Посвящается

светлой памяти доктора Ричарда Стивенса
(Richard Stevens)

Я и сейчас отчетливо помню его во время перерыва в комнате докладчиков на конференциях SANS — собранные сзади длинные светлые волосы, проницательный взгляд, которым он смотрел на всех своих студентов. Я помню все его комментарии на проверенных заданиях. Ричард Стивенс был лучшим преподавателем. Сейчас его уже нет с нами, но не проходит и нескольких дней, чтобы я не обратился к его *TCP/IP Illustrated, Volume 1*. Как правило, я смотрю на схемы заголовков пакетов, изображенные на первой странице обложки. Я очень рад, что у меня есть эта книга, она помогает мне не забывать механизм работы протоколов IP и TCP — тех самых протоколов обмена информацией, которые сейчас царствуют в мире компьютеров. Через несколько недель я начинаю преподавать основы TCP/IP приблизительно четырем сотням студентов. Мне так страшно, что я не смогу заменить Ричарда или хотя бы приблизиться к его уровню, но процесс передачи знаний не должен прерываться. У меня не хватает слов, чтобы донести всю важность проделанной им работы. В конце концов не существует универсального средства для обнаружения несанкционированного доступа, но благодаря доктору Стивенсу решение этой задачи стало намного проще. Кроме того, каждый специалист по безопасности работы в компьютерных сетях должен иметь базовые знания о работе протокола IP, чтобы вовремя определить нестандартную ситуацию. Именно этими способностями обладал доктор Стивенс, все мы учились у него, и эти уроки положены в основу материала книги *Обнаружение типовых нарушений безопасности в сетях*!

Стивен Норткат (Stephen Northcutt)

Весь наш вклад в дело обеспечения безопасности и в разработку методов анализа трафика нельзя сравнить с тем, что удалось сделать в этой области доктору Ричарду Стивенсу. Он был талантливым и очень плодовитым автором. Моей настольной книгой с потрепанными, замусоленными страницами и жирными пятнами является экземпляр *TCP/IP Illustrated, Volume 1*. Это просто шедевр для любой технической библиотеки, так как Ричард Стивенс стоял у истоков разработки TCP/IP и Unix, и к тому же он обладал редким даром делать сложный материал легко понятным. Я знакома с несколькими преподавателями SANS, которые считают эту книгу "Библией TCP/IP". Однажды мне повезло прослушать курс лекций, которые он читал в SANS, и я сидела, разинув рот, потрясенная глубиной его познаний. Прошлым летом он согласился отредактировать для издания курс лекций, которые я написала для SANS по основам работы стека протоколов TCP/IP. Результат его работы достоин сравнения с критическим просмотром Шекспиром какой-нибудь бухгалтерской книги. Это издание всегда со мной, и мне никогда не забыть этого человека.

Джуди Новак (Judy Novak)

Об авторах

Стивен Норткат (Stephen Northcutt) закончил колледж имени Мэри Вашингтон. До того как приступить к работе в области обеспечения безопасности работы в компьютерных сетях, он служил в вертолетном подразделении ВМС США и был одновременно спасателем, шеф-поваром, картографом, тренером по боевым искусствам и проектировщиком компьютерных сетей. Стивен является автором книг *Incident Handling Step by Step*, *Intrusion Signatures and Analysis*, *Inside Network Perimeter Security* и двух предыдущих редакций этой книги. Стивен Норткат — автор системы обнаружения вторжений Shadow. Он занимал пост начальника отдела защиты от несанкционированного доступа в сетях с помощью системы Shadow, а затем главы ведомства информационной безопасности департамента защиты от нанесения удара баллистическими ракетами Министерства обороны США. В настоящее время Стивен Норткат работает руководителем отдела обучения и аттестации института SANS.

Джуди Новак (Judy Novak) — старший специалист по вопросам безопасности балтиморской консалтинговой фирмы Jacob and Sundstrom, Inc. До этого она работала в лаборатории прикладной физики Университета Джона Хопкинса (Johns Hopkins University) и занималась обнаружением вторжений и отслеживанием трафика, а также исследованиями в области безопасности обмена информацией. Джуди является одним из основателей группы по реагированию на происшествия исследовательских лабораторий вооруженных сил США, в которой она состоит на протяжении трех лет. Она принимала участие в создании курса по TCP/IP и написала учебник по практическому курсу "Анализ сетевого трафика с помощью tcpdump". Обе эти книги используются на курсах сертификации института SANS. Выпускница университета штата Мэриленд, Джуди Новак — опытный специалист, она энергична, страстная велосипедистка, а героем современности считает Ланса Армстронга!

О технических рецензентах

Рецензенты внесли свою немалую лепту в создание книги *Обнаружение нарушений безопасности в сетях, 3-е издание*. Эти высококлассные профессионалы проштудировали весь изложенный материал, проверяя его как с точки зрения технической правильности, так и со стороны удобства изложения и литературной грамотности. Их вклад, без сомнения, способствовал тому, чтобы данная книга стала качественным источником информации для наших читателей.

Карен Кент Фредерик (Karen Kent Frederick) занимает должность ведущего инженера по безопасности в группе быстрого реагирования проекта NFR. Степень магистра наук в области информационных технологий со специализацией в области компьютерной безопасности она получила в университете штата Айдахо по программе переподготовки инженеров. Карен уже 10 лет занимается технической поддержкой, системным администрированием и вопросами компьютерной безопасности. Ее квалификация подтверждена рядом сертификатов, среди которых SANS GSEC, GCIA, GCUX и GCIH. Карен Фредерик — соавтор книг *Анализ типовых нарушений безопасности в сетях (Intrusion Signatures and Analysis)*, *Inside Network Perimeter Security*. Ее многочисленные статьи по теме обнаружения вторжений можно найти на сайте `SecurityFocus.com`.

Дэвид Хэйнбач (David Heinbuch) был зачислен в лабораторию прикладной физики университета Джона Хопкинса в 1998 году. Он имеет большой опыт в обнаружении несанкционированного доступа, моделировании и выполнении экспериментов, исследовании уязвимости компьютерных систем и разработке программного обеспечения. Являясь участником группы Information Operations, он работал с разнообразными программами, в том числе с системами выполнения безопасных вычислений, а также принимал участие в имитации, выявлении и анализе атак хакеров. Дэвид получил степень бакалавра в области информационных технологий в колледже штата Виржиния и степень магистра — в университете Джона Хопкинса.

Благодарности

Стивен Норткат. Над разработкой аналитических и практических методов обнаружения несанкционированного доступа, которые описаны в этой книге, трудилось множество специалистов всей планеты. Мы с вами должны выразить им свою признательность за то, что все тайное теперь стало явным.

Я благодарю всех, кто помогал нам в работе и предоставил нам полезную информацию, а особенно команде, поддерживающей сайт `Incidents.org`. Они смогли указать множество новых шаблонов для выявления действий хакеров, помогли минимизировать ущерб, причиненный множеству скомпрометированных систем, и одновременно с этим даже проводили обучение методам обнаружения вторжений. Так держать!

Устранение последствий нарушений безопасности не имело бы большого значения, если бы люди не делились информацией о проведенных атаках. Энтузиасты, которые работали над информацией сайта `dshield.com`, сделали нечто большее. Они не только предоставили сведения об атаках, но и провели их анализ, чтобы все остальные стали умнее и поняли, как искать уязвимые места в системе защиты.

Спасибо Джуди Новак за совместную работу над этой книгой. Исключительно благодаря ее стараниям мы добились положительного результата. Я искренне признателен нашим техническим редакторам Карен Кент Фредерик и Дэвиду Хэйнбачу за исправление тех ошибок, которые вкрались в наш материал. Вы часто работали допоздна и даже на борту самолета. Спасибо Кэти Пендергаст за терпение и умение организовать работу в одни из самых напряженных месяцев моей жизни. Огромная признательность Линде Бамп за то, как она заставляла нас придерживаться графика работ!

Хочу воспользоваться возможностью и выразить свою благодарность Алану и Марше Поллер за дружбу, поддержку, одобрение и советы.

Кэти и Хантер, еще раз спасибо за любовь и помощь, которую вы мне оказали. Отдельное спасибо Кэти за то, что она бросила свою работу, чтобы я смог выдерживать необходимый темп работы. Я люблю тебя.

“Если же у кого из вас недостает мудрости, да просит у Бога, дающего всем просто и без упреков, — и дастся ему”. Иакова 1,5.

За все свои знания и навыки я благодарю Господа нашего, Иисуса Христа, за что ему, а не мне, и следует воздавать честь и славу.

Надеюсь, что эта книга понравится и будет полезной всем читателям!

Джуди Новак. Хочу от всей души поблагодарить Стивена Норткатa за его неутомимость при обучении людей всего мира делу безопасности компьютерных систем и за то, что он постарался привлечь меня к этой благородной работе. Он полностью изменил мою жизнь, а полученные в результате нашего совместного труда возможности и вознаграждения превзошли все мои ожидания. Словами трудно выразить мою признательность, поверьте, что она от всего сердца.

Мне также хочется сказать огромное спасибо удивительно мудрым техническим редакторам Дэвиду Хэйнбачу и Карен Кент Фредерик за их кропотливый и внимательный труд при поиске ошибок. Благословляю этих людей, которые ук-

репили мою уверенность в собственных силах! Кроме того, хочу высказать особою благодарность Полу Ритчи (Paul Ritchey), отредактировавшему главы, посвященные анализатору Snort. Его работа была быстрой и четкой.

И, наконец, я благодарю всю мою семью — Боба и Джесси. Они старались дать мне как можно больше свободного времени для работы над книгой и дипломатично отвлекали меня, когда видели, что я переутомлена. Ведь так рискованно слишком долго оставаться в одиночестве!