LINUX/BSD как бастион на пути вирусов

крис касперски ака мыщъх, no-email

количество дыр, обнаруженных в Windows уже давно перешагнуло через все мыслимые границы и неуклонно продолжает расти. выходить в Интернет стало небезопасно. дальше так жить нельзя и надо защититься. в статье рассматривается организация защитного бастиона, основанного на LINUX/BSD, и пригодного как для офиса, так и для домашнего использования.

введение

Почему Windows NT небезопасна? Почему в ней обнаруживаются все новые и новые дыры? Вопрос чисто абстрактный, но мы все-таки постараемся дать на него ответ. Начнем с того, что умный людей в Microsoft осталась не так уж и много, налицо явная текучка кадров. Опытные специалисты покидают "империю зла" и уходят в другие компании. Достаточно вспомнить памятный скандал с менеджером, в которого Стив Балмер зашвырнул креслом (от такого руководителя я бы тоже ушел). Падение культуры программирование легко проследить с помощью дизассемблера. Если MS-DOS 6.x еще содержала огромное количество ассемблерного кода, а Windows 95 представляет собой настоящий шедевр оптимизации (без всякой иронии!!!), запрограммированный на смеси ассемблера с чистым Си, то в Windows 98 уже доминирует Си++, "мастера" и прочие автоматические кодогенераторы, заменившие живой ум. Windows NT 4.x (которая, как известно создавалась приблизительно в то же самое время, что и Windows 95, только другим коллективом программистов) это блестяще оптимизированная, хотя и слишком навороченная система, запрограммированная руками и головой, но в Windows 2000 и тем более XP уже доминирует Си++ и "мастера". Программисты старого поколения так не поступают! Вывод — все это писали новички, со всеми вытекающими отсюда последствиями. В дизассемблере код выглядит просто ужасно. Поражает даже не тяжеловесность, а… "рассосредоточенность" кода, тонким слоем размазанного по куче функций. В частности, никакой единой функции переключение контекста в Windows NT нет! SwitchContext это только малая часть, весь остальной код размазан по всему ядру, регистры многократно сохраняются/восстанавливаются в разных местах, делается куча проверок на допустимость их значений и т. д. Сетевые компоненты выглядят еще хуже.

К тому же, Windows очень стремительно развивается и содержит массу избыточного, никому не нужного кода, который не так-то просто удалить из системы или хотя бы просто отключить. Причем, развитие идет по принципу, "не трогаем того, что написали, а набрасываем сверху еще и еще". Как следствие, количество связей между отдельными компонентами системы лавинообразно нарастает, а времени на тестирование нет и продукт выбрасывается на рынок таким как есть. Кража исходных текстов Windows 2000 только подлила масла в огонь. Они есть практически у каждого хакера, но отсутствуют у легальных специалистов по безопасности, а это, значит, что игра идет в одни ворота. Хакеры ищут дыры, а специалисты вынуждены лишь признавать их постфактум.

Вместо того, чтобы вылизывать систему и работать над ее улучшением, Microsoft несется вперед, предлагая новые революционные решения, которые даже она при своих миллиардных доходах просто физически не в состоянии отладить. Так что количество дыр в последующих версиях Windows сокращаться не собирается и хакерство будет только процветать. Как в этих условиях хранить и обрабатывать конфиденциальные данные, не говоря уже про "электронные кошельки", кража которых в последнее время принимает массовый характер?

Служба поддержки Microsoft отвечает — регулярно устанавливайте на компьютер свежие заплатки, которые и так устанавливаются службой Windows Update. Предложение, конечно, заманчивое, но… заплатки выпускаются не мгновенно и только для уже известных дыр. Для домашнего компьютера такая степень защищенности вполне подходит, да и то… Только представьте сколько электронных денег сможет утащить хакер, если он напишет вируса прежде, чем будет выпущен "патч"? А для фирмы захват сервера вообще может стать фатальным. Причем, заплатки выпускаются не бесконечно, а только в течении так называемого "жизненного цикла продукта", определяемого самой Microsoft. В практическом плане это означает, что даже если старая операционная система полностью удовлетворяет нашим скромным потребностям, ее все равно придется менять, попутно обновляя "железо", что

выливается в солидные расходы и вызывает множество проблем от необходимости обучения персонала до "старые программы не запускаются".

Про то, что заплатки занимают огромный объем и для их перекачки необходимо иметь по меньшей мере DSL модем мы промолчим. К тому же, Windows Update реально воспользоваться все равно не удастся. Задумайтесь, что произойдет, если операционная система упадает? Ведь после установки с дистрибьютивного диска выходить в Интернет и качать заплатки ни в коем случае нельзя, ведь в эти минуты наш узел совершенно беззащитен перед хакерами, а вероятность атаки не так уж и мала, особенно если вспомнить про червей, которые стучаться во все компьютеры подряд. Теоретически можно скачать заплатки в виде отдельных файлов, сохранив их на любом носителе, но… тогда придется разбираться в них самостоятельно, а это не так-то просто, поскольку заплатки содержат зависимости и абы как не встают или встают, но не работают.

Исчезает самое главное преимущество Windows – простота управления. Воздвигнуть NT-сервер и оставить его без присмотра сегодня уже не получится. Если только не нанять администратора, разбирающегося в безопасности, с высокой степенью вероятности сервер будет взломан. Тоже самое относится и к домашним машинам. Вирусы так и прут! Они создают излишний трафик, воруют пароли и другую секретную информацию или просто нарушают нормальную работу операционной системы, вызывая сбои и зависания, убытки от которых зачастую весьма значительны. Давайте посмотрим, что в этой ситуации можно то предпринять…

по ту сторону барьера

Анализ ситуации позволяет выявить три основных объекта атаки. Первый и наиболее коварный: это атака на саму операционную систему или ее базовые службы, которые в большинстве случаев реализуются через переполнение буферов. Ошибки были обнаружены как в фундаментальных драйверах (например, TCPIP.SYS), так и в прикладных службах (например, DCOM), без которых в принципе можно и обойтись, но не всегда легко отключить через пользовательский интерфейс. Причем, если дыры в прикладных службах элементарно закрываются брандмауэром (конечно, при условии, что без этой службы действительно можно обойтись), то атакам на драйвера брандмауэры противостоять практически не в силах (ну разве, что это будет специальным образом спроектированный брандмауэр, которых нет и навряд ли когда будут). Антивирусы и прочие защитные системы подобного типа здесь так же бессильны. Да, они ловят вирусов, но только если знают о них. Нашумевших вирусов не так уж и много и все чаще и чаще приходится сталкиваться с локальной заразой, обитающей в ограниченном ареале и исчезающей прежде, чем разработчики антивирусов узнают о ней. Единственным способом обороны остаются заплатки, но они недостаточно эффективны в силу уже упомянутых причин.

Другая популярная мишень — браузер. Слово "Интернет" уже давно стало синонимом "IE" и атакуют преимущественно его. Несмотря на то, что IE поддерживает целый комплекс мер безопасности, он ломается без особых проблем. В лучшем случае атакующий берет под контроль только сам IE, в худшем же — захватывает всю операционную систему. Достаточно зайти на страницу, содержащую зловредный код и… Самое неприятное, что такой код может содержаться даже на "престижных" сайтах, например, в гостевой книге, в которую могут писать все желающие и которые далеко не всегда выполняют качественную фильтрацию HTML-содержимого. Жесткая настойка политик безопасности до некоторой степени уменьшает вероятность успешной атаки, но не исключает ее полностью. Большинство дыр (таких, например, как переполнение буфера при обработке bmp-файлов) остаются открытыми и устраняются только заплатками, про проблемы которых мы уже говорили. Установив альтернативный браузер (например, FireFox), мы будем практически полностью застрахованы от подобных атак, однако, вместе с браузером еще потребуется другой почтовый клиент (например, Thunderbird), поскольку стандартный Outlook Express негласно использует IE для отображения HTML-писем, которые являются идеальным средством атаки и множество червей распространяются именно так.

Третья и последняя мишень — сам человек, клюнувший на предложение "от которого нельзя отказаться" и запустивший исполняемый файл (зачастую замаскированный под графическую картинку или что-то другое). Ну что тут можно сказать? Теоретически достаточно строго-настрого запретить всем пользователям запускать что бы то ни было скаченное из сети или полученное по электронной почте, только ведь все равно они будут качать и запускать. За всеми не уследишь и не остановишь! Организационные меры уже доказали свою

неэффективность и проблему можно решить только техническим путем. Самое простое — запускать FireFox'a и Thunderbird'a из-под специального пользователя, с минимальными правами, не имеющего доступа ни к каким файлам, кроме файлов самой программы. И хотя в Windows уровень привилегий легко может быть повышен в обход всех защит, подавляющее большинство атакующих программ до этого еще не доросли и такая мера достаточно эффективна. А вот пример неверного, но весьма популярного решения — ставим виртуальную машину с Windows, устанавливаем на ней Лиса с Птицей и связываем виртуальной сетью с основной машиной. На первый взгляд — все прекрасно. Атакующий может воздействовать на браузер, но из застенков виртуальной машины он никуда не выберется, а там все равно нет ничего интересного кроме кэша браузера и еще быть может почтовой базы, которую в принципе можно расположить и на отдельной виртуальной машине, благо в VM Ware между ними легко переключаться. Проблема в том, что если основная машина доступна по виртуальной сети (а если она не будет доступна, то как прикажите выходить в Интернет), атакующая программа сможет воздействовать на основную операционную систему, через имеющиеся в ней дыры, так что такая схема все равно не очень надежна, хотя большинство распространенных вирусов она отсекает сразу, только необходимо следить, чтобы на виртуальной машине не образовался "зоопарк", ведь вирусы имеют тенденцию заражать все, к чему прикасаются…

Хорошо, цели атаки определены. Будем стоить оборонительные сооружения!

среди пингвинов

Некоторые организации предпринимают попытки полного перехода на LINUX/BSD, однако, при этом возникает большое количество труднопреодолимых проблем. Далеко не для всего оборудования можно найти драйвера. Даже если данная видеокарта или другое устройство входит в список поддерживаемого железа, далеко не факт, что составитель дистрибьютива действительно протестировал ее и она согласиться работать как надо. На многие сканеры и другую периферию драйверов вообще нет.

В LINUX/BSD все не так как в Windows и пользователей приходится переучивать, но кто их будет переучивать? И кто будет нести расходы? А если приходит новый сотрудник? К тому же, Star Office это все же совсем не Microsoft Office и хотя он может открывать некоторые Office-документы, реально с ним работать невозможно (разве что из горячей любви к LINUX'у или отсутствию альтернативы).

Наконец, практически на любом предприятии так или иначе используются специализированные программы, как правило написанные на DELPHI и не имеющие прямых аналогов в мире LINUX'a. Теоретически их можно перенести и на другие платформы, но фирмы-разработчики пока не видят в этом никакого смысла, поскольку LINUX-рынок еще не сложился.

Хотим ли мы того или нет, но отказаться от использования Windows на рабочих станциях пока невозможно. Примем это как факт и подумаем как все-таки ее защитить. Сервера в этом плане чувствуют себя намного лучше и LINUX-сервер — вполне нормальное решение, хотя BSD все-таки более предпочтительна. В ней меньше дыр и к тому же последние версии LINUX'a все меньше ориентируются на серверное применение и все больше — на десктоп.

схемы построения защитного бастиона

Рассмотрим для начала сеть небольшой организации с десятком клиентских машин и одним выделенным компьютером - сервером. На клиентские машины лучше всего поставить Windows 2000/XP с FireFox'ом и Thunderbird'ом, запущенным из-под наименее привилегированного пользователя без прав доступа ко всем файлам, кроме файлов программы (хотя лично я из браузеров предпочитаю консольный links, который очень надежен в плане безопасности, но устанавливать его на компьютер секретарши может только администратор-садист). На сервере устанавливается любая UNIX-подобная операционная система (LINUX или BSD), поднимается HTTP-proxy и либо собственный почтовый сервер, либо транслятор портов, либо брандмауэр уровня приложений, играющий роль POP3/SMTP proxy. Впрочем, простейший proxy для почты можно написать и самостоятельно — он не займет и сотни строк на Си/Perl.

Полноценный выход в Интернет клиентским машинам лучше всего не давать, поскольку, в этом случае они могут быть легко атакованы извне. А вот работа через LINUX/BSD бастион на основе proxy-сервера позволяет отказаться от установки заплаток на Windows-машины, поскольку теперь их можно атаковать только изнутри сети, а против внутрисегментных атак даже залатанные системы все равно незащищены.

Как вариант, можно установить SOCKS-Proxy сервер и предоставить клиентам практически полненный доступ в Интернет. Взаимодействие через SOCKS-Proxy снимает многие проблемы. Так, например, не требуется специальная настройка клиентского программного обеспечения (достаточно просто установить proxy-клиента) и программы, не умеющие работать через HTTP-Proxy, скорее всего заработают через SOCKS, однако, не все. Ведь proxy – это все-таки proxy, со всеми вытекающими достоинствами и ограничениями. Внешние подключения запрещены (точнее, невозможны) и если только не устроить трансляцию портов специально, атакующий не сможет увидеть ни одного клиентского узла! (только необходимо помнить, что от атак на приложения, например, на браузер, proxy не спасает).

Рисунок 1 локальная сеть небольшой организации с одним выделенным компьютером-бастионом

Предложенная схема отличается высокой надежностью и простой управления. Современные дистрибьютивы LINUX/BSD ставятся из "коробки" не хуже, чем Windows и с настройками по умолчанию работают вполне достойно. Времена колдовства и плясок с бубном уже прошли. Конечно, гуру тут же скажут, что все это ерунда и настройки по умолчанию неправильны/небезопасны/непроизводительны. На то они и гуру. Их хлеб — темные магические ритуалы, после которых система буквально преображается, только вот… жизненно важной необходимости в этом нет. Дыр в LINUX/BSD практически нет (во всяком случае в новых билдах, скаченных с официального сервера, а не купленных в ближайшем ларьке) и настройки по умолчанию в последнее время стали вполне продуманными. Во всяком случае, BSD-сервер даже в штатной конфигурации защищен намного лучше чем Windows. Многие организации именно так и поступают. На внешний сервер ставят BSD (или LINUX), а на вытуренные машины — Windows 98, Windows XP и т. д., так что в этом решении нет ничего нового или экзотического.

Кстати говоря, львиная доля дыр BSD/LINUX-серверов приходится отнюдь не на саму операционную систему, а на установленное поверх нее программное обеспечение — Sendmail, Apache и т. д. Это сложные программные комплексы, содержащие огромное количество строк исходного кода, в которых запутались даже сами разработчики. Их очень сложно настраивать и еще сложнее отлаживать. Новые дыры обнаруживаются практически постоянно и LINUX/BSD-сервер с Sendmail'ом и Apach'ем по своей надежности недалеко ушел от Windows NT с IIS. Принципиальное отличие между ними только в том, что альтернативных серверов под NT очень немного, а под LINUX/BSD их море… Даже не нужно рыскать по Интернету, достаточно взять дистрибьютив и ознакомится с его содержимым. Чем "легче" будет Proxy-сервер, тем меньше вероятность, что в нем будут дыры.

В принципе, можно установить и несколько серверов, соединив их последовательно друг с другом. Внешний сервер "видит" только своего внутреннего собрата и локальная сеть ему недоступна. Если на одном из серверов будет стоять LINUX, а на другом BSD, то хакеру, чтобы проникнуть в локальную сеть придется взломать сразу обе системы, что довольно затруднительно, если не сказать маловероятно. Proxy-сервер можно ставить как на внешнем сервере (а на внутреннем тогда поднимать NAT), либо, наоборот, прятать Proxy за внешнем сервером, на котором стоит NAT плюс брандмауэр. Каждое решение имеет свои сильные и слабые стороны, но все-таки лучше размещать Proxy на внешнем сервере и вот почему: если в нем вдруг окажется дыра (а она там окажется) и хакер захватит контроль над узлом, его остановит внутренний сервер. Напротив, NAT сам по себе никак не защищает внутренний Proxy от атак (ну, практически, не защищает), и если хакер сумеет его взломать, он тут же получит доступ во внутреннюю сеть, в которой находятся слабо защищенные машины с Windows!

Рисунок 2 локальная сеть небольшой организации с двумя выделенным компьютерами-бастионами

А вот WEB-сервер (если он только есть) лучше всего разместить на внешнем сервере, ни в коем случае не совмещая его с тем узлом, который имеет доступ во внутреннюю сеть. WEB-сервер — это очень-очень сложный агрегат, в нем неизбежно присутствуют ошибки и потому WEB-сервера ломают чаще всего!

домашние сети — проблемы и решения

Для дома или мелкого офиса выделять одну из машин в отдельное "делопроизводство" чаще всего неприемлемо, хотя собрать сервер на основе устаревшего оборудования, оставшегося от апгрейда, может практически каждый. LINUX/BSD-серверам не нужен монитор, а при желании можно обойтись и без жесткого диска, в результате чего расходы на безопасность окажутся не так уж и велики, тем более что домашняя сеть из 2-3 машин уже не редкость, а норма, так почему бы не поставить еще одну машину, не установить на нее LINIX/BSD и не попробовать себя в роли администратора?

Но давайте все-таки будем исходить из того, что компьютер у нас один, причем это далеко не самый мощный компьютер (например, P-III) и покупать еще один мы не можем/не хотим, предпочитая использовать виртуальные машины.

Возможных вариантов построения сети всего два — установить на основною машину LINUX/BSD, запуская Windows под эмулятором или, наоборот, запихать LINUX/BSD в эмулятор и предоставить ей прямой доступ в Интернет в обход Windows. Тогда выход в сеть будет осуществляться по следующей схеме: компьютер (железо) → Windows (несетевые компоненты) →эмулятор (LINUX/BSD) → Windows (сетевые компоненты).

Первый способ наиболее очевиден, но он не обходится без проблем. Во-первых, для достижения приемлемой производительности, мы должны иметь довольно мощный компьютер и много оперативной памяти, что противоречит условиям задачи, во-вторых, Windows, запущенная из-под эмулятора, не имеет прямого доступа к оборудованию и это оборудование не может реализовать свой функционал, а зачастую отказывается работать вообще!

Второй способ всех этих недостатков лишен. Ему не нужен высокопроизводительный (а, значит, весьма дорогостоящий) процессор и требуется совсем немного памяти, Windows работает на "живом" оборудовании с полной скоростью, самоотверженностью и отдачей, а защищенность ничуть не хуже, чем в случае выделенного компьютера. Захватывающие, перспективы, не правда ли? Но обо всем по порядку!

Для начала нам потребуется выбрать эмулятор. Это должен быть очень быстрый эмулятор, к тому же поддерживающий виртуальную сеть, достаточно надежный в работе и по возможности дешевый, впрочем, учитывая специфику российского рынка, цена продукта не является решающим фактором, особенно для домашних сетей.

Классический выбор это, конечно же VM Ware, достойных конкурентов которому пока не наблюдается. Единственный недостаток — виртуальная сеть достаточно сложно настраивается и неспециалистам приходится попыхтеть, прежде чем она заработает. Остальное никаких проблем не вызывает. Устанавливаем эмулятор, создаем новую виртуальную машину с настойками по умолчанию, водружаем на нее LINUX или BSD, а затем даем ей доступ к физическому оборудованию.

Если выход в Интернет осуществляется через Dial-Up по COM-модему, заходим в настройки виртуальной машины (VM → Setting) и открываем доступ к физическому порту, на котором "висит" модем (Hardware → Add → Serial Port → Use physical serial port on the host → COMx). Причем, VM Ware видит не только настоящие физические порты, но и порты, созданные драйверами различных устройств, например, GPRS-драйвером сотового телефона или софт-модемом, что снимает проблему поиска драйвером под LINUX/BSD. Ну а найти драйвер стандартного модема — не проблема, тем более что для распространенных моделей существуют и "родные" драйвера. Остается только настроить выход из LINUX'а в Интернет. Проще всего воспользоваться популярной программой KPPP, которая по легкости управления ничуть не отличается от своего Windows-аналога, если даже не превосходит его. Теперь инсталлируем HTTP/POP3/SMTP-proxy и все! Выбор конкретных программ может быть любым. Тут все зависит от конкретных вкусов и предпочтений. В офисной сети, наверное, лучше будет использовать знаменитый squid, но для дома это слишком уж тяжеловесное решение. Лично у меня прижился small http-proxy (http://home.lanck.net/mf/srv/), pop3proxy (http://www.quietsche-entchen.de/download/pop3proxy-1.2.0.tar.gz) и smtpproxy (http://www.quietsche-entchen.de/download/smtpproxy-1.1.3.tar.gz), хотя это далеко не самое лучшее решение, и гурманы программного обеспечения наверняка подберут что-то свое. Из SOCKS Proxy я предпочитаю Dante (http://www.inet.no/dante/). Не столько из-за его качеств, а сколько из-за того, что он написан и распространяется на бесплатной основе горячими парнями из Норвегии — родине моей любимое группы Sirenia (такое мрачное оркестровое хоральное готическое пение).

Рисунок 3 виртуальная сеть домашнего компьютера с бастионом

С DSL-модемами в этом плане чуть-чуть труднее. В принципе, VM Ware позволяет эмулируемому приложению видеть физические USB-порты (VM → Setting → USB Controller → Automatically connect new USB devices to this virtual machine when it has focus), но найти подходящий драйвер для USB DLS-модема под LINUX'ом может стать непреодолимой проблемой, поскольку не для всех моделей такие драйвера есть. Правда, тут можно схитрить. Установить "родной" Windows драйвер — как правило он создает виртуальную сетевую карту и встраивает ее в TCP/IP стек, благодаря чему мы можем выходить в Интернет. Если удалить TCP/IP протоколы, оставив виртуальную карту одну-одинешеньку, никакого Интернета у нас, разумеется, не будет, но тем не менее, на физическом уровне пакеты могут беспрепятственно приходить/уходить с нашего узла. Идея состоит в том, чтобы дать LINUX-машине "физический" доступ к виртуальной сетевой карте, связав их в сеть и тогда LINUX сможет выходить в Интернет через Windows, но сама Windows при этом будет "засвечена" в Интернете лишь частично, что защитит ее от подавляющего большинства атак. Тем не менее, поскольку сетевые пакеты проходят через многие Windows-компоненты, потенциально не свободные от дыр, в принципе атака все-таки возможна, но это уже из области паранойи и теоретических абстракций.

Основная проблема состоит в том, что VM Ware не позволяет выбирать к какой именно "физической" карте она подключается и по умолчанию выбирает первую обнаруженную карту. Если компьютер не имеет никаких других сетевых карт, кроме той, что установлена DSL-модемом, все ОК и мы можем не переживать, но стоит воткнуть одну или несколько "настоящих" Ethernet-карт (или задействовать Ethernet-карту, интегрированную в материнскую плату), как виртуальная карта сойдет с пьедестала и все пойдет наперекосяк. Если так, говорим: Edit → Virtual Network Setting → Automatic Bridging → Excluded Adapters → Add и перечисляем сетевые адаптеры, которые мы ***не хотим использовать*** в виртуальной сети.

Другая проблема состоит в том, что VM Ware может не "увидеть" виртуальную сетевую карту и тогда связать ее с LINUX'ом не получится. Надежнее всего использовать DSL-модемы с Ethernet-портом, подключаемые к физической сетевой карте, которую VM Ware увидеть просто обязана. Ну а настроить DSL-модем из-под LINUX'а сейчас уже не проблема. Во всех или практически всех дистрибьютивах на этот случай имеются удобные мастера. В частности в KNOPPIX достаточно нажать "К" → Интернет → ADSL\PPPOE Configuration и ответить на несколько несложных вопросов.

>>> врезка QEMU как альтернатива VM Ware

VM Ware – это замечательный эмулятор, главные и, пожалуй, единственные недостатки которого — высокая стоимость ($200 по текущему прайсу) и отсутствие исходных текстов. За эти деньги можно свободно купить поддержанный компьютер без монитора, создать выделенный LINUX сервер и не мучатся. Исходные тексты нужны не только для удовлетворения любопытства. Вот например, если VM Ware не видит виртуальную карту DSL-модема, то нам остается только развести руками, а при их наличии можно было бы разобраться почему так и устранить проблему. Даже если это не можем сделать мы, наверняка сможет кто-нибудь другой.

Поэтому, имеет смысл рассмотреть и бесплатные эмуляторы, из которых нам больше всего подходит QEMU (http://fabrice.bellard.free.fr/qemu/). Это динамический эмулятор, основанный на BOCHS (http://bochs.sourceforge.net/), но работающей в десятки раз быстрее его и ничуть не уступающий VM Ware по производительности (а на некоторых задачах даже обгоняющей ее), совершенно бесплатный, портированный под множество платформ (и LINUX/BSD/Windows в том числе), имеющий кучу разных расширений на все случаи жизни от независимых разработчиков и т. д.

Виртуальная сеть в отличии от VM Ware встает сама, не требуя никакой настройки, что и плохо, и хорошо одновременно. С одной стороны, мы можем организовать выход в Интернет через модем без плясок с бубном, с другой стороны обеспечить "физический" доступ к сетевой карте уже не получится и придется либо ковырять исходные тексты, либо искать дополнительные расширения, которые не всегда работают стабильно и к тому же требуют обязательной перекомпиляции QEMU, поэтому выбор конкретного эмулятора остается за вами.

заключение

Отразить большинство атак вполне реально, хотя за это приходится расплачиваться множеством труднопреодолимых неудобств (покупка дополнительного оборудования или снижение производительности при работе через эмулятор, неполноценный выход через proxy и

т. д.). А может… ничего и не надо отражать? Стоит же XP, автоматически забирает свежие обновления из Интернета, на электронном кошельке спокойно лежат деньги, все жужжит и не падает… Так ведь на жителей Помпеи долгое время тоже ничего не падало, а потом в один миг небо почернело и на город обрушилась лава и камни. Беда никогда не предупреждает о своем приходе и восклицание "еще вчера все работало" служит очень слабым утешением. Можно тысячу раз "смело" выходить в Интернет, не боясь ни вирусов, ни хакеров, но только хакерам все равно боитесь вы их или нет. И если атака окажется успешной… впрочем, о последствиях успешной атаки лучше не говорить. Зачастую они весьма плачевны.

Мы ни к чему не призываем, ни за что не агитируем и ни от чего не отговариваем. Некоторые считают, что Windows XP это достаточно защищенная система и им ничего не грозит. Другие же не чувствуют себя в безопасности даже за каменной стенной Proxy-сервера, окруженного по периметру брандмауэром.

Воздвигнуть защищенную систему легко, сложнее подобрать оптимальную политику безопасности, сочетающую комфорт и надежность. Описанная схема на эту роль совсем не претендует. Это крепость параноика, который защищается от всего мира потому, что боится, что именно в этот момент кто-то смотрит в него через прицел.