Предисловие

Программное обеспечение (ПО) с открытыми исходными текстами (далее для краткости — открытое ПО. Прим. ред.) составляет неотъемлемую часть Интернет, так что можно смело утверждать, что Интернет в своем нынешнем виде не существовал бы без него. Интернет не развивался бы столь быстро и динамично без таких программ с открытыми исходными текстами, как BIND, которая управляет доменной системой имен, как Sendmail, которая обеспечивает работу большинства серверов электронной почты, как INN, работающая на многих серверах телеконференций, как Major Domo, которая обслуживает многие тысячи списков почтовой рассылки в Интернет и, конечно, без популярного Web-сервера Apache. Несомненно, Интернет обходится много дешевле благодаря открытому ПО. Это — заслуга Фонда свободного программного обеспечения, BSD UNIX, Linux и Линуса Торвальдса, а также тысяч безымянных программистов, вложивших свои труд и душу в программы, на которых сегодня держится Интернет.

Хотя программы с открытыми исходными текстами охватывают почти все области программного обеспечения — от полнофункциональных операционных систем и игр до текстовых процессоров и систем управления базами данных, — эта книга ориентирована в первую очередь на инструментарий информационной безопасности. Существуют программные реализации всех возможных сервисов безопасности. Имеются межсетевые экраны с открытыми исходными текстами, системы обнаружения вторжений, сканеры уязвимостей, судебный инструментарий и самые современные программы для таких областей, как беспроводные коммуникации. Обычно в каждой категории есть множество вариантов выбора среди зрелых, устоявшихся программ, которые по меньшей мере не уступают коммерческим продуктам. Я попытался выбрать лучшие в каждой из основных областей информационной безопасности (по моему мнению, разумеется!). Они представлены детальным образом, с разъяснением не только того, как их установить и запустить, но и как использовать в повседневной деятельности, чтобы повысить безопасность сети. С помощью открытого ПО, описанного в этой книге, вы сможете защитить свою организацию от внутренних и внешних угроз безопасности с минимальными расходами и максимальной выгодой как для организации, так и для вас лично.

На мой взгляд, сочетание концепций информационной безопасности и открытого ПО представляет собой одно из самых мощных средств для защиты инфраструктуры вашей организации и, по индукции, всего Интернет. Общепризнано, что крупномасштабные вирусные инфекции и черви могут распространяться в силу недостаточной защищенности многих систем. Убежден, что путем обучения системных администраторов и предоставления им инструментария для выполнения их работы можно сделать Интернет более безопасным, защищая сеть за сетью.

На кого рассчитана эта книга

Предполагается, что читательская аудитория этой книги будет состоять из сетевых и/или системных администраторов, чьи должностные обязанности не ограничены исключительно обеспечением безопасности, а стаж работы насчитывает по крайней мере несколько лет. Это не значит, что гуру от безопасности не найдут в книге ничего для себя полезного; возможно, некоторые из обсуждаемых областей и средств будут им внове. Аналогично, любой новичок в области информационных технологий многое узнает, устанавливая и применяя эти средства. Рассмотренные концепции и используемые методики предполагают минимальный уровень компьютерной и сетевой подготовки.

Существует также большая группа читателей, которая зачастую не учитывается многими авторами, пишущими об открытом ПО. Это системные администраторы Windows. Элита информационной безопасности часто пренебрежительно относится к администраторам «только Windows», поэтому не так уж много написано о качественном программном обеспечении с открытыми исходными текстами для Windows. Однако факт остается фактом: серверы Windows составляют львиную долю инфраструктуры Интернет, и игнорирование этого обстоятельства оказывает плохую услугу всему сообществу информационной безопасности. Хотя книга в целом в большей степени ориентирована на Linux/UNIX (так как большинство программ с открытыми исходными текстами работают только в Linux/UNIX), я попытался включить в каждую главу описание защитных средств на платформе Windows. Я поместил также полезные советы и подробные объяснения для тех, кто никогда не работал в UNIX системах.

Содержание книги

В книге рассмотрено большинство наиболее важных областей информационной безопасности и предназначенные для них средства с открытыми исходными текстами. Главы выстраиваются вокруг основных аспектов информационной безопасности, освещая ключевые концепции. Инструментарий, помещенный на компакт-диске, позволяет организовать нечто вроде лабораторных работ, в которых каждый может принять участие. Все, что требуется помимо диска, — это ПК.

Книга содержит также краткое введение в базовую сетевую терминологию и концепции. Я обнаружил, что хотя многие технические специалисты хорошо освоили конкретные платформы и приложения, им зачастую не хватает понимания сетевых протоколов и их взаимодействия при передаче данных из точки А в точку В. Понимание этих концепций жизненно необходимо для защиты сети и правильного применения описыва-

емых средств. Акцент книги на сетевую сторону безопасности может показаться чрезмерным, однако большинство угроз в настоящее время приходит оттуда, так что сеть — лучшая отправная точка.

Рассмотрению каждого средства безопасности предшествует его обзор, контактная информация и перечень различных ресурсов для поддержки и получения дополнительной информации. Хотя рассмотрение защитных средств ведется с высоким уровнем детализации, многие из них заслуживают (и уже заслужили) написания отдельной книги. Указанные ресурсы откроют перед вами возможность дальнейших исследований.

Полезные, порой шутливые советы, маленькие хитрости, замечания используются в книге, чтобы акцентировать, подчеркнуть наиболее важные моменты. Они даются от имени Флэми Теха — нашего талисмана, порой склонного к назидательности, но всегда готового помочь и проинформировать новичков, а также обратить внимание технически подготовленных читателей на разделы, где мы на самом деле вносим небольшие изменения в тексты программ. Он напоминает, возможно, виденных вами обитателей мира открытых исходных текстов. Исследуя этот мир, вы встретите множество самых разных, блестящих, порой эксцентричных личностей (надо быть, мягко говоря, немного со сдвигом, чтобы на общественных началах тратить на все эти программы столько своего времени, сколько тратят некоторые из нас). Знание принятого этикета и правил поведения позволит вам достичь большего, не наступая лишний раз на грабли. Ну, а если серьезно, то необходимо отметить, что многие из описанных в книге средств при ненадлежащем использовании могут быть деструктивны или вредоносны. Можно неумышленно нарушить закон, если применять их без предупреждения или небрежно (например, случайно просканировать в небезопасном режиме IP-адреса, которые вам не принадлежат). Если подобное возможно, то Флэми всегда тут как тут, чтобы предостеречь вас.

Индекс защитных средств с открытыми исходными текстами

Сразу за предисловием помещен список всех подобных средств с номерами страниц, где они рассматриваются. С помощью индекса вы, при желании, сможете пропустить весь сопровождающий материал и перейти непосредственно к установке защитного инструментария.

Глава 1: Информационная безопасность и программное обеспечение с открытыми исходными текстами

Эта глава содержит введение в мир информационной безопасности и программного обеспечения с открытыми исходными текстами. Обсуждается текущее состояние компьютерной безопасности вместе с краткой историей движения за открытость исходных текстов.

Глава 2: Средства уровня операционной системы

В этой главе обосновывается важность максимально безопасной настройки вашей системы защитных средств. Рассматривается средство повышения безопасности Linux систем, а также вопросы укрепления защиты систем Windows. Описано также несколько инструментов уровня операционной системы. Эти базовые инструменты — что-то вроде отвертки для администратора безопасности; они будут использоваться снова и снова как по ходу изложения, так и в процессе вашей работы.

Глава 3: Межсетевые экраны

Здесь сначала описаны основы коммуникаций по протоколам TCP/IP и принципы работы межсетевых экранов, а затем рассмотрены вопросы установки и настройки вашего собственного межсетевого экрана с открытыми исходными текстами.

Глава 4: Сканеры портов

В этой главе стек TCP/IP и, в особенности, прикладной уровень и порты рассматриваются более детально. Описывается установка и применение сканера портов, используемого в следующей главе.

Глава 5: Сканеры уязвимостей

В данной главе подробно описан инструмент, который использует некоторые более ранние методы, такие как сканирование портов, но делает следующий шаг и на самом деле проверяет защищенность выявленных открытых портов. Этот защитный инструмент, как швейцарский армейский нож, вскроет всю сеть, просканирует ее и создаст подробный отчет обо всех обнаруженных пробелах в защите.

Глава 6: Сетевые анализаторы

В этой главе основное внимание уделено нижним уровням эталонной модели ВОС и тому, как извлекать из проводов необработанные данные. Многие описываемые далее средства используют эти базовые методы. В главе показано, как можно применять анализатор для диагностики всех аспектов работы сети, в дополнение к отслеживанию проблем безопасности.

Глава 7: Системы обнаружения вторжений

Средство, основанное на описанных в предыдущей главе методах сетевого анализа, использовано для создания сетевой системы обнаружения вторжений. Обсуждаются также установка, сопровождение и оптимальное применение.

Глава 8: Средства анализа и управления

В данной главе изучаются средства отслеживания данных системы безопасности и их эффективного протоколирования для последующего просмотра. Рассматриваются также инструменты, помогающие анализировать данные безопасности и преобразовывать их в более удобный формат.

Глава 9: Криптографические средства

Пересылка данных ограниченного доступа через Интернет в наше время представляет собой большую проблему, решение которой все в большей степени становится обязательным требованием. Описываемые средства помогут зашифровать ваши сообщения и файлы с помощью сильной криптографии, а также организовать виртуальные защищенные сети на основе спецификаций IPsec.

Глава 10: Средства для беспроводных сетей

Беспроводные сети становятся все более популярными, и инструментарий, представленный в этой главе, поможет убедиться, что все беспроводные сети вашей организации защищены, а неизвестные вам беспроводные сети отсутствуют.

Глава 11: Судебные средства

Средства, обсуждаемые в данной главе, помогут расследовать имевшие место вторжения и должным образом собрать цифровые улики.

Глава 12: Еще о программном обеспечении с открытыми исходными текстами

В завершение, в этой главе предоставлены ресурсы для получения дополнительной информации о программном обеспечении с открытыми исходными текстами. Перечислены ключевые Web-сайты, списки почтовой рассылки и другие Интернет-ресурсы. Указан ряд способов приобщения к движению за открытость исходных текстов, если вы того желаете.

Приложение A: Публичные лицензии для ПО с открытыми исходными текстами

Приложение A содержит две основные лицензии для ПО с открытыми исходными текстами: лицензии на программное обеспечение GPL и BSD.

Приложение B: Основные команды Linux/UNIX

В приложении B для тех, кто не имеет опыта работы с системами Linux/UNIX, кратко описаны основные команды навигации и обработки файлов.

Приложение C: Общеизвестные номера портов TCP/IP

Приложение содержит список всех общеизвестных номеров портов согласно списку IANA. Отметим, что этот раздел не был задуман как исчерпывающий источник информации, поскольку данный список является объектом постоянных изменений. Самую свежую информацию можно найти на Web-сайте IANA.

Приложение D: Общая форма разрешения и отказа от претензий

Содержит шаблон для получения разрешения на сканирование сторонней сети (то есть сети, которая не является вашей собственной). Это — только пример, не являющийся юридическим документом.

Приложение E: Встраиваемые модули Nessus

Содержит частичный список встраиваемых модулей для сканера уязвимостей Nessus, рассмотренного в главе 5. Этот список, разумеется, не самый свежий, поскольку модули обновляются ежедневно. Полный список модулей можно найти на Web-сайте Nessus.

Содержимое и организация компакт-диска

Компакт-диск, приложенный к этой книге*, содержит большинство рассмотренных средств безопасности с открытыми исходными текстами. Диск организован как дерево каталогов, помеченных названиями средств. Если версии для Windows и Linux содержат несовпадающие файлы, они располагаются в отдельных каталогах. Каталог «Misc» содержит различные драйверы и документацию, такую как спецификации RFC, вообще говоря, полезные как дополнительный материал.

Использование инструментария

Везде, где возможно, описанные в книге средства представлены в формате менеджера пакетов RedHat (RPM). Разумеется, чтобы использовать RPM, не обязательно работать в RedHat Linux. Этот формат был первоначально разработан в RedHat, но теперь он поддерживается большинством версий Linux. Менеджер пакетов RedHat автоматизирует процесс установки программ, гарантирует наличие всех вспомогательных программ и т.д. Это похоже на процесс установки в Windows, в рамках графического диалога. Использование RPM почти всегда предпочтительнее установки вручную. Если требуется задать специфические параметры установки, или если файл RPM отсутствует на вашем дистрибутиве, в книге

* Речь идет об английском издании.

приводится описание установки программ вручную. Если файл RPM доступен, загрузите его из Интернет или скопируйте с компакт-диска и щелкните на нем мышью. Ваша версия RPM позаботится обо всем остальном.

Если вы используете другой вариант ОС UNIX (BSD, Solaris, HP/UX и т.д.), то они, скорее всего, будут работать с инструментарием из этой книги, но инструкции по установке могут быть другими. Вы можете запускать большинство описанных в книге средств на альтернативных версиях UNIX или Linux, хотя, оставаясь в рамках Linux, вы, несомненно, повышаете вероятность совместимости с инструментами, помещенными на компакт-диск. Если вам пришлось загрузить другую версию программы, то некоторые из обсуждаемых свойств могут не поддерживаться. Однако, если вы приверженец ОС Solaris или убеждены, что только BSD идет верной дорогой, — флаг в руки! Используйте вашу любимую ОС в качестве платформы безопасности. Помните только, что инструкции в книге составлены в расчете на определенную реализацию, и, чтобы заставить защитный инструментарий работать, могут потребоваться дополнительные усилия. Поддерживаемые платформы перечислены в начале описания каждого средства.

Эталонная установка

Большинство средств, описанных в этой книге, были проверены и рассмотрены на следующих платформах:

- Mandrake Linux 9.1 на ПК серии HPVectra и ПК-блокноте Compaq Presario.
- Windows XP Pro и Windows 2000 Pro на ПК серии Compaq Prestignia и ПК-блокноте Compaq Armada.

Исходные данные или переменные

В программных и командных примерах курсивом выделяются элементы, задаваемые пользователем. Набранные курсивом слова следует заменить переменными или значениями, специфичными для вашей установки. Команды уровня операционной системы выглядят так:

```
ssh -l входное_имя имя_хоста
```

В силу ограниченности размеров страниц, продолжение слишком длинных строк кода набрано с небольшим отступом.

Я надеюсь, что, читая эту книгу, вы получите удовольствие и новые знания. Существует много, очень много других средств, включить которые в книгу не было возможности из-за ограниченности ее объема, и я заранее

приношу извинения, если я пропустил ваше любимое средство. У меня хватило места только для описания моих излюбленных инструментов, как я надеюсь, лучших в своей категории. Несомненно, многие не согласятся с моим выбором. Вы можете написать мне об этом по адресу tony@howlett.org, и, возможно, в будущих изданиях появятся новые средства.

Благодарности

Эта книга не увидела бы свет без неутомимого труда программистов по всему миру, создающих замечательное программное обеспечение с открытыми исходными текстами. Я мог бы назвать некоторых из них, но, несомненно, слишком многие окажутся пропущены. Спасибо всем вам за превосходное программное обеспечение! Я хотел бы поблагодарить моего делового партнера Глена Крамера (Glenn Kramer) за помощь в правке книги (а также за заботы о делах, пока я работал, пытаясь уложиться в сроки), и моих коллег по проекту Nessus Command Center (NCC): Брайана Кредейра (Brian Credeur), Лорел Хэткок (Lorell Hathcock) и Мэтта Сиска (Matt Sisk). И, наконец, моя любовь и благодарность моей милой жене Синтии и дочерям Карине и Алане, которые пожертвовали бесчисленными часами, проведенными без мужа и отца, чтобы появилась эта книга.

Об авторе

Тони Хаулет — президент компании Network Security Services, поставщика услуг на основе приложений компьютерной безопасности, полностью построенных на программном обеспечении с открытыми исходными текстами. Сертифицированный специалист по безопасности информационных систем (CISSP) и GIAC аудитор систем и сетей (GNSA), он имеет четырнадцатилетний опыт работы, включая обслуживание крупнейших региональных поставщиков Интернет-услуг и коммерческих операторов местной связи, а также построение общенациональных сетей ATM/DSL. М-р Хаулет часто выступает с докладами по вопросам компьютерной безопасности по технологической тематике, пишет для журналов SysAdmin, Computer Currents, Windows Web Solutions, Security Administrator и других изданий.

www.phptr.com/perens/

Индекс средств с открытыми исходными текстами

Название средства	Есть на компакт-диске?	Linux/ UNIX?	Windows?	Номер страницы
ACID	да	да	нет	315
AirSnort	да	да	нет	427
Autopsy Forensic Browser	да	да	нет	456
Bastille Linux	да	да	нет	64
dd	да	да	нет	453
Dig	нет	да	нет	73
Ethereal	да	да	да	242
Finger	нет	да	нет	75
Forensic Toolkit	да	нет	да	463
Fport	нет	нет	да	444
FreeS/WAN	да	да	нет	383
GnuPG	да	да	нет	370
Iptables	да	да	нет	120
John the Ripper	да	да	да	391
Kismet Wireless	да	да	нет	420
lsof	да	да	нет	447
NCC	да	да	нет	339
Nessus	да	да	нет	184
NessusWX	да	нет	да	204
NetStumbler	да	нет	да	405
Nlog	да	да	нет	157

Название средства	Есть на компакт-диске?	Linux/ UNIX?	Windows?	Номер страницы
Nmap	да	да	да	139
NPI	да	да	нет	328
OpenSSH (клиент)	да	да	нет	380
OpenSSH (сервер)	да	да	нет	377
PGP	нет	да	да	361
Ping	нет	да	да	361
PuTTY	да	нет	да	87
Sam Spade	да	нет	да	83
Sleuth Kit	да	да	нет	456
SmoothWall	да	нет	нет	118
Snort	да	да	нет	263
Snort for Windows	да	нет	да	284
Snort Webmin	да	да	нет	280
StumbVerter	да	нет	да	413
Swatch	да	да	нет	301
Tcpdump	да	да	нет	225
Traceroute	нет	да	да	68
Tripwire	да	да	нет	291
Turtle Firewall	да	да	нет	111
Whois	нет	да	да	71
Windump	да	нет	да	239

Глава 1. Информационная безопасность и программное обеспечение с открытыми исходными текстами

Когда Том Пауэрс устраивался на работу в качестве системного администратора в энергетическую компанию среднего размера, он знал, что критическим фактором были его навыки в области компьютерной безопасности. За последний год компания несколько раз подвергалась атакам хакеров, а на ее домашнюю страницу помещали непристойные изображения. Руководство хотело, чтобы, помимо обеспечения повседневной работы компьютерной сети, он сделал информацию компании более защищенной от цифровых атак.

После первого же дня работы он понял, что перед ним стоит сложная проблема. В компании отсутствовала даже самая элементарная система безопасности. Соединение с Интернет, защищенное только обычным маршрутизатором поставщика Интернет-услуг, было широко открыто миру. Общедоступные серверы плохо поддерживались и выглядели так, будто к ним не прикасались с момента установки. А бюджет для исправления ситуации был практически нулевым.

Однако в течение четырех месяцев Том обеспечил устойчивость сети, остановил все атаки, обезопасил точки общего доступа и очистил внутреннюю сеть, а также добавил сервисы, которых раньше не было. Как он смог все это сделать с такими ограниченными ресурсами? Он знал базовые принципы и концепции информационной безопасности (ИБ) и нашел подходящее программное обеспечение (ПО) для выполнения работы. Он разработал описанный далее план усовершенствования системы безопасности компании и методично выполнил его с помощью подходящих защитных инструментов.

Защита периметра

Прежде всего, Том создал несколько базовых средств для защиты своей сети от внешнего мира, чтобы затем спокойно заняться безопасностью серверов и внутренней части сети. Он настроил межсетевой экран для соединений с Интернет, используя программу Turtle Firewall (рассмотренную в главе 3). С помощью этой программы и старого сервера, который больше ни для чего не использовался, он сконфигурировал машину так, чтобы разрешить соединения с внешним миром только изнутри сети; все входящие соединения, не запрошенные изнутри, блокировались. Правда, он сделал несколько исключений для общедоступных серверов.

Затыкание дыр

Том знал, что ему необходимо проверить свою сеть на наличие дыр в системе безопасности и определить, где проникают злоумышленники. Хотя теперь межсетевой экран защищал внутренние рабочие станции от случайных вторжений, общедоступные серверы, такие как Web-серверы и серверы электронной почты, все еще были уязвимы. Межсетевой экран также стал теперь потенциальной целью нападений, поэтому требовался какой-то способ обеспечения его защиты. Том установил на этом сервере программу Bastille Linux, чтобы проверить, что он сконфигурирован безопасным образом (глава 2). Затем он выполнил программу Nmap, как извне, так и изнутри сети (глава 4). Она сообщила, какие прикладные порты были видимы извне по всем общедоступным IP-адресам. Внутреннее сканирование позволило узнать, имеются ли какие-то необычные или ненужные службы, выполняющиеся на внутренних машинах.

Затем он воспользовался программой Nessus для повторного сканирования сети извне и изнутри (глава 5). Это программа «копает» значительно глубже, чем Nmap, она проверяет открытые порты для большого числа уязвимостей и позволяет выявлять неправильно сконфигурированные машины внутри сети. Программа Nessus создала отчеты, которые показали, где в системе безопасности на общедоступных серверах имеются слабые места, и предоставила подробные инструкции по их устранению. Он использовал эти отчеты для разрешения проблем, а затем еще раз выполнил программу Nessus, чтобы убедиться, что уязвимости ликвидированы.

Создание системы раннего предупреждения

Том ликвидировал все известные прорехи, но он также хотел знать, нет ли какой-то нетипичной активности в сети или на общедоступных серверах. Он воспользовался сетевым анализатором Ethereal для получения контрольных данных о различных типах активности в сети (глава 6). Он также настроил на сервере сетевую систему обнаружения вторжений, используя программный пакет Snort (глава 7). Эта программа круглосуточно следила за сетью, выявляя подозрительную активность, которую Том определил специальным образом. Программа извещала его о новых атаках и нетипичном поведении пользователей внутри сети.

Создание системы управления данными безопасности

Вначале Том был перегружен всевозможными данными этих систем. Однако он настроил базу данных и использовал несколько программ для

управления выводом программ системы безопасности. Одна из них, ACID (Analysis Console for Intrusion Database — Консоль анализа базы данных вторжений) помогла рассортировать и интерпретировать данные сетевой системы обнаружения вторжений (глава 8). Программа «Командный центр Nessus» помещала результаты сканирования в базу данных и создавала на их основе отчеты (глава 8). Том использовал также программу Swatch, которая отслеживала по файлам журналов различные аномалии (глава 8). Эти программы позволили ему за полчаса просматривать отчеты на Web-странице, в которой были объединены все его задания по мониторингу безопасности. Для Тома, который воплощал в одном лице техническую поддержку, программиста и, естественно, администратора системы безопасности, это было значительной экономией времени.

Реализация защищенного беспроводного решения

Еще одним заданием для Тома было построение для компании беспроводной сети. Том знал, что технология беспроводных сетей изобилует проблемами безопасности, поэтому он использовал две программы, NetStumbler и WEPCrack, для контроля защищенности и развернул беспроводную сеть с требуемыми параметрами безопасности (глава 10).

Защита важных файлов и коммуникаций

Одной из проблем, беспокоивших руководство компании, было использование электронной почты для пересылки потенциально уязвимых документов. Том знал, что пересылка информации через обычную электронную почту аналогична отправке ее почтовой открыткой. Любой из посредников, обрабатывающих сообщение, мог его прочитать. Том заменил эту практику системой, использующей программное средство PGP, которое позволяет посылать файлы с конфиденциальной или уязвимой информацией в зашифрованном виде и защищать важные внутренние файлы от любопытных глаз неавторизованных пользователей (глава 9).

Расследование вторжений

Наконец, когда сеть была защищена настолько, насколько это возможно, Том проверил каждый сервер на наличие каких-либо следов прошлых вторжений, чтобы убедиться, что не было оставлено ничего вредоносного, и, если было, попытаться выяснить, кто это сделал. Используя утилиты системного уровня, такие как wtmp и lsof, и программу The Coroner's Toolkit, Том смог идентифицировать возможных нарушителей,

ответственных за прошлые вторжения (глава 11). Хотя собранные доказательства были недостаточно надежными, чтобы возбудить уголовное преследование, он заблокировал IP-адреса злоумышленников в новом межсетевом экране, чтобы те не смогли помешать работе. Он использовал также эту информацию, чтобы пожаловаться на злоупотребления поставщику Интернет-услуг.

За несколько первых месяцев работы Том произвел впечатляющие преобразования. Что самое удивительное, он смог сделать все это при почти полном отсутствии бюджета. Как ему это удалось? Его подготовка в области информационной безопасности помогла разработать план действий и реализовать его. Он смог воспользоваться этими знаниями для установки недорогих, но эффективных защитных решений, используя ПО с открытыми исходными текстами для создания всех своих систем. С помощью этих пакетов Том смог превратить плохо защищенную сеть в сеть, безопасность которой могла бы соперничать со значительно более дорогими аналогами. И он сделал это без дополнительного персонала и с минимальным количеством средств.

Вы также можете использовать открытое ПО для защиты своей организации. Эта книга познакомит вас с десятками программных пакетов, которые помогут это сделать, а также обучит правильным политикам и процедурам, обеспечивающим информационную безопасность. Как неоднократно подчеркивается в этой книге, программно-технические средства – прекрасное подспорье, но это лишь половина дела. Хорошо организованная программа информационной безопасности состоит также из политик и процедур, позволяющих в максимальной степени использовать возможности программного обеспечения. Поэтому, прежде чем переходить к установке ПО, давайте обсудим основы ИБ и происхождение ПО с открытыми исходными текстами.

Практика информационной безопасности

Наука информационной безопасности включает множество различных аспектов, однако имеются три области, которые являются основанием ИБ: конфиденциальность, целостность и доступность. Для их обозначения часто используется акроним КЦД. Эта триада представляет цели информационной безопасности (см. рис. 1.1). Каждая из них требует различных инструментов и методов и защищает определенный элемент или тип информации.

Конфиденциальность

Элемент конфиденциальности информационной безопасности защищает данные от просмотра неавторизованными лицами. Это мо-

Рис. 1.1. Принципы информационной безопасности

жет быть информация, которая является внутренней для вашей организации, такая как инженерные планы, исходные тексты программ, секретные рецепты, финансовая информация или маркетинговые планы. Это может быть информация о заказчиках или сверхсекретные правительственные данные. Конфиденциальность относится также к необходимости сокрытия информации от любопытных глаз внутри организации. Разумеется, нежелательно, чтобы все служащие могли читать электронную почту высшего руководства или просматривать платежные ведомости.

Существует много способов защиты приватных данных от просмотра. Один из них состоит в запрещении доступа к данным. Но иногда это невозможно, как в случае данных, передаваемых через Интернет. В подобных случаях необходимо использовать другие средства, такие как шифрование, чтобы скрыть и утаить данные во время их передачи.

Целостность

Элемент целостности помогает гарантировать, что неавторизованные лица не могут модифицировать данные. Он означает также, что авторизованные лица не вносят изменений без соответствующего разрешения. Следует различать два момента. Если кассир банка втайне дебетует чей-то счет и кредитует другой, то это проблема целостности. Он авторизован делать изменения счетов, но только после получения указания на внесение изменений. Целостность данных означает также, что данные соответствующим образом синхронизированы во всех системах.

[. . .]