Введение

Профессиональные программисты уже давно осознали всю важность вопроса о безопасности программного кода. После выпуска в 2001 году книги *Building Secure Software (Создание безопасных приложений)* авторов Виега и Мак-Гроу, уже появилось огромное количество книг, в которых окончательно определена безопасность как критически важный элемент программы.

Книга *Building Secure Software* предназначена для профессионалов в области программного обеспечения от разработчиков до менеджеров и может использоваться как пособие для создания более безопасного кода. Новая книга *Взлом программного обеспечения: руководство начинающего хакера* предназначена для той же целевой аудитории, но имеет более конкретную специализацию по вопросам о поиске уязвимых мест в программном обеспечении. Эта книга является особенно интересной для специалистов в области защиты информации, которые хотят углубить свои знания, включая группы "скорой компьютерной помощи" и высокоморальных хакеров.

Книга *Взлом программного обеспечения: руководство начинающего хакера* рассказывает о том, как взламывать программный код, и о том, как преодолевать технические проблемы, с которыми сталкиваются специалисты в области безопасности. Основной целью этой книги авторы видят помощь в обеспечении безопасности программ, а не в защите от атак по сети.

Мы понимаем, что специалистам по обеспечению безопасности программ нужны конкретные сведения о применении изложенного материала на практике. Проблема в том, что такие простые и популярные методы используются поставщиками "программ для обеспечения безопасной работы" в качестве универсальных решений всех проблем (например, средства тестирования, принципы работы которых не известны пользователю, так называемый "черный ящик"). Однако эти методы весьма поверхностны и не раскрывают сути ошибок. Эта книга позволяет пройти весь путь от рекламных заявлений до "самой сердцевины" каждой конкретной проблемы. Нам нужно ясно понимать то, против чего мы собираемся бороться. И эта книга предназначена именно для этой цели.

О чем эта книга

В этой книге подробно рассмотрены многие реальные программы атаки на приложения, объяснено, как и почему эти программы срабатывают, на чем основаны шаблоны атаки и (в некоторых случаях) как можно выявить факт проведения атаки. Параллельно читателям демонстрируются способы выявления новых уязвимых мест в программном обеспечении и способы их использования для взлома компьютеров.

В главе 1, "Программное обеспечение — источник всех проблем", описывается, почему программное обеспечение является основным источником проблемы безопасности компьютерных систем. Авторы расскажут о *трех основных проблемах* при использовании программного обеспечения — сложности, расширяемости и взаимодействии в пределах сети, — и объяснят, почему проблема безопасности становится все серьезней.

В главе 2, "Шаблоны атак", рассказывается об ошибках в реализации и недостатках в архитектуре программ. Будет рассмотрена проблема обеспечения безопасности открытой системы, а также будет показано, почему управление риском является

единственным надежным методом решения этой проблемы. В этой главе будут рассмотрены две реальные программы атаки: одна очень простая, а вторая, наоборот, сложная с точки зрения технической реализации. Авторы покажут, как шаблоны атак согласуются с классической парадигмой сетевого взаимодействия.

Темой главы 3, "Восстановление исходного кода и структуры программы", является восстановление исходного кода программы (reverse engineering). Злоумышленники выполняют дизассемблирование, декомпиляцию и реконструирование программ, чтобы понять, как они работают и как можно нарушить их работу. В этой главе описываются малоизвестные методы анализа программ, включая идею использования заплаты для составления плана возможной атаки. Речь пойдет о современном средстве, используемом хакерами для взлома программного кода, — Interactive Disassembler (IDA) . Также подробно будет рассмотрено, на каких принципах построены реальные программы взлома и как они работают.

В главах 4, "Взлом серверных приложений", и 5, "Взлом клиентских программ", изучаются два аспекта модели клиент/сервер. В главе 4, "Взлом серверных приложений", обсуждается получение данных с доверенных хостов, расширение привилегий, вставка вредоносного кода, отслеживание пути хранения файла и другие методы проведения атак на программное обеспечение сервера. В главе 5, "Взлом клиентских программ", рассказывается об атаках клиентских программ с помощью служебных сигналов, сценариев и динамического кода. В обеих главах приведено множество шаблонов и примеров реальных атак.

Созданию вредоносных входных данных посвящена глава 6, "Подготовка вредоносных данных". Изложенный в ней материал выходит далеко за пределы стандартных сведений. Здесь обсуждаются: анализ по частям, отслеживание функций кода и восстановление кода после синтаксического анализа. Особое внимание уделяется созданию эквивалентных запросов с помощью различных методов шифрования. Опять-таки предоставляются как примеры реальных атак, так и выделены шаблоны этих атак.

"Ночной кошмар" специалистов по обеспечению защиты информации — атаки на переполнение буфера — являются темой главы 7, "Переполнение буфера". В этой главе подробно рассматривается сам механизм атак на переполнение буфера, при том предположении, что читатели уже знакомы с общими принципами этих атак. Будут рассмотрены: переполнение буфера во встроенных системах и в базах данных, атаки на переполнение буфера для Java-программ и эти же атаки на основе содержимого передаваемых данных. В главе 7, "Переполнение буфера", также рассказывается, как выявлять ошибки переполнения буфера всех видов, включая переполнения буфера в стеке, арифметические ошибки, уязвимые места на основе строк форматирования, переполнения буфера в куче, использование функции `vtable` в программах на C++ и "трамплины". Технология внедрения вредоносного кода подробно рассмотрена для множества платформ, включая x86, MIPS, SPARC и PA-RISC. Кроме того, изложены усовершенствованные методы атак, например встроенная защита и использование переходов для обхода уязвимых механизмов обеспечения защиты. В главе 7, "Переполнение буфера", приведено огромное количество шаблонов атак.

Глава 8, "Наборы средств для взлома", посвящена наборам средств для взлома (rootkit), которые можно назвать вершиной искусства создания универсальных пакетов для атаки. В этой главе основное внимание уделено программному коду для реального набора средств для взлома систем под управлением Windows XP. Будут

рассмотрены перехваты вызовов, подмена выполняемых файлов, сокрытие запущенных файлов и процессов, атаки по сети и внесение изменений в двоичный код. Также рассматриваются проблемы с аппаратным обеспечением, включая методы для сокрытия наборов средств для взлома в EEPROM. Завершают главу несколько коротких разделов, посвященных методам, используемым в усовершенствованных наборах средств для взлома.

Итак, в книге *Взлом программного обеспечения: руководство начинающего хакера* описан полный спектр возможных атак на программы, начиная от внедрения вредоносного кода и заканчивая запуском скрытых наборов средств для взлома. С помощью шаблонов атак, примеров реального кода и программ атаки авторы доступно раскрывают методы, *ежедневно* используемые хакерами для взлома чужих программ.

Как пользоваться этой книгой

Эта книга пригодится различным специалистам: системным администраторам, обеспечивающим безопасность сетей, специалистам по защите информации, консультирующим различные организации, хакерам, а также разработчикам программ и программистам, которые работают над созданием новых программ для обеспечения защиты.

- Тем, кто отвечает за надежную работу компьютерной сети или работу программ на системах пользователей, следует прочесть эту книгу, чтобы узнать о типах уязвимых мест на контролируемых системах и способах их выявления.
- Тем, кто консультирует различные организации по вопросам защиты, следует прочесть эту книгу, чтобы быстро и эффективно выявлять и оценивать опасность уязвимых мест в системе безопасности.
- Если перед вами поставлена задача победить в информационной войне с противником, этой книгой можно воспользоваться, чтобы узнать, как проникнуть во вражеские системы посредством программного обеспечения.
- Разработчики программного обеспечения благодаря этой книге узнают, как хакеры обращаются с созданными ими продуктами. В современном мире все разработчики обязаны помнить о безопасности. Знания являются оружием, позволяющим разобраться с реальными проблемами в области обеспечения безопасности сетей.
- Программисты, которые непосредственно заняты созданием кода программ защиты, просто полюбят эту книгу.

Таким образом, эта книга в основном предназначена для специалистов в области защиты информации, но она содержит полезные сведения для *всех* профессионалов в области информационных технологий.

Не слишком ли опасна эта информация?

Очень важно понимать, что изложенные в книге сведения отнюдь не являются новыми для сообщества хакеров. Некоторые из рассмотренных методов использовались еще в “незапамятные времена”. Целью авторов было ознакомить с некоторой общедоступной информацией и повысить уровень знаний относительно безопасности программного обеспечения.

Некоторые специалисты по защите информации могут быть обеспокоены тем, что описание методов атаки может подтолкнуть многих людей к проверке их на практике. Возможно, в этом есть доля истины, но хакеры всегда имели более развитую систему обмена информацией, нежели специалисты по защите. Информация должна быть осмыслена и классифицирована профессионалами в области безопасности в целях определения наиболее приемлемых решений. Следует ли нам взять быка за рога или лучше спрятать голову в песок?

Возможно, эта книга вас шокирует. Тем не менее, она позволит узнать много полезных сведений.

Благодарности

Создание этой книги потребовало достаточно много времени. Нам помогало множество людей — и прямо, и косвенно. Хотя не обошлось без ошибок и недочетов, но мы хотим разделить все похвалы с теми людьми, которые принимали участие в процессе нашей работы.

Перечисленные ниже люди внесли важные замечания относительно материала этой книги: Александр Антонов, Ричард Бейтлич (Richard Bejtlich), Найшал Бхала (Nishchal Bhalla), Антон Чувакин, Грег Каммингс (Greg Cummings), Маркус Лич (Marcus Leech), Маркус Ранум (Marcus Ranum), Джон Стивен (John Steven), Уолт Стоунбюрнер (Walt Stoneburner), Герберт Томсон (Herbert Thompson), Картик Триведи (Kartik Trivedi), Адам Янг (Adam Young) и большое количество анонимных обозревателей.

Мы считаем своим долгом поблагодарить сотрудников издательства Addison-Wesley, особенно нашего редактора Карен Гетманн (Karen Getmann) и ее двух помощниц Эмили Фрей (Emely Frey) и Элизабет Здунич (Elizabeth Zdunich). Благодарим за то, что они воплотили в жизнь этот казавшийся бесконечным проект.

Благодарности Грега

В первую очередь я должен поблагодарить своего бизнес-партнера, а теперь и мою жену Пенни. Эта работа никогда не была бы выполнена без ее поддержки. Отдельное большое спасибо моей дочери Кэлси! В процессе создания книги многие люди внесли свою лепту (в виде затраченного времени и технических консультаций) в конечный результат. Большое спасибо Мэту Хагету за яркие идеи и обзор исторических перспектив, необходимый для успеха книги. Кроме того, благодарю Шона Брейкена (Shawn Bracken) и Джона Гэри (Jon Gary) за то, что они сидели в моем гараже и использовали старую дверь вместо рабочего стола. Благодарю и Алвара Флейка (Halvar Flake) за необходимые дополнения. Спасибо Дэвиду Айтелу (David Aitel) за предоставление технических сведений по использованию методов атак с применением кода командного интерпретатора. Благодарю Джеми Батлер (Jamie Butler) за прекрасные знания по наборам средств для взлома, а также благодарю Джефа и Пинга Мосс (Jeff and Ping Moss).

Неоценимую помощью в подготовке этой книги к изданию оказал мой соавтор Гари Мак-Гроу, который планировал нашу работу. Большинство моих знаний были получены самостоятельно, а Гари подвел необходимый научный базис под эти знания. Он очень честный и откровенный человек. Добавьте ко всем этим качествам отличные теоретические знания, прекрасно дополняющие мои практические навыки. К тому же Гари хороший друг.

Благодарности Гари

Выражаю благодарность компании Citigal (http://www.citigal.com), которая предоставила просто прекрасное место для работы. Творческая атмосфера и приятные в общении люди позволили работать с удовольствием (сколько времени было сэкономлено из-за отсутствия приступов хандры!). Особая благодарность административной группе за организацию производственного процесса: Джефу Пейни (Jeff Payne),

Джефу Воас (Jeff Voas), Чарли Крю (Charlie Crew) и Карлу Левису (Karl Lewis). В кабинете руководителя технического отдела, штат которого набирали профессионалы своего дела Джон Стивен (John Steven) и Рич Милз (Rich Mills), мои таланты раскрылись в полной мере. В прекрасную команду специалистов входят Френк Чарон (Frank Charron), Тод Мак-Энали (Tod McAnally) и Майк Дебнам (Mike Debnam). Эти люди смогли воплотить многие теоретические идеи на практике. Группой Software Security Group (SSG) от компании Cigital, основанной мной в 1999 году, теперь руководит Стен Виссеман (Stan Wisseman). Группа SSG продолжает работать над распространением принципов безопасности для программного обеспечения по всему миру. Хочется отдельно сказать "спасибо" членам этой команды Брюсу Поттеру (Bruce Potter) и Пако Хоупу (Pako Hope), Пэту Хигинсу (Pat Higgins) и Майку Фиретти (Mike Firetti). И наконец, особая благодарность Ивонне Вайли (Yvonne Wiley), которая довольно удачно отслеживала мое местонахождение на этой планете.

Эта книга никогда бы не появилась без моего соавтора Грега Хогланда. Его знания использованы на каждой странице этой книги. Если вам понравятся технические детали этой книги, благодарите Грега.

Как и три мои предыдущие книги, эта книга появилась в результате совместных усилий многих людей. Среди моих друзей, помогавших мне в изучении принципов защиты информации, хочу назвать Росс Андерсон (Ross Anderson), Анни Энтон (Annie Anton), Мэта Бишопа (Matt Bishop), Стива Белловина (Steve Bellovin), Билла Чесвика (Bill Cheswick), Криспина Кована (Crispin Cowan), Дрю Дин (Drew Dean), Джереми Эпштейна (Jeremy Epstain), Дейва Эванса (Dave Evans), Эда Фелтена (Ed Felten), Ануп Гош (Anup Ghosh), Ли Гонг (Li Gong), Питера Ханимана (Piter Honeyman), Майка Ховарда (Mike Hovard), Стива Кента (Steve Kent), Поля Кочера (Paul Kocher), Карла Лэндвирха (Karl Landwerh), Патрика Мак-Дэниэла (Patrick McDaniel), Грега Морисетта (Greg Morrisett), Питера Ноймана (Piter Neumann), Джона Пинкуса (John Pincus), Маркуса Ранума (Marcus Ranum), Ави Рубина (Avi Rubin), Фреда Шнейдера (Fred Schneider), Брюса Шнейдера (Bruce Schneider), Джина Спаффорда (Gene Spafford), Кэвина Салливана (Kevin Sullivan), Фила Винейблеса (Phil Venables) и Дэна Воллача (Dan Wallach). Благодарю сотрудников DARPA (Defense Advanced Research Projects Agency) и AFRL (Air Force Reseach Laboratory) за многолетнюю поддержку моих изысканий.

Но больше всего я хочу поблагодарить мою семью. Я признаюсь в любви Эми Бэрли (Amy Barly), Джеку и Эли. Особая признательность моему отцу и моим братьям.

От издательства

Вы, читатель этой книги, и есть главный ее критик и комментатор. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересно услышать и любые другие замечания, которые вам хотелось бы высказать в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо, либо просто посетить наш Web-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится или нет вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Посылая письмо или сообщение, не забудьте указать название книги и ее авторов, а также ваш обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию последующих книг. Наши координаты:

E-mail:	`info@williamspublishing.com`
WWW:	`http://www.williamspublishing.com`

Информация для писем из:

России:	115419, Москва, а/я 783
Украины:	03150, Киев, а/я 152