENIX в 1990-ом, а также в 1994-ом в основополагающей книге о файрволах *Firewalls and Internet Security: Repelling the Wily Hacker*, в соавторстве со Стивеном Белловином. Чесвик так вспоминает удивительную популярность этой книги: "Файрвол Checkpoint Firewall Zone 1 (который, в итоге, был переименован в Checkpoint Firewall) впервые появился весной 1994-го, на конференции Interop в Лас-Вегасе, то есть, примерно, через неделю после публикации нашей книги. Наш издатель ожидал, что тираж книги составит 8 000 - 12 000 копий. Первая партия в 10 000 копий была продана за неделю, и они так быстро выпустили вторую партию в 20 000, что мы не успели исправить недоработки. Всего было продано около 100 000 копий, переведенных, примерно, на десяток языков. Эта книга вышла в самый подходящий момент".

Брайан Рид вместе с другими сотрудниками Digital Equipment Corporation (DEC) также работал над файрволами, устанавливая связь между корпоративной сетью DECnet и интернетом. Однако, их файрвол больше фокусировался на блокировке исходящего доступа, так как раньше DEC потеряли важное ПО в результате утечки данных.

Маркус Ранум написал первый серьезный коммерческий файрвол для DEC в 1990-ом, а его следующая версия называлась Screening External Access Link

(SEAL) и была написана совместно с Джеффом Муллиганом в 1991-ом. В то же время, Джеффри Могул выпустил screend, один из первых файрволов (https://www.researchgate.net/publication/2443301_Using_screend_to_Implement_IPTCP_Security_Policies). Затем последовали коммерческие файрволы от многих других производителей, включая TIS Gauntlet, Checkpoint, Raptor Eagle от DuPont. В 1993-ем Ранум создал бесплатный Firewall Toolkit, как часть проекта для DARPA (организации, которая отвечала за финансирование разработки ранней версии интернета) и Белого Дома.

Все эти действия привели к тому, что файрволы стали неотъемлемым компонентом в любой популярной операционной системе. В 2001 году Microsoft создали свой файрвол, который назывался Windows Firewall, и появился на Windows XP. После установки второго пакета обновлений, вышедшего в 2004-ом, он был включен по умолчанию. В результате этого изменения, огромное количество вредоносных программ не смогли проникнуть в операционные системы на базе Windows. Сегодня, во многих устройствах, включая ваш коммутатор, Wi-Fi-роутер и ТВ-приставку, есть настраиваемый файрвол.

Правила для файрволов

У всех файрволов есть правила (или порядок действий). Самое общее правило для файрволов выглядит так: по умолчанию разрешен весь исходящий трафик, но запрещены любые неопределенные входящие подключения, которые не были предварительно инициированы исходящими соединением. Самые безопасные настройки файрволов также запрещают исходящий трафик, неопределенный ранее. К сожалению, использование самых строгих правил часто вызывает затруднения в работе, поэтому, в большинстве случаев применяются правила по умолчанию.

Куда устанавливаются файрволы?

Файрволы могут быть установлены на сетевом уровне или, непосредственно, на компьютере.

Межсетевой экран

Традиционно, большинство файрволов - это сетевые устройства, расположенные между двумя (или более) сегментами сети. Единственное, что изменилось - увеличилось количество контролируемых сегментов, и увеличилось настолько, что сейчас файрволы могут одновременно контролировать десятки сегментов. Появляющиеся сегодня программно-определяемые сети (software-defined networks, SDN) содержат компоненты

передачи пакетов, которые могут отслеживать происхождение пакетов и сообщать о нем традиционным файрволам.

Персональный файрвол

Многие уверены, что нельзя доверять даже той сети, где установлен файрвол. Даже Чесвик как-то сказал, что внутри сети, защищенной файрволом, есть "мягкое, уязвимое место". Он имел в виду, что все компьютеры внутри сети должны быть правильно и безопасно настроены, чтобы защититься от угроз, которые могут обойти защиту файрвола.

В этом случае на помощь приходят персональные файрволы. Как правило, они также фильтруют сетевой трафик, но часто у них есть и дополнительные свойства, так как они работают непосредственно с хостом и его операционной системой. Например, файрвол Windows можно легко настроить, в зависимости от условий работы, для одного пользователя или группы. В Windows есть встроенный файрвол с более, чем 100 правилами, которые включаются операционной системой, даже если отключить приложение для настройки.

Многие пуристы информационной безопасности уверены, что каждый компьютер должен общаться только с точно определенными компьютерами, следуя самым безопасным, строгим правилам файрвола, которые четко определяют, какой трафик между этими компьютерами может быть разрешен, а какой нет. Такой сверхдетальный контроль считается Святым Граалем в области применения файрволов. К сожалению, сложность управления такими файрволами не дает им стать широко распространенными, за исключением редких случаев, когда нужно обеспечить сверхнадежную безопасность.

Расширенные файрволы

Файрволы с расширенным функционалом существуют уже несколько десятилетий, и, как правило, также используют традиционную фильтрацию пакетов, но при этом, предлагают дополнительные возможности. Традиционный файрвол может блокировать трафик по протоколу (имени или номеру порта), в то время, как файрвол с расширенным функционалом может осуществлять блокировку, основываясь на отдельном компоненте протокола (то есть фильтровать пакеты на основе их содержимого, это называется "deep packet inspection"). Также, такой файрвол может собирать множество пакетов для определения отдельного вида атаки. Традиционный файрвол может заблокировать определенное количество пакетов, но только файрвол с расширенным функционалом может сообщить, что на вас совершается DDoS-атака. Файрволы прикладного уровня отслеживают трафик приложений, обнаруживают вредоносную активность или предотвращают ее влияние на компьютер. Например, расширенный файрвол может заблокировать

переполнение буфера при подключении к серверу. Расширенные файрволы настолько распространены, что почти все файрволы можно назвать расширенными.

От чего защищают файрволы

Файрволы защищают от атак, основанных на несанкционированной передачи трафика. Как правило, самой главной угрозой, которую предотвращали файрволы, были удаленные атаки переполнения буфера уязвимых сервисов. Но, со временем, сервисы стали надежнее (в основном, благодаря тому, что их операционные системы стали безопаснее по умолчанию), а наличие файрволов значительно снизило эффективность таких атак. Таким образом, сегодня файрвол может защитить лишь от нескольких видов атак. Например, если после получения электронного письма пользователь запустит троянскую программу, то файрвол уже не поможет. Тем не менее, большинство людей уверены, что файрволы должны быть в каждой сети и на каждом устройстве, так как они доступны (часто бесплатные, и установлены по умолчанию) и могут защитить от определенных атак. В любом случае, это убеждение доказывает высокую эффективность файрволов.

В Главе 18 представлен один из первых создателей файрвола.

Глава 18. Профиль: Уильям Чесвик

Как уже говорилось в предыдущей главе, Уильям Чесвик - один из первых создателей современных файрволов. Он взял за основу принцип работы первого файрвола, файрвола канального уровня. В то же время употребление слова "прокси" в контексте информационной безопасности стало возможным благодаря ему. Чесвик - обладатель более десятка патентов, а также соавтор первой книги, описывающей файрволы *Firewalls and Internet Security: Repelling the Wily Hacker* (https://www.amazon.com/Firewalls-Internet-Security-Repelling-Hacker/dp/020163466X), которую он написал вместе со Стивеном Белловином в 1994-ом. Я интересовался файрволами еще до прочтения этой книги, однако, именно благодаря ней я получил большую часть своих знаний о файрволах, а потрепанный экземпляр почти двадцать лет стоял у меня на полке.

Его нашумевшая работа "An Evening with Berferd in which a Cracker Is Lured, Endured, and Studied" (Вечер с Берфердом в котором взломщик заманивается, допрашивается и изучается) (http://www.cheswick.com/ches/papers/berferd.pdf) познакомила многих из нас с honeypots. Благодаря Чесвику термин "jail" – это прямая команда в системе FreeBSD, а "chroot jail" - один из самых легких и популярных способов изолировать определенную подсистему в Unix и Linux. Мало кто оказал такое же значительное влияние на информационную безопасность, как он. Также, среди экспертов в сфере информационной безопасности, он - один из оптимистов, которые, при этом понимают, что еще многое нужно сделать.

Я спросил Чесвика, как он попал в AT&T Bell Labs, где работали многие таланты в области информационной безопасности. Он сказал: "В 1968-ом я интересовался химией, но увидел самые первые компьютеры и понял, что в будущем они будут более популярны, так что ими я тоже заинтересовался. И в конце концов ими я заинтересовался больше, чем химией. В итоге, я оказался в консалтинговой компании SET, в качестве специалиста технического профиля. Мы осуществляли технические работы для других компаний. После девяти лет работы, я познакомился с людьми в Bell Labs. Мне понравились и люди, и место, где они работают. Даже, если бы меня взяли уборщиком, я все равно был бы счастлив. Так что осенью 1987-го я проходил собеседование, чтобы туда устроиться. Собеседование со мной проводили гиганты - боги в своей области, такие, как Деннис Ритчи (создатель языка программирования C) и Кен Томпсон (один из создателей Unix, как и Ритчи). Я был уже безмерно счастлив, даже если бы все закончилось только этим собеседованием, но, по какой-то причине, я им понравился и стал частью их команды. В один из первых дней

работы, я подошел к Дэйву Пресотто (создателю первого файрвола) и попросил посмотреть на работу файрвола. И он согласился."

Я попросил у создателя файрвола канального уровня объяснить, что это. Он ответил: "Такой файрвол буквально воссоздает трафик, бит, за битом, между двумя (или более) интерфейсами. Каждый пакет пересоздается и изменяется таким образом, что для всех остальных участников сети, источником этих пакетов является именно файрвол. То есть, вне сети, защищенной этим файрволом, источником трафика является именно файрвол. Без его использования, источником трафика будет сам компьютер". Сегодня, у каждого файрвола эта функция работает по умолчанию.

Я спросил у Чесвика, как он встретился со своим будущим соавтором, Стивеном Белловином. Он сказал: "Стивен работал в Bell Labs еще до моего прихода. Дэйв Пресотто вел лекции по TCP/IP, на которых также присутствовал Стивен. Мы стали друзьями, и все время обсуждали файрволы и различные угрозы. В итоге мы создали "пакетный телескоп" (один из первых снифферов). В AT&T у нас была большая сеть, класса A, и в ней было столько IP-адресов, что мы не могли с ними справиться. В то время, разделение такой сети на подсети, не давало нужного результата. Поэтому я анонсировал «12-ю сеть», и решил посмотреть, что произойдет. Очень скоро мы стали получать по 25 мегабит входящего трафика каждый день. Большая часть была "смертельным трафиком" с других взломанных компьютеров. Мы многое узнали. Стивен рассказал об этом в своей публикации "There Be Dragons" (Там будут драконы) (https://academiccommons.columbia.edu/catalog/ac:126916). Благодаря полученным знаниям, мы, в итоге, сделали первый DNS-прокси. А после этого написали нашу книгу. Она вышла в самый подходящий момент, потому что других книг про файрволы не было, а сами файрволы уже были популярны. Мы продали много копий, и заработали немало денег".

Я спросил о его патентах. Я сам пытался получить несколько, и это очень сложно. Он сказал: "У меня было бы гораздо больше патентов, если бы я знал, что то, что мы делаем, можно запатентовать. Поначалу все казалось "очевидным" ("очевидный" - это действующий термин, означает "нельзя запатентовать"), точнее, я так думал. То, что мы делали, в общем смысле, казалось очевидным для меня и 12-ти других ребят, с которыми я это обсуждал. У меня даже были патентные поверенные, которые спрашивали, можно ли запатентовать то, над чем я работал. Я сказал нет, потому что это очевидно. Оглядываясь назад, если бы я тогда заткнулся, то сейчас у меня было бы гораздо больше фундаментальных патентов. Спустя много лет кто-то патентует твою работу, на которую, гораздо раньше, ты потратил много времени и сил. У меня даже есть несколько патентов и авторских прав, которые часто игнорируют, например карты интернета (http://cheswick.com/ches/map/), которые я сделал. Тогда, это была революция. Мы даже сформировали компанию Lumeta для создания карт. Сейчас я везде вижу свои интернет-

карты, и нигде не указан, как создатель. Недавно, я был на конференции, и один из выступающих показал мою карту интернета, на которой я, конечно же, не был указан, и, примерно, половина аудитории посмотрела на меня, потому что они знали, что это одна из моих карт. Другой пример - DNS прокси. У меня есть на них патент, но существует множество DNS прокси, и они игнорируют мой патент".

Я спросил Чесвика, что его больше всего волнует в информационной безопасности. Он ответил: "Проблемы остаются все те же. Почти ничего не меняется. Разве что Stuxnet, но старые проблемы никуда не делись. Еще с 1979-го мы знали, что пароли ненадежны, так почему их до сих пор используют? Сейчас я прорабатываю кое-что новое относительно паролей и аутентификации. Еще один пример - недавние DDoS-атаки на Dyn (http://dyn.com/blog/dyn-analysis-summary-offriday-october-21-attack/). Они стали возможны из-за наличия root-паролей сохраненных в прошивке устройств из интернета вещей. За написанный в открытом виде пароль, я бы отправил студента на пересдачу. Производители даже не стараются".

Тем не менее, Чесвик считает, что в будущем информационная безопасность станет значительно лучше. Он сказал: "Я много выступаю по всему миру, и одна из моих речей для выступления называется "Безопасность в интернете: Я думаю мы победим". Вот пример этой презентации: https://cacr.iu.edu/events/2016/bill-cheswick-comp-sec-we-can-win.php. Сейчас мы находимся на уровне Model T в информационной безопасности. Мы даже не стараемся что-то улучшить, но будем стараться. Сейчас мы видим несостоятельность рынка, но рынок решит эту проблему. В будущем, безопасность в интернете значительно улучшиться. Многие не верят моим словам, но это произойдет. Поначалу, те же проблемы были в других индустриях, но они выросли и стали лучше. То же самое произойдет с интернетом".

Я спросил, где произойдут самые значимые улучшения. Он ответил: "Меня все еще поражает, что на компьютере можно запустить случайное ПО. Даже, при наличии антивируса, это как установить камеру в ванной, чтобы наблюдать за бродягами, которых вы туда пустили. Операционное системы должны разрешать работу только проверенных приложений, и это происходит. Операционные системы уже начали двигаться в этом направлении".

Я спросил, почему понадобилось столько времени, чтобы улучшить информационную безопасность. Он ответил: "Есть много причин, но одна из главных - поддержка старого ПО. Это как с городами. Во всех городах есть проблемы с поддержкой старых зданий и улиц, построенных ранее, которые нельзя игнорировать".

Я спросил Чесвика, что, по его мнению, происходит в последнее время. Он сказал: "Одна из главных проблем заключается в отсутствии точного способа измерения безопасности ПО. Было много попыток придумать такой способ. Как

вообще должна выглядеть точная система измерений? Простой пример - измерение количества всех сервисов в вашей сети, где каждый сервис является потенциальным вектором атаки, соответственно, уменьшив количество сервисов, вы уменьшаете риск. Но это слишком простой пример. Также, можно посчитать количество фоновых программ ("демоны" в UNIX), с правами суперпользователя (setuid root, то есть, у программы появляются самые высокие права). Как и в предыдущем примере, чем их меньше, тем лучше. Но это также слишком простой пример. Еще один способ измерения безопасности, допустим, операционной системы - это стоимость нулевого дня на открытом рынке. В 2012-ом в журнале *Forbes* была опубликована статья на эту тему (http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-daysan-price-list-for-hackers-secret-software-exploits/#43f3035e6033). Цена этого эксплойта является фактором, определяющим сложность и целесообразность взлома программы или ОС. Например, цена эксплойта для ОС может составлять $500 000, но цена эксплойта для программы, которую часто взламывают - всего $50 000. Чем выше цена, тем лучше производитель работает над безопасностью.

Все, включая генерала, с которым я недавно разговаривал, хотят получить более точную систему оценки своих действий по улучшению безопасности. Им нужны конкретные цифры. Им нужна возможность показать, что в прошлом году у них было 27, а в этом - уже 63, и они делают большие успехи. Самой реалистичной была бы та система измерений, которая бы объединяла в себе все возможные параметры, которые можно измерить, чтобы получить итоговую картину. Это нужно каждому руководителю, включая того генерала. Сейчас, я много думаю об этой проблеме. Даже жалобы ФБР на то, что они не могут что-то взломать - это хороший знак. Информационная безопасность становится лучше".

Подробнее о Уильяме Чесвике

Подробнее о Уильяме Чесвике вы можете найти на этих ресурсах:

- Веб-сайт Уильяма Чесвика: http://www.cheswick.com/ches/index.html
- Книга *Firewalls and Internet Security: Repelling the Wily Hacker* (в соавторстве со Стивеном Белловином): https://www.amazon.com/Firewalls-Internet-Security-Repelling-Hacker/dp/020163466X
- Работа "An Evening with Berferd in which a Cracker Is Lured, Endured, and Studied": http://www.cheswick.com/ches/papers/berferd.pdf

Глава 19. Honeypots

Honeypot'ы заинтересовали меня в 1989-м, когда я прочитал книгу Клиффорда Столла *The Cuckoo's Egg* (https://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787), в которой он дал им определение и описал поимку иностранного шпиона. С тех пор, я одновременно использую 8 honeypot'ов для отслеживания вредоносных программ и действий хаккеров. Я нередко участвую в разработке профессиональных honeypot'ов, и даже написал про них книгу, которая называется «*Honeypots for Windows*» (Honeypot'ы для Windows) (https://www.amazon.com/Honeypots-Windows-Books-Professionals/dp/1590593359/). Я думаю, что все компании должны использовать honeypot'ы для улучшения защиты.

Что такое Honeypot?

Honeypot - это "поддельная" система, которая создается специально для обнаружения несанкционированных действий. В зависимости от цели администратора, honeypot может выступать в роли операционной системы, устройства, сетевого маршрутизатора, беспроводной точки доступа, принтера, и так далее. Honeynet - это объединение honeypot'ов. Honeypot можно использовать, развернув его на реальной системе, которую не используют в компании, либо развернув специальное программное обеспечение, которое эмулирует работу систем.

Эмуляция может работать на любом уровне модели OSI (Open Systems Interconnection): физическом, сетевом, транспортном, сеансовом, представительском, канальном или прикладном, а также на нескольких уровнях одновременно. Существует огромное количество бесплатных и коммерческих вариантов honeypot'ов, каждый предлагает различные возможности и уровень реализма. Однако, покупатель должен выбирать осторожно. На рынке есть варианты, которые продаются уже более десяти лет, хотя большинство honeypot'ов, платных и бесплатных, появилось всего несколько лет назад, стоит избегать решений, которые существуют уже давно.

Взаимодействие

"Уровень взаимодействия" honeypot'а зависит от того, как он эмулирует систему или работает на различных уровнях модели OSI. Honeypot "низкого

взаимодействия" просто повторяет самые простые подключения к портам и записывает лог-файлы. При подключении пользователю может быть показано окно для входа в систему, но, как правило, войти в систему нельзя. Honeypot "среднего взаимодействия" позволяет пользователю войти в систему, а также частично эмулирует работу реальной системы. В случае с веб-сайтами, honeypot'ы, как правило, эмулируют хороший, но статичный веб-сайт. Если это эмуляция FTP, то на сервер FTP можно войти с пользовательскими данными, скачать файлы и использовать различные команды. Honeypot "высокого взаимодействия" настолько повторяют работу реальной системы, что хакер, не сможет увидеть разницу между реальной системой и эмуляцией. Конечно, реальные системы лучше любой эмуляции, но, в долгосрочной перспективе, их сложнее настраивать и контролировать.

Для чего используют honeypot'ы?

Есть множество причин использовать honeypot'ы:

- В качестве системы раннего оповещения об обнаруженных вредоносных программах и хакерских действиях
- Чтобы узнать намерения хакера
- Чтобы исследовать действия хакеров и вредоносное ПО
- Для проведения экспертного анализа

Правильно настроенный honeypot - это невероятно полезный инструмент, в котором нет ничего лишнего, особенно это касается просмотра лог-файлов или создания оповещений безопасности. Например, лог-файлы файрволов заполнены десятками тысяч сообщений об отброшенных пакетах, большинство из которых, совсем не вредоносные. А даже, если там и есть вредоносный пакет, попробуйте разобрать, какой из бесконечного количества этих пакетов, вам нужен.

Honeypot - это ложная система, и ее суть в том, что никто (или ничто) не должен к ней подключаться. На настройку нужно потратить немного времени, отфильтровать обычный трафик с широковещательных каналов и попытки подключения от действительных источников (например, от программы обновления антивируса, различного ПО и других инструментов управления системой). Но, когда настройка honeypot завершена (как правило, это занимает от двух часов до двух дней), любая попытка подключения, по определению, является вредоносной.

Honeypot - это, без сомнения, лучший способ поймать злоумышленника, который обошел все остальные способы защиты. Это ловушка, которая просто ожидает попытки подключения. За десятки лет работы, я выследил многих

хакеров и пентестеров, факт в том, что после получения первоначального доступа, они всегда движутся по сети. Немногие хакеры могут отличить honeypot от настоящей системы, и, когда они перемещаются от устройства к устройству и просто "касаются" honeypot'а, вы уже знаете об их присутствии.

Наглядный пример: одна из самых опасных атак - это APT-атака (advanced persistent threat), описанная в Главе 14. Хакеры, которые ее совершают, легко продолжают вертикальное или горизонтальное движение, как правило, не будучи обнаруженными. Но, если установить один или несколько honeypot'ов, в качестве веб-сервера, сервера базы данных или сервера приложений, то не обнаружить APT-атаку будет практически невозможно.

Конечно, есть хакеры, которые после первоначального взлома переходят к определенному объекту или группе объектов, но это редкий случай. Как правило, после взлома своей главной цели, они будут осматривать все устройства в сети. И, как только, они попадут в honeypot, бум, они у вас. Или, по крайней мере, вы знаете об их присутствии. Я большой поклонник установки в инфраструктуре honeypot'ов с низким - средним уровнем взаимодействия. Это позволяет сразу узнать о взломе.

Мой личный пример поимки Русского шпиона

За годы работы я установил десятки honeypot-систем, но один из моих любимых случаев - установка honeynet'а для защиты организации заказчика. Его беспокоил взлом извне, но наши honeypot'ы быстро обнаружили неавторизованную атаку изнутри.

Мы отследили, что это был человек из расчетного отдела в России. У нас уже была камера в этом деле, поэтому мы видели все, что она делает. Она устанавливала в свой компьютер беспроводной адаптер, чтобы создать "мост" между двумя сетями с "воздушным зазором" и, в огромных количествах, передавать частную информацию своему партнеру. После двух дней наблюдения, мы выяснили ее намерения (ее определенно интересовали самые секретные проекты) и пришли в ее офис вместе с охраной. Она тут же бросилась в слезы, и была настолько хорошей актрисой, что если бы мы не наблюдали за ней эти дни, то я бы ей поверил. Она была суперхакером, но в расчетном отделе все были уверены, что она вообще не дружит с компьютерами, и отправляли ее на уроки печати на клавиатуре.

Она была одним из многих сотрудников из России, которых взяли из агентства по временному трудоустройству. В конце концов, все они оказались шпионами, и получили соответствующее наказание.

Ресурсы для изучения Honeypot

Проект Honeynet (http://www.honeynet.org) - это отличный ресур в котором собрана подробная информация о honeypot'ах и форензике. Их загрузочный образ Honeywall (http://www.honeynet.org/project/HoneywallCDROM) - это отличное, бесплатное, многофункциональное ПО для тех, кто не боится использовать Linux. В Honeywall есть удобное меню с множеством настроек, и его проще освоить, чем новый Honeyd.

Honeyd (http://www.honeyd.org) - это гибкая, бесплатная, функциональная программа для создания honeypot, однако, она требует серьезного уровня знаний Linux и сетей, как для установки, так и для использования. Она прекрасно эмулирует более 100 операционных систем, и ее можно легко использовать в связке с другими продуктами и скриптами. Минус в том, что ее годами не обновляли. Я думаю, это отличный вариант для тех, кто хочет увидеть все возможные способы использования honeypot'ов.

Моя любимая программа для создания honeypot'ов - Kfsensor (www.keyfocus.net). Это коммерческий продукт, который работает только на Windows, но он постоянно обновляется и улучшается. У Kfsensor есть и недостатки, но эта программа предоставляет большой набор возможностей, и ее легко настроить. В ней есть сотни опций, в том числе возможность авторизации, и возможность оповещения через базы данных и логи. Также доступна пробная версия.

В целом, существует множество (более ста) решений для создания honeypot'ов. Каждый год, в интернете появляется новое решение. Если вам интересны honeypot'ы, попробуйте некоторые из этих программ. Без сомнения, в каждой организации, заинтересованной в раннем обнаружении хакерской атаки или вредоносного ПО должна быть сеть honeynet'ов.

В Главе 20 мы поговорим о Лэнсе Шпитцнере, который, работал с honeypot'ами больше, чем кто-либо еще.

Глава 20. Профиль: Лэнс Шпитцнер

"Ничего не расстраивает меня больше, чем слова фанатов информационной безопасности о том, что «нельзя пропатчить глупость»" - Лэнс Шпитцнер

В начале 1980-ых я прочитал книгу Клиффорда Столла, которая называется «*The Cuckoo's Egg*» (https://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/B0051CSCG6/). Это история о том, как ошибка в $0.75 позволила американскому астроному обнаружить международную шпионскую сеть. Главным инструментом в расследовании Столла был honeypot. Благодаря этой книге, я действительно начал интересоваться информационной безопасностью и борьбой с хакерами.

Прошло десять лет, перед тем, как я узнал еще одного большого сторонника honeypot'ов, Лэнса Шпитцнера. Сегодня многие считают Шпитцнера отцом современных honeypot'ов. В 2000-х он написал и опубликовал столько трудов о них, в том числе книгу (https://www.amazon.com/Honeypots-Tracking-Hackers-Lance-Spitzner/dp/0321108957), что даже спустя десять лет, никто не написал больше. Благодаря свежему взгляду Шпитцнера на эту технологию, я изучаю honeypot'ы уже несколько десятилетий, и даже написал о них собственную книгу (https://www.amazon.com/Honeypots-Windows-Books-Professionals/dp/1590593359/).

Целью Шпитцнера было полностью изменить отношение к honeypot'ам, чтобы в информационной сфере их стали рассматривать не просто как игрушки, а как очень полезный инструмент. Больше всего ему было интересно узнать, как и почему хакеры взламывают организации, он называл это "Знай своего врага". Он также создал определения, чтобы классифицировать и описать различные виды honeypot'ов, проверяя на деле, что работает, а что нет. Шпитцнер - человек действия, он учился и познавал на практике.

Он также наглядно показал, что человек, чьей основной специальностью не были компьютеры, может построить карьеру в сфере информационной безопасности. Он поступил в колледж и стал изучать историю. Затем вступил в Корпус подготовки офицеров запаса (Reserve Officer Training Corps, ROTC), чтобы оплачивать обучение, и после подготовки четыре года отслужил в армии на танке M1A1 Abrams.

Шпитцнер абсолютно уверен, что не обязательно иметь профильное компьютерное
образование, чтобы сделать карьеру в сфере информационной безопасности. Он сказал: "Не обязательно учиться или начинать обучение в этой сфере, чтобы построить хорошую карьеру в информационной безопасности. Двадцать или тридцать лет назад такую карьеру было проще построить, потому что не было стандартной карьерной лестницы, как сейчас. Сейчас меня беспокоит, что в области информационной безопасности работает слишком много специалистов с профильным образованием. В нашей профессии нужно больше тех людей, у которых есть выраженные "личные качества", а не тех, которые просто разбираются в битах и байтах. Сегодня, многие основные проблемы, которые нам нужно решать, даже не связаны с технологиями".

Должно быть у танкистов и специалистов в информационной безопасности есть что-то общее, потому что за все эти годы, я знал лишь несколько представителей этих сфер, которые бы отлично справлялись со своей работой. Он сказал: "В армии постоянно учат тому, что нужно знать своего врага. Меня обучали вести бой не только на моем танке, но и на вражеских, и обучали тому, как они могут нас атаковать. Так как нас готовили к тому, что мы должны знать все о плохих парнях, я был удивлен, что в сфере информационной безопасности так плохо знают своего врага. Это был 1997-ой или 1998-ой, и тогда еще никто, на самом деле, о ней не беспокоился".

Я попросил его подробнее рассказать о том, как он попал в сферу информационной безопасности после службы танкистом. Он ответил: "Меня засосало в мир информационной безопасности, когда, после армии, я получал степень магистра по менеджменту. После службы на танке это было естественным желанием. Нам нужно было установить несколько файрволов, а так как я был новеньким, всю работу свалили на меня. Мне это нравилось. У меня была возможность изучать файрволы, практиковать их установку и останавливать плохих парней. Это было отличное время. После этого я четыре года работал в команде по безопасности в Sun Microsystems, защищая клиентов по всему миру".

Я спросил, как его любовь к файрволам переросла в любовь к honeypot'ам. Он ответил: "Я прочитал три работы по honeypot'ам. Первым был документ Доктора Фреда Коэна, которого считают изобретателем приемов защиты от компьютерных вирусов (https://en.wikipedia.org/wiki/Fred_Cohen). Затем была книга Клиффорда Столла *The Cuckoo's Egg*. А третьей была публикация 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 (представленный в Главе 18) был одним из первых создателей файрволов и одним из первых использовал honeypot'ы. Клиффорд Столл начал использовать honeypot'ы в 1986-ом. Билл Чесвик - в 1991-ом. Долгое время, эти два источника были единственной информацией о honeypot'ах".

Шпитцнер продолжил: "Долгое время не существовало и хороших honeypot'ов. Я почти не умел программировать, поэтому не мог написать свою honeypot-программу. Так что я решил использовать настоящие компьютеры в качестве honeypot'ов. Я просто установил файрвол, который я хорошо знал, на реальные системы. Все остальное, о чем я писал, было основано на этом опыте".

Самые продуктивные годы Шпитцнера были с 2004-го по 2009-ый, когда он посвятил все свое время работе над на проектом Honeynet (http://www.honeynet.org). Проект Honeynet финансировался Национальным разведывательным советом США (National Intelligence Council (https://www.dni.gov/index.php/about/organization/nationalintelligence-council-who-we-are). Национальный разведывательный совет (NIC) был основан в 1979-ом в качестве стратегического центра анализа данных. В нем работают лучшие умы из научного сообщества, правительства и частного бизнеса.

NIC уже долгое время предоставляет консультации экспертов и предлагает сотрудничество по вопросам разведки, а также возглавляет несколько масштабных и значимых проектов.

Все, кто заинтересован в honeypot'ах знают, что основная часть актуальной информации и инструментов для работы с ними были на сайте NIC, и до сих пор так и остается. Их сайт все еще работает. Если вы интересуетесь honeypot'ами, то вам нужно, как следует, изучить сайт проекта Honeynet. Именно во время работы над проектом Honeynet, Шпитцнер написал большую часть своих публикаций и помогал всем, кто задавал вопросы (включая меня).

К сожалению, в конце концов, Шпитцнер покинул проект Honeynet и больше не работает с honeypot'ами. Я спросил его почему, и он ответил: "Пока я работал в проекте Honeynet, я хорошо понял, как действует враг. Так как технологии, призванные защищать технологии, стали значительно лучше, я увидел, что киберпреступники быстро адаптировались и переключились на людей. Сегодня хакеры максимально используют социальную инженерию. Когда вы последний раз слышали об эпидемии сетевого червя? Во времена Conficker (Пик этого червя был в 2009-ом). Есть причина, по которой мы больше не слышим об эпидемии сетевых червей. Технологии, сами по себе, стали лучше, и теперь злоумышленники переключились на самое слабое звено - человека. Я увидел это и создал собственную компанию, где мы помогаем укрепить культуру информационной безопасности. В конце концов, в 2010-ом мою компанию купили SANS Institute (http://www.sans.org), и теперь наше подразделение называется «SANS Securing the Human» (https://securingthehuman.sans.org/). У нас более 1000 клиентов. Мы помогаем им создавать эффективные программы для укрепления культуры информационной безопасности. Я активно работаю с клиентами, и, как всегда, работаю в поле, а также веду лекции и выступаю на конференциях".

В завершении интервью, я спросил Шпитцнера, какую проблему информационной безопасности он считает самой важной. Он ответил: “Ну, подготовке людей все еще уделяется мало внимания. Технологиям все еще уделяется излишнее внимание, в то время, как подготовкой людей почти никто не занимается. Вот почему я работаю в этой области. Мне нравится то, что я делаю, и я верю, что это принесет плоды. Плохие парни так хорошо научились делать то, что делают, что сейчас нечего обнаруживать, нет зараженных вложений, нет вредоносных программ, нет руткитов. Они просто находят цель отправляя фишинговые электронные письма или выставляя поддельные счета на оплату, и им удается обмануть цель. Они так же используют обычные инструменты, такие как PowerShell, чтобы перемещаться по сети и совершать задуманное. Антивирусы и другие средства защиты не могут их обнаружить. Ирония в том, что зачастую, человеческому фактору уделяется меньше всего внимания из-за взглядов других специалистов по информационной безопасности. Технологиям уделяется столько внимания, что многие специалисты в сфере информационной безопасности уверены, что защищать можно только биты и байты. Ничто не расстраивает меня больше, чем слова фанатов информационной безопасности о том, что нельзя пропатчить глупость, то есть нельзя повлиять на человеческий фактор. В результате подготовке людей почти не уделяется внимания, но при этом, именно их мы обвиняем в том, что они самое слабое звено. Это безумие”.

Подробнее о Лэнсе Шпитцнере

Подробнее о Лэнсе Шпитцнере вы можете найти на этих ресурсах:

- Книга *Honeypots: Tracking Hackers*: https://www.amazon.com/Honeypots-Tracking-Hackers-Lance-Spitzner/dp/0321108957
- Твиттер Лэнса Шпитцнера: https://twitter.com/lspitzner
- Лекции Лэнса Шпитцнера в SANS: https://www.sans.org/instructors/lance-spitzner
- Публикация “Знай своего врага”: http://old.honeynet.org/papers/enemy/
- Серия публикаций “Знай своего врага”: http://www.honeynet.org/papers

Глава 21. Взлом Паролей

Взлом паролей всегда широко применялся киберпреступниками, однако сейчас это уже не простой подбор паролей. В представлении Голливуда хакер - это тот, кто на экране входа в систему может просто "с потолка" узнать правильный пароль. Несмотря на то, что такие случаи действительно происходят, это большая редкость. Как правило, реальный взлом пароля требует гораздо больше попыток, или вообще не использует метод отгадывания.

Элементы системы аутентификации

Чтобы понять, как работают пароли, очень важно сначала разобраться, как, в целом, устроены системы аутентификации. Пользователь (или устройство), также известный, как участник или субъект, должен предоставить данные (например, текстовую подпись, сертификат и так далее), по которым система аутентификации сможет точно определить пользователя и попытку входа в систему. Как правило, в большинстве случаев, текстовая подпись - это имя пользователя.

Затем субъект должен подтвердить, что он действительно владелец текстовой подписи, предоставив другую часть информации, связанной с этой подписью, о которой знают только субъект и система аутентификации. Это и есть пароль. Если имя пользователя и пароль верны, это означает, что субъекту действительно принадлежит данное имя пользователя, и система предоставляет доступ к аккаунту (другими словами, аутентификация пройдена, authenticated), и система может отслеживать действия субъекта во время сеанса (отслеживать и сопровождать, auditing and accounting). Многие операционные системы также обеспечивают субъекту доступ к необходимым объектам (контроль доступа, access control). В связи с этим вы, возможно вы слышали, что весь процесс аутентификации состоит из «четырех А» (authentication, access, auditing and accounting). Все эти этапы связаны, но, как правило, оцениваются по отдельности.

Пароли

Паролем может быть набор любых символов, которые принимает система аутентификации. Например, в Microsoft Windows локальная база данных SAM (Security Accounts Management) или сетевая база данных NTDS (Active Directory

authentication system) могут принимать тысячи различных символов, многие из которых требуют специальных комбинаций клавиш (например, Alt+0128).

Базы данных проверки подлинности

Пароли хранятся в локальной и/или сетевой базе данных под названием «база данных проверки подлинности». Такая база данных, как правило, защищена или зашифрована, и обычные пользователи не могут получить к ней доступ. Также, пароли часто хранятся в локальном и/или удаленном хранилище (если это сетевая база данных), пока пользователь или устройство находятся в системе.

Хеши паролей

В целях безопасности, пароли обычно преобразуются в промежуточную форму. В большинстве операционных систем, пароли преобразуются в криптографический хеш. Сам хеш может использоваться во время аутентификации. Самые распространенные хеш-функции для локального хранения преобразованных паролей на системах Windows - это LANManager (LM), NTLANManager (NT) и PBKDF2. На системах Linux часто используются MD5, Blowfish (хеш-функция, созданная Брюсом Шнайером, представленным в Главе 3), SHA-256 или SHA-512. Самые надежные хеш-функции используют случайное значение (“соль”) при создании и хранении хеша пароля. Таким образом хакеру, получившему хеш пароля сложнее преобразовать его обратно в открытый текст.

Вызов-ответ

Это безопасный способ аутентификации, который не подразумевает передачу пароля или его хеша по каналу связи. Вместо этого, происходит вызов-ответ. Как правило, удаленный сервер, которому уже известен пароль или хеш пароля клиента, создает случайное значение и совершает криптографическую операцию, на которую может ответить только настоящий пользователь, у которого есть настоящий пароль или его хеш. Сервер отправляет клиенту случайное значение, и последний использует пароль (или его промежуточную версию), чтобы сделать необходимые вычисления и отправить результат серверу. Сервер сравнивает полученное и собственное значение для данного пользователя, и, если результат совпадает, то аутентификация пройдена. Таким образом, если, во время аутентификации в сети, злоумышленник перехватывает пакеты, то он не сможет сразу получить пароль или его хеш,

тем не менее, во многих случаях, возможно расшифровать сам пароль или его хеш, используя криптоанализ.

Факторы аутентификации

Из-за того, что пароли можно легко украсть (а иногда подобрать), в системах аутентификации все чаще применяются дополнительные "факторы", подтверждающие, что субъект действительно является владельцем учетной записи. Существует три основных вида этих факторов: то, что мы знаем (например, пароль, PIN-код, проверочное слово или графический ключ), то, что мы имеем (токен безопасности, телефон или смарт-карта) или то, что является частью нас (например, биометрические данные, такие как отпечаток пальца, рисунок сетчатки глаза или отпечаток ладони).

В целом, чем больше факторов используется для аутентификации, тем лучше. Суть в том, что злоумышленнику сложнее украсть два (или более) фактора, чем украсть один. Использование двух факторов называется «двухфакторной аутентификацией (2FA)», а если используется больше, то это называется «многофакторной аутентификацией (MFA)». Использование двух (или более) одинаковых факторов менее эффективно, чем использование различных факторов.

Взлом паролей

Существует множество способов взломать пароль, включая те, что перечислены ниже.

Подбор пароля

Прямо как в кино, хакер может просто подобрать правильный пароль. Если используется простой пароль, и хакер кое-что знает о самом человеке, то он может попробовать подобрать пароль, основываясь на интересах этого человека. Известно, что пользователи часто создают пароли на основе своего имени, имени любимого человека или своих хобби. На экране входа в систему, хакер может попробовать вручную подобрать пароль или использовать один из многих инструментов автоматического подбора паролей. Если программа для подбора паролей "вслепую" перебирает все возможные комбинации, то это называется "брутфорс". Если она использует определенный набор значений, как правило, это словарь, то такой метод называется "перебор по словарю". Большинство инструментов для подбора паролей сначала используют словарь, а затем добавляют к обычным словам различные комбинации чисел и специальных символов, чтобы взломать более сложный пароль.

ПРИМЕЧАНИЕ За всю свою жизнь, я только однажды, буквально наобум, сразу подобрал пароль пользователя, о котором ничего не знал. Пароль был "rosebud", я выбрал его, так, как только что посмотрел фильм Орсона Уэллса *Гражданин Кейн*, где весь сюжет построен вокруг этого загадочного слова. Но это было единственный раз за всю мою карьеру.

Фишинг

Хакеры также могут использовать мошеннический, но похожий на настоящий, онлайн запрос (через веб-сайт или электронную почту), чтобы обманом заставить пользователя ввести свой пароль. Это называется "фишинг". Если при попытке фишинга используются личные данные или внутренняя информация организации, то это называется "целевой фишинг". Также хакеры могут использовать телефонный звонок или попробовать обмануть пользователя лично. Это работает гораздо чаще, чем вы думаете.

Запись нажатия клавиш (Килоггинг)

Если хакер уже получил доступ к компьютеру жертвы, то он может установить на нем "килоггер", программу, записывающую нажатие клавиш на клавиатуре. Килоггеры отлично перехватывают пароли, и им все равно насколько длинный или сложный пароль.

Взлом хеша пароля

Если хакер получает доступ к базе данных проверки подлинности, то он также может получить доступ к сохраненным в ней паролям, а точнее к их хешам. Сильные хеш-функции, как правило, устойчивы к криптоанализу. Объектом для "взлома хеша" являются более слабые хеш-функции, не использующие "соль", а также хеши коротких паролей. Взломщик перебирает (используя методы брутфорса или словаря) все возможные пароли, преобразует их в хеш, а затем сравнивает вновь созданный хеш с украденным. Если они совпадают, то хакер получает пароль в открытом виде. Как правило, для взлома хешей используются "радужные таблицы", которые позволяют сохранять промежуточные формы паролей, или, если выразиться точнее, проводить сравнение хешей, что значительно ускоряет процедуру взлома. В интернете можно найти множество бесплатных программ для подбора или взлома паролей. Если вас интересует взлом хешей, попробуйте начать с John the Ripper (http://www.openwall.com/john/), это отличный, бесплатный инструмент.

Повторное использование учетных данных

Если хакер уже получил доступ, то он может украсть хеш пароля или другие виды учетных данных из памяти компьютера или базы данных проверки подлинности, а затем повторно воспроизвести их на других компьютерах, чтобы пройти аутентификацию. За последнее десятилетие такой вид атак стал очень популярен, а именно атака “Pass-the-hash” (или PtH). Как правило, во время PtH-атаки злоумышленник взламывает компьютер одного или нескольких обычных пользователей, находит хеши аккаунтов, а затем использует полученные данные, чтобы, в конечном счете, получить доступ к хранилищу всех учетных данных в сети или на локальной машине, по сути, взламывая всю IT-инфраструктуру. За последние десять лет, практически все компании и организации, подключенные к интернету, подверглись PtH-атакам.

Взлом сервиса восстановления пароля

Во многих случаях, взлом сервиса восстановления пароля - это самый быстрый способ взломать пароль. Многие системы аутентификации, особенно большие онлайн-системы, позволяют конечному пользователю сбросить пароль, ответив на несколько определенных вопросов. Хакеры поняли, что намного легче подобрать или выяснить точный ответ на такой вопрос (например, “Девичья фамилия матери”, “Номер начальной школы”, “Марка первого автомобиля”, “Любимый цвет” и так далее), чем подбирать сам пароль. Многие знаменитости были взломаны именно таким способом.

Защита пароля

Способов защиты пароля существует не меньше, чем способов его взлома.

Сложность и длина

Длинные и сложные пароли намного меньше подвержены взлому. Длина пароля дает большую защиту, чем сложность (если, конечно, у вас не получится придумать настолько сложный пароль, что его будет практически невозможно взломать). Сегодня, большинство экспертов советуют использовать в пароле не менее 12 символов, и это только для обычных пользователей. В аккаунтах с большими привилегиями, должно быть, как минимум, 16 символов. Минимальная длина пароля постоянно увеличивается. Однако, этот способ не эффективен против атак повторного использования учетных данных, таких как PtH-атаки.

Частое изменение пароля без повторений

Ограничение максимального количества дней использования одного пароля (в основном, 90 дней или менее) становится распространенным требованием/рекомендацией для защиты пароля. Идея в том, что для взлома длинного и сложного пароля, злоумышленнику нужно много времени, однако, если у него будет и время и достаточно вычислительных мощностей, то, в конце концов, он взломает пароль. Ограничение периода использования снижает риск взлома пароля до того момента, как будет использоваться новый.

ПРИМЕЧАНИЕ Несколько недавних публикаций посвящены вопросу об эффективности традиционных способов защиты пароля, таких как длина, сложность, частая смена и уникальность. Хотя, на первый взгляд, эти способы могут показаться эффективными, статистика показывает обратное. Посмотрите публикацию Робина Хикока в Microsoft, под названием "Password Guidance" (https://www.microsoft.com/en-us/research/publication/passwordguidance/), а также публикации Доктора Кормака Херли, представленного в следующей главе, в которых оспаривается эффективность традиционных рекомендаций для защиты пароля.

Разные пароли для разных систем

Это один из лучших способов защиты, однако внедрить его крайне сложно (может быть даже невозможно). У пользователя должны быть разные пароли для каждой системы со своей базой данных проверки подлинности. Использование одних и тех же учетных данных для разных систем повышает вероятность, что хакер получивший доступ к данным одной системы, использует их для другой.

Блокировка учётной записи

Этот способ защиты часто используется против подбора паролей. Если хакер пытается получить доступ на экране входа в систему, то после определенного количества неверных попыток система блокирует или "замораживает" аккаунт. Блокировка может автоматически сниматься со временем, или требовать от конечного пользователя обратиться в службу технической поддержки, чтобы повторно ввести данные или изменить их, используя сервис восстановления пароля. Такой механизм защиты хорошо работает против методов перебора, но также имеет свои минусы, так как хакеры могут использовать его для совершения масштабной DoS-атаки, и заблокировать аккаунты всех пользователей.

Устойчивые хеш-функции

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

Не используйте пароли

В наши дни, народная мудрость гласит, что требования к паролям становятся настолько сложными, что лучше вообще не использовать пароли. Вместо них можно применять двухфакторную аутентификацию, цифровые сертификаты, токены, биометрическую аутентификацию и все, что сложнее обычных имени пользователя и пароля. Эти рекомендации существуют уже десятки лет, но именно сейчас им начинают следовать многие компании и популярные онлайн-системы. Если веб-сайт предоставляет дополнительные средства безопасности, помимо пароля, то их нужно использовать.

ПРИМЕЧАНИЕ Основной движущей силой в этом направлении становится сервис FIDO Alliance (https://fidoalliance.org), несмотря на то, что до этого многие компании безуспешно пытались продвинуть отказ от паролей.

Защита от кражи учетных данных

Из-за того, что в последнее время стали широко применяться PtH-атаки, во многих операционных системах есть встроенные средства защиты от кражи учетных данных. Как правило, они не допускают хранения паролей или их хешей в памяти, что усложняет их кражу, либо они не передают пароль или его хеш по сети.

Защита сервисов восстановления пароля

Часто самым слабым звеном в системе аутентификации являются сервисы восстановления пароля. Они должны давать пользователю возможность придумать сложные вопросы и ответы, которые будут эффективны против метода перебора. Если такой возможности нет, можно придумать "псевдоответ" на обычные вопросы и сохранить его в безопасном месте. Например, ответом на вопрос "Девичья фамилия матери" может быть "жирафсобакарыба". По сути, ответ на секретный вопрос превращается в еще один пароль.

В Главе 22 представлен Доктор Кормак Херли, чьи исследования ставят под сомнение эффективность традиционных способов защиты пароля.

Глава 22. Доктор Кормак Херли

Доктор Кормак Херли – неумышленный вредитель. Его высказывания опровергают давно существующие догмы, и многие не хотят их слышать, особенно, если они потратили миллионы долларов и десятки лет работы именно на то, что он опровергает. В поисках правды, Доктор Херли анализирует различные данные. И он прекрасно понимает, что понадобятся десятилетия, а, возможно, и больше, чтобы его бунтарские высказывания, подкрепленные реальными данными, хотя бы начали слушать.

Один из примеров его исследований - пароли. Народная мудрость гласит, что пароли должны быть сложными, длинными, и постоянно меняться. Исследование Доктора Херли (https://www.microsoft.com/en-us/research/wpcontent/uploads/2016/09/pushingOnString.pdf) показало, что стандарты и требования к информационной безопасности, принятые по всему миру, и поддерживаемые практически всеми экспертами, по крайней мере, не эффективны, и скорее всего, только усугубляют проблему. Также его исследование показало, что, в наши дни, длина и сложность пароля не только не снижают риск его взлома, но и доставляют неудобства конечному пользователю, и в результате могут стать источником еще больших проблем (так как пользователю нужно будет где-то записать такой пароль или использовать его на разных сайтах).

Ему даже хватило наглости сказать, что "большинство рекомендаций по информационной безопасности - это пустая трата времени" (https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SoLongAndNoThanks.pdf). И он говорит это, имея на руках данные исследований и доказательства. Для меня Доктор Херли - это свой человек.

Докторскую степень Херли получил в Колумбийском университете, диплом инженера (MSEE) - в Технологическом институте Джорджии, а степень бакалавра технических наук - в Ирландском национальном университете Корка. Сейчас он главный научный сотрудник в Microsoft Research's Redmond Machine Learning Department. Несмотря на то, что он работает в сфере информационной безопасности только 10 лет, он уже опубликовал "тонну" результатов исследований, а основные СМИ (такие как *The New York Times*, *The Wall Street Journal*, Bloomberg и NPR) цитируют его высказывания и берут интервью.

Я спросил Доктора Херли, как он попал в сферу информационной безопасности. Он ответил: "Я думаю, что по счастливой случайности. Раньше, я занимался обработкой аудио- и видеосигналов и цифровой фотографией. Эта

сфера очень сильно связана с данными. Нужно собирать большое количество данных, анализировать их, получать статистику и искать правду. Это дало мне отличную базу для работы в сфере информационной безопасности, хотя я сильно удивился, когда узнал, что в этой области не происходит ничего из вышеперечисленного. Я думаю, я стал интересоваться информационной безопасностью, когда мне прислали на проверку новое средство защиты от фишинга, работающее на основе анализа логотипа, где были аспекты, на которых я специализировался. Там было много уязвимостей. Оно не было достаточно надежным. В конце концов, меня заинтересовали пароли и информационная безопасность. Я видел множество заявлений о том, какими должны быть пароли, но ни одно из них не было подкреплено фактами, что эти рекомендации на самом деле работают. Для меня было очень странно, что никто не делал того, что уже давно нужно было сделать, то есть, не собирали данные, не проводили эксперименты с двумя группами (включая контрольную группу) и не анализировали результаты. Вместо этого, были только заявления, которые, даже спустя десятилетия, не подкреплены данными. Несмотря на то, что в сфере информационной безопасности бывает трудно получить данные, я опираюсь только на них. Именно так нужно отвечать на вопросы. Все остальное - просто оценочное суждение или еще хуже.

У нас есть основы для защиты самых важных объектов, которые гласят, что мы должны сделать все возможное, но что делать с обычными решениями для бизнеса? Очевидно, что нам нужно расставить приоритеты. Мы не можем делать все одновременно. Это невероятно сложно, но тогда нужно уточнить, чем можно пренебречь. Создайте список объектов по порядку важности или дайте мне возможность создать такой список. На самые сложные вопросы можно точно ответить только при наличии данных, в противном случае - это ходьба вокруг да около”.

В сфере информационной безопасности много людей, которые либо игнорируют работу Доктора Херли, либо обеспокоены ей. Я спросил, что он об этом думает, и он ответил: “Я не для того начал работать в области информационной безопасности, чтобы старательно, намеренно выставлять кого-то врагом. Но, так как я недавно пришел в эту область, я не подвержен тому долгому влиянию убеждений, которому подвержены многие другие специалисты. У меня другое прошлое, основанное на получении и подтверждении данных. После того, как я не увидел достаточно подтверждающих данных, я смог задать фундаментальные вопросы о том, что давно считается истиной. Я хотел получить данные, проводить тесты, эмпирический анализ… расчеты. Это не моя личная прихоть, а необходимость. У вас может быть модель того, как будут вести себя 2 миллиарда пользователей, но поведение двух миллиардов пользователей не ограничивается вашей моделью. Можно надеяться, что большинство из них будет делать одно и то же, но, тем не менее, необходимо провести

исследования, чтобы убедиться, что ваша модель соответствует действительности. И если она не соответствует, ее необходимо изменить".

Исследования Доктора Херли уже подняли на уши всю сферу информационной безопасности. Я поинтересовался, что он чувствует, зная, что понадобится не менее десяти лет, чтобы его результаты исследований безопасности паролей и соответствующие предложения, получили широкое распространение. Он сказал: "Ну, NIST (www.nist.org) стали критиковать за их рекомендации по безопасности паролей, я ответил на эти комментарии, и они развернули свои орудия. Я прекрасно понимаю, почему это расстраивает организации и специалистов по информационной безопасности. Им 30 лет говорили, как правильно делать, а сейчас несколько человек утверждают, что это не работает. При этом тысячи других специалистов говорят обратное, и, даже если высказывания нескольких человек подкреплены реальными данными, я понимаю насколько это сложно, особенно для руководителей отдела безопасности и IT-директоров. У меня была возможность и много свободного времени, чтобы проводить исследования, собирать данные и учитывать альтернативные варианты развития событий. Но у руководителей отдела безопасности и IT-директоров нет такой роскоши, как свободное время на исследование одной проблемы. Они видят несколько утверждений, которые противоречат друг другу, и пытаются понять, что из этого правда. В каждой ситуации им необходимо делать все возможное и использовать свою мудрость".

Я спросил Доктора Херли, что, по его мнению, является самой главной проблемой в информационной безопасности. Он ответил: "Мы отлично знаем, как защитить самые важные объекты, такие как коды запуска ядерных ракет. Взлом такого объекта абсолютно недопустим, поэтому мы делаем все возможное, чтобы его защитить. В случае с менее важными объектами, нам нужно решать, что делать, а что не делать. И в таких случаях, оценка достаточного количества усилий далека от идеала. У нас действительно мало инструментов и данных, чтобы точно определить необходимый набор мер защиты. В результате люди делают все возможное, продираясь через все возможные варианты, и по сути наобум принимают решения, которых от них ждут. С наиболее важными объектами все проще. Мы отчетливо осознаем риск, измеряем его и создаем меры безопасности. В случае с менее важными объектами, наибольшее внимание, как правило, уделяется тем моментам, где угроза кажется наиболее очевидной, и возможные риски легче просчитать, но при этом, упускаются более существенные моменты. Например, я не уверен, что безопасность пароля должна быть в списке десяти важнейших задач, но ей, совершенно точно, уделяется огромное количество внимания и ресурсов". И, в конечном счете, это вредит нам всем.

Подробнее о Докторе Кормаке Херли

Подробнее о Докторе Кормаке Херли вы можете найти на этих ресурсах:

- Веб-сайт Доктора Кормака Херли: http://cormac.herley.org/
- Твиттер Доктора Кормака Херли: https://twitter.com/cormacherley
- Профиль Доктора Кормака Херли в Microsoft: https://www.microsoft.com/en-us/research/people/cormac/
- Ссылки на работы Доктора Кормака Херли в Академии Google: https://scholar.google.com/citations?user=1FwhEVYAAAAJ&hl=en&oi=ao

Глава 23. Взлом беспроводных сетей

Сегодня информационный мир состоит из беспроводных сетей. Сетевой кабель редко подключают к настольному компьютеру, ноутбуку, и тем более, его не подключают к телефонам и другим устройствам, хотя мир проводных технологий быстрее и безопаснее. Мир беспроводных технологий постоянно подвергается хакерским атакам.

Мир беспроводных технологий

Мир беспроводных технологий огромен. Беспроводные сети, которые мы используем дома в качестве беспроводной точки доступа используют Wi-Fi-стандарт 802.11, но термин "беспроводной" охватывает огромную часть спектра электромагнитного излучения, в том числе рентгеновское излучение, световые волны, радиоволны и другие виды беспроводной энергии. Определение и назначение беспроводного спектра измеряется в количестве волн в секунду (то есть, частоте) и длине волны. Стандарт 802.11 работает в частотных диапазонах 900 МГц, 2.4, 3.6, 5.0, 5.8 и 60 ГГц. Компьютеры используют различные беспроводные технологии, включая магнитное поле, свет, сателиты, короткие радиоволны, Bluetooth, Ближнюю бесконтактную связь (Near Field Communications, NFC), RFID и микроволновое излучение. Значительная часть спектра применения беспроводных технологий регулируется законами и контролирующими органами, и это хорошо, потому что в противном случае использование этих технологий было бы невозможным и небезопасным.

Виды взлома беспроводных сетей

В зависимости от стандартов связи, определяющих беспроводные технологии, против них могут применяться различные виды хакерских атак, однако большая часть атак на сети Wi-Fi наглядно демонстрирует, какие атаки могут использоваться против других видов беспроводной связи. В основном, при взломе беспроводных сетей используется прослушка, перехват информации, несанкционированное использование беспроводного вещания, DoS-атаки, управление самой сетью или взлом подключенных клиентов.

Атака на точку доступа

Для осуществления приема/передачи во всех беспроводных технологиях используется одна или несколько точек доступа (access point, AP), как правило, это наземные или другие системы связи. Чтобы взломать беспроводную сеть, хакеры могут атаковать непосредственно AP. Они могут взломать пароль администратора AP, изменить работу самой точки, осуществить прослушку или обманом заставить жертву подключиться к ложной AP.

DoS-атака

Самый простой вид взлома беспроводной сети - это грубая остановка или значительное усиление сигнала связи, также известные как "джамминг" ("jamming") или "флудинг" (flooding). Если можно остановить подключение к беспроводному каналу связи и вызвать отказ в обслуживании, то такую связь уже нельзя использовать. Также, хакер может перехватить управление самим каналом. Если "флудинг" сделан правильно, то точка доступа может случайно подключиться к другому, вредоносному источнику.

Подбор пароля беспроводной сети

Некоторые беспроводные технологии требуют пароль (или другие способы аутентификации) для подключения к точке доступа. Однако в редких случаях AP блокирует доступ после определенного количества попыток. Поэтому использовать метод перебора можно сколько угодно, пока не найдется настоящий пароль.

Перехват сессии

Многие атаки ставят своей целью перехват сессии жертвы. Как правило, это делается с помощью "флудинга" сети, вызывающим сбой в обслуживании, а затем пользователя обманным путем заставляют либо передать доступ хакеру, изменяя сессию, либо подключиться к ложной точке доступа. Такой вид атак стал очень популярным, особенно среди хакеров, которые хотят украсть "cookies" через общественные беспроводные сети (например, в кофейнях, аэропортах и так далее).

Кража информации

Кража информации - это скорее результат взлома беспроводных сетей, но здесь я выделяю ее, как отдельный хакерский метод, потому что во многих случаях вся процедура взлома совершается с целью кражи информации. Например, взлом RFID. Миллионы пластиковых карт поддерживают RFID, он

используется для того, чтобы клиент мог оплачивать покупки, не вставляя карту в считывающее устройство. Хакеры могут использовать сканеры RFID чтобы незаметно заставить работать передатчик RFID. Технология RFID также может использоваться на других устройствах и в документах, например, в мобильных телефонах или паспортах.

ПРИМЕЧАНИЕ Прослушка электромагнитного поля может использоваться против устройств, которые не преднамеренно передают электромагнитные волны. У всех электронных приборов есть электромагнитное излучение, которое можно считать с большого расстояния, при наличии чувствительных прослушивающих устройств.

Определение местонахождения пользователя

Многие хакеры, в основном, из правоохранительных структур, используют особенности и уязвимости конкретной беспроводной технологии, чтобы обнаружить местонахождение участников сети и их устройств. В частности, правоохранительные структуры используют устройства "stingray", которые создают ложные точки доступа для обнаружения местонахождения цели по месту нахождения ее телефона. Чтобы лучше ознакомиться с этими замечательными устройствами и сомнительной правомерностью их использования, прочитайте эту статью: https://en.wikipedia.org/wiki/Stingray_phone_tracker.

Примеры инструментов для взлома беспроводных сетей

Существуют десятки, если не сотни, инструментов для взлома беспроводных сетей. Можно использовать любую программу перехвата трафика, например Wireshark (http://www.wireshark.com/) или Ethereal (https://sourceforge.net/projects/ethereal/), но большинство хакеров использует специализированные программы. Эти инструменты позволяют отлично изучить беспроводные технологии, и их взлом.

Aircrack-Ng

Самая популярная программа для взлома протокола 802.11 - это Aircrack-Ng. Она появилась в 2005-ом, в качестве бесплатного инструмента проверки безопасности беспроводных сетей, и со временем, учитывая постоянные обновления, стала выбором как защитников, так и атакующих. Ее создатель, Томас д'Отреп де Бувет представлен в следующей главе.

Kismet

Kismet (https://www.kismetwireless.net/) - еще одна популярная программа для взлома протокола 802.11. Она может как взламывать беспроводные сети, так и сообщать о том, что беспроводная сеть была взломана.

Fern Wi-Fi Hacker

Fern Wi-Fi Hacker (https://github.com/savio-code/fern-wifi-cracker) позволяет хакерам использовать методы, которые я перечислил выше.

Firesheep

Попробуйте зайти в кофейню и запустить Firesheep (http://codebutler.com/firesheep). Эта программа будет искать и перехватывать все доступные в общественной беспроводной сети HTML cookies. Перехват HTML cookies был возможен задолго до появления Firesheep, но именно эта программа сделала этот процесс таким же простым, как запуск браузера. С появлением Firesheep многие общественные заведения серьезно задумались о безопасности своих беспроводных сетей (а также веб-сайтов).

Защита беспроводных сетей

Способов защиты существует не меньше, чем способов атаки.

“Прыгающие частоты”

Одна из главных проблем всех беспроводных технологий заключается в том, что можно легко создавать помехи для их работы. Во время Второй Мировой Войны известная голливудская актриса Хеди Ламарр (совместно со своим партнером, композитором Джорджем Антейлом) изобрела и запатентовала технологию “Псевдослучайной перестройки рабочей частоты”. Такой метод передачи информации используется в качестве механизма защиты, так как сигнал передается на разных несущих частотах (которые очень быстро меняются), известных (или рассчитываемых) только отправителю и получателю. Тому, кто захочет прервать сигнал придется глушить широкий спектр частот. Без такого механизма защиты, у нас бы сейчас не было многих беспроводных технологий. Почитайте об открытии Ламарр. Моя любимая книга на эту тему - книга Ричарда Родса *Hedy’s Folly*.

Предварительная Идентификация

Во многих беспроводных технологиях есть механизмы защиты, которые позволяют осуществлять подключение только определенным клиентам. Например, многие точки доступа, работающие с протоколом 802.11, разрешают подключение только устройствам с определенным MAC-адресом. Также точки доступа могут принимать только цифровые сертификаты, полученные от определенных, доверенных центров сертификации или работать только с устройствами с определенным физическим адресом. Может использоваться любой параметр идентификации.

Устойчивые протоколы

Лучшая защита - это устойчивый протокол. Стандарт 802.11 сначала использовал протокол Wired Equivalent Privacy (WEP), однако позже в нем были обнаружены серьезные уязвимости, и он больше не используется. Его заменили протоколом Wi-Fi Protected Access (WPA), который с тех пор доказал свою устойчивость. WPA может работать с паролями, цифровыми сертификатами и другими корпоративными методами аутентификации. Против различных версий WPA было применено несколько успешных атак, но, тем не менее, их было гораздо меньше, чем предсказывали многие эксперты, а последствия большинства атак можно устранить, применив другой метод работы WPA.

Длинные пароли

Если для подключения к беспроводной точке доступа необходим пароль, то он должен быть действительно длинным (от 30 символов). Также, пароль администратора AP необходимо изменить со стандартного на длинный и сложный.

Установка патчей точки доступа

Часто, точки доступа имеют уязвимости, поэтому необходимо вовремя устанавливать патчи от производителя.

Электромагнитное экранирование

Для предотвращения атак на беспроводные технологии, как, например, атаки на пластиковые карты с RFID, поверх передатчика (или всего устройства) устанавливают электромагнитный экран, не допускающий прослушивание. К электромагнитному экранированию также относятся экранирование ЭМП, радиочастотная защита или Клетка Фарадея. В некоторых электронных

устройствах, например, мобильных телефонах, есть встроенная защита, но, как правило, те, кто беспокоятся о прослушивании электромагнитных волн покупают экраны от сторонних производителей. Экраны также используются в кабелях, например в обычном телевизионном кабеле, для предотвращения прерывания сигнала.

Существует гораздо больше способов взлома беспроводных технологий и гораздо больше способов их защиты, чем может может уместиться в одной маленькой главе, но я надеюсь, что описал самые основные.

В Главе 24 представлен Томас д'Отреп де Бувет, создатель приложения для тестирования безопасности Wi-Fi-сетей, которое называется «Aircrack-ng».

Глава 24. Профиль: Томас д'Отреп де Бувет

Предыдущая глава была посвящена взлому беспроводных технологий, и самый уважаемый человек в сообществе хакеров, специализирующихся на этих технологиях - это Томас д'Отреп де Бувет, создатель Aircrack-Ng (http://aircrackng.org/). Aircrack-Ng - это самый популярный, бесплатный инструмент для проверки безопасности Wi-Fi сетей, который состоит из 16 различных программ. Впервые, Томас выпустил Aircrack-Ng в 2006-ом. Сегодня эта утилита, по умолчанию, есть в каждом дистрибутиве Linux, и, как правило, используется для проверки и взлома Wi-Fi сетей перед покупкой коммерческого продукта с тем же назначением. Она настолько популярна, что появляется в телешоу и фильмах (http://aircrack-ng.org/movies.html), где хотят реалистично показать суперхакера. Также Томас разработал и выпустил программу обнаружения вторжений для беспроводных сетей, которая называется «OpenWIPS-ng» (http://www.openwips-ng.org/).

Я спросил его, как он попал в сферу информационной безопасности. Он ответил: "Я очень рано начал интересоваться компьютерами, мне было лет шесть или восемь. Я сразу заинтересовался программированием, и уже тогда написал простенькую игру. Как и любой ребенок, я сначала играл в компьютерные игры, пока они мне не надоели. Тогда я решил почитать книги, которые шли с компьютером и узнал, что на нем можно программировать. Мой родной язык французский, а все руководства были на английском, и было нелегко разобраться, как попасть в режим "программирования" который был похож на BASIC. Более того, нельзя было сохранить свой код, поэтому я был вынужден записывать его на бумаге. Я и сейчас помню, что это была за игра, и как ее пройти.

Затем я увидел программу Aircrack, которую изначально написал Кристоф Девин, и после этого, я начал интересоваться информационной безопасностью. Я участвовал в ее доработке, делал небольшие патчи, чтобы поправить различные недочеты, а затем, в декабре 2005-го, ее создатель внезапно ушел из проекта. Он был единственным разработчиком, и тогда, эта утилита воспринималась только в качестве инструмента для взлома соседского WEP-ключа. Он внезапно исчез из канала в IRC, и больше никогда не заходил туда. Затем в этом канале стали распространятся слухи о том, что произошло, я думаю, их распространяли его друзья… этих слухов было достаточно, чтобы я начал скачивать все ресурсы, релизы и все, что было связано с этой

программой, перед тем, как несколько дней спустя, сервер полностью был отключен. Тогда было много слухов о том, что произошло с разработчиком, но позже я встречался с ним несколько раз, и узнал, что он просто переключился на свою настоящую работу, и тогда у него был выбор, либо продолжать тратить время на разработку бесплатной программы или сохранить свою работу. Но тогда мы еще не знали, что произошло.

После трех месяцев ожидания, я решил сделать собственную версию Aircrack. Это был декабрь 2005-го. Я никогда не получал за нее деньги, но мне нравится работа над этим проектом, люди, с которыми я познакомился и сама разработка. И, хотя я никогда не получал денег за Aircrack-Ng, благодаря этой программе, я получил работу. Мне всегда нравилось взламывать свою собственную сеть. И сейчас я открываю свой бизнес. Даже мои родители были против того, чтобы я разрабатывал Aircrack-Ng, они говорили, что из-за этого у меня будут проблемы (когда я только начинал), и я, на самом деле, рад, что не послушал их, потому что это одна из лучших вещей, которые со мной происходили: у меня появилась возможность познакомиться с отличными людьми, а большинство моих нынешних друзей - это люди, с которыми я так или иначе познакомился, благодаря этому проекту".

Я спросил его, улучшилась ли безопасность беспроводных технологий за эти годы. Он сказал: "Да, определенно. Когда я только начинал, для доступа к беспроводной сети достаточно было взломать WEP-ключ. Сейчас WEP почти не используется. Сегодня в беспроводных сетях используются WPA и WPA2 с устойчивым шифрованием. Сейчас, чтобы взломать беспроводную сеть, нужно найти уязвимость либо в самом чипе (вот видео с примером такой уязвимости: https://www.youtube.com/watch?v=4WEQpiyfb50), либо ошибку человека. Можно применить самое надежное шифрование в мире, но, если производитель или клиент использует пароль для Wi-Fi из восьми символов, то такую сеть можно взломать.

Еще один пример: в гостинице, где я последний раз снимал номер, в качестве пароля для точки доступа использовался MAC-адрес. Мне сказали, что нужно просто перевернуть (роутер), чтобы узнать пароль. Ну, такой пароль можно легко узнать, при наличии сетевого адаптера, работающего в режиме мониторинга, и, скорее всего, я бы смог расшифровать данные других жильцов, если бы захотел. Вдобавок ко всему, администрация гостиницы запрещала менять пароль.

Дело в том, что в устройствах некоторых производителей есть предварительно сгенерированная парольная фраза, которая, как правило, представляет из себя хеш, основанный на MAC-адресе, в котором символы перемешаны различными способами. Наглядный пример: проводной модем от (популярного производителя) защищен WPA (или WPA2), и парольная фраза состоит из четырех букв названия производителя, за которыми следуют последние четыре шестнадцатеричной записи MAC-адреса. Это означает, что

нужно, в худшем случае, перебрать всего 10 000 комбинаций, чтобы найти верный ключ (на что, максимум, потребуется минута или две)".

Я спросил, в чем по мнению Томаса, заключается главная проблема информационной безопасности. Он сказал: "В сфере информационной безопасности много серьезных проблем, но главный источник всех этих проблем - это сами пользователи. Они хотят удобство и безопасность (например, частных данных, шифрования). Но безопасность и удобство - это, по сути, враги. Нельзя получить и то и другое одновременно. Чем больше удобства, тем меньше безопасности. И, само собой, повышение уровня безопасности значительно уменьшает удобство использования".

Подробнее о Томасе Отреппе де Буветте

Подробнее о Томасе Отреппе де Буветте вы можете найти на этих ресурсах:

- Видео Томаса Отреппе де Буветте и Рика Фарины по безопасности беспроводных сетей с презентации DEF CON: https://www.youtube.com/watch?v=XqPPqqV_884
- Слайды Томаса Отреппе де Буветте и Рика Фарины с презентации DEF CON в формате PDF: https://defcon.org/images/defcon-16/dc16-presentations/defcon-16-de_bouvette-farina.pdf

Глава 25. Тестирование на Проникновение

Эта глава описывает требования, которые делают из хакера профессионального пентестера, работающего по договору, плюс, в ней будут советы, которые могут помочь продвижению карьеры пентестеров. Кроме того, я расскажу о самых востребованных сертификатах.

Самые яркие моменты в моей карьере пентестера

Без сомнения, период работы пентестером был одним из самых увлекательных в моей карьере. Взламывать весело. Сложно выбрать лучшие проекты, в которых я участвовал, но в следующих разделах описаны самые запомнившиеся моменты.

Как мы взломали все ТВ-приставки в стране.

Нас наняли, чтобы протестировать новую ТВ-приставку, которую собиралась выпустить крупнейшая в мире кабельная компания. Я использовал сканер портов, чтобы просмотреть все сетевые порты, и примерно, десять из них оказались открыты. Затем я использовал Nikto, сканер, проверяющий веб-серверы, чтобы просканировать все порты, в надежде, что на одном из них может быть веб-интерфейс. Так и было. С помощью Nikto я узнал, что один из портов - это неизвестный веб-сервер, который я никогда раньше не видел, и что у него есть определенная уязвимость. Но оказалось, что этой уязвимостью нельзя было воспользоваться. Но я знал, что это было старое ПО для реализации веб-сервера, то есть, скорее всего, в нем было полно багов, которые уже давно исправили в новых веб-серверах. Первое, что я попробовал - это обход директории (то есть, я вписал http://..//..//..//), и это сработало. Я получил права администратора и полный доступ к ТВ-приставке.

В отчете мы указали клиенту на эту уязвимость, и на следующий день, все топ-менеджеры компании вылетели на мою презентацию. Оказалось, что эта уязвимость была на всех ТВ-приставках, в том числе на миллионах приставок, которые эта компания уже использовала в стране, и все они были подключены к интернету.

Как мы одновременно взломали сеть и получили доступ к порнографическому контенту крупнейшей телевизионной компании

Та же компания, чьи приставки мы тестировали, наняла нас, чтобы узнать, сможем ли мы украсть порнографический контент, один из главных источников дохода этой компании, а также, чтобы узнать, сможем ли мы украсть фильмы, которые были основной составляющей телевещания. Мы "застряли" в компьютерном зале, с двумя ТВ-приставками и двумя телевизорами, которые вещали 24/7, на одном транслировалась порнография, а на втором - самые популярные фильмы. Как можно догадаться, просмотр порнографии изо дня в день, на протяжении многих часов, быстро надоедает. Но, тем не менее, десятки людей каждый день "поглядывали", чем мы там занимаемся. Кстати говоря, у нас получилось украсть как порнографический контент, так и фильмы, и доказать, что можно украсть номера кредитных карт клиентов этой компании.

У нас даже получилось использовать уязвимость межсайтового скриптинга, чтобы получить контроль над всей кабельной компанией, и это с помощью одной приставки. Мы узнали, что на приставке был веб-сервер, в котором содержались логи файрвола. И в этих логах была ошибка межсайтового скриптинга. Мы совершили такую "атаку", которая позволила бы нам применить другие хакерские приемы (в данном случае, чтобы получить пароли администраторов). Затем мы попросили одного из технических специалистов проверить логи файрвола, потому что нам было интересно, вдруг нас «атакуют хакеры». Когда специалист из техподдержки проверил интересующий нас лог файрвола, на наших экранах появился пароль системного администратора. Оказалось, что все администраторы компании использовали один и тот же пароль.

Как мы взломали сайт крупной Платежной Системы

Для прохождения сертификационного теста, нашу компанию наняли для взлома "тестируемого" веб-сайта. Это было соревнование, чтобы узнать, насколько этот сайт подвержен взлому - сколько уязвимостей мы сможем найти, и какую выгоду сможем из этого извлечь. Мы соревновались с десятками других компаний, и тот, кто найдет больше всего уязвимостей победит, получит сертификат, а также получит возможность "выдавать сертификаты" десяткам тысяч других веб-сайтов. Помимо того, что один из членов моей команды смог основательно взломать этот сайт, вся наша команда, в итоге смогла получить

полный контроль над производственной средой нашего нанимателя. Мы выиграли это соревнование.

Как я создал “Камерный Вирус”

Однажды мне стало интересно, как можно заставить мой “вредоносный” код автоматически запускаться при подключении цифровой камеры. Я попробовал один трюк, и он сработал. Я показал это своему коллеге, и он обнаружил, что вирус может запускаться с любого подключаемого устройства с картой памяти. Мы еще немного протестировали мой код и он всегда работал. Он мог запускаться с цифровых камер, музыкальных плееров и мобильных телефонов. В то время, моим нанимателем была компания, занимающаяся тестированием на проникновение, и они были в восторге от моего открытия. Мы решили, что я представлю его на предстоящей конференции Blackhat. Я также сообщил о своем открытии соответствующему производителю. Они убедились в наличии этой проблемы и попросили несколько месяцев, чтобы выпустить патч, исправляющий ее.

Это была дилемма. Если ждать, то для участников конференции Blackhat, эта информация уже не будет такой интересной. Это будут “вчерашние” новости, для которых уже выпустили патч. Если не ждать, то производитель и его клиенты будут уязвимы до тех пор, пока производитель не сможет “залатать дыру”. Помню, я долго разрывался между двумя вариантами. В конце концов, я решил, что я порядочный хакер и для меня важнее безопасность в мире информационных технологий, а не собственные эго и слава. Я дал производителю время. Через несколько месяцев, та же уязвимость была обнаружена на другом общественном мероприятии, но к тому времени, производитель уже был готов, и немедленно выпустил патч. Мой вклад в обнаружение этой уязвимости остался незамеченным, потому что тогда все говорили, что уязвимость обнаружили недавно. Мой “камерный вирус” так и не стал серьезной угрозой, так что мы все остались в выигрыше.

Как стать пентестером

Тестирование на проникновение (пентест) позволяет легально взламывать различные объекты, используя все возможные хакерские методы, и получать от этого удовольствие. Для этой работы нужно уметь больше, чем просто взламывать компьютеры и устройства, хотя наличие этих умений используется в качестве отправной точки.

Методология взлома

Чтобы стать успешным пентестером необходимо следовать тем же шагам методологии взлома, которые описаны в Главе 2:

1. Сбор информации
2. Проникновение
3. Опционально: Обеспечение простого доступа в будущем
4. Разведка системы
5. Опционально: Горизонтальное или вертикальное движение
6. Выполнение запланированного действия
7. Опционально: Заметание Следов

Первым делом, получите необходимое разрешение

Самое главное отличие киберпреступников от пентестеров заключается в том, что у последних есть разрешение на атаку/тестирование соответствующих объектов. У вас должно быть предварительно задокументированное и подписанное разрешение от компании или владельца объектов, или человека, у которого есть официальная доверенность от владельца.

Неэтично обнаружить в чьем-то сайте уязвимость, и просить, чтобы вас взяли на работу. Многие начинающие пентестеры используют эту тактику, чтобы получить профессиональную работу. В большинстве случаев, они думают, что приносят пользу, и что, компания, с которой они связались, возможно посчитает их открытие невероятно полезным и предложит им работу. На самом деле, независимо от истинных намерений, такие действия, в основном, рассматриваются, как неэтичные, представляющие угрозу, и, скорее всего, незаконные. Если вы действительно случайно обнаружили уязвимость, просматривая интернет или "играясь" с устройством, сообщите о ней производителю/владельцу без лишнего шума и помогите ему, если у него возникнут вопросы. Вас даже могут взять на работу, но не нужно сразу просить денег или трудоустройства.

Получите подписанный контракт

У пентестера всегда должен быть подписанный контракт. В нем должны быть указаны имена участвующих сторон, сфера охвата обязательств (какие цели нужно проверить, даты, что должно быть сделано, и так далее), соглашение о неразглашении для защиты обеих сторон, инструменты и методы, которые будут использованы и предупреждение об освобождении от ответственности за возможный сбой в работе при более тщательном тестировании. Если у вас на руках нет шаблона контракта, свяжитесь с юристами и/или поищите такой шаблон в интернете.

Написание отчета

Верх профессионализма - это хорошо написанный, детальный отчет. В начале должно быть краткое содержание, за которым следует более детальное описание проекта, сферы охвата обязательств, проделанных работ и обнаруженных уязвимостей. Приложите описания обнаруженных уязвимостей в качестве отдельных вложений. Многие консультанты считают, что чем длиннее отчет, тем лучше. Лично я думаю, что клиенты больше ценят короткие отчеты с детальной информацией об обнаруженных уязвимостях. Но всегда нужно иметь при себе более подробную информацию, которую можно предоставить и обсудить.

Сертификация

Получите сертификат. Наличие сертификата не означает, что вы умнее или глупее того, у кого его нет, но он несомненно дает вам преимущество при устройстве на работу. Сертификаты позволяют легко определить необходимый минимум знаний и профессионализма. В следующих разделах описаны сертификаты организаций, с которыми я знаком и которые я могу рекомендовать.

CISSP

Без сомнения сертификат CISSP (Сертифицированный профессионал в области безопасности информационных систем, Certified Information Systems Security Professional) (https://www.isc2.org/cissp/default.aspx) Международного консорциума по сертификации в области безопасности информационных систем (International Information Systems Security Certifications Consortium, ISC^2) (https://www.isc2.org/) является самым желанным и востребованным сертификатом в сфере информационной безопасности. Их основной экзамен по оценке знаний в области защиты информации охватывает восемь различных сфер Общего объема знаний (Common Body of Knowledge, CBK). Сертификационный тест состоит из 250 вопросов с множеством вариантов ответа, который нужно пройти менее, чем за шесть часов. У кандидатов уже должен быть опыт работы от четырех до пяти лет в двух (или более) сферах CBK, и они должны быть одобрены другим обладателем CISSP. Цена за экзамен начинается от $599.

SANS Institute

Я большой поклонник всего, что делает SANS Institute (SysAdmin, Networking, and Security Institute) (http://www.sans.org), будь то обучение, исследования, образовательный материал, книги или сертификаты. В Главе 42 мы поговорим о

Стивене Норткатте, сооснователе этой организации. Если вы хотите стать уважаемым техническим специалистом, то вам нужен их сертификат. Их бренд SANS Technology Institute даже предлагает две степени магистра. У SANS много сертификатов, начиная от узконаправленных специализаций (например, вредоносное ПО, мониторинг, файрволы, безопасность на локальных машинах и управление системой безопасности), и заканчивая их самым уважаемым званием
эксперта по безопасности GIAC (Global Information Assurance Certification) (http://www.giac.org/certifications/get-certified/roadmap). Сертификаты GIAC классифицируются, в зависимости от знаний в следующих областях:

- Защита от кибератак и кибербезопасность на предприятиях
- Тестирование на проникновение
- Цифровая криминалистика и мероприятия по реагированию
- Разработчик
- Менеджмент и управление
- Эксперт по безопасности

Самые популярные экзамены GIAC - это экзамен GIAC Information Security Professional (Профессионал по информационной безопасности) (http://www.giac.org/certification/gisp), GIAC Certified Incident Handler (Сертифицированный специалист по экстренным ситуациям) (http://www.giac.org/certification/gcih) и GIAC Reverse Engineering Malware (Специалист по воспроизведению вредоносного ПО) (http://www.giac.org/certification/grem), но курсы GIAC охватывают весь диапазон специальностей, включая знания Windows, веб-серверов, тестирования на проникновение, безопасности Unix-систем, беспроводных сетей, программирования, управления персоналом и сопровождения программного продукта. Тесты GIAC проводятся после прохождения курсов в SANS, которые, как правило, длятся неделю. Если покупать GIAC-тест вместе с соответствующим обучением, то цена составит $659. Но любой тест можно купить отдельно (без прохождения подготовки) за $1149.

Для тех, кого интересуют сертификаты по системам Unix и Linux, SANS также предлагает сертификат администратора безопасности в системах Unix (GIAC Certified Unix Security Administrator, GCUX) (http://www.giac.org/certification/certified-unix-security-administrator-gcux).

Certified Ethical Hacker (CEH)

Сертификат Certified Ethical Hacker (Сертифицированный этичный хакер, CEH) (https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/)
Международного совета консультантов по электронной торговле (EC-Council)

высоко ценится, а получая его, вы становитесь истинным хакером в белой шляпе (то есть, профессиональным пентестером). Благодаря CEH, я узнал о некоторых интересных инструментах взлома, которые до сих пор использую. Экзамен состоит из 125 вопросов с множеством вариантов ответа, и на него отводится до четырех часов. Плата за участие в программе составляет $100.

EC-Council также проводит множество других полезных экзаменов, включая экзамен на следователя-криминалиста по взломам (Computer Hacking Forensic Investigator) (https://cert.eccouncil.org/computer-hackingforensic-investigator.html), лицензированного пентестера (Licensed Penetration Tester) (https://cert.eccouncil.org/licensed-penetration-tester.html), сертифицированного специалиста по экстренным ситуациям (Certified Incident Handler) (https://cert.eccouncil.org/ec-council-certified-incidenthandler.html) и сертифицированного профессионала по восстановлению в аварийных ситуациях (Certified Disaster Recovery Professional) (https://cert.eccouncil.org/ec-council-disaster-recovery-professional.html). У них даже есть экзамен на начальника службы информационной безопасности (Chief Information Security Officer) (https://cert.eccouncil.org/certified-chief-information-security-officer.html).

CompTIA Security+

Ассоциация индустрии информационных технологий (Computing Technology Industry Association, CompTIA) (https://certification.comptia.org/) предлагает всеобъемлющие экзамены для новичков по поддержке IT-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). Так как экзамены CompTIA часто сдают новички в информационной индустрии, их сертификаты считаются самыми базовыми, а экзамены - слишком легкими. Но это не правда. Экзамены включают в себя множество тем, и чтобы их сдать, нужно старательно готовиться. Помимо знания других тем, чтобы получить сертификат CompTIA Security+, необходимо хорошо знать безопасность сетей, криптографию, управление идентификационной информацией, технику безопасности во время эксплуатации, угрозы и настройку безопасности на локальной машине. На тест отводится 90 минут, и в нем 90 вопросов. Цена $311.

ISACA

Ассоциация контроля и проверки информационных систем (Information Systems Audit and Control Association, ISACA) (https://www.isaca.org) предлагает ряд уважаемых, среди профессионалов, сертификатов по проверке, управлению и применению стандартов. В том числе, сертификаты аудитора информационных

систем (Certified Information Systems Auditor, CISA) (http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx), менеджера информационной безопасности (Certified Information Security Manager, CISM) (http://www.isaca.org/Certification/CISMCertified-Information-Security-Manager/Pages/default.aspx), по управлению корпоративными IT (Certified in the Governance of Enterprise IT, CGEIT) (http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Pages/default.aspx) и по управлению рисками использования информационных систем (Certified in Risk and Information Systems Control, CRISC) (http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/default.aspx). Если вы бухгалтер или аудитор, то эти экзамены могут подтвердить ваши навыки, поскольку они связаны с компьютерами и информационной безопасностью.

Сертификаты производителей

Во многих компаниях, таких как Microsoft, Cisco, и RedHat, есть экзамены, посвященные информационной безопасности.

Много лет назад в Microsoft были отдельные экзамены для специалистов по безопасности, например, экзамен MCSE: Security. Но когда безопасность приобрела важнейшее значение для всех платформ и технологий, вопросы по ней появились во всех экзаменах. После анонса нового (еще в разработке) экзамена по безопасности Windows Server 2016 (Securing Windows Server 2016) (https://www.microsoft.com/en-us/learning/exam-70-744.aspx) безопасности стали уделять больше внимания. Этот экзамен охватывает гораздо больше вопросов, а не только техническое обеспечение безопасности. В нем есть вопросы по проектированию красного/зеленого леса (red/green forest), JIT-администрированию (just-in-time - точно в срок), JEA-администрированию (just enough - сколько нужно) и последним технологиям Microsoft для обеспечения безопасности, таким как Advanced Threat Analytics (ATA). Иногда, техническим специалистам по безопасности нужно пройти тест Microsoft's Security Fundamentals (https://www.microsoft.com/en-us/learning/exam-98-367.aspx), который стоит $127.

Экзамены в Cisco всегда считались одними из самых сложных в индустрии. Получить сертификат эксперта сетей Cisco (Cisco Certified Internetwork Expert, CCIE) (https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccie-program.html) сложнее всего в индустрии. Согласно Cisco, этот сертификат получают менее 3% претендентов, даже при условии, что они тратят тысячи долларов, создают домашние лаборатории и тратят, в среднем, полтора года на обучение. Сертификат специалиста по сетям (Cisco's Certified Network Associate (CCNA) (https://www.cisco.com/c/en/us/training-events/training-

certifications/certifications/associate/ccna-security.html) легче получить, но, несмотря на это, он высоко ценится. Чтобы получить сертификат CCNA, нужно иметь другой действующий сертификат Cisco. После получения сертификата CCNA (или прохождения любой сертификации CCIE) можно пройти экзамен на получение сертификата профессионала по маршрутизации и коммутации (Cisco Certified Network Professional, CCNP) (https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security.html). Но экзамен CCIE (https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccie-security.html) - это экзамен для самых крутых парней. Он состоит из двух частей: письменной, которая длится два часа (и которую нужно сдать первой), и лабораторной, проводимой в течение восьми часов. Все сертификаты Cisco сложно получить, но наличие любого из сертификатов CCIE позволяет неплохо зарабатывать практически в любой стране мира.

Red Hat позволяет получить десятки сертификатов (https://www.redhat.com/en/services/all-certifications-exams), и как и любой крупный производитель, эта компания предлагает, по крайней мере один сертификат специалиста по информационной безопасности. Экзамен в Red Hat позволяет получить сертификат специалиста по улучшению защиты серверов (Red Hat Certificate of Expertise in Server Hardening) (https://www.redhat.com/en/services/certification/rhcoe-server-hardening). Помимо знаний об улучшении защиты Linux-серверов, успешные кандидаты должны быть готовы к работе с Common Vulnerabilities and Exposure (CVE) и отчетами Red Hat Security Advisory (RHSA). Цена экзамена $600.

Профессиональный институт Linux (Linux Professional Institute, LPI) (https://www.lpi.org/) предлагает независимые от производителя сертификаты по безопасности систем Linux (https://www.lpi.org/study-resources/lpic-3-303-exam-objectives/). Экзамен LPIC-3 Exam 303 включает множество тем, касающихся безопасности, и чтобы его сдать, кандидаты должны сначала успешно пройти четыре экзамена LPI более низких уровней. Стоимость экзаменов LPI третьего уровня, таких как LPIC-3 303 составляет $188.

Как уже было сказано выше SANS также предлагает сертификат администратора безопасности в системах Unix (GIAC Certified Unix Security Administrator, GCUX) (http://www.giac.org/certification/certified-unix-security-administrator-gcux).

В Apple, судя по всему, нет отдельных экзаменов по безопасности, но обычные экзамены по ОС можно найти тут: https://training.apple.com/us/en/courses

Каждый полученный мной сертификат улучшил мои навыки. Получение сертификата помогает улучшить знания, карьеру и возможность найти работу.

Будьте этичными

Работайте этично и профессионально. Никогда не совершайте несанкционированных действий, чтобы улучшить свое положение за счет проблем клиента. Если вы сомневаетесь в этичности какого-то действия, то скорее всего, это действие не этично. В Главе 50 описан кодекс этичного хакера.

Минимизируйте риск сбоев в работе системы клиента

Постарайтесь сделать все возможное, чтобы не стать причиной сбоев в работе системы клиента. Во многих инструментах для тестирования есть "безопасный режим", который уменьшает этот риск. Всегда тщательно проверяйте инструменты и методологию, перед их широким применением. Всего один раз я вызвал сбой в работе всей системы, и мне до сих пор стыдно. Это произошло, потому что я не уделил достаточно внимания проверке перед тестированием.

Если вы последуете всем шагам, описанным в этой главе, то, скорее всего, станете успешным пентестером, которого раз за разом будут приглашать в различные проекты.

В Главе 26 представлен Аарон Хигби, один из лучших пентестеров, которых я когда-либо встречал, а в Главе 27 - Бенилд Джозеф, специалист по тестированию на проникновение, эксперт по кибербезопасности и известный этичный хакер.

Глава 26. Профиль: Аарон Хигби

Езда на автомобиле Аарона Хигби - это неповторимый опыт, знакомый только заядлым технарям, которые постоянно стремятся что-то усовершенствовать. В его машине столько гаджетов и датчиков, подключенных к электронному блоку управления, что она сильно напоминает машину из *Назад в будущее*. Те, кто знает его хотя бы несколько лет не удивляются этому. Хигби всегда доводит дело до конца. Он либо полностью вовлечен в процесс, либо вовсе не заинтересован. Очевидно, что девиз "Иди до конца или иди домой" играет большую роль в его жизни.

Впервые я работал с Хигби, когда проводил тестирование на проникновение в крупнейшей в мире кабельной компании. Я рассказывал об этом в предыдущей главе про тестирование на проникновение, но кое-что упустил. Мы успешно взломали не только объект, интересовавший компанию, ТВ-приставку, но и всю эту компанию. И это было в первый же день! Хигби стало скучно, когда не осталось ничего интересного, а у нас была неделя по договору, поэтому он начал взламывать оборудование, которое нам дала эта компания. Он стал проводить манипуляции с оборудованием, которое получают клиенты: переключал провода, перемычки на материнской плате и менял полюса кабеля питания. Он продолжал пробовать разные конфигурации, чтобы взломать оборудование, и в один момент, в буквальном смысле сжег его. Приставка задымилась, и мы в спешке, стали отключать электричество и тушить небольшой пожар. Нам пришлось подождать несколько минут, пока дым развеется, чтобы узнать, сработала ли пожарная сигнализация и нужно ли нам уходить.

Когда дым развеялся, мы все вдохнули с облегчением, и я удивился, когда увидел, что Хигби продолжил взламывать оборудование. Никакие уговоры остальной команды не могли его остановить. В конце концов, он стал причиной еще большего возгорания оборудования, которое уже нельзя было так легко потушить. Все время, пока мы бежали от, теперь уже гарантированного, срабатывания средств тушения, он смеялся, и, не предупредив меня, снимал все на телефон. Через несколько минут его видео оказалось в интернете. Эта история абсолютно точно не о том, что должны делать другие пентестеры. Было не лучшей идеей делать то, что хотя бы в теории может вызвать пожар. Но этот забавный случай наглядно демонстрирует, каково было работать с Хигби. Многие его друзья и коллеги могут рассказать подобные истории.

Будучи веселым парнем, Хигби один из лучших, целеустремленных пентестеров. Он вырос в религиозной семье со строгими правилами. Я думаю

такое строгое воспитание стало причиной его страсти к жизни и желания рассмешить всех вокруг, включая себя. Сегодня он намного профессиональнее относится к работе, но с тем же юношеским восторгом борется с хакерами и спамерами.

Позже, мы оба ушли из компании, в которой работали. Я ушел в Microsoft, а Хигби стал сооснователем собственной, невероятно успешной компании PhishMe (https://phishme.com/). PhishMe специализируется на подготовке пользователей к фишинговым атакам. В частности, с помощью PhishMe, можно легко сделать "поддельную" фишинговую рассылку, сэмулировать фишинг, с помощью которомй можно узнать, кто из сотрудников выдаст важные данные. Такие рассылки можно было делать и до PhishMe, но с их помощью это стало невероятно легко. С годами компания расширилась, сейчас в ней работают 350 сотрудников, а доход составляет $12 миллионов и продолжает расти. Несмотря на то, что у меня нет финансовых проблем, скажем так, у Хигби дела еще лучше.

Я спросил, как он попал в сферу информационной безопасности. Он ответил: "Я начал интересоваться компьютерами во времена BBS (bulletin board system, электронная доска объявлений), и чтобы попасть на некоторые BBS нужно было совершать звонки на дальнее расстояние, которые в то время были дорогими. Так что я начал изучать способы телефонного обмана, чтобы бесплатно совершать такие звонки, и благодаря этому, начал изучать другие хакерские приемы. Моя первая работа в сфере информационной безопасности была в компании EarthLink… я в буквальном смысле был тем парнем, который отвечал за электронный адрес abuse@earthlink.net. Я обрабатывал все, что приходило на этот адрес. Я фильтровал спам, мошенничество с использованием банковских карт, обрабатывал требования по соблюдению правовых норм и все, что туда приходило. Мне настолько нравилась эта работа, что я бросил колледж. Родители говорили, что я совершаю большую ошибку. Они думали, что интернет - это преходящее увлечение, как гражданские рации".

Я очень уважаю стремление Хигби и PhishMe бороться именно с фишингом. Многие их конкуренты расширили свою деятельность и стали предлагать другие услуги, но PhishMe продолжают работать только в этом направлении. И, судя по всему, такая целеустремленность PhishMe приносит гораздо больше доходов им и их клиентам. Хигби отметил: "Некоторые люди не понимают, чем занимается PhishMe. Они думают, что это пустая трата времени, что вместо того, чтобы помогать людям решать нынешние проблемы фишинга по электронной почте, нужно исправлять саму электронную почту… то есть, сделать компьютеры абсолютно безопасными по умолчанию.

Это отличная мысль. Но, в то же время, это заоблачные мечты. Я имею ввиду, впервые я увидел письмо с фишингом в 1997-ом, когда работал в EarthLink. Если бы мне тогда сказали, что это так и останется проблемой… огромной проблемой, как сейчас… и что я буду зарабатывать тем, что помогаю

ее решить, то я бы не поверил. Главная проблема в том, что принцип работы электронной почты ненадежен, и его вряд ли исправят в ближайшем будущем. Десять лет спустя он все еще будет ненадежен. На протяжении многих лет было немало попыток привнести какие-то дополнения, чтобы сделать электронную почту лучше, но ни одно из этих дополнений так и не "прижилось". И я этого не понимаю, ведь мы исправили многие другие протоколы, а от некоторых избавились окончательно, например, от Telnet. Никто больше не использует Telnet. Вместо него мы используем SSH. Но по каким-то причинам email-протокол продолжает существовать в неизменном виде, несмотря на свои огромные проблемы, и раз уж его все еще используют, я хочу помогать компаниям сделать его безопаснее".

Я рассказал Хигби, что удивлен нежеланием многих компаний проводить антифишинговую подготовку, потому что это должна быть задача номер один или номер два, с помощью которой можно снизить риски в информационной безопасности. Он ответил: "Отчасти проблема заключается в том, что некоторые компании проводят фишинговые тесты без подготовки сотрудников, и это заканчивается проблемами. Мы уделяем этому много внимания. Мы не проводим внезапно тест PhishMe. Мы просим компании сообщить сотрудникам и менеджерам, что в течение следующего года мы будем проводить фишинг-тесты. Меньше неожиданностей, больше подготовки. Также мы обучаем клиентов, как решать подобные проблемы, так что выигрывают все.

Наверное, больше всего в интервью с Хигби мне понравилось то, что он остался таким же веселым и жизнерадостным, каким был во время нашей совместной работы более десяти лет назад. Он сказал, что создавать и продвигать бизнес было очень тяжело, но это оправдало ожидания и все еще доставляет удовольствие. Видимо, также думают сотрудники его компании. Недавно, в издании *Washington Business Journal* PhishMe признали одной из лучших компаний для работы, к тому же недавно в Канкуне состоялась ежегодная встреча сотрудников этой компании.

Боже, почему 10 лет назад я не додумался открыть собственную антифишинговую компанию?

Подробнее об Аароне Хигби

Подробнее об Аароне Хигби вы можете найти на этих ресурсах:

- Твиттер Аарона Хигби: https://twitter.com/higbee
- Профиль Аарона Хигби в LinkedIn: https://www.linkedin.com/in/aaron-higbee-6098781
- Блог Аарона Хигби: https://phishme.com/author/aaronh/

Глава 27. Профиль: Бенилд Джозеф

25-летний Бенилд Джозеф из Городского округа Бангалор, Индия - один из самых молодых специалистов, представленных в этой книге. Но за короткие 8 лет работы в этой сфере (по меркам других участников интервью) у него уже есть немалый список достижений, и он старательно работает над улучшением информационной безопасности своей страны и города. Он специализируется на безопасности веб-приложений, и уже обнаружил критические уязвимости на многих популярных веб-сайтах, включая Facebook, AT&T, Sony Music, BlackBerry и Deutsche Telekom. Этого было достаточно, чтобы его заметили. В данный момент, он главный исполнительный директор в "Th3 art of h@ckin9", подразделении Международного проекта безопасности информационных технологий (International IT Security Project, организация, поддерживаемая правительством Индии), а также член правления Ассоциации по безопасности информационных технологий (Information Systems Security Association, ISSA) Индии. Microsoft Social Forum включили его в "Десятку лучших этичных хакеров Индии", а издание *Silicon India* включило его в список "8 самых знаменитых этичных хакеров Индии". Он постоянно пишет и преподает.

Индия - это удивительная развивающаяся страна, где много ярких людей, но в то же время, устойчивое развитие интернета в этой стране началось примерно десять лет назад. Большая часть населения живет в бедности. Принимая это во внимание, я спросил Джозефа, как он попал в сферу информационной безопасности. Он ответил: "Мне всегда было интересно взламывать, и поначалу, я совсем не интересовался информационной безопасностью. В то время в Индии об этом никто не знал и не говорил. В основном, мне было интересно взламывать электронную почту своих друзей. Я решил пойти на курсы этичного хакера, чтобы больше узнать о способах взлома. Помню, я даже говорил инструктору, что я здесь не для того, чтобы учиться быть этичным хакером или специалистом по информационной безопасности, мне просто интересно взламывать электронную почту друзей. Я был уверен, что получение сертификата - это пустая трата времени. Но он что-то увидел во мне, и научил меня основам этичного взлома и информационной безопасности, которые я узнал. Он стал моим наставником. Даже когда я все больше узнавал об этичном взломе, он говорил, что мне еще многому нужно научиться, чтобы стать профессионалом по безопасности. Он бросал мне вызовы, и я продолжал учиться".

Сейчас Джозеф работает на агентства, борющиеся с киберпреступностью и на государство, включая такие проекты как Бюро расследований

киберпреступлений (Cyber Crime Investigation Bureau, CCIB), Международная группа оперативного реагирования на киберугрозы (International Cyber Threat Task Force, ICTTF) и Общественную инициативу кибербезопасности (Cyber Security Forum Initiative, CSFI). Он также является соавтором *CCI*, книги написанной для правоохранительных структур Индии. Он специализируется на пентесте веб-приложений (Web Application Penetration testing) и расследовании цифровых преступлений (Digital Forensic Investigation). Неплохо для парня, который просто хотел взламывать электронную почту друзей. Он продолжил: "На данный момент я уже работал во многих компаниях и проектах. Мои роли продолжают меняться. Сейчас я работаю на правительство Индии в проекте по киберслежке, мы стараемся остановить киберпреступников. Также я много думаю о кибероружии, которое часто применяется против Индии. Не только против правительства и бизнеса, но и против обычных граждан".

Я спросил о самой большой проблеме информационной безопасности, с которой столкнулась его страна. Он ответил: "Индия входит в десятку стран с самыми развитыми информационными технологиями, но у нас не развита информационная безопасность. Десять лет назад о ней даже не слышали. Ее не преподавали. Не было работы специалиста по информационной безопасности. Долгое время в моей стране были большие экономические проблемы. Поначалу, если кто-то хотел купить себе компьютер, то это приходилось делать через интернет-магазин. Сейчас компьютер может быть либо у людей дома, либо в руках, в виде смартфона. Так что компьютеры и проблемы информационной безопасности в моей стране - это новшество. У нас много врачей, юристов, инженеров и других специалистов, но не хватает людей, занимающихся информационной безопасностью. Однако, ситуация меняется. Правительство и бизнес поняли, что нам нужна надежная защита информации и хорошие специалисты. Сегодня во многих университетах есть программы магистратуры по информационной безопасности. Правительство понимает, насколько это важно, и запускает соответствующие программы. Я провожу много времени, путешествуя по Индии и другим уголкам планеты, преподавая информационную безопасность. Сейчас Индия изменилась, и я помогаю ее развитию".

Остается только надеяться, что в Индии и остальных странах достаточно таких людей, как Бенилд Джозеф.

Подробнее о Бенилде Джозефе

Подробнее о Бенилде Джозефе вы можете найти на этих ресурсах:

- Бенилд Джозеф в LinkedIn: https://www.linkedin.com/in/benild
- Бенилд Джозеф в Google+: https://plus.google.com/+BenildJoseph
- Видео Бенилда Джозефа на YouTube о проектах Kaizen и Hacker5: http://www.youtube.com/watch?v=BH_BNXfj0pQ

Глава 28. DDoS-атаки

Возможно вы считаете, что у вас лучшая система безопасности т.к. ваше ложное чувство безопасности не обнаруживает проблем, которые вы не можете контролировать. Поприветствуем распределенные атаки типа "отказ в обслуживании" (DDoS-атаки). То, что начиналось с перегрузки сервера одним хакером, который отправлял серверу намного больше трафика, чем сервер мог обработать, превратилось в масштабную войну на разных уровнях (модели OSI), где трафик отправляется хакерскими группами или профессиональными поставщиками подобных услуг. Сегодня масштабные DDoS-атаки часто используют домашние компьютеры обычных пользователей, отправляя сотни гигабит вредоносного трафика в секунду. DDoS-атаки совершаются по разным причинам, включая месть, вымогательство, желание поставить в неловкое положение, политические цели и даже с целью получить преимущество в онлайн-играх.

Виды DDoS-атак

Существует множество видов DDoS-атак. В следующих разделах описаны самые заметные.

Отказ в обслуживании

Обычная DoS-атака осуществляется с одного компьютера, чтобы "зафлудить" (flood) жертву огромным потоком трафика и вызвать отказ в обслуживании. Самый простой пример такой атаки, который применялся раньше - это "ping-флуд", когда на сетевое оборудование отправлялось максимально возможное количество ICMP-пакетов (эхо-запросов). Затем начал использоваться флуд пакетов через протокол TCP, который позволял генерировать больше трафика из-за "трехэтапного согласования" (3-way handshake). На смену отправки запросов через протокол TCP пришел UDP-флуд, так как можно «заспуфить» IP-адрес источника, что усложняет отслеживание и блокировку UDP-флуда.

Эти простые виды атак дали начало масштабным DDoS-атакам, использующим множество хостов (иногда десятки тысяч), целью которых является только один объект. С помощью обычной DoS-атаки можно отправлять десятки мегабит вредоносного трафика в секунду, в то время как самая "слабая" DDoS-атака позволяет отправлять сотни мегабит в секунду. Никто уже не удивляется, если DDoS-атака передает менее 600 гигабит

трафика в секунду. Каждый год устанавливается новый рекорд. Первая атака, в которой будет терабит (1000 гигабит) трафика в секунду, может быть совершена к моменту выхода этой книги или сразу после него.

Прямые атаки

Прямая DoS-атака совершается непосредственно одним компьютером, генерирующим весь вредоносный трафик. Злоумышленник может (в случайном порядке) менять IP-адреса, чтобы оставаться незамеченным, но в таких атаках весь трафик отправляется с одного компьютера, без посредников. Сейчас прямые атаки редко используются, потому что их легко обнаружить, понять, что это за атака и снизить негативные последствия.

Reflection-атаки

Такой вид атак использует промежуточные компьютеры для вызова отказа в обслуживании. Во многих случаях, для применения такой DDoS-атаки используется вредоносное ПО, установленное на "компьютерах-ботах". Они ожидают команду атаковать конкретную цель. Как правило, цель атакуют десятки или сотни тысяч компьютеров. Основной сервер "командования и управления" (command-and-control, C&C) отправляет инструкции, которым следуют боты. Таким образом, несколько пакетов от C&C-сервера могут превратиться в миллионы пакетов в секунду.

Усиление (Amplification)

Усиленные DDoS-атаки используют "шумные" протоколы, которые на один пакет отвечают несколькими (это и есть усиление), отправляя их жертве. Например, атакующий может отправить веб-серверу один искаженный запрос, в котором IP-адрес будет изменен на IP-адрес жертвы. Промежуточный веб-сервер получает искаженный запрос и отправляет на первоначальный IP-адрес (то есть, IP-адрес жертвы) множество ответов или сообщений об ошибке. Еще один распространенный вид усиленных DDoS-атак использует DNS-серверы, отправляя им запросы, на которые DNS-сервер отвечает несколькими, если не десятками, пакетов, отправляя их жертве. Подробнее об атаках DNS-усиления можно прочитать здесь: https://technet.microsoft.com/en-us/security/hh972393.aspx. Чем больше усиление, тем счастливее злоумышленник. Когда усиленные запросы отправляются десятками или сотнями тысяч ботов, получается масштабная DDoS-атака.

Применение на каждом уровне модели OSI

DoS/DDoS-атаки могут осуществляться на каждом уровне модели OSI (физическом, сетевом, транспортном, сеансовом, представительском, канальном и прикладном). Физическая атака реализуется путем физического уничтожения центрального служебного оборудования, например, роутера, DNS-сервера или сетевой линии. Все остальные атаки используют один или несколько протоколов на разных уровнях.

Усиливающиеся атаки

Сегодня самые успешные DDoS-атаки используют широкий, изменяющийся набор атак на всех уровнях модели OSI. Они могут начинаться, как простой флуд в протоколах нижнего уровня и, со временем, увеличивать количество трафика с небольшими паузами. Сначала может использоваться простая reflection-атака, а затем могут применяться методы усиления. Затем хакеры могут переходить на верхние уровни модели OSI и добавлять еще больше трафика. Часто злоумышленники используют прикладной уровень, подделывая трафик, чтобы тот выглядел, как трафик от пользователей и при этом они начинают занимать огромную часть канала.

Таким образом, как только жертва решает, что все под контролем, хакеры начинают использовать другие виды DDoS-атак. Начиная атаку медленно, чтобы жертва решила, что понимает масштаб проблемы и знает, как ее решить, через какое-то время злоумышленники меняют подход. Жертва и защитники теряются и не могут сразу выстроить грамотную защиту. И каждый раз, когда жертва думает, что решение найдено, атака снова меняется, каждый раз разные направления, и так до тех пор, пока у атакующего не закончатся варианты атак.

Атака на исходящий и входящий каналы

В последнее время на сайтах, являющихся целью DDoS-атак, реализуются технологии защиты от этих атак, и как правило, такие технологии довольно неплохо справляются со своей задачей. В таких случаях хакеры ищут зависимые объекты в этой же сети. Сотни гигабит вредоносного трафика в секунду вынудят практически любого провайдера молить о пощаде. Провайдеру придется решить, стоит ли поддержание работоспособности одной жертвы неудобства всех остальных клиентов. Если повезет, у жертвы будет время перейти на другой сервис перед полным отключением, и продолжить работу уже с другим провайдером, который не боится принять на себя стремительную атаку хакеров. Бывает и так, что жертву просто полностью

отключают на несколько дней, если не больше, пока последствия DDoS-атаки не будут полностью устранены. Каждый год бывает несколько случаев, когда сайт жертвы навсегда пропадает из интернета.

Подробнее о DDoS-атаках можно прочитать по ссылкам: 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 продуктов, позволяющих реализовать DDoS-атаки.

Инструменты

В интернете есть десятки инструментов и скриптов для реализации DoS и DDoS-атак. Достаточно просто вписать "инструменты для DDoS-атак" в адресной строке браузера, чтобы найти все, доступные в сети. Многие называют свои инструменты «инструментами для тестирования», чем часто вводят пользователей в заблуждение. Вот 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-Http-Unbearable-Load-King.html). Хакеры должны использовать эти инструменты только против сайтов, которые дали на это разрешение. Многие начинающие хакеры проходят сложный путь изучения, попадая под арест, потому что очень сложно спрятаться, если за тобой наблюдают нужные люди.

DDoS-сервисы

В интернете есть даже десятки сервисов, позволяющих запустить DDoS-атаку за определенную плату. У многих ценник ниже $100. Как и в случае с инструментами, многие сервисы утверждают, что предоставляют такие возможности для тестирования (но, при этом, не проверяют у пользователя наличие разрешения на применение этих сервисов против определенных сайтов). К сожалению, даже сервисы, предоставляющие защиту от DDoS-атак, были замечены и в их реализации. В отношении некоторых из таких двуличных сервисов была проведена проверка, и их закрыли, но остальные продолжают процветать. Журналист, ведущий собственное расследование, Брайан Кребс, написал по этому поводу несколько замечательных историй, включая вот эту: https://krebsonsecurity.com/2016/10/spreading-the-ddos-disease-and-selling-the-cure/.

Способы защиты от DDoS-атак

Существует множество способов защиты от DDoS-атак.

Подготовка

Весь персонал, занимающийся размещением вашего сайта и сервисов должен знать о DDoS-атаках и о том, как их предотвратить. Подготовка персонала - это первый шаг к обнаружению и предотвращению.

Стресс тесты

Проводите стресс тесты своих сайтов, возможно, с использованием тех же "тестирующих" инструментов, которыми пользуются хакеры. Думайте, как хакер и атакуйте все узлы и зависимые объекты, необходимые для поддержки работоспособности вашего сайта. Выясните, что нужно, чтобы "отключить себя от интернета" и найдите слабые узлы. Как только вы их найдете, исключите самые простые и оцените соотношение цена/польза для остальных.

Правильная настройка сети

Убедитесь, что ваши сайты и сервисы используют файрволы, способные обнаружить и остановить DDoS-атаки. Проверьте, чтобы все локальные машины были настроены так, чтобы выдержать DDoS-атаку с минимальными перебоями в обслуживании. Минимизируйте риск настолько, насколько это возможно. С другой стороны, многие компании используют "соглашение о взаимодействии" с другими производителями и даже конкурентами, чтобы оказавшись под воздействием DDoS-атаки, иметь возможность сменить провайдера или позаимствовать ресурсы. Некоторые из таких соглашений используют бесплатные ресурсы или минимальную комиссию за покрытие убытков.

Исключите потенциально слабые места

Создавая сервис, подумайте обо всех местах, потенциально уязвимых для DoS-атак. Например, Microsoft поняли, что через протокол RDP (Remote Desktop Protocol) к системам Windows может подключаться огромное количество пользователей, не прошедших аутентификацию, эффективно расходуя все ресурсы. Microsoft изменили RDP таким образом, что теперь необходимо пройти аутентификацию, перед тем, как Windows начнет выделять большое количество ресурсов, а также ограничили количество попыток соединения, которые одновременно могут осуществляться с различных источников. Благодаря двум

этим новым функциям, осуществить DoS-атаку, используя протокол RDP стало намного сложнее.

Сервисы, предоставляющие защиту от DDoS-атак

Существует множество премиум сервисов, предоставляющих такую защиту, включая Imperva (https://www.incapsula.com/) и Prolexic/Akamai (http://www.prolexic.com/). Для защиты клиентов многие из них используют сочетание значительного расширения пропускной способности канала и специализированные средства безопасности, направленные на снижения влияния DDoS-атак. Минус в том, что такие сервисы достаточно дорогие, и многие компании не могут позволить себе такие траты, чтобы защититься от атаки, которой может и не быть. Если вы все же решите использовать такой сервис, проведите расследование и убедитесь, что поставщик таких услуг не только предоставляет защиту от DDoS-атак, но и не совершает их.

В мире существует не только огромное количество хакеров, совершающих DDoS-атаки, но и защитников, которые их предотвращают. Если продумать защиту от DDoS-атак, то можно существенно снизить их негативное воздействие.

В Главе 29 мы поговорим о Брайане Кребсе, журналисте, освещающим вопросы информационной безопасности и ведущим собственные расследования. Его имя знают все хакеры, которые используют DDoS-атаки.

Глава 29. Профиль: Брайан Кребс

Во время подготовки к небольшому праздничному ужину, в дом Брайана Кребса зашли "поздороваться" ребята из отряда S.W.A.T., в полном обмундировании, с винтовками и дробовиками, нацеленными на него. После того, как ему крикнули не двигаться, обыскали и надели наручники, Кребс понял, что это был еще один обычный день его жизни следователя и репортера, которую он посвятил сражению с киберпреступниками. Более десяти лет он неустанно борется со спамерами, скиммерами и различными хакерами. Он принимал участие в расследованиях и облавах, в результате которых все те же хакеры теряли миллионы долларов и отправлялись под арест. В ответ, хакеры подбрасывали ему всевозможную контрабанду, включая наркотики и поддельную валюту, а также угрожали убить его и его семью. Подробный отчет о случае, когда в дом Кребса прибыл отряд SWAT можно прочитать здесь: https://arstechnica.com/information-technology/2013/03/security-reporter-tells-ars-about-hacked-911-call-that-sent-swat-team-to-his-house/.

Полиция столько раз была у него дома после звонка от анонимного "доброго самаритянина", что, в конце концов, местные правоохранительные органы получили как письменные, так и электронные уведомления, с призывом не слишком активно реагировать на последние наводки. В итоге, Кребс устал от всей этой травли и решил на время "отойти от дел". Он посчитал, что его семье, как и ему самому, нужно отдохнуть от постоянных угроз. Но это не победа хакеров. Кребс продолжает ежедневные расследования. Он по прежнему выводит на чистую воду хакеров, причиняющих вред другим людям.

Так было не всегда. Долгие годы Кребс был типичным журналистом в издании *The Washington Post*. Он начал уделять расследованиям киберпреступлений столько времени, что он ушел из газеты. Сразу после этого он создал собственный блог Krebs on Security (https://krebsonsecurity.com/) и продолжил свои расследования с еще большим усердием и вниманием. Его блог постоянно называют одним из самых популярных в интернете, он также написал один из самых увлекательных бестселлеров *Spam Nation* (https://www.amazon.com/Spam-Nation-Organized-Cybercrime-Epidemic/dp/1492603236/), а в Голливуде даже хотят снять фильм о его жизни.

Он проводит первоклассные журналистские расследования. Когда Кребс узнал, что самые крупные компании, занимающиеся спамом, расположены в России, он научился читать, писать и говорить по-русски, а затем отправился туда, чтобы взять интервью у самых богатых и влиятельных людей, стоящих за этими фирмами. Когда я общался с ним после поездки в Россию, я сказал, что

не мог поверить в то, что он рисковал своей жизнью, чтобы поделиться всеми подробностями этой истории. Он сказал, что видел все совершенно иначе, но некоторые его друзья говорили то же самое. Расследование Кребса, которое он представил общественности, лишило тех людей десятков миллионов долларов, а теперь он едет в их страну, где у него почти нет прав. Многие из нас ожидали увидеть новость о безвременной кончине Кребса во время "визита" в Россию. Вместо этого, он вернулся и привез с собой достаточно фактов, чтобы написать книгу (Spam Nation), а некоторые из тех, у кого он брал интервью отправились в тюрьму.

Большинство журналистов, которые пишут об информационной безопасности, просто повторяют известные факты, о которых они узнали из прессы. Кребс расследует и изучает неизвестные факты. В своем блоге, он объяснил, почему НЕ рассказывает о недавних известных случаях хакерской деятельности: "В основном, я не говорю об этих ситуациях, потому что у меня нет оригинальной информации по ним, которую я мог бы добавить, и потому что я, в целом, не хочу говорить об историях, которые у всех на слуху. Вместо этого, я хочу проводить собственные расследования, связанные с информационной безопасностью и киберпреступлениями".

Несмотря на то, что Кребс проводит расследования различных видов хакерской активности, его основной интерес - это финансовые преступления, спамеры, поставщики сервисов DDoS-атак и использование скиммеров. У Кребса отлично получается идти по следам денег и данных. Он показал имена и фотографии тех, кто стоит за крупнейшими в мире хакерскими организациями и атаками. Во многих случаях, после того, как Кребс указывает на таких людей, им предъявляются обвинения, и они отправляются под арест. Как будто мировые структуры правопорядка читают его блог и ждут, когда Кребс раскроет личность настоящих виновных, чтобы получить ордер на арест. Я уверен, что на самом деле все не так, но эта теория выглядит правдоподобно. Одним из лучших показателей успешной работы Кребса является феномен, который его последователи назвали "Цикл Кребса". Часто Кребс узнает о многих крупнейших хакерских атаках и утечках данных за несколько дней до того, как об этом узнает атакуемый производитель. Цикл Кребса - это время между его сообщением о последней атаке и официальным сообщением о ней производителя.

Кребс не боится указывать на организации, которых все считают "хорошими парнями". Он обвинял компании по выпуску пластиковых карт и банки в содействии финансовым преступлениям. Он утверждал, что организации по оформлению налоговой документации, работающие онлайн, помогают преступникам подделывать налоговую отчетность. Он ясно дал понять, что крупные фармацевтические компании разрешают незаконную продажу своих лекарств, потому что они не хотят мириться с тем, что их настоящие лекарства (не подделки) продаются за меньшую стоимость. Он доказал, что некоторые

фирмы, заявляющие, что предоставляют защиту от хакеров, сами и являются хакерами, что они либо совершают хакерскую деятельность, либо покрывают хакеров. Он утверждал, что интернет-провайдеры и надежные хостинг-сервисы содержат хакеров. И что это их бизнес модель. Кребс всегда оказывается там, где замешаны деньги.

Из-за этого, его веб-сайт постоянно подвергается DDoS-атакам (описанным в предыдущей главе). В одно время его веб-сайт подвергался крупнейшим атакам в интернете. Хакеры, совершающие DDoS-атаки часто используют во вредоносном трафике личные оскорбления Кребса, кроме того новички, желающие вступить в хакерскую организацию должны показать на что способны, атаковав его веб-сайт. И во многих случаях, Кребс узнает имена настоящих преступников, и они отправляются в тюрьму.

Кребсу под силу задача, с которой, судя по всему, не могут справиться другие журналисты и структуры правопорядка - установить личность хакера. Это нормально, если он неделю или дольше ничего не пишет в блоге, но, когда он пишет, он называет имя очередного хакера. Часто он находит личность преступника, следуя по цифровым следам, которые тот оставляет, и в конце концов, эти следы приводят к реальному профилю в сети. В итоге мы видим фотографии этих неэтичных, вредоносных хакеров, на которых они отдыхают с семьей, обнимая жену и детей, и мы знаем, что эти замечательные, "богатые деньки" скоро закончатся. Многие из тех, о ком он рассказал были объявлены в международный розыск, в то время как остальные, судя по всему, наслаждаются преимуществами подкупа чиновников. В любом случае, они все ненавидят Кребса, но весь остальной мир его обожает. Я считаю Брайана Кребса настоящим американским героем!

Помимо того, что Кребс выводит на чистую воду отдельных хакеров и различные организации, ведущие сомнительный бизнес, его статьи позволяют читателю увидеть масштабы хакерского бизнеса. Это не какие-нибудь подростки, которые сидят у себя в комнате, едят хлопья и запивают колой. Это огромные организации со своими платежными ведомостями, отделом кадров, исполнительными директорами, и в некоторых случаях, акциями, продающимися на бирже. Иногда даже официальные бренды, которые мы все любим, и которым доверяем, тоже в деле. Мир хакеров также сложен, как и сама жизнь. Расследования Кребса многим открыли глаза, в том числе и мне. Это пилюля, которую сложно проглотить, но нам всем станет от нее легче.

Подробнее о Брайане Кребсе

Подробнее о Брайане Кребсе вы можете найти на этих ресурсах:

- Твиттер Брайана Кребса: https://twitter.com/briankrebs
- Профиль Брайана Кребса в LinkedIn: https://www.linkedin.com/in/bkrebs

Глава 30. Безопасность ОС

Одна из самых популярных шуток про информационную безопасность имеет несколько панчлайнов и звучит так: "Самый безопасный компьютер - это тот,

- у которого вытащили сетевую карту и заперли его в шкафу
- у которого нет клавиатуры
- которым никто не пользуется".

Сегодня операционные системы (ОС) компьютеров безопаснее, чем когда-либо. Они достаточно безопасны по умолчанию, требуют пароли, автоматически обновляются, по умолчанию шифруют данные и имеют бесконечное количество других функций. Но это не значит, что все они стремятся быть самыми безопасными. Тем не менее, общий уровень "безопасности по умолчанию" достиг той отметки, когда хакерам, для работы вредоносноого ПО, необходимо использовать или социальную инженерию или уязвимости, которые не были пропатчены самим пользователем.

Это произошло не случайно. Разработчикам операционных систем понадобились годы, если не десятилетия, опыта и анализа уровня безопасности, чтобы найти правильную, ту самую грань между "слишком безопасно" и "слишком небезопасно". Конечный пользователь просто хочет, чтобы его операционная система делала то, что нужно без дополнительных затруднений. Если настройки безопасности слишком раздражают конечного пользователя, то он попытается их изменить, отключить или вообще перейдет на другую операционную систему. Многие эксперты по информационной безопасности критикуют любую операционную систему, которая не использует самые высокие настройки безопасности для каждого случая, при этом они не учитывают как это повлияет на продажи такой системы или ее необходимость конечному пользователю. Учитывая вышесказанное, сегодня пользователю предоставлен немалый выбор безопасных операционных систем.

Как обезопасить операционную систему

Существует три основных способа обезопасить операционную систему: "собрать" ее так, чтобы она использовала самые безопасные настройки по умолчанию, улучшить безопасность, используя встроенные инструменты или прочитать соответствующие руководства. Конечно, большинство современных

операционных систем предлагают все эти методы для обеспечения безопасности.

Безопасная “сборка” ОС

Лучший, и, как говорят некоторые, единственный способ сделать безопасную ОС - “собрать” ее так, чтобы она была безопасной по умолчанию. Безопасность системы должна подразумеваться не только во время ее создания, в ней также должны быть соответствующие настройки, делающие систему безопасной по умолчанию. Опыт показывает, что настройки безопасности по умолчанию устраивают большинство пользователей, но, если эти настройки выставлены неверно, то это подрывает безопасность.

Основные критерии

Международный стандарт оценки и ранжирования уровней безопасности операционных систем называется «Общие критерии оценки защищенности информационных технологий» (Common Criteria for Information Technology Security Evaluation), хотя, как правило, его называют просто Общие критерии (Common Criteria). Производители предоставляют свои операционные системы и приложения для оценки соответствия Общим критериям, надеясь пройти сертификацию и получить определенный Уровень безопасности (Evaluation Assurance Level, EAL), который варьируется от EAL1 до EAL7, где наибольшее значение соответствует наивысшей безопасности. Хотя может показаться, что многие производители операционных систем, которые заботятся о безопасности, стремятся получить высший уровень (EAL7), но это не так.

Уровни EAL5 и выше не только невероятно сложно получить, но также, они подразумевают сильное ограничение функционала операционной системы. Хотите зайти в интернет и скачать программу? Ну, на системе с уровнем EAL5 и выше у вас это вряд ли получится. Как правило, системы с уровнем EAL5 и выше используются в определенных устройствах безопасности (например, смарт-картах, аппаратных модулях безопасности и так далее) или важнейших операционных системах, которые правительства используют, например, в системах запуска ракет. Основная часть операционных систем, которые мы знаем и любим, включая различные версии Windows, Linux, Solaris, AIX и BSD имеют уровень EAL4 или EAL4+ (плюс означает, что система более безопасна, и ей нельзя присвоить “чистый” уровень EAL).

Сейчас осуществляются попытки перейти от оценок EAL к Профилям защиты (Protection Profiles, PP). Подробнее можно найти по ссылке https://www.ca.com/en/blog-highlight/common-criteria-reforms-sink-or-swim-how-should-industry-handle-the-revolution-brewing-with-common-criteria.html.

ПРИМЕЧАНИЕ Насколько мне известно, система Apple iOS никогда не представлялась для прохождения сертификации EAL.

Если система имеет более высокий уровень EAL или PP, это не означает, что хакер не сможет ее взломать, но это совершенно точно означает, что, при прочих равных, взломать такую систему будет гораздо сложнее. Это также не означает, что операционная система, не имеющая такого рейтинга небезопасна или, не смогла бы его получить, если бы была представлена.

Федеральные стандарты обработки информации

В Соединенных Штатах есть еще один популярный стандарт, под названием «Федеральные стандарты обработки информации» (Federal Information Processing Standards, FIPS), который также занимаются оценкой и сертификацией безопасности операционных систем и их составляющих. Несмотря на то, что FIPS (https://www.nist.gov/topics/federal-information-standards-fips) официально применяется для операционных систем, связанных с правительством США, этот стандарт применяют во всем мире. Стандарты FIPS имеют соответствующие цифровые обозначения, например, 199-3 или 140-2. FIPS 140-2 используется для оценки алгоритмов шифрования и имеет уровни от 1 до 4, где 4 - наивысший уровень безопасности.

Из-за наличия соответствующего спроса, большинство производителей операционных систем и приложений, прошедших сертификацию Общих критериев или FIPS, используют это в качестве рекламы. В некоторых случаях, перед покупкой ПО, клиентам важно убедиться в наличие у него соответствующего уровня безопасности.

Рассказ о двух безопасных операционных системах

В мире популярных операционных систем общего назначения есть две операционные системы (обе с открытым исходным кодом), которые стремятся быть безопаснее большинства: OpenBSD и Qubes OS.

OpenBSD была создана Тео де Раадтом в 1995 году, как ответвление от NetBSD. Если есть выбор между удобством использования и безопасностью, де Раадт почти всегда выбирает безопасность. Многие функции безопасности, которые в других операционных системах может включить сам пользователь, в OpenBSD включены по умолчанию. Разработчики этой системы часто проверяют свой код в поисках багов и уязвимостей. OpenBSD особенно уважают за то, что из всех популярных операционных систем, в ней меньше всего багов, найденных сторонними компаниями.

ОС Qubes (https://www.qubes-os.org/) была создана компанией Invisible Things Lab, расположенной в Варшаве, Польша, совместно с другим руководителем

этой компании Йоанной Рутковской (представленной в следующей главе) в 2012 году. Qubes работает на базе изолированного гипервизора Xen, что позволяет дополнительным операционным системам и компонентам работать на изолированных виртуальных машинах. Даже у сети есть свой отдельный домен. Каждый домен имеет свой уровень доверия, и может работать с дополнительными операционными системами. Возможно, не без иронии, но сами создатели описывают свое творение, как "в меру безопасную операционную систему". Другие считают ее самой безопасной популярной операционной системой, доступной на данный момент, в частности, ее обожают многие эксперты в области безопасности информации.

Не то, чтобы это требовалось для разработки и продвижения более безопасной ОС, но в некоторых кругах и де Раадт и Рутковская известны своим умом и резкими высказываниями. Они не боятся задеть чувства других, настаивая на своем или высказывая мнение по какому-либо поводу, особенно, когда оспаривают давно существующую, но ошибочную догму. Ни один из них, мягко говоря, не выносит глупости. Они ответственно подходят к разработке продуктов, применяя весь свой интеллект. Не обязательно выбирать OpenBSD или Qubes если вы хотите использовать относительно безопасную систему, однако эти системы по умолчанию используют настройки безопасности выше средних.

Руководства по настройке безопасности

Как правило, операционные системы используют настройки по умолчанию, обеспечивающие достаточный уровень безопасности, но эти настройки не всегда соответствуют рекомендованному уровню. Например, в Windows 10 минимальная длина пароля ограничена 6 символами, хотя Microsoft и многие другие компании рекомендуют использовать, как минимум 12, если не 16 символов. Проблема в том, что популярные операционные системы должны соответствовать требованиям большого количества людей и сценариев безопасного использования. Если включить "рекомендуемые" параметры для таких, на первый взгляд, безобидных настроек, как минимальная длина пароля, то это помешает работе огромного количества людей, и может даже ухудшить уровень безопасности. Поэтому, как правило, производители ОС выставляют индивидуальные настройки на определенный параметр, даже, если он менее безопасен, чем рекомендуемый.

Такие руководства можно скачать с официальных сайтов производителей или сайтов сторонних компаний, занимающихся безопасностью информации. Например, рекомендации Microsoft можно скачать здесь: https://blogs.technet.microsoft.com/secguide/2016/07/28/security-compliance-manager-4-0-now-available-for-download/, а рекомендации Apple здесь:

https://support.apple.com/en-gb/HT202739. Бенчмарки организации Center for Internet Security, одной из самых популярных сторонних компаний, оценивающих безопасность системы, можно скачать здесь: https://benchmarks.cisecurity.org/downloads/.

Консорциумы по информационной безопасности

В мире информационной безопасности достаточно авторитетных консорциумов, которые стремятся улучшить защиту информации. Две группы, которые в последнее время оказали значительное влияние на индустрию - это Trusted Computing Group и FIDO Alliance.

Trusted Computing Group

Мой любимый консорциум - это Trusted Computing Group (https://trustedcomputinggroup.org/), который работает над созданием и стандартизацией более безопасных программных и аппаратных компонентов. Благодаря ему появились многие широко применяемые стандарты продуктов, безопасных по умолчанию, такие как Trusted Platform Module и OPAL - стандарт шифрования для жестких дисков, автоматически шифрующих данные. Если вы хотите узнать, чего стоит создание действительно безопасных устройств и операционных систем, прочтите все публикации Trusted Computing Group.

FIDO Alliance

FIDO (Fast IDentity Online) Alliance (https://fidoalliance.org/) ставит своей целью замену традиционного метода аутентификации, путем ввода логина и пароля, более надежными альтернативами. Образованный в 2012-ом, FIDO фокусируется на более надежных методах аутентификации и использовании специальных устройств для авторизации на веб-сайтах, веб- сервисах и облачных сервисах. На данный момент все методы аутентификации FIDO осуществляются с использованием зашифрованного публичного/приватного ключа, что делает их более устойчивыми к фишинг- и man-in-the-middle-атакам. Сегодня у FIDO есть два вида аутентификации: Universal Authentication Framework (UAF), "беспарольный" метод, и Universal Second Factor (U2F), который представляет из себя двухфакторную аутентификацию (2FA). Последний метод может использовать пароль, который не обязательно должен быть сложным, так как дополнительный фактор гарантирует общую надежность. Методы аутентификации FIDO должны поддерживаться вашим устройством или браузером, а также сайтом или сервисом, которые вас

интересуют. Методы аутентификации FIDO только приобретают популярность, но через год или два, их наверняка уже будут использовать повсеместно.

Ни одна операционная система не может гарантировать идеальную безопасность или предотвратить целенаправленный взлом. Но многие операционные системы относительно безопасны “из коробки”, или предоставляют возможность повысить уровень безопасности, следуя соответствующим руководствам.

В Главах 31 и 32 представлены Йоанна Рутковская и Аарон Маргозис. На данный момент они являются ведущими умами в разработке безопасных операционных систем.

Глава 31. Профиль: Йоанна Рутковская

Гражданка Польши, Йоанна Рутковская эффектно появилась на сцене информационной безопасности. В 2006-ом она представила непревзойденный руткит. Руткит - это вредоносная программа, которая изменяет операционную систему, чтобы оставаться незамеченной для самой операционной системы и программ, установленных на ней. Рутковская обнаружила метод, с помощью которого, вредоносная программа может маскироваться таким образом, что ее нелегко будет обнаружить любым известным способом, даже, если известно, что эта вредоносная программа уже запущена в системе. Она назвала эту идею "синяя таблетка" (Blue Pill).

Аллегория с синей таблеткой взята из известного фильма *Матрица* (http://www.imdb.com/title/tt0133093/). В кино, главному герою по имени Нео сначала сказали, что мир, в котором он живет - это кибериллюзия, а потом предложили две таблетки: одна синяя, другая красная. Если он примет красную таблетку, то сможет попасть в реальный мир. Но если примет синюю, то останется в привычном иллюзорном мире. Все, кто смотрел фильм, знают, что он выбрал красную и стал сражаться с главными злодеями, чтобы спасти мир!

Рутковская назвала свое открытие синей таблеткой, потому что ее руткит использует функции виртуализации современных процессоров для запуска гипервизора, который незаметно контролирует работу операционной системы. Подчиненная операционная система думает, что контролирует свою работу сама, в то время, как на самом деле, и сама система, и все ее компоненты, полностью контролируются гипервизором.

Рутковская так описала свое открытие: "Идея синей таблетки проста: операционная система проглатывает синюю таблетку и просыпается в Матрице, контролируемой сверхтонким гипервизором. Все это происходит на лету (то есть, без перезагрузки системы), при этом, не страдает производительность, и все устройства, такие, как видеокарты, полностью доступны для операционной системы, которая отныне работает внутри виртуальной машины".

В то время ее заявление было революционным. Гипервизоры и виртуализация только начали обретать популярность. Многие, включая большинство экспертов в области информационной безопасности, не до конца понимали, как работает сама эта технология, и еще меньше, как она связана с безопасностью, и как ее правильно применять. И тут Рутковская заявляет, что все эти новые технологии можно использовать, чтобы обойти любые методы обнаружения. В мире информационной безопасности это создало экзистенциальный кризис. Какое-то время были опасения, что хакеры начнут

писать вредоносное ПО, наподобие синей таблетки, и для защитных программ настанут тяжелые времена.

В то время я написал колонку в *InfoWorld*, чтобы сказать людям, что они слишком сильно волнуются. Хотя я был согласен с тем, что предложила Рутковская, я был уверен, что дополнительные сложности отпугнут разработчиков вредоносного ПО. Я сказал, что пока работает их вредоносное ПО, которое проще написать, вряд ли они перейдут на новые, более сложные методы, но если они и начнут создавать такие программы, то разработчики защитного ПО и операционных систем смогут дать адекватный ответ. В последующие десять лет мое предположение (о том, что не стоит сильно беспокоиться о синих таблетках) подтвердилось. Тем не менее Рутковская не только сразу показала свои знания и ум, но также оспаривала надежность традиционных методов обеспечения информационной безопасности.

С момента выхода Blue Pill в 2006-ом, Рутковская стала часто выступать на конференциях, и продолжала задавать нужные вопросы и предоставлять надежные решения. Она продолжает писать о своих идеях и решениях на сайте Invisible Things Lab (http://invisiblethingslab.com/) и в блоге (https://blog.invisiblethings.org/), несмотря на то, что в она также уделяет много внимания другим проектам. В последнее время она практически полностью занята своим проектом Qubes (о котором я говорил в предыдущей главе).

Рутковская всегда исследовала реальные и искусственные границы безопасности операционных систем. Она нашла неприемлемые уязвимости практически в каждом дистрибутиве Linux, где одна программа могла получить доступ к другой программе, которая работала в той же операционной системе, на том же компьютере (http://theinvisiblethings.blogspot.com/2011/04/linuxsecurity-circus-on-gui-isolation.html). Такая уязвимость есть у большинства операционных систем. Несмотря на то, что для многих производителей операционных систем и экспертов по безопасности это допустимый риск, потому что проблема возникает только при использовании конкретной ОС на конкретной машине. Рутковская считает, что это недопустимо, если вам действительно важна безопасность. Особенно учитывая, что такое простое действие, как просмотр страниц в интернете, может закончиться тотальным взломом операционной системы и всех ее приложений.

Из-за этих и других причин, в 2010-ом она разработала Qubes OS (http://qubes-os.org/). Qubes - это настольная операционная система, использующая гипервизор, и ориентированная на безопасность с помощью изоляции. Она может запускать другие операционные системы, каждая из которых, будет работать в отдельной виртуальной машине, а внутренняя среда администрирования и сетевая среда также работают в отдельных виртуальных машинах. Qubes - продукт, ориентированный на безопасность, который упрощает создание, управление и работу всех виртуальных машин. GUI создает

рабочий стол, на котором все виртуальные машины выглядят, как одно целое, хотя, на самом деле, они полностью разделены границами безопасности гипервизора. Как и любое ПО, эта система имеет свои уязвимости, и она подвержена влиянию уязвимостей, которые не может контролировать (например, уязвимости Xen). Хотя сама Рутковская называет Qubes "в меру безопасной" операционной системой, это, наверное, самая безопасная ОС общего назначения, которую можно бесплатно скачать и использовать.

В то же время, Рутковская продолжает исследовать другие проблемы информационной безопасности, такие как вредоносные PDF-файлы и уязвимости USB-интерфейса. Она активный сторонник эффективных методов защиты информации, и она продолжает улучшать мир, бросая ему вызовы.

Подробнее о Йоанне Рутковской

Подробнее о Йоанне Рутковской вы можете найти на этих ресурсах:

- Твиттер Йоанны Рутковской: https://twitter.com/rootkovska
- Веб-сайт Invisible Things Lab: http://invisiblethingslab.com/
- Блог Invisible Things Lab: https://blog.invisiblethings.org/
- Веб-сайт проекта Qubes: http://qubes-os.org/

Глава 32. Профиль: Аарон Маргозис

Хотя все и говорят, что безопасность и надежность - это САМОЕ главное в компьютере, на самом деле, но это мнение разделяют не все. Это один из грустных фактов в мире информационной безопасности. Пользователей гораздо больше интересуют новые, классные, "ух ты какие" фишки, к черту безопасность! Производителей и разработчиков, которые уделяют слишком много внимания безопасности, в итоге, обходят конкуренты. Разработчики, которые делают свои приложения и устройства слишком безопасными, в итоге, остаются без работы. Продукт можно сделать безопасным, только если меры безопасности не будут мешать удобству пользователя, а это очень сложная задача.

В связи с этим, большинство людей не использует самые безопасные операционные системы на планете. Подавляющее большинство использует популярные, достаточно надежные операционные системы, получающие постоянные обновления, но это не самые безопасные системы. Если бы приоритетом конечных пользователей действительно была бы безопасность, то они бы использовали Qubes (https://www.qubes-os.org/), ОС, разработанную Йоанной Рутковской, представленной в предыдущей главе или OpenBSD (https://www.freebsd.org/). Это самые безопасные операционные системы общего назначения, и они бесплатные, тем не менее, они не так широко используются. И это не обязательно плохо, в жизни мы принимаем много подобных решений. Безопасность - далеко не всегда самый первый или единственный критерий для принятия решения. Самые популярные операционные системы в мире, по крайней мере на данный момент - это Microsoft Windows, Apple iOS и Android.

К счастью, в основном, современные операционные системы достаточно безопасны. Как правило, если следовать рекомендациям производителя, своевременно устанавливать патчи и не попадаться на уловки социальной инженерии, то вас не взломают. Важную роль в обеспечении безопасности играют рекомендации производителя ОС. Если вы когда-нибудь интересовались, как выбираются эти рекомендации, то они основаны на накопленном опыте самого производителя, уроках прошлого, кроме того, есть люди, которые целенаправленно изучают рекомендации для каждого случая и пытаются найти баланс затрат/пользы для основной части клиентов производителя. Один из моих давних друзей, Аарон Маргозис, сотрудник Microsoft, отвечающий за настройку безопасной конфигурации Windows.

Сейчас у Маргозиса волосы, как у рок-звезды, и он увлечен информационной безопасностью не меньше, чем бейсболом. Уже почти двадцать лет он изучает тысячи настроек безопасности, создавая бесплатные инструменты настройки и публикуя статьи о том, каким должен быть безопасный компьютер. Вместе со своим соавтором, Марком Руссиновичем (представленным в Главе 11), он написал две книги, из потрясающей серии Windows Sysinternals, описывающей "закулисную" работу Windows. Многие технические специалисты по настройке систем Windows считают эти книги "библией" для решения проблем.

Почти каждый день Маргозис решает проблемы настройки безопасности под конкретный случай или пытается выяснить, почему организация, будь то Microsoft или кто-то еще, рекомендует использовать именно такие настройки. За эти годы, он нашел десятки крайне неудачных рекомендаций, многие из которых могли бы вызвать проблемы для своей среды использования или стать причиной кризисных ситуаций, которые сложно решить. Маргозис сделал больше, чем все, кого я знаю, для того, чтобы рекомендации популярных интернет-организаций, таких как Center for Internet Security (https://www.cisecurity.org/), стали основными рекомендациями большинства компаний. Вместе с тем, Маргозис писал, вел блог и делился всем, что знает. Сейчас он работает над функциями AppLocker и Device Guard, которые ищут вредоносные программы, предотвращая их выполнение, они используются в больших организациях. Это естественное продолжение того, чем он занимался всю свою карьеру.

Я начал наше интервью с вопроса о том, как он попал в сферу информационной безопасности. Он ответил: "Я изучал психологию в университете Вирджинии, но меня всегда интересовали компьютеры. В 1970-ых, когда мне было 12, я начал программировать на BASIC. Пока я учился в университете Вирджинии, я ходил на курсы информатики, но я не выбрал информатику основной специальностью, потому что это означало бы смену специальности на инженера. Позже, я начал работать с компьютерами, вернулся в университет Вирджинии и получил степень магистра по информатике.

После колледжа я работал в нескольких компаниях, включая две компании, которые делали оборудование для тестирования слуха, компанию, разрабатывающую бухгалтерское ПО, и в компании оператора мобильной связи. Где-то между периодами работы во всех этих компания, я работал в Maynard Electronics. Они разрабатывали программу резервного копирования, появившуюся в первой версии Windows NT, а также продукт под названием "Backup Exec", продаваемый несколькими поглощенными компаниями (ныне Symantec). Меня беспокоило, что посторонние люди (например, коллеги) могут воспользоваться моим компьютером, и поэтому я начал интересоваться информационной безопасностью. В итоге, в 1999-ом я оказался в Microsoft, и до сих пор там работаю".

Маргозис был одним из первых, кто сказал мне не использовать аккаунт администратора на постоянной основе. В то время, на системах Linux и Unix становилось популярно не заходить под root-аккаунтом, но среди пользователей Windows об этом почти никто не слышал. На самом деле, практически все разработчики предполагали, что у пользователя всегда будут права администратора, чтобы их ПО могло нормально работать. Благодаря большому вкладу и влиянию Маргозиса, в Microsoft решили, что Windows Vista (вышедшая в 2006-ом) будет той системой Windows, которая проведет черту. В ней была представлена функция под названием «Контроль учётных записей пользователей» (User Account Control, UAC), которая по умолчанию давала права обычного пользователя, а не администратора. Это вызвало колоссальное недовольство, десятки тысяч программ перестали работать. В то время взять на себя ответственность, и попытаться изменить взгляды производителей и разработчиков было серьезным испытанием. Некоторые думали, что такие изменения безопасности приведут к концу существования Microsoft Windows. Настолько противоречивыми были эти меры.

Я спросил Маргозиса, какова была его роль в этом процессе. "В то время, в Microsoft в целом, почти никто не думал о переходе от "всегда администратор" к правам обычного пользователя. Некоторые считали, что это необходимо, например, Майкл Ховард (представленный в Главе 7). Он говорил об этом, и вдохновил меня на попытку всегда работать с правами обычного пользователя. Я начал это практиковать во время бета-тестирования Windows XP, и многие программы перестали работать. Это было увлекательное испытание. Я начал думать, как продолжить эффективную работу без прав администратора, таким образом у меня появились инструменты и техники, которые работали, и я поделился ими с остальными. Мое первое публичное выступление состоялось на презентации Microsoft TechEd в 2005-ом, где было более 1500 человек, и в этом выступлении я говорил, как пользоваться Windows XP без прав администратора. Мои блоги, инструменты и выступления оказали огромное влияние на команду разработчиков Windows Vista. Тогда многие сомневались, и было неочевидно, получится ли внедрить права обычного пользователя по умолчанию, но Джим Оллчин и команда разработчиков UAC настаивали на своем. И я счастлив, что был частью этого. В итоге, выиграли абсолютно все пользователи".

Я спросил Маргозиса, как он начал выпускать такие классные, бесплатные инструменты для решения проблем с настройками безопасности, как LUA Buglight и Local Group Policy Object (LGPO). Он ответил: "Все началось, когда я продвигал идею не использовать права администратора. Государство представило список настроек безопасности Federal Desktop Core Configuration (FDCC), который включал огромный набор настроек, а также требование, чтобы конечный пользователь работал только с обычными правами, то же самое делал и я. Благодаря этому я многое узнал очень многое о настройках

безопасности и групповой политике, а также разработал инструменты для автоматического выполнения задач, которые не были достаточно подробно описаны ранее. Оказалось, что подробно исследованные и хорошо протестированные исходные параметры приносят огромную пользу клиентам. Если бы у нас не было этих параметров, каждому клиенту пришлось бы делать все самому, что заняло бы много времени и, вероятно, могло бы привести к нежелательному результату. Легко можно ошибиться или сделать неверное предположение."

Я спросил Маргозиса над чем он еще сейчас работает, помимо параметров и настроек безопасности. Он ответил: "Я много работаю с белыми списками приложений, используя AppLocker от Microsoft и технологии Device Guard. Это будет надежная и необходимая для организаций защита от программ-вымогателей и других видов вредоносного ПО. Пользователям домашних компьютеров сложнее работать с белыми списками, потому что они сами должны принимать решения о внесении приложения в список. В организации конечный пользователь не должен принимать таких решений, и от него никто этого не ждет, поэтому белые списки больше подходят для организаций с грамотным менеджментом.

В своей нынешней работе по контролю приложений я вижу сходства с тем, что делал, когда предлагал отказаться от постоянного использования прав администратора. И то и другое повышает безопасность, и вызывает сбои в работе ПО, потому что предположения разработчиков, которым они привыкли следовать, больше не учитываются. Производителям ПО пришлось отказаться от варианта, в котором их программа будет сохранять данные в каталоге Program Files, и им придется перестать рассчитывать на возможность запуска программы из папки пользователя или других папок, запись в которые может осуществлять пользователь. Это будет интересное испытание совместимости".

Я спросил, о чем с точки зрения информационной безопасности, он хотел бы знать больше. Он поразмышлял минуту и сказал: "Я бы хотел знать, как быстрее всего убедить человека принять правильное решение. Я не уверен, что достаточно хорошо освоил эту технику. Я знаю, что то, что я делаю - правильно, но, если бы я знал, как быстрее убедить в этом других, это бы сильно помогло".

Я думаю многие из тех, кто представлен в этой книге поймут боль Маргозиса.

Подробнее об Аароне Маргозисе

Подробнее об Аароне Маргозисе вы можете найти на этих ресурсах:

- Книга *Troubleshooting with the Windows Sysinternals Tools* (2-ое издание): https://www.amazon.com/Troubleshooting-Windows-Sysinternals-%20Tools-2nd/dp/0735684448
- Книга *Windows Sysinternals Administrator's Reference*: https://www.amazon.com/Windows-Sysinternals-Administrators-Reference-Margosis/dp/073565672X
- Блог Аарона Маргозиса об использовании прав обычного пользователя, совместимости приложении и внутренних компонентах: https://blogs.msdn.microsoft.com/Aaron_Margosis
- Блог Аарона Маргозиса о US Government Configuration Baseline (USGCB, Конфигурации безопасности для организаций, связанных с правительством США): https://blogs.technet.microsoft.com/fdcc
- Блог Аарона Маргозиса с рекомендациями по настройке безопасности: https://blogs.technet.microsoft.com/secguide/

Продолжение книги: Часть III