HACKING

The Art of Exploitation

Jon Erickson

NO STARCH
PRESS

HIGH TECH

ХАКИНГ

Искусство эксплойта

Джон Эриксон

СИМВОЛ®

Санкт-Петербург — Москва
2005

Серия «High tech»

Джон Эриксон

Хакинг: искусство эксплойта

Перевод С. Маккавеева

Главный редактор	*А. Галунов*
Зав. редакцией	*Н. Макарова*
Научный редактор	*А. Петухов*
Редактор	*В. Овчинников*
Художник	*В. Гренда*
Корректор	*О. Макарова*
Верстка	*Н. Гриценко*

Эриксон Д.
Хакинг: искусство эксплойта. – Пер. с англ. – СПб: Символ-Плюс, 2005. – 240 с., ил.
ISBN 5-93286-076-6

Это не каталог эксплойтов, а учебное пособие по основам хакинга, построенное на примерах. В нем подробно рассказано, что должен знать каждый хакер и, что важнее, о чем должен быть осведомлен каждый специалист по безопасности, чтобы принять меры, которые не позволят хакеру совершить успешную атаку. От читателя потребуется хорошая техническая подготовка и полная сосредоточенность, особенно при изучении кода примеров. Но это очень интересно и позволит многое узнать. О том, как создавать эксплойты с помощью переполнения буфера или форматных строк, как написать собственный полиморфный шеллкод в отображаемых символах, как преодолевать запрет на выполнение в стеке путем возврата в libc, как перенаправлять сетевой трафик, прятать открытые порты и перехватывать соединения TCP, как расшифровывать данные беспроводного протокола 802.11b с помощью атаки FMS.

Автор смотрит на хакинг как на искусство творческого решения задач. Он опровергает распространенный негативный стереотип, ассоциируемый со словом «хакер», и ставит во главу угла дух хакинга и серьезные знания.

ISBN 5-93286-076-6
ISBN 1-59327-007-0 (англ)

Издательство «Символ-Плюс». 199034, Санкт-Петербург, 16 линия, 7,
тел. (812) 324-5353, edit@symbol.ru. Лицензия ЛП N 000054 от 25.12.98.
Налоговая льгота – общероссийский классификатор продукции
ОК 005-93, том 2; 953000 – книги и брошюры.
Подписано в печать 22.07.2005. Формат 70x100 1/16 . Печать офсетная.
Объем 15 печ. л. Тираж 2000 экз. Заказ N
Отпечатано с готовых диапозитивов в ГУП «Типография «Наука»
199034, Санкт-Петербург, 9 линия, 12.

Оглавление

Отзывы на книгу «Хакинг»

Очень рекомендую эту книгу. Ее написал человек, который знает, о чем говорит, а программный код, инструменты и примеры вполне работоспособны.

– IEEE CIPHER

Из всех прочитанных мною книг эту считаю для хакера главной.

– SECURITY FORUMS.COM

Непрограммисты узнают из этой книги, насколько легко взломать систему, в которой исполняется уязвимый код. А программисты поймут, насколько проще может быть устранение уязвимостей в ПО с открытым исходным кодом.

– COMPUTER POWER USER MAGAZINE

...очень глубокая, информативная книга. Читая ее, я получил огромное удовольствие и посоветовал бы ее всякому, кто по-настоящему интересуется компьютерной безопасностью.

– GEEKSHELTER.COM

Тем, кто имеет дело с компьютером лишь время от времени, эта книга может показаться немного перенасыщенной технической информацией, но это захватывающее чтение как для тех, кто хочет узнать больше, так и для тех, кто желает отточить свое профессиональное мастерство.

– THE TRIBUNE REVIEW

Эта книга должна входить в программу обязательного чтения для любого программиста, стремящегося к совершенству, и по ней надо преподавать фундаментальные основы программирования во всех учебных заведениях, где готовят программистов.

– FLASH-MX.COM

...нужна поистине фантастическая книга, чтобы отучить кого-нибудь от видеоигр. Штабель из коробок с ними все рос, а я не мог оторваться от чтения. Одно только это говорит о качестве книги.

– PGNX.NET

Из книг о программировании я бы отметил только эту.

– UNIXREVIEW

Эриксон так представляет материал, что не запутаешься и читать приятно.

– IEEE SECURITY & PRIVACY

Отличная книга.

– ABOUT.COM

Благодарности

Я благодарю Билла Поллока (Bill Pollock), Карол Хурадо (Karol Jurado), Энди Кэррола (Andy Carroll), Лэя Сэкса (Leigh Sacks) и всех остальных сотрудников издательства No Starch Press, сделавших возможным выход этой книги и позволивших мне творчески участвовать в процессе. Кроме того, я благодарю своих друзей Сета Бенсона (Seth Benson) и Аарона Эдамса (Aaron Adams) за чтение корректуры и редактирование, Джека Мэтсона (Jack Matheson) за помощь с ассемблером, д-ра Зейделя (Dr. Seidel) за поддержание интереса к вычислительной технике, моих родителей за покупку того самого первого Commodore Vic-20 и хакерское сообщество за стремление к новому и творческий дух, породившие технологии, о которых рассказывается в книге.

Предисловие

В книге рассказывается о деталях различных хакерских технологий, многие из которых являются весьма специальными. Здесь также приводятся начальные сведения о базовых понятиях программирования, на которых основываются эти технологии, но для лучшего понимания последних желательно общее знакомство читателя с программированием. Приводимые в книге примеры программ написаны для компьютера x86, работающего под Linux. Во время чтения полезно иметь под рукой подобный компьютер, тогда можно будет самостоятельно получить такие же результаты и провести собственные исследования. В этом и заключается хакерство.

Во время написания использовался дистрибутив Gentoo Linux, доступный по адресу *http://www.gentoo.org*.

0x100

Введение

Слова «хакинг» или «хакерство» могут вызывать в воображении картины электронного вандализма, шпионажа, крашеных волос и тел, разукрашенных пирсингом. У большинства людей хакинг ассоциируется с нарушением закона, а потому все, кто занимается хакерской деятельностью, становятся в их глазах преступниками. Несомненно, есть люди, применяющие хакерские технологии в нарушение законов, но суть хакерства состоит не в этом. На самом деле хакинг больше тяготеет к соблюдению законов, чем к их нарушению.

Сущность хакинга состоит в поиске непреднамеренных или упущенных из виду применений законов и свойств данной ситуации и последующем применении их новыми и изобретательными способами для решения некоторой задачи. Такая задача может состоять в получении доступа к компьютерной системе или отыскании способа использования устаревшего телефонного оборудования для управления моделью железной дороги. Обычно хакеры предлагают для решения таких задач уникальные способы, невообразимые для тех, кто придерживается стандартной методологии.

В конце 1950-х годов клуб железнодорожного моделирования Массачусетского технологического института получил в подарок ряд деталей в основном от старой телефонной аппаратуры. С помощью этого оборудования члены клуба смастерили сложную систему, позволявшую нескольким операторам управлять различными частями дороги путем набора номера соответствующего участка. Такое необычное и оригинальное применение оборудования они назвали «хакингом», и многие считают эту группу первыми хакерами. Затем они занялись написанием программ на перфокартах и перфолентах для первых компьютеров, таких как IBM 704 и TX-0. В то время как все другие удовлетворялись

тем, что писали программы, которые решали задачи, первые хакеры были озабочены тем, чтобы писать программы, которые решают задачи хорошо. Программа, способная получить тот же результат с помощью меньшего количества перфокарт, считалась лучшей, хотя она и делала то же самое. Главным отличием было то, как программа получает результаты, – ее *элегантность*.

Умение сократить количество перфокарт, необходимых для программы, свидетельствовало об артистизме в управлении компьютером, вызывавшем восхищение у тех, кто способен был его оценить. Аналогично деревянная колода справляется с ролью подставки для вазы, но стол, красиво вырезанный из нее с применением изящной техники, выглядит гораздо лучше. Первые хакеры превращали программирование из технической задачи в разновидность искусства, которая, как и многие другие виды искусства, могла быть оценена только посвященными и оставалась непонятой остальными.

Такой подход к программированию создал информационную субкультуру, разделившую тех, кто ценил красоту хакинга, и тех, кто ее не замечал. Эта субкультура была в основном нацелена на более глубокое изучение данного искусства и овладение вершинами мастерства в нем. Ее участники верили, что информация должна свободно распространяться, а все препятствия на пути этой свободы должны так или иначе преодолеваться. В число таких препятствий входили авторитетные личности, администрация учебных заведений и дискриминация. В отличие от большинства студентов, движимых желанием получить документы об образовании, эта неофициальная группа хакеров отвергала традиционное стремление к хорошим оценкам, преследуя задачу получения собственно знаний. Эта тяга к непрерывной учебе и исследованиям выходила даже за пределы традиционных границ, очерченных дискриминацией, о чем свидетельствует признание этой группой 12-летнего Питера Дойча, который продемонстрировал свое знание TX-0 и желание учиться. Возраст, раса, пол, внешность, ученые степени и положение в обществе не были основными критериями ценности участников – не из стремления к равенству, а из стремления развивать нарождающееся искусство хакинга.

Хакеры обнаружили красоту и элегантность в таких обычно сухих науках, как математика и электроника. Они рассматривали программирование как вид художественного самовыражения, и компьютер был инструментом их искусства. Их желание все препарировать и понять принцип работы не было направлено на разоблачение художественного творчества, а служило средством добиться более высокой оценки со стороны. Эти ценности, обусловленные стремлением к знаниям, в итоге назовут «хакерской этикой»: понимание логики как формы искусства, способствование свободному обмену информацией, преодоление традиционных пределов и ограничений с единственной целью – лучше понять окружающий мир. Такая позиция не нова: схо-

жую этику и субкультуру создали пифагорейцы в Древней Греции, хотя компьютеров у них и не было. Они увидели красоту математики и открыли многие базовые понятия геометрии. Эта жажда знаний и ее благотворные побочные продукты встречаются на всем протяжении истории от пифагорейцев до Ады Лавлейс, Алана Тьюринга и хакеров из клуба железнодорожного моделирования MIT. Развитие вычислительных наук продолжилось и дальше, приведя к таким фигурам, как Ричард Столмен и Стив Возняк. Эти хакеры дали нам современные операционные системы, языки программирования, персональные компьютеры и многие другие технологические достижения, используемые теперь в повседневной жизни.

Так как же различить хороших хакеров, творящих чудеса технологического прогресса, и плохих хакеров, крадущих номера наших кредитных карточек? В какой-то момент для обозначения плохих хакеров стали использовать термин «крэкер», который должен был отличать их от хороших хакеров. Журналистам объяснили, что крэкеры – нехорошие ребята, а хакеры – хорошие. Хакеры придерживались хакерской этики, а крэкеры думали только о том, как преступить закон. Считалось, что крэкеры значительно менее талантливы, чем элита хакеров, и просто пользуются написанными хакерами инструментами и скриптами, не понимая, как они работают. Слово «крэкер» должно было стать общим ярлыком для всех, кто делает с помощью компьютера что-либо бессовестное: ворует программное обеспечение, уродует веб-сайты и, что хуже всего, не понимает, как он это делает. Но сегодня этот термин употребляют очень немногие.

Термин не прижился, может быть, из-за конфликта определений: первоначально словом «крэкер» называли тех, кто нарушал авторские права и вскрывал системы защиты от копирования. А может быть, причина кроется в новом определении, относящемся как к тем, кто занимается незаконной деятельностью с помощью компьютеров, так и к тем, кто является относительно малоквалифицированными хакерами. Очень немногие журналисты считают необходимым описывать тех, кто не обладает высокой квалификацией, с помощью термина «крэкеры», незнакомого широкой публике. Напротив, большинство людей слышало о таинственности и мастерстве, ассоциируемых со словом «хакер». Журналисты, не колеблясь, делают выбор между терминами «крэкеры» и «хакеры». Аналогично для обозначения крэкеров иногда употребляют термин «скрипт-кидди», но в нем нет такого оттенка журналистской сенсационности, как в темном хакере. Некоторые все же станут утверждать, что между хакерами и крэкерами есть четкая разграничительная линия, но я считаю, что хакер – это всякий, в ком живет хакерский дух, независимо от того, какие законы он, возможно, нарушает.

Это нечеткое различие между хакерами и крэкерами становится еще более расплывчатым благодаря современным законам, накладывающим ограничения на применение криптографических средств и иссле-

дования в этой области. В 2001 г. профессор Эдвард Фелтен (Edward Felten) и группа ученых из Принстонского университета собирались опубликовать результаты своих исследований в статье, обсуждавшей слабости различных систем цифровых водяных знаков. Эта статья была ответом на вызов, брошенный группой основателей стандарта SDMI (Secure Digital Music Initiative), в котором всем желающим предлагалось попытаться взломать эти системы водяных знаков. Однако против публикации этой статьи и с угрозами в адрес исследователей выступили Фонд SDMI и Американская ассоциация звукозаписывающей индустрии (RIAA). Несомненно, что Акт об авторских правах цифрового тысячелетия (Digital Millennium Copyright Act, DMCA) от 1998 года делает незаконным обсуждение или предоставление технологии, с помощью которой можно обходить устанавливаемый индустрией контроль над покупателями. Это тот закон, который был применен против Дмитрия Склярова, русского программиста и хакера. Он написал программу, позволяющую обходить довольно простое шифрование в программах фирмы Adobe, и представил свои результаты на конференции хакеров в Соединенных Штатах. ФБР налетело, как сокол, арестовав его, за чем последовали долгие юридические баталии. По закону сложность системы контроля над покупателями не имеет значения: формально незаконным является вскрытие или даже обсуждение «поросячьей латыни», если она используется как промышленное средство контроля над покупателями. Так кого теперь считать хакерами, а кого – крэкерами? Если закон становится препятствием для свободы слова, то «хорошие ребята», которые говорят то, что думают, внезапно становятся плохими? Я полагаю, что дух хакерства выше правительственных законов и не должен определяться ими. Но в любой группе специалистов всегда найдутся те, кто использует свои знания для совершения нехороших поступков.

Такие науки, как ядерная физика и биохимия, могут использоваться для того, чтобы убивать, но при этом имеют большое значение для научного прогресса и современной медицины. Само знание не является ни плохим, ни хорошим; стандарты нравственного поведения относятся к применению этого знания. При всем желании мы не смогли бы запретить знание о том, как превратить материю в энергию или остановить непрерывный технологический прогресс в обществе. Точно так же невозможно отменить сущность хакерства, как и подвергнуть его упрощенной классификации или анализу. Хакеры всегда будут раздвигать существующие границы, вынуждая нас к дальнейшим исследованиям.

К сожалению, существует немало так называемых «книжек для хакеров», представляющих собой всего лишь краткие руководства по хакам, осуществленным другими людьми. Они предлагают читателю воспользоваться инструментами на прилагаемом CD, не объясняя теории, лежащей в основе этих инструментов, порождая людей, умеющих пользоваться чужими инструментами, но не способных понять,

как они устроены, или создать собственные. Возможно, что термины «крэкер» и «скрипт-кидди» еще не отжили свое.

Настоящие хакеры – это первопроходцы, разрабатывающие методы и создающие инструменты, которыми заполняются упомянутые диски. Если оставить в стороне юридические вопросы и порассуждать логически, то для каждого эксплойта, о котором можно прочесть в книге, существует «патч» (заплата), позволяющий защититься от него. Должным образом пропатченная система должна быть защищена от атак данного класса. Добычей агрессора, взявшего на вооружение эти методы, не внеся в них ничего нового, неизбежно окажется лишь слабость и глупость. Настоящие хакеры – творцы, умеющие обнаруживать дыры и слабости в программном обеспечении и создавать собственные эксплойты. Если хакеры решают не сообщать создателю программного обеспечения о найденных ими уязвимостях, то могут с помощью этих эксплойтов беспрепятственно проходить через полностью пропатченные и «защищенные» системы.

А если нет никаких патчей, то как можно помешать хакерам обнаружить в программах новые дыры и воспользоваться ими в своих интересах? Для этого и существуют группы исследования компьютерной безопасности, которые пытаются обнаружить эти дыры и уведомить о них поставщиков программного обеспечения, прежде чем будут созданы эксплойты. Происходит полезная совместная эволюция хакеров, обеспечивающих защиту систем, и хакеров, пытающихся осуществить взлом. Благодаря соревнованию между ними мы получаем более прочную защиту и более утонченные методы атаки. Появление и развитие систем обнаружения несанкционированного доступа (Intrusion Detection Systems, IDS) служит главным примером этого совместного эволюционного процесса. Хакеры, строящие защиту, пополняют свой арсенал системами IDS, а атакующие хакеры разрабатывают методы противодействия IDS, которые учитываются при создании новых и более мощных IDS. Итоговый результат такого взаимодействия оказывается положительным, потому что приводит к появлению более квалифицированных специалистов, более совершенной защиты, более стабильных программ, изобретательных технологий решения проблем и даже новой экономики.

Эта книга написана с целью показать подлинную суть хакинга. Мы рассмотрим различные хакерские технологии, как старые, так и современные, и проанализируем их, чтобы понять, как и почему они работают. Благодаря выбранному способу изложения информации вы получите такое понимание и представление о хакинге, которое позволит вам усовершенствовать существующие или даже изобрести оригинальные новые методы. Я надеюсь, что книга послужит стимулом для развития в читателе любознательного хакерского начала и побуждением внести свой вклад в искусство хакинга, по какую бы сторону баррикад он ни находился.