Михаил Фленов

Linux
ГЛАЗАМИ
ХАКЕРА
3-е издание

Санкт-Петербург

«БХВ-Петербург»

2010

УДК 681.3.06
ББК 32.973.26-018.2
Ф69

Фленов М. Е.

Ф69 Linux глазами хакера: 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2010. — 480 с.: ил. + CD-ROM

ISBN 978-5-9775-0547-5

Рассмотрены вопросы настройки ОС Linux на максимальную производительность и безопасность. Описаны базовое администрирование и управление доступом, настройка Firewall, файлообменный сервер, WEB-, FTP- и Proxy-серверы, программы для доставки электронной почты, службы DNS, а также политика мониторинга системы и архивирование данных. Приведены потенциальные уязвимости, даны рекомендации по предотвращению возможных атак и показано как действовать при атаке или взломе системы, чтобы максимально быстро восстановить ее работоспособность и предотвратить потерю данных. В третьем издании материал переработан и дополнен новой информацией в соответсвии с современными реалиями. На компакт-диске находятся дополнительная документация и программы в исходных кодах.

Для пользователей, администраторов и специалистов по безопасности

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Редактор	*Юрий Якубович*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Наталия Першакова*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.04.10.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 38,7.
Тираж 2500 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.005770.05.09 от 26.05.2009 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0547-5

Оглавление

Предисловие

Эта книга посвящена рассмотрению одной из самых популярных операционных систем (ОС), устанавливаемых на серверы, — ОС Linux. Для домашнего использования эта система пока еще не получила такой же популярности, как среди профессиональных администраторов, но в последнее время наметились предпосылки для захвата и этого рынка. ОС Linux становится все проще, удобнее и красивее. Единственное, чего не хватает этой системе (на мой взгляд) — такого же количества игр, как для платформы Windows.

Установка ОС Linux становится проще, а графический интерфейс и удобство работы в некоторых случаях не уступает самой распространенной в среде малого бизнеса ОС Windows. Есть еще некоторые шероховатости, которые не позволяют ОС Linux получить широкое распространение среди домашних пользователей, но мы только рады этому. Конкуренция заставляет компании развиваться и улучшать свои продукты, и это развитие заметно даже без бинокля.

Эта книга будет полезна администраторам Linux и тем пользователям, которые хотят познакомиться с этой системой поближе. Рассматриваемые вопросы настройки и безопасности пригодятся специалистам по безопасности сетей, использующих различные ОС, потому что значительная часть приводимой информации не привязана к определенной системе, а теория защиты различных систем похожа.

Так как некоторые примеры из этой книги могут быть использованы не только для обороны, но и для нападения, я хотел бы предостеречь юных взломщиков. Здоровое любопытство — это хорошо, но помните, что правоохранительные органы не спят и всегда добиваются своего. Если один раз вам повезло со взломом, и никто не обратил на это внимания, то в следующий раз вы можете оказаться в руках правосудия.

Часть книги написана с точки зрения хакера и демонстрирует, как можно проникнуть в систему. В надежде на то, что эту информацию не будут

использовать для взлома серверов, я старался сделать упор именно на защиту и некоторые вещи оставлял за пределами изложения или просто не договаривал, чтобы не появилось соблазна воспользоваться методами хакеров и нарушить закон. Но, несмотря на то, что книга может послужить отправной точкой для хакера, я надеюсь, что этого не произойдет. Помните о законности ваших действий.

Я интересуюсь взломом и постоянно изучаю новые методы, но только потому, что я хочу строить безопасные системы, и безопасность меня интересует намного больше. Любой объект может быть рассмотрен с разных точек зрения. Простой пример из жизни: нож, являясь столовым прибором, при определенных обстоятельствах становится орудием убийства или средством самообороны. Точно так же и методы хакеров, которые будут рассматриваться в этой книге, могут быть восприняты как советы для повседневного ухода за ОС и способы защиты от проникновения или же как средства взлома системы. Я надеюсь, что вы не будете использовать полученные знания в разрушительных целях. Это вас не украсит и не добавит ума. Зачем вам нужна "черная" популярность взломщика? Не лучше ли посвятить себя более полезным и добрым вещам?

Несмотря на явное стремление Linux поселиться в домашних компьютерах, настройка этой ОС пока еще слишком сложна. Для того чтобы правильно это сделать, нужно знать множество параметров, которые большинству пользователей не нужны. Если же просто закрыть глаза и оставить все значения по умолчанию, то об истинной безопасности Linux не может быть и речи. Ни одна ОС не может работать надежно и с максимальной защитой при настройках по умолчанию. Дело в том, что производитель не может заранее знать, что именно нам понадобится, и делает все возможное, чтобы программа работала на любой системе, а для этого приходится включать много дополнительных возможностей, что делает систему избыточной. В последнее время разработчики дистрибутивов и других серверных программ стали максимально урезать установки по умолчанию, то есть разрешать только базовые возможности, а все сетевые сервисы, которые могут позволить хакеру проникнуть на компьютер, отключать. При этом чаще всего производитель предоставляет нам простое и удобное средство для быстрого включения и конфигурирования нужного сервиса.

Так уж повелось, что администраторы Linux должны иметь больше опыта и знаний, чем специалисты Windows, и это связано как раз со сложностями настройки. В этой книге я постарался максимально доступно рассказать вам про ОС Linux.

Почему книга называется "Linux глазами хакера", и что это за глаза? Этот вопрос интересует многих моих читателей. Когда мы берем в руки какую-

нибудь вещь, то надеемся, что ее внешний вид соответствует внутреннему содержанию. В данном случае вопрос в том, какая информация будет отвечать этому названию? Для ответа на этот вопрос необходимо четко понимать, кто такой хакер, и что он видит в операционной системе.

Когда меня спрашивают, что я подразумеваю под словом "хакер", я привожу простейший пример: если как администратор вы установили и заставили работать ОС, и вам удалось настроить ее на максимальную производительность и безопасность, то вы — хакер. Умения хакера позволяют создавать что-либо, превосходящее свои аналоги (то есть более быстрое, удобное и безопасное). Именно такой является сама ОС Linux, созданная хакерами со всего мира.

Данная книга рассматривает ОС, начиная с самых основ и заканчивая сложными манипуляциями с системой. Весь излагаемый материал представлен простым и доступным каждому языком. Благодаря этому вам не понадобится дополнительная литература для изучения ОС Linux. Всю информацию можно будет получить из одних рук. Для более глубокого изучения вопроса вам может потребоваться только хорошее знание английского языка, которое позволяет читать документацию или файлы HOWTO, поставляющиеся с системой Linux.

Главное отличие этой книги от многих учебников по ОС Linux в том, что о безопасности и производительности мы будем говорить не в отдельных заключительных главах, что является большой ошибкой, а все время. Когда человек уже приобрел навыки неэффективной работы с системой, то переучиваться сложно. Именно поэтому мы будем разбирать последовательно (от азов до сложных вопросов) все аспекты каждой рассматриваемой темы, аккуратно раскладывая полученные знания "по полочкам".

Описание утилит для администрирования Linux всегда можно найти в Интернете или в документации на ОС, а вот информацию по эффективному их использованию найти сложнее, а все имеющиеся сведения являются фрагментарными и их тяжело сводить в одно целое. А ведь безопасность не любит обрывочных данных. Если упустить хоть одну мелочь, компьютер оказывается уязвимым для взлома.

В качестве дополнительной информации по безопасности компьютера и сетей советую прочитать мою книгу "Компьютер глазами хакера" [3], в которой приводится достаточно много общих сведений по этим вопросам. Здесь же мы больший упор делаем на определенную ОС — Linux. Несмотря на то, что книга [3] направлена в большей степени на поддержание безопасности ОС Windows, многие рассматриваемые в ней проблемы могут вам пригодиться и при построении безопасного Linux-сервера. Точно так же книга "Linux глазами хакера" будет полезна и специалистам по безопасности Windows-систем.

В этой книге не рассматриваются вопросы, связанные с вирусами, потому что в настоящее время вирусная активность в ОС Linux минимальна, но это не значит, что опасности не существует. Угроза есть всегда, а защита от вирусов схожа с защитой от троянских программ, которых для Linux достаточно много. О вирусных атаках и возможностях их отражения можно также прочитать в книге "Компьютер глазами хакера" [3].

Итак, давайте знакомиться с Linux с точки зрения хакера. Я уверен, что вы посмотрите на нее совершенно другими глазами и найдете для себя много нового и интересного.

QualitySource

Мой взгляд на Linux может вам понравиться, а может и шокировать. Дело в том, что я не принадлежу к сторонникам или поклонникам Open Source, к которому относится Linux. Я являюсь сторонником движения QualitySource, то есть качественного кода. Мне все равно, какой это код — открытый или закрытый, главное, чтобы он был качественный. Если бы код ОС Windows был открытым, вы бы полезли его смотреть или изменять? Я бы нет, и большинство тоже.

Большинство из нас, когда устанавливает ОС или какую-то программу, хочет, чтобы она стабильно работала и выполняла положенные действия. Какая нам разница, открыт код или нет? Какая нам разница, на каком языке написана программа? Для меня эти вопросы не существенны. Если программа стоит того, чтобы я отдал за нее запрашиваемые деньги, если она достаточно качественна, — то я отдам эти деньги, независимо от того, открыт ли ее код и на каком языке ее написали.

ОС Linux и Windows, на мой взгляд, являются качественными проектами, и я использую их одновременно, но для разных задач. Устанавливать сложный, тяжеловесный и дорогой Windows Server ради банального файлового сервера — это глупость, поэтому здесь я использую Linux. Но для сложных баз данных я предпочитаю использовать великолепную связку MS Windows и MS SQL Server. Это мое личное предпочтение, которому не обязательно следовать. Вы можете выбрать в качестве базы данных связку Linux и MySQL.

Единственное, о чем я прошу вас, — не делайте ничего бездумно. Не стоит устанавливать софт только потому, что он относится к OpenSource, как и не стоит считать, что коммерческий софт заведомо лучше. Выбирайте своим умом, пробуйте, тестируйте и принимайте самостоятельное решение в зависимости от конкретной ситуации.

Программа не может быть лучше, надежнее или безопаснее других только потому, что у нее открыт код, это бред полнейший. Яркий пример — sendmail.

Бездарных программ с открытым кодом очень много, как и коммерческих, поэтому выбирайте за качество, а не за наличие или отсутствие исходных кодов, которые большинству пользователей просто не нужны.

Второе издание

Чем отличается второе издание этой книги? Я бы назвал эти книги разными, потому что в новом варианте намного больше информации. Я переписал абсолютно все и обновил весь текст в соответствии с современными реалиями.

В ходе этой работы были исправлены некоторые ошибки, присутствовавшие в предыдущем издании. Их было немного, но в Интернете по этому поводу очень красиво писали те, кто почему-то не любит меня и мои книги. Не знаю, почему, ведь я никому ничего плохого не сделал. Ошибки есть везде, даже в авторитетных американских изданиях. Просто там новые издания появляются каждый год, поэтому ошибки исправляются достаточно быстро.

Третье издание

В третьем издании я уже в основном обновлял информацию в соответствии с современными реалиями. Компьютерный мир изменяется очень быстро, за что я его и люблю, потому что приходится постоянно изучать что-то новое. Очень много новой информации попало на компакт-диск к этой книге в виде текстовых файлов.

Я хотел донести до читателя как можно больше информации, и при этом не делать книгу слишком толстой и дорогой. Единственный способ сделать это — максимально использовать компакт-диск. Наиболее интересная информация попала в книгу, чтобы ее было увлекательно читать. Наиболее нудные участки текста ушли на компакт-диск.

Благодарности

В каждой своей книге я стараюсь поблагодарить всех, кто помогал в ее создании и появлении на свет. Без этих людей просто ничего бы не получилось.

Первым делом я хотел бы поблагодарить издательство "БХВ-Петербург", с которым работаю уже несколько лет. Спасибо руководству издательства, редакторам и корректорам, которые работают со мной и помогают сделать книгу такой, какой я ее задумывал. Ведь писать приходится в тяжелых по срокам условиях, но иначе нельзя, так как информация устареет раньше, чем книга попадет на прилавок.

Не устану благодарить родителей, жену и детей за их терпение. После основной работы я прихожу домой и тружусь над очередной книгой. Таким образом, семья может видеть меня только за компьютером, а общаться со мной очень сложно, потому что все мысли устремляются далеко в виртуальную реальность.

Большая благодарность моим друзьям и знакомым, которые что-то подсказывали, помогали идеями и программами.

Так уж выходит, но в написании каждой книги участвуют и животные. Эта работа не стала исключением. Во время написания первого издания мой кот Чекист с 23:00 до 1:00 ночи гулял по квартире и кричал просто от скуки. Я не мог уснуть, а значит, больше времени уделял работе.

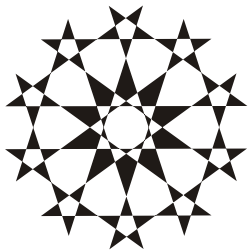
Хочется поблагодарить еще одного кота, который является ассистентом в пакете программ MS Office. Книгу я писал в MS Word, а ОС Linux работала в виртуальной машине, чтобы можно было делать снимки экрана. Во время написания первого издания, если на меня бросали ребенка, то кот-ассистент помогал занять моего годовалого сына, выступая в роли няни. Я сажал сына Кирилла рядом, и он спокойно играл с котом на экране монитора, а я мог продолжать работать над книгой. Правда, иногда приходилось спасать кота и монитор, когда сын начинал маленькой ручонкой неуклюже гладить полюбившееся животное.

А самая большая благодарность — вам, за то, что купили книгу, и моим постоянным читателям, с которыми я регулярно общаюсь на моем блоге **www.flenov.info**. Последние работы основываются на их вопросах и предложениях. Если у вас появятся какие-то проблемы, то милости прошу на сайт. Я постараюсь помочь по мере возможности, и жду любых комментариев по поводу этой книги. Ваши замечания помогут мне сделать ее лучше.

В последнее время в России перестают читать книги, качая из Интернета пиратские копии, нанося ущерб авторам и издательствам. Доход от книг падает, и многие хорошие авторы перестают писать, ибо хорошему специалисту просто найти хороший источник дохода без лишних мучений. От этого количество хороших книг уменьшается. Боюсь, эта тенденция сохранится. Если вам нравится книга, купите ее бумажный вариант, не портите глаза, читая с монитора. Здоровье важнее. Ну а я со своей стороны постарался наполнить книгу и прилагаемый компакт-диск максимальным количеством полезной информации. На компакте вы найдете множество дополнительных документов.

Если вы нашли какую-то ошибку в книге, просьба сообщить мне об этом через обратную связь на моем сайте **www.flenov.info**. Я также жду ваших мнений о книге и пожеланий о том, что вы хотите увидеть в будущем, если появится новое издание.

На этом завершаем вступительное слово и переходим к наиболее интересной и главной части книги — рассмотрению ОС Linux.



Глава 1

Прежде чем начать...

Однажды я показывал администратору ОС Windows, как устанавливать и работать с Linux. Сам процесс инсталляции ему понравился, потому что в последних версиях он достаточно прост. Но когда мы установили и решили настроить сервер Samba, последовала куча вопросов типа: "А зачем настраивать Samba?" Почему нельзя получить доступ автоматически?" Администраторы Windows-систем ленивы и привыкли, что ОС сама делает за них все, что нужно, и лишь когда их систему взламывают, начинают задавать вопросы: "А почему Microsoft не дала нам нужных инструментов, чтобы запретить определенные действия?"

Простота настройки сетевого окружения в Windows 9*x* и сложность настройки в Linux связана с безопасностью. В Windows версий 9*x* не было вообще никакой защиты и разграничений доступа, только банальный пароль. Начиная с Windows 2000 настройка усложнилась, потому что теперь автоматически устанавливаемого всеобщего доступа к компьютеру нет, и теперь обе системы находятся в одинаковых условиях. Теперь можно и нужно давать права доступа только к тем ресурсам, которые реально нужны пользователю.

Если смотреть на ОС Linux с точки зрения пользователя, то после установки системы ничего настраивать не надо. Можно сразу же приступать к работе с любыми офисными приложениями и пользовательскими утилитами. Но если речь идет о сетевых и серверных программах, то здесь уже требуются более сложные настройки, и ничего автоматически работать не должно. По умолчанию в системе должны быть запрещены практически все действия, которые могут привести к нежелательному результату или вторжению по сети. Для изменения ограничений нужно настраивать конфигурационные файлы, редактировать которые крайне неудобно, или использовать специализированные утилиты, большинство из которых имеют интерфейс командной строки.

Из-за этих неудобств мой знакомый администратор Windows-систем сказал: "Linux придумали администраторы, которым нечего делать на работе, для того, чтобы играться с конфигурационными файлами". Через неделю этот же человек настраивал сервис IIS (Internet Information Services, Информационные сервисы Интернета) на новом сервере с ОС Windows 2003. И ему пришлось делать схожие вещи, потому что эта служба по умолчанию не устанавливается с ОС, и прежде чем она начнет работать, ее нужно подключить и четко прописать, что должно использоваться, а что нет.

Корпорация Microsoft начинала делать ОС по принципу "лишь бы было удобно", поэтому достаточно было подключить требуемые компоненты. Но теперь Windows становится с каждым годом все сложнее и безопаснее, а большинство удобных функций, которые могут нарушить защиту, просто отключаются. При необходимости их приходится включать. Начиная с 2008 года эта тенденция приняла совершенно новый и интересный оборот — в Windows Server появилась версия без графического режима. Да, Windows запускается в текстовом режиме, в котором можно полноценно управлять сервером! В Linux все было наоборот, эту ОС создавали с точки зрения "лишь бы было безопасно", а теперь двигаются в сторону наращивания и упрощения сервисов.

Удобство и безопасность во многом противоречат, поэтому производителю приходится чем-то жертвовать. Что мне не нравится в некоторых дистрибутивах Linux — если установить какой-либо сервис, то инсталлятор мало того, что устанавливает сервис в максимальной конфигурации, он еще и запускает его автоматически при старте системы. Это очень плохо, и такие вещи нужно пресекать.

1.1. Что такое Linux?

ОС Linux — это свободная операционная система, исходные коды которой открыты для всеобщего просмотра и даже для внесения изменений. Большинство не смотрит на исходные коды, но воспринимает их наличие, как дополнительную приятную халяву. Но даже халява должна быть полезной, а если она бесполезна, то только мусорит.

Нет, наличие исходных кодов — это хорошо, и я тут не спорю. Это преимущество для такого продукта, как ОС, потому что можно перекомпилировать ядро и максимально оптимизировать его работу именно под ваше железо. Если для пользовательских утилит перекомпиляция не нужна и, скажем, текстовый редактор можно оптимизировать лишь незначительно, то для ОС возможность компиляции исходных кодов — большой и жирный плюс, который

позволяет выжать из компьютера максимум. Но в ОС Linux есть много других преимуществ, куда более важных.

К чему я это говорю? К тому, что я люблю ОС Linux не за халяву и не за наличие исходных кодов, а за качество. Я буду любить, даже если исходные коды закроют или будут взимать плату.

Основа ядра ОС была создана в 1991 году студентом хельсинкского университета (University of Helsinki) по имени Линус Торвальдс (Linus Torvalds). Все начиналось с того, что Линус начал писать программу терминала, функции которого постепенно стали выходить за пределы простой коммуникации. Он написал костяк, функционально схожий с UNIX-системами, сделал его доступным для всеобщего просмотра и доработки и обратился с просьбой помогать ему в улучшении и наращивании возможностей новой системы. Откликнулось достаточно много людей, и работа закипела.

Хакеры из различных стран присоединились к этому проекту на общественных началах и начали создавать самую скандальную ОС. А буза вокруг Linux возникает чуть ли не каждый день, потому что ОС получила большое распространение и является абсолютно бесплатной. Некоторые производители программного обеспечения считают этот проект перспективным, другие рассматривают как врага. В любом случае равнодушных очень мало.

Официальная версия ядра ОС под номером 1.0 была выпущена в 1994 году, то есть через три года после первых "слухов" о Linux. Такая скорость разработки была достигнута благодаря большому количеству профессионалов, которые согласились развивать интересную задумку Линуса.

ОС Linux — это многопользовательская и многозадачная система, которая позволяет работать с компьютером сразу нескольким пользователям и выполнять одновременно разные задачи.

Почему именно эта ОС получила такую популярность, ведь были и есть другие открытые проекты, некоторые из которых по реализации даже лучше Linux? Я связываю эту популярность с тем, что Linux создавался хакерами и для хакеров. Очень приятно, когда ты работаешь в операционной системе, в которой есть частичка тебя. Любой пользователь может вносить в исходный код системы любые изменения и не бояться преследования со стороны закона.

Linux — не единственная свободная система и не единственная ОС, исходные коды которой открыты. Но, несмотря на это, именно она стала популярной. ОС Linux не идеальна, и я не буду говорить, что она лучшая, но, все же, она покорила сердца миллионов, а может даже миллиардов, людей. Если учесть, что Linux является чуть ли не официальной ОС китайцев, то если миллиарда пользователей еще нет, то он точно появится.

Почему мы влюбляемся во что-то или в кого-то? Вот сижу я сейчас, смотрю на свою жену, и не могу ответить на этот вопрос однозначно. Наверное, про-

сто любим! Так же я не могу объяснить, почему люблю Windows или Linux. Я не могу понять, почему я сегодня предпочитаю KDE, а завтра загружаю GNOME.

Изначально популярность среди администраторов росла благодаря тому, что эта ОС поддерживала основные стандарты UNIX, к которым относятся POSIX, System V и BSD. При этом система была написана для дешевой (по сравнению с дорогостоящими серверами Sun и IBM) платформы x86 и обладала всеми необходимыми возможностями. Используя Linux, многие фирмы смогли оптимизировать свои расходы на инфраструктуру информационных технологий (ИТ) за счет перевода некоторых серверных задач на бесплатный продукт — Linux. А о домашних пользователях я вообще молчу, ведь для них полноценный UNIX был слишком дорог.

Среди первых задач, которые стали доверять Linux, — организация WEB-сервера, и с ней эта ОС справляется великолепно. Трудно точно оценить, какой процент хостинговых компаний сейчас использует Linux, но большинство статистических анализов показывает, что на Linux совместно с сервером Apache приходится большая часть, по некоторым данным, более половины. Но тут заслуга не только Linux, но и WEB-сервера Apache, который также бесплатен, надежен и просто великолепен.

На данный момент в Linux можно сделать практически все. Для этой ОС уже написано множество продуктов, которые распространяются бесплатно и позволяют решать всевозможные задачи. Компьютеры с установленной Linux используют в различных областях науки, экономики и техники, в том числе и при создании специальных эффектов для кино.

Не менее важным фактором популярности стала демократичность ОС. Вас не ограничивают в возможностях и не заставляют следовать определенным предпочтениям разработчика. В комплект поставки ОС включается по несколько программ одинакового назначения, например, несколько браузеров или офисных программ. В Windows такое невозможно. Мы, наверное, никогда не увидим в одном дистрибутиве браузеры Internet Explorer, Mozilla и Opera, хотя европейский суд и пытается добиться этого. В Linux конкуренция действительно свободная, никто не запрещает использовать сторонние разработки и не борется с этим. Напротив, пользователю предоставляется реальный выбор.

1.2. Открытый исходный код — безопасно?

Бытует мнение, что программы с открытым исходным кодом надежнее и безопаснее, чем фирменные. Сторонники этого утверждения считают, что такую систему исследуют множество людей разными способами и тем самым

выявляют все возможные погрешности. А самое главное, что ошибки исправляются своевременно, доступны для свободного скачивания и легки в установке.

Да, искать ошибки на уровне кода совместно с тестированием готового продукта намного проще и эффективнее, но результат далек от идеала. Несмотря на массовое тестирование, в Linux достаточно часто находят ляпсусы. А если посмотреть, какая армия пользователей обследовала последние версии Windows, то можно было бы подумать, что она станет безупречной. Тестирование — это одно, а применение в "боевых условиях" зачастую демонстрирует совершенно непредсказуемые результаты.

К тому же, сколько бы человек не посмотрело на исходные коды, безопасность от этого не увеличится, если смотрящие не обладают нужной квалификацией. Допустим, что на коды посмотрит миллиард людей, не понимающих в программировании, безопасность изменится? Нет. Количество реальных специалистов в безопасности, смотревших код, не так высоко, а именно они способны быстро и качественно находить ошибки. Это — отдельный навык, который требует специального обучения.

Открытость в отношении Linux имеет одно преимущество — отличное соотношение цены и качества. Возможность бесплатно установить ОС позволяет сэкономить большие деньги на установке, но увеличиваются затраты на поддержку, которая для Linux стоит достаточно дорого. К тому же администрирование Linux требует бóльших навыков и умений, чем настройка Windows. Отсутствуют мастера, которые облегчают жизнь. Необходимо знать команды Linux и уметь ими пользоваться без подсказки. Поэтому со своевременными обновлениями и свежей информацией могут возникнуть проблемы.

Из-за дорогой поддержки в конечном итоге цена владения Linux может оказаться выше, чем Windows. В Северной Америке, где оплата труда сотрудников отделов ИТ достаточно высока, Linux часто проигрывает Windows в стоимости владения.

Почему же Linux так сложен? Ответ прост: производительность и удобство — несовместимые вещи. В Windows все предельно ясно, но для выполнения какой-либо операции может понадобиться множество щелчков мыши и просмотр нескольких диалоговых окон, что отнимает драгоценное время. В Linux нужно запустить консоль и выполнить нужную команду. Проблема только в том, что нужно помнить множество команд, но если вы их помните, то сможете выполнить требуемую операцию быстрее, чем щелчками мышью.

ОС Windows везде, где только можно, использует визуальное представление и графический интерфейс. В Linux же графические утилиты слишком просты и зачастую не обладают достаточными возможностями, но это поправимо,

и сейчас появляется все больше оконных утилит, упрощающих процесс настройки. Пройдет какое-то время, и Linux станет тривиальной в использовании и при этом сохранит всю мощь и скорость использования командной строки.

Так как настройка Linux — достаточно сложная процедура, требующая высокой квалификации, очень часто именно из-за неправильно установленных параметров эта система попадает под огонь хакеров. Любая система (Windows, Linux или Mac OS X) с настройками по умолчанию далека от идеала. Часто безопасностью жертвуют для обеспечения производительности или удобства. В некоторых программах включаются сервисные функции, которые облегчают работу администратора (например, отладка в интерпретаторе PHP), но и упрощают взлом со стороны хакера. Именно поэтому безопасность системы зависит прежде всего от человека, который ее обслуживает.

Наша задача — не просто научиться работать с ОС Linux, а делать это эффективно, то есть суметь настроить ее на максимальную производительность и безопасность. Именно такую цель мы и поставим перед собой.

1.3. Ядро

Ядро — это сердце ОС, в котором реализовано управление памятью и другими ресурсами компьютера. Помимо этого оно позволяет получить доступ к различному железу. Например, ранние версии ядра обеспечивали работу только двух USB-устройств: клавиатура и мышь. Современное ядро (на момент написания этих строк ядро под номером 2.6.31) поддерживает большинство современных устройств, а дистрибутивы включают драйверы для большинства популярного оборудования.

Номер версии ядра Linux состоит из трех чисел (последнее указывается не всегда):

- первое число — старший номер, который указывает на значительные изменения в ядре;
- второе — младший номер, увеличение которого указывает на появление небольших изменений. По нему можно определить, является ядро проверенным или предназначено для тестирования, и нет уверенности, что оно не содержит ошибок. Если число четное, то ядро прошло тщательное тестирование. В противном случае установка данной версии не гарантирует стабильной работы;
- третье число — сборка, то есть номер очередного рабочего релиза. В некоторых случаях это число опускают, ибо оно несет не такую значительную смысловую нагрузку, как предыдущие номера. Например, часто говорят о версии 2.6, и в данном случае не указана именно сборка.

Новые версии ядра можно скачать по адресу **www.kernel.org** или с сайта производителя вашего дистрибутива. Обновление ядра позволяет не только получить новые возможности по работе с железом и повысить производительность системы, но и исправить некоторые ошибки. Самое главное, что обновление ядра в Linux не влечет за собой переконфигурирования всей ОС, как это происходит в некоторых других системах. Я видел компьютеры, ОС которых были установлены еще несколько лет назад и не перенастраивались с тех пор, а только обновлялось ядро и программное обеспечение. Такое бывает редко, потому что, как правило, периодически приходится обновлять железо, наращивая мощности, ведь запросы программ и пользователей растут не по дням, а по часам.

1.4. Дистрибутивы

На данный момент существует множество различных дистрибутивов Linux, но между ними легко проглядывается сходство, так как большинство имеет общие корни. Например, многие дистрибутивы построены на основе Red Hat Linux. Компании-производители вносят некоторые коррективы в процедуру инсталляции (чаще всего только графические), изменяют список включаемого программного обеспечения и продают под своей маркой. При этом ядро системы и устанавливаемые программы чаще всего поставляются абсолютно без изменений.

Даже если установочные версии имеют разных производителей, в качестве графической оболочки почти везде используется KDE или/и GNOME, а при отсутствии в поставке их всегда можно установить. Таким образом, вне зависимости от основного дистрибутива у всех будет одинаковый графический интерфейс.

Я долго не мог решить, какой дистрибутив использовать, но потом решил выбрать Ubuntu. Я заглянул на пару сайтов, посвященных Linux, и посмотрел в статистике (такую статистику предоставляет счетчик mail.ru) ОС, с которых заходили на сайт пользователи. Наиболее популярным оказался Ubuntu. В принципе, зная один дистрибутив, очень легко перейти на другой, ведь каждый из них — все же Linux.

Разнообразие дистрибутивов является самым слабым звеном ОС Linux (на мой взгляд). Когда вы начнете работать с ОС, то увидите, что большая часть операций не стандартизирована (это можно расценивать как следствие открытости кода). Получается как в поговорке "Кто в лес, кто по дрова". Это серьезная проблема, которая усложняет восприятие. Но в реальности в 99% случаев в дистрибутивах все идентично, поэтому проблема больше раздута, чем имеет реальную почву.

На мой взгляд, неудобство от разнообразия дистрибутивов заключается в том, что производителям приходится много топтаться на месте и писать один и тот же код. Лучше бы они объединились и начали быстрее двигаться вперед. Да, пострадает конкуренция и возможность выбора, но развитие будет намного быстрее.

В этом смысле ОС Windows более унифицирована и проще для обучения. Хотя в последнее время и здесь наблюдается отступление от установленных канонов. Так, внешний вид программ стал совершенно непредсказуем. Меню и панели в Office 2000/XP/2003/2007 постоянно изменяются (только успевай привыкать к ним!). В Linux, несмотря на отсутствие стандартов, элементы интерфейса пока везде остаются одинаковыми.

Дистрибутивы Linux являются условно бесплатными. Их также нужно приобретать в коробочном варианте, но их лицензионное соглашение намного мягче, чем у коммерческих ОС. Например, купив одну коробку с Linux, вы можете устанавливать ее на любое количество рабочих станций.

Цена одной копии Linux намного ниже, чем Windows, и при этом в дистрибутив входит громадное количество офисных программ, интернет-утилит, графических редакторов и т. д. Таким образом, после установки полной версии ваш компьютер сразу готов решать большинство производственных и домашних задач.

В ОС Windows графический редактор (Paint), текстовый процессор (WordPad) и другие программы слишком примитивны, и для нормальной работы нужно потратить сотни долларов. Поэтому реальная стоимость рабочего места на базе ОС Windows намного выше цены дистрибутива Linux.

При таком сравнении ОС Linux окажется победителем. Но, как уже говорилось, у Windows намного более дешевая поддержка, а для получения полноценной помощи в Linux нужен доступ к сети разработчика дистрибутива, который стоит достаточно дорого. Расходы на поддержку могут сделать стоимости владения этими операционными системами примерно одинаковыми. Именно поэтому я не буду вас убеждать, что Linux лучше, потому что бесплатна: это не совсем верно. Но мы увидим, что ОС Linux достаточно гибка и надежна, чтобы ее можно было выбрать в качестве рабочей лошадки для вашего компьютера. Именно эти качества являются наиболее существенными, и я покажу, что все они присущи Linux.

Итак, давайте рассмотрим основные дистрибутивы, которые вы можете встретить на рынке. Помните, что Linux — это всего лишь ядро, а большинство программ, сервисов и графическая оболочка принадлежат разным разработчикам и компаниям. Какой именно продукт будет включен в состав дистрибутива, определяется производителем.

Ваш выбор должен зависеть от того, что именно вы хотите получить от системы, но и это не является обязательным, потому что любой дистрибутив можно "нарастить" дополнительными пакетами программ.

1.4.1. Red Hat Linux

Данный дистрибутив считается классическим и является законодателем моды в развитии ОС. Помимо этого, Red Hat ведет разработку ОС Linux в двух направлениях: для серверных решений и для клиентских компьютеров. Серверный вариант является платным, а клиентский вариант (Fedora) бесплатен и доступен для скачивания с сайта **fedoraproject.org**. Шли разговоры о том, что Fedora будет независимым проектом, но пока он остался под крылом Red Hat.

Все дистрибутивы Linux всегда ругают за сложность установки ядра и программ, которые чаще всего поставляются в исходных кодах и требуют компиляции. Компания Red Hat уже давно упростила этот процесс, разработав менеджер пакетов RPM (Redhat Package Manager). Такие пакеты для установки используют большинство других разработчиков.

Если вы выбираете себе дистрибутив для сервера, то я настоятельно рекомендую обратить внимание на этого производителя или его клонов, потому что Red Hat заботится о безопасности системы и старается исправлять ошибки с максимально возможной скоростью.

1.4.2. Slackware

Мое знакомство с Linux начиналось именно с дистрибутива Slackware (**www.slackware.com**). Это один из самых старых и сложных для домашних пользователей дистрибутивов. До сих пор нет удобной программы установки, и большинство действий приходится делать в текстовом режиме. Конечно же, вы можете добавить к этому дистрибутиву KDE или GNOME (графические оболочки), а также другие пакеты, облегчающие работу, но установку проще не сделаешь.

Если вы ни разу не работали с Linux, то я бы не рекомендовал начинать знакомство с этого дистрибутива. Лучше выбрать что-нибудь попроще.

1.4.3. SuSE Linux

Мне приходилось работать с разными программами от немецких производителей, но удобство работы с ними не просто хромало, а создавалось впечатление, что эти программы — безногие калеки с детства. Но разработка от SuSE (**www.suse.de**) опровергает мое мнение. Этот дистрибутив отличается

симпатичным интерфейсом и отличной поддержкой оборудования, потому что содержит громадную базу драйверов.

Честно сказать, я бы удивился, если бы кто-то умудрился испортить KDE или GNOME, ведь внешний вид ОС зависит от этих оболочек. И SuSE сумела не испортить эту красоту своими картинками и логотипами.

Но нельзя сказать, что программисты SuSE вообще ничего не делали. Они добавили в дистрибутив набор утилит под названием YaST, которые значительно упрощают администрирование. Я бы посоветовал SuSE только любителям и для использования на клиентских компьютерах. Тем более, что это один из платных дистрибутивов, который распространяется в коробке.

В настоящее время этот дистрибутив находится под патронажем компании Novell.

1.4.4. Debian

Несмотря на то, что цель любого производителя — получение прибыли, существует множество дистрибутивов, которые были и остаются некоммерческими. Основным и самым крупным из них можно считать Debian (**www.debian.org**). Этот продукт создают профессионалы для себя, но пользоваться этим дистрибутивом может каждый.

ОС Debian имеет больше всего отличий от классической Red Hat, и у вас могут возникнуть проблемы из-за разного расположения некоторых конфигурационных файлов. Но на этом проблемы не заканчиваются. Как и все некоммерческие проекты, этот дистрибутив сложнее других. Разработчики позиционируют Debian как надежную ОС, и это у них получается, а вот о простых пользователях они заботятся мало, поэтому домашние компьютеры этот дистрибутив завоюет не скоро.

1.4.5. Ubuntu

Это, наверное, один из самых простых дистрибутивов. Его основной целью во время создания была простота, а в прошлом году компания заявила, что в течение двух лет планирует сделать дистрибутив красивее и удобнее Mac OS. Пока быстрых продвижений в сторону красоты не заметно, но с точки зрения простоты дистрибутив уже давно является одним из лучших. А судя по статистике счетчиков Linux ресурсов в Интернете, в России этот дистрибутив самый популярный. Сайт разработчиков — **www.ubuntu.com**.

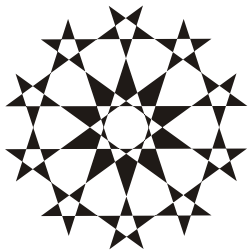
Дистрибутив построен на базе технологий Red Hat и схож с Fedora. Единственное, что меня пугает — большинство статистических обзоров показывает,

что ежегодно в этом дистрибутиве находят больше уязвимостей, чем в конкурентах. Статистикам и аналитикам верить очень сложно, особенно с точки зрения безопасности, потому что безопасность измерить невозможно. В дистрибутиве может быть найдена сотня уязвимостей, но он останется надежным, если все они незначительные. С другой стороны, достаточно одной уязвимости, но очень серьезной, которую можно легко использовать и которую залатают с большим опозданием, чтобы надежность опустилась до нуля.

Существует еще множество дистрибутивов, варьирующихся от больших и мощных систем, включающих все необходимое, до маленьких, загружающихся с дискеты и работающих на очень старых компьютерах.

Основная задача книги — создание безопасной и быстрой системы — усложняется из-за большого количества дистрибутивов. Описать особенности каждого из них в одной книге очень сложно, да и не имеет смысла, потому что способы реализации защиты могут отличаться от дистрибутива к дистрибутиву и даже от версии к версии ядра из-за большого разнообразия возможных используемых программ. Поэтому мы будем обращать внимание в основном на общие закономерности, и лишь изредка говорить об особенностях дистрибутивов.

На этом закончим вводную часть и перейдем непосредственно к установке ОС Linux, чтобы начать знакомиться с системой на практике и увидеть все своими глазами.



Глава 2

Установка и начальная настройка Linux

Установка когда-то была самой сложной процедурой для всех дистрибутивов Linux. Вспоминаются времена, когда нужно было последовательно загружаться с нескольких дискет, а потом следовать сложным инструкциям или самостоятельно набирать команды Linux, которые уже надо было знать.

Еще одна непростая задача — разбиение дисков на разделы. Их нужно иметь как минимум два (основной и раздел подкачки). Проблема в том, что многие боятся манипулировать с дисками, особенно с теми, на которых уже есть информация. И это правильно, потому что известны примеры, связанные со случайной потерей данных.

Во время инсталляции любая ОС должна определить установленное оборудование и подготовить все необходимое для его нормальной работы. Еще лет семь назад перечень поддерживаемых устройств можно было просмотреть за несколько минут, так как многие производители игнорировали Linux, не писали необходимые драйверы и при этом не давали нужной информации. Сейчас чтение такого списка займет дни, потому что все крупные игроки компьютерного мира начали считаться с пингвином (животное, которое ассоциируют с Linux). Определение оборудования теперь происходит безошибочно и, чаще всего, не требует дополнительного вмешательства со стороны пользователя. А базы данных драйверов в дистрибутиве Linux скоро не будут уступать Windows, а может быть, уже не уступают.

В настоящее время вся инсталляция происходит практически автоматически и сравнима по сложности с установкой других ОС. Именно поэтому корпорация Microsoft начинает бояться Linux и ее продвижения в бездну домашних компьютеров. Теперь уже любой, даже начинающий пользователь справится с установкой. И все же мы бегло рассмотрим этот процесс и остановимся на наиболее интересных моментах.

Если вы уже имеете опыт установки Linux, я все же рекомендую вам прочитать эту главу, потому что некоторые детали могут оказаться интересными и полезными. А может быть, что-то просто покажется веселым.

Основные принципы безопасности и производительности закладываются уже на этапе установки, и впоследствии мы будем только следовать им и расширять наши познания.

2.1. Подготовка к установке

Какой дистрибутив устанавливать? Я не могу ничего советовать, потому что выбор всегда остается за вами. Отдайте предпочтение тому, который удовлетворяет вашим потребностям и может решить поставленные задачи. В *разд. 1.4* мы рассмотрели наиболее популярные на данный момент дистрибутивы и их основные отличия, что облегчит вам принятие правильного решения.

Лично я предпочитаю Ubuntu и Fedora. Не знаю почему и объяснить не могу, но, судя по статистике различных сайтов в Интернете, в том числе и по ОС Linux, именно Ubuntu является самым популярным дистрибутивом в России. Если устанавливать серверную версию этого дистрибутива, то он будет ставиться в текстовом режиме. Серверу не нужен графический интерфейс, он там даже лишний. Мы же в этой книге будем немного затрагивать графический интерфейс, хотя бóльшую часть времени будем разговаривать об утилитах командной строки и конфигурационных файлах. Мы будем больше говорить о серверной роли ОС Linux.

Важное замечание, которое я должен сделать, — устанавливайте самый свежий стабильный дистрибутив, включающий последнюю версию ядра и приложений. Мы говорили и будем еще не раз повторять, что во всех программах есть ошибки, просто в новой версии о них еще никто не знает :). Кроме того, надо помнить, что программные средства необходимо своевременно обновлять. Если воспользоваться старым дистрибутивом, то объем обновлений может оказаться слишком большим. Не лучше ли установить сразу все новое и максимально быстро запустить сервер в эксплуатацию?

Если установить старый дистрибутив и не обновить его до последней версии, то в нем, скорей всего, будут известные хакерам ошибки, а значит, они без проблем смогут взломать сервер. Если этого не сделают сразу, то через какое-то время обязательно сделают. Если вы считаете, что ваш сервер никому не нужен, то сильно ошибаетесь. Даже пустышка кому-то нужна.

Полгода назад мой знакомый спросил меня: "А можно узнать, как взломали Linux сервер?" Конечно же можно, если журналы сохранились и их никто не успел уничтожить. Меня связали с горе-администратором, сервер которого

взломали. Первый вопрос, который я задал, оказался весьма удачным — какой дистрибутив установлен на сервере. Администратор точно не знал, потому что ему кто-то посоветовал срочно переустановить Linux. Переустановка — банальное решение, но она не всегда решает проблему, особенно, если проблема в конфигурации, а не в самом сервере.

В данном случае администратору переустановка помогла. Он нашел диск, с которого он устанавливал Linux много лет назад (и не обновлял с тех пор), и на нем было написано три циферки 6.22. Да, это очень старая версия, начала 2000-х годов. Точные годы ее появления не помню, но это было даже раньше Windows XP. В этой истории удивляет только то, как сервер смог прожить столько времени до 2008 года, когда это происходило, невзломанным. Сервер долгое время был никому не нужным, но кто-то нашел его и использовал для перекачки нелегала, и горе-администратор получил несколько гигабайт лишнего трафика, за которые пришлось платить.

Мастера установки для разных дистрибутивов могут отличаться, но все они, как правило, имеют схожие окна, и даже последовательность выполняемых действий зачастую одинакова. Дело в том, что программ установки не так уж и много, и большинство разработчиков используют одни и те же программы и не пишут ничего самостоятельно. Разве что оформление отличается.

Итак, приступим к рассмотрению процесса установки. Первое, что нужно сделать, — это определить место, где будет располагаться ОС. Если у вас новый компьютер, жесткий диск не разбит на части, и вы будете использовать только Linux, то во время установки просто отведите под эту ОС все доступное пространство. Доверьте разбиение системе, и она сделает это вполне оптимально.

Если у вас уже установлена Windows, и вы хотите, чтобы на компьютере было сразу две ОС, то придется сделать несколько телодвижений. Для установки Linux нужно пустое пространство на диске. Нет, это не свободное место на логическом диске C:, а пустота на винчестере, место, не занятое какими-либо разделами. В последних версиях инсталляторов есть возможность изменять размер раздела прямо в программе установки, причем без потери данных. Раньше для изменения разметки диска приходилось уничтожать информацию.

Если у вас все пространство диска уже используется и вы хотите откусить небольшой кусок пространства от существующего диска, то это вполне реально. Данные на существующем диске просто сдвигаются, а в опустошенной части диска может быть создан новый раздел для Linux.

Для повышения надежности процесса сдвига многие рекомендуют сначала произвести дефрагментацию. Эта операция более безопасна и заключается