Содержание

От автора
Предисловие (версия 1.5)

Авторы первого издания книги относительно ее содержания единодушны в одном: после первоначального изложения материала у них появилось желание представить материал своих глав по-другому. Объясняется это допущенными ошибками, недостаточным, с точки зрения авторов, пояснениями изложенного в книге материала, нехваткой времени для написания еще одного примера программы или тем, что авторы забыли рассмотреть дополнительные вопросы. Как и в любом другом проекте, время в конечном счете истекло, и пришлось завершить работу.

Предоставленный шанс повторно вернуться к работе над книгой позволил авторам исправить недостатки, выявленные с момента первого ее издания. Большая часть была выявлена благодаря читателям, написавшим авторам: «Вам следовало бы по-другому написать об этом…» В абсолютном большинстве случаев они были правы. В результате была предпринята попытка исправления максимально возможного числа недостатков первого издания книги «Защита от хакеров корпоративных сетей» (*Hack Proofing Your Network*).

К моменту первого издания книги в продаже было совсем немного книг, посвященных в полном объеме методам преодоления средств компьютерной защиты. Для издательства Syngress Publishing эта книга стала первой в подобной серии. Руководство издательства немного нервничало. Оно не было уверено в том, что обучение хакерским методам – это хорошо. (Похоже, что другие издательства были напуганы. Когда автор говорил с представителями некоторых из них о книге, посвященной методам работы хакеров, то они даже не захотели просмотреть план книги. «Никаких книг о хакерских мето-

дах». Конечно, некоторые из них к настоящему времени уже выпустили книги по этой тематике.)

Поэтому в издательстве Syngress полагали, что если будет написана книга *Hack Proofing Your Network*, то она должна в полном объеме описать мероприятия по защите информации. Так и было сделано. Кто-то может возразить вам, что он не имеет ничего против методов защиты, что он применяет их годами. Но когда в книге упоминается о защите, речь идет о совершенно других технологиях. В первом издании ряд глав был посвящен вопросам защиты, которые трудно реализовать целиком и которые, вообще говоря, неудобны для работы.

По сравнению с первым изданием произошли некоторые изменения. Например, под словосочетанием *Hack Proofing* теперь понимается серия книг, а не одна книга. Кроме книги, которая перед вами, в серию входят:

- *Hack Proofing Your E-commerce Site* (ISBN: 1-928994-27-X)
- *Hack Proofing Your Web Applications* (ISBN: 1-928994-31-8)
- *Hack Proofing Sun Solaris 8* (ISBN: 1-928994-44-X)
- *Hack Proofing Linux* (ISBN: 1-928994-34-2)
- *Hack Proofing Windows 2000 Server* (ISBN: 1-931836-49-3)
- *Hack Proofing Your Wireless Network* (ISBN: 1-928994-59-8)
- *Hack Proofing ColdFusion 5.0* (ISBN: 1-928994-77-6)

Готовятся к печати и другие книги этой серии, которых объединяет их ориентация на описание методов защиты.

Это версия 1.5 предисловия. С течением времени содержимое данной книги пересматривается (точнее, тщательно проверяется и совершенствуется, но вы поняли идею). Однако слова Мудге все еще остаются в силе. Читая книгу, скоро вы убедитесь в этом сами. Полагайте, что перед вами протокол изменений содержимого книги. Обратите внимание на изменения, внесенные во второе издание, которые заключаются или в добавлении нового материала, или в улучшении старого. В издание добавлено несколько новых глав, включая:

- Хакинг аппаратных средств ЭВМ;
- Туннелирование;
- Уклонение от IDS;
- Атаки, основанные на форматирующей строке.

Эти главы поясняют некоторые сложные темы, включение которых в книгу способно сделать ее содержание актуальнее. Сведения об использовании форматирующей строки стали общедоступны только после завершения работы над первым изданием. В первом издании ничего не рассказано об этом, поскольку в то время были неизвестны методы работы с форматирующей строкой.

Каждая глава второго издания была обновлена, переработана с точки зрения возможных атак, сжата и вообще улучшена. Есть бесконечное число вариантов изложения, но некоторые читатели предложили разбить материал первого издания по темам таким образом, чтобы каждый используемый метод был освещен в одной главе. Это выглядело привлекательно, поэтому и было осуществлено во втором издании. В начале книги пара глав посвящена теории, но сразу за этими «вводными» главами по существу обсуждается каждый тип нападения. Наконец, для большей пользы книгу завершает краткая глава о правилах информирования нас о найденных вами изъянах в системах защиты.

Одно из центральных изменений второго издания состоит в том, что авторы издания оставили попытку объяснить свои действия. В первом издании потрачено много времени и усилий для разъяснения, *почему* знания о хакерских методах полезны, *почему* в разное время люди используют слово «хакер» и *почему* восстановление алгоритмов работы существующих программ (reverse engineering) должно относиться к основным человеческим правам.

После выхода первого издания большинство людей, купивших книгу, уже согласились с тем, что представленная в книге информация должна быть доступна (или, по крайней мере, они захотели ознакомиться с ней). А люди, которые не соглашались со мной… Что ж, они не согласны со мной и после прочтения книги, *даже после ознакомления с приведенными в книге доводами*! Говоря искренне, я был потрясен. Я не убедил их своими тщательно подобранными аргументами. Действительно, невозможно всегда всем нравиться.

Возвращаясь к обсуждаемым вопросам, отметим, что люди, которым нравится то, что, мы делаем, могут не читать объяснений, почему мы занимаемся этим. Эти объяснения для тех, кто не разделяет наших позиций. Авторы используют слово *хакер* для обозначения субъекта, который взламывает компьютер без разрешения. Однако это слово не используется исключительно в данном контексте. Оно также обозначает ряд других «субъективных» понятий. Вы как образованный читатель и профессионал в области безопасности должны, в зависимости от контекста, понять его смысл. Если вы прочтете остальную часть этой книги, то найдете там разные значения этого слова.

Если вы хотите точно знать, что было в первом издании книги и чего нет во втором, то посетите сайт Syngress Solutions по адресу www.Syngress.com/solutions. В дополнение к электронной версии первого и второго издания книги у вас появится возможность задать авторам вопросы по электронной почте о книге и получить ответы на них. Если этого недостаточно, в течение года вам будет предоставлена возможность ознакомиться с периодическими

обновлениями содержимого книги в форме официальных изданий. Для издательства это еще один дополнительный способ познакомить вас с новыми материалами, ставшими известными только после выхода издания книги. Сайт Solutions – это ваш ресурс, используйте его. Кроме того, мне интересно узнать мнение читателей.

Я надеюсь, что книга вам понравится.

Райан Рассел (Ryan Russell)

Глава 1

Хакерские методы

В этой главе обсуждаются следующие темы:

- Что понимают под «хакерскими методами»
- Обзор содержимого книги
- Правовое обеспечение хакинга

- ☑ Конспект
- ☑ Часто задаваемые вопросы

Введение

В этой книге собраны сведения, которые могут пригодиться для преодоления системы безопасности компьютера. Если это шокирует читателя, то, вероятно, он незнаком с разрешенными, с юридической точки зрения, причинами ее вскрытия. Взлом компьютера на законных основаниях допустим при испытании безопасности компьютерных систем, защите прав потребителя и гражданских прав, действий в военных целях. В книге в основном раскрываются хакерские методы, а не причины их применения.

Повсюду на страницах книги умышленно используется словосочетание «хакерские методы». Следует понимать, что у различных людей эти слова обозначают разные понятия. Поэтому в этой главе поясняется смысл, который авторы понимают под ними, а также приведена структура книги и рассмотрены требования к подготовке читателя, необходимой для усвоения приведенных в книге методов. В этой главе рассматривается современный взгляд на хакерство, реинжиниринг, защиту от копирования и действующее законодательство, поскольку не хотелось бы вручить читателю новую игрушку без предупреждения обо всех неприятностях и конфликтах с законом, с которыми он может столкнуться.

Что понимают под «хакерскими методами»

Когда автор был ребенком, диалоговый мир сетевых компьютерных онлайн-систем состоял из электронных досок объявлений (BBS). На многих BBS были текстовые файлы, заголовок которых представлял собой вариацию на тему «Как стать хакером». Почти все эти файлы были бесполезны и содержали советы подобно следующим: «попробуйте приведенные мастер-пароли» или «нажмите на клавиатуре комбинацию клавиш **Ctrl + C** и посмотрите, не приведет ли это к выходу из программы». Название главы «Хакерские методы» – это способ автора воздать должное подобным файлам. Они стали его источником вдохновения для написания *приличного* набора инструкций по применению хакерских методов – хакингу.

Итак, какой смысл подразумевается под словом *хакерство*? Под ним понимается обход мер безопасности компьютерных систем и вычислительных сетей. Слово *хакерство* применимо и как существительное, характеризуя умную или быструю программу. В реальной жизни (в выпусках новостей, беседах, списках адресатов почты и т. д.) люди применяют слово *хакерство, хакинг*

или *хакер* без объяснения вкладываемого в него смысла. Но его можно понять из контекста или чтения между строк. Эта книга не является исключением. Кроме того, авторы иногда используют выражения, как, например, хакер-новичок (*script kiddie*), для обозначения чего-либо связанного или производного от значения слова *хакер*. Если читателю не нравится термин, который применяется для рассматриваемой человеческой деятельности, то авторы искренне призывают его мысленно заменить обсуждаемый термин на привычное для читателя слово и далее считать, что именно привычный для него термин используется в книге.

Если читатель действительно хочет познакомиться с философским обсуждением значения слова, то, пожалуйста, посетите Web-сайт Syngress Solutions и загрузите электронную копию первого издания книги. В ее первой главе под названием «Политика» обсуждаются различные значения слова *хакер*. В этом издании подобное обсуждение опущено, но если читатель хочет пойти своим путем в поисках старой истины, то не говорите, что его не предупреждали.

Вообще говоря, авторы надеются избежать использования слова хакер в значении «плохой программист».

Зачем применяют хакерские методы?

Если читатель хочет услышать длинный рассказ о причинах чьего-либо любопытства о том, как это делается, автор отсылает его к первому изданию книги с длинными рассуждениями о слове хакер. Но кратко: *лучшая защита – это нападение*. Другими словами, единственный способ остановить хакера заключается в том, чтобы думать как он. И если после этого вы не сможете взломать ваши системы, то кто сможет? Эти фразы звучат банально, но они олицетворяют подход, который, по мнению авторов, позволит наилучшим образом обеспечить безопасность вашей собственной системы (или системы работодателя, или ваших клиентов и т. д.).

Приоткрывая завесу

«Мы не нанимаем хакеров»

Вы, возможно, слышали о заявлениях различных компаний безопасности о том, что они «не нанимают хакеров». Очевидно, смысл подобных заявлений заключается в том, что компании имеют в виду исправившихся хакеров-преступников, хакеров, ныне работающих в облас-

Продолжение ⇒

ти безопасности, или что-то другое. В основном это делается из-за опасения отказа некоторых людей от сотрудничества с компанией в случае, если им станет известно о найме подобных работников, поскольку бытует мнение, что преступнику нельзя доверять безопасность систем клиентов. В действительности это дело принципа. Некоторые просто не желают видеть, как хакеры-преступники получают что-либо, напоминающее вознаграждение за их противозаконную деятельность.

Иногда компании полагают, что разумнее сделать наоборот: Если о хакере уже слышали (даже если у него скандальная репутация), то, вероятно, компании испытывают определенное желание принять на работу такого высококлассного профессионала. Будет ли от этого положительный эффект? Это зависит от сферы деятельности компании. Конечно, если вы говорите о компании, предоставляющей сервисные услуги, то люди могут колебаться, но меньше, чем в случае, когда компания тестирует безопасность компьютерных систем.

В целом это палка о двух концах. Ну и конечно, у хакеров всегда есть вопрос к компаниям, которые «не нанимают хакеров»: «Как вы об этом узнали?»

Чтобы рассказать о том, как злоумышленник будет преодолевать нашу защиту, авторам потребуется выступить в его роли. Означает ли это, что, информируя читателя о методах взлома, авторы в то же время сообщают их и «злоумышленникам»? Да. Но авторы полагают, что в этой игре все должны иметь равные права: все стороны должны быть вооружены одними и теми же общедоступными методами. А с другой стороны, как вы сможете отличить законопослушного пользователя от злоумышленника?

Обзор содержимого книги

Теперь, после обсуждения вопросов «как» и «почему», поговорим о том, что найдет читатель далее в этой книге. Оценки начальная, средняя и высокая для каждой главы позволяют определить уровень знаний читателя, необходимых для успешного усвоения изложенного в ней материала.

В трех последующих главах книги представлен минимум теоретического багажа знаний. В главе 2 исследуется сформулированный авторами список законов, которые определяют работу (или отказ) систем компьютерной безопасности. Далее в книге вы увидите, как можно применять эти законы в хакерских технологиях. В главе 3 описываются типы атак и возможный потен-

циальный ущерб компьютерной системы в случае их успешного осуществления, а также приведены примеры каждого типа атак. В главе 4 рассказывается о различных методологиях, которыми кто-нибудь (например, вы) может руководствоваться при обнаружении проблем безопасности. Первые четыре главы этой книги должны быть доступны читателям любого уровня подготовки. Читатели с высоким уровнем профессиональной подготовки могли бы пропустить эти главы, если они уже знакомы с излагаемой теорией, но мы рекомендуем им, по крайней мере, просмотреть текст и удостовериться в отсутствии для них новой информации в изложенном материале. Раздел «Краткие выводы» хорошо подходит для этих целей.

Начиная с пятой главы мы рассматриваем методы хакинга. Глава 5 описывает простейший метод хакинга – поиск различий (*diffing*), состоящий в простом сравнении кода до и после осуществления некоторого действия. Это удивительно полезно. Материал данной главы доступен даже новичкам.

Глава 6 – о криптографии и различных средствах обеспечения конфиденциальности информации. В главе исследуются дилетантские попытки шифрования, примеры использования которых в мире наблюдаются почти каждый день. Вы познакомитесь с распознаванием шифров, основами их вскрытия и очень простыми криптоподобными схемами кодирования. Эта глава не рассчитана на уровень подготовки выше среднего (в главе приводится вводный материал для читателей с небольшим опытом в рассматриваемой области).

Глава 7 посвящена проблемам безопасности, возникающим при программных сбоях в результате непредсказуемого ввода данных пользователем. К ним относится хакинг сервера через дефектную программу CGI интерфейса, получение SQL доступа при помощи Web-формы или сценария, позволяющего вскрыть командный процессор операционной системы UNIX обманным путем (tricking scri pts). (С технической точки зрения сюда же можно отнести переполнение буфера и ошибки форматирования строк (format string holes), но этим вопросам посвящены отдельные главы.) Глава по уровню предполагаемой подготовки читателя заслуживает оценки от средней до высокой. Это обусловлено обсуждением различных языков программирования и необходимостью понимания принципов работы командной оболочки.

В главах 8 и 9 показаны методы использования машинно-ориентированного языка для максимального использования преимуществ переполнения буфера или ошибок форматирования строк. Эти главы предполагают высокий уровень подготовки читателя. Но написаны они вполне доступно, с подробным объяснением изложенного материала. Для усвоения материала потребуются определенные знания языка С и ассемблера.

Глава 10 описывает возможности применения мониторинга сетевых коммуникаций *sniffing* методами в интересах хакинга. Приведены простые примеры. Описано, при помощи каких протоколов лучше всего получить доступ

к паролям, и даже приведены основы программирования мониторинга сетевых коммуникаций методами *sniffing*. Эта глава ориентирована на читателей с начальным и средним уровнями подготовки.

Глава 11 представляет тему, посвященную пиратским подключениям (hijacking connections). В большинстве случаев эта разновидность взлома является расширенным применением мониторинга сетевых коммуникаций методами *sniffing* за счет активного участия злоумышленника. В главе описан тип атак «злоумышленник посередине» (man-in-the-middle). Для изучения приведенного материала требуется средний уровень квалификации читателя.

Глава 12 обсуждает концепцию доверия и то, как ниспровергать ее при помощи имитации соединения (*spoofing*). Эта глава обсуждает ряд потенциальных нападений и требует уровеня подготовки читателя от среднего до высокого.

Глава 13 описывает механизм туннелирования для перехвата сетевого трафика посредством враждебного сетевого окружения (настолько надежным способом, что при перегрузке перехват возобновляется). Приводится подробное обсуждение SSH, для которого требуется уровень подготовки от среднего до высокого.

Глава 14 – о хакерстве аппаратных средств компьютера. Эта глава приводит основные сведения о хакерстве аппаратных средств ЭВМ с целью получения максимальной безопасности. Это ознакомительная глава, потому что фактическая реализация приведенных методов потребует высокой подготовки.

Глава 15 посвящена вирусам, Троянским коням и червям. Описано, не только чем они являются и как работают, но также принципы их построения, используемые ими методы и что ожидать в будущем. Это глава по сложности излагаемого материала занимает промежуточный уровень.

В главе 16 описаны способы, при помощи которых системы обнаружения вторжения уклоняются от атак или обезвреживают их. Также описаны уловки (ловкие приемы), которые эффективны на уровнях от сетевого до уровня приложений. Разобраны такие темы, как фрагменты и использование полиморфизма. Уровень сложности обсуждаемого материала – от среднего до сложного (читатель должен хорошо знать протокол TCP/IP).

В главе 17 обсуждается автоматизация некоторых из задач читателя при помощи автоматизированного обозревания безопасности и инструментов нападения (после того как читатель познакомится с правилами их написания). Обсуждение охватывает коммерческие и свободно распространяемые программные средства. Это позволяет хорошо представить следующее поколение программных средств, которые будут не только определять уязвимости тестируемой системы, но и позволят укрепить ее.

Последнее, но не менее важное. В главе 18 сообщается о действиях читателя при обнаружении проблем безопасности. Не подумайте, что авторы

книги не поощряют обнаружение брешей в системе защиты информации. Поощряют, но при условии, что читатель несет полную ответственность за свои действия.

Правовое обеспечение хакинга

Автор – не юрист: грубо говоря, это означает следующее: «Он не может дать вам никакого уместного юридического совета, а читатель не обязан ему следовать. Если читатель что-то сделает, то не подумайте, что его не предупреждали о последствиях. Но автор попытается заставить читателя прислушаться к своему мнению тем или иным способом».

В этой книге читатель узнает о методах, которые в случае неправильного их применения приведут его к нарушению законодательства и связанным с этим последствиям. Слова автора подобны словам инструктора по вождению автомобиля: «Я собираюсь научить вас ездить на автомобиле, но если вы водите плохо, то можете кого-нибудь сбить». В обоих случаях вам придется отвечать за причиненный ущерб.

Автор использует очень простое правило, заключающееся в ответе на вопрос: «У меня есть разрешение сделать это на этом компьютере?» Если ответ – нет, то не делайте этого. Ваши действия принесут вред и почти наверняка будут противозаконны. Но если ответ не столь очевиден, то, возможно, есть исключения, ну и т. д. Например, в большинстве мест (нет, не в вашей организации, по этому поводу проконсультируйтесь у юриста) сканирование порта разрешено. Хотя это рассматривается как предпосылка к незаконному проникновению в систему со злым умыслом, но это законно – кроме тех случаев, когда сканирование портов запрещено.

Самый простой способ обезопасить себя заключается в хакинге своей собственной сети (автор подразумевает домашнюю сеть *читателя*, а не сеть на работе, потому что иначе у вас могут быть неприятности). Вы хотите освоить тонкости сложной программы, работающей на платформе Sun Sparc? Идите и купите старый Sparc за 100$. Вы хотите заняться хакерством на многомиллионной универсальной ЭВМ? Хорошо, но, вероятно, вас постигнет неудача.

Можно было бы склониться к предположению о полной безопасности хакерских действий на собственном оборудовании. Но, строго говоря, это не так в случае действий, направленных на вскрытие программного обеспечения. Много людей думают также, то есть если я купил копию программы, то я имею естественное право делать с ней все, что я захочу на своем собственном компьютере. Право интеллектуальной собственности так не считает. В Соединенных Штатах, а также в соответствии с международным соглаше-

нием в ряде других стран обход средств недопущения копирования материалов, защищенных авторским правом, противозаконен. Это – часть акта DMCA. Формально противозаконно заниматься этим даже у себя дома, но если вы все-таки сделали это и пользуетесь результатами своих действий только сами, то кажется маловероятным, что у вас появятся проблемы. Но при попытке поделиться полученными результатами с другими людьми вам следует проявить осторожность.

Предупреждая о безопасности, автор хотел бы рассказать о чрезвычайной истории, произошедшей в результате нарушения новых законов. Это касается российской компании – разработчика программного обеспечения ElcomSoft Co. Ltd., специализирующейся на вскрытии паролей, снятии защиты от копирования и восстановлении поврежденных файлов. Имейте в виду, что на тот момент времени в России не было никакого закона против восстановления алгоритма работы программы по ее коду. Один из программистов компании ElcomSoft Co. Ltd., Дмитрий Скляров, прибыл на конференцию DEF CON 9 в Лас-Вегасе и сделал доклад относительно формата электронных документов eBook компании Adobe. Формат содержит некоторые смехотворные попытки безопасности. На следующий день Дмитрий был арестован и обвинен в «распространении изделия, предназначенного для обхода средств защиты авторского права». При этом упоминалась программа его компании, которая конвертировала формат eBook документа в стандартный формат Adobe Acrobat .PDF файлов. Выполнение подобного конвертирования покупателем одного из этих средств eBooks для себя юридически законно, поскольку пользователю разрешается делать резервные копии.

Короче говоря, Дмитрий был арестован 17 июля 2001 года и отпущен домой только 31 декабря 2001 года. Компания Adobe отозвала свою жалобу из-за повсеместных протестов, но американское правительство отказалось снять обвинения. Поскольку вопрос не закрыт до сих пор, Дмитрий все еще полностью не освобожден от ответственности.

Относительно сказанного хочется добавить, что используемые им методы для разгадывания системы безопасности изделия были относительно просты. Мы осветим подобные методы декодирования в главе 6.

Пожалуйста, будьте осторожны с информацией, которая изложена в книге.

Конспект

В этой книге авторы собираются рассказать о подробностях поиска брешей в системе безопасности и их использования на основании таких методов, как анализ пакетов, пиратское подсоединение, имитация соединения для получения доступа, схем раскрытия шифров, уклонение от систем обнаружения атак и даже хакинг аппаратных средств ЭВМ. Это не книга о проектировании безопасности, политике, архитектуре, управлении рисками или планировании. Если читатель так думает, то его ввели в заблуждение.

Все обнаруженные бреши в системе защиты должны быть преданы огласке. Публичное сообщение об ошибках приносит пользу каждому, включая вас самих, поскольку это может способствовать вашему признанию.

Вы должны научиться хакерским методам, для того чтобы знать, как защитить вашу сеть или сеть вашего работодателя. Вы должны это знать, потому что это интересно. Если вы не соглашаетесь с чем–либо, о чем говорится в этой главе или книге, то это хорошо! Первое, что хакеры должны уметь делать, – это самостоятельно думать. Нет никаких причин для слепой веры в изложенный авторами книги материал. Если у вас есть замечания к книге, то зайдите на Web-сайт www.syngress.com/solutions, найдите адрес электронной почты авторов и пошлите им письмо. Возможно, ваше опровержение будет помещено на сайт.

Часто задаваемые вопросы

Вопрос: Могу ли я назвать себя хакером?

Ответ: Существует два ответа на этот вопрос. Первый, созвучный мыслям многих: хочешь быть хакером – будь им. Второй: если вы называете себя хакером, то будьте готовы к широкому диапазону оценок вследствие большого количества определений слова «хакер» и их двусмысленности. Одни будут думать, что вы только что сказали им, что вы – преступник. Другой, кто сам себя считает хакером, осмеет вас, если вы будет заподозрены в недостаточной квалификации. Некоторые не будут знать, что и подумать, но затем попросят вас о хакерской услуге для себя… Автор советует вам сначала приобрести необходимые навыки и практику. Лучше всего, если кто-либо другой назовет вас хакером.

Вопрос: Законно ли написание вирусов, Троянских коней и червей?

Ответ: Фактически (в большинстве случаев) да. Пока. Это утверждение заслуживает серьезного разъяснения. Существует ряд программистов, которые открыто пишут вирусы и делятся результатами своей работы. До сих

пор они, кажется, никому не мешали. Однако если хотя бы часть написанного ими кода выйдет из-под контроля и привлечет к себе внимание, то дело примет серьезный оборот. Если вы пишете программы вирусов, будьте осторожны, чтобы не потерять контроль над ними. Вы можете захотеть ограничить их способность к распространению, проявляя необходимую предосторожность. В этой связи задумайтесь, как вы будете выглядеть, если кто-то доработает ваш вирус и выпустит его на волю. Также обратите внимание на то, не противоречит ли отправление по почте подобного кода правилам, установленным вашим Интернет-провайдером, особенно если вы – учащийся. Ваши действия могут и не противоречить установленным правилам, но могут легко привести к разрыву соединения с вашим Интернет-провайдером, получения предупреждения или лишения вас прав пользователя.

Вопрос: Несете ли вы ответственность за хакинг систем?

Ответ: Вообще, *если* вы санкционированный (авторизованный) пользователь, нет. Пожалуйста, примите во внимание *если*. Когда есть сомнения, получите письменное разрешение от юридического лица – владельца компьютерной системы, например школы или работодателя. Множество людей, отвечающих за безопасность компьютерных систем, регулярно тестируют их хакерскими методами. Дополнительные сведения и примеры вы сможете найти по адресу www.lightlink.com/spacenka/fors.