Автор: Артур Скальский © Вести СТРАНА, РОССИЯ 1990 12.01.2000, 21:55 205

Безопасность в Интернет

Безопасность для интернет-дачников
(**Максим Мошков** moshkow@ipsun.ras.ru)

Мы едем на дачу

Старожилы Рунета, наверное, помнят еще те времена, когда и Рунета-то не было, веб-странички на русском исчислялись сотней штук, а русских серверов было то ли двадцать, то ли пятьдесят. Давно ли это было? Всего лишь 5-6 лет назад. Поиграем в ассоциации. Пускай большая, невиртуальная жизнь - это город. Город Москва. С заводами, институтами и житейскими заботами. А Интернет - это дачи. В отпусках, в свободное от работы время, "самозахватом" или организованно - начинающие дачники заселяли окрестные серверы, поливали свои огородики и менялись друг с другом саженцами и редкими сортами тюльпанов. Кто-то сколачивал из подручных лесин, натыренных на стройке в соседней области, хибарку, кто-то подгонял казенный грузовичок и отстраивал кирпичную дачку. К старожилам приезжали из города знакомые и родственники погостить и... оставались тоже, нарезая участочки-хомячки по соседству. Тихая патриархальная жизнь нарушалась регулярными бытовыми ссорами и замирениями, ну а милиции в тех краях отродясь не было. Да и от кого тут нужны милиционеры? Убийств, ограблений и хулиганства - не наблюдалось, а когда наведывались редкие бомжи, с которыми не справлялся местный сторож, из соседнего совхоза "Красный Релком" на мотороллере приезжали крепкие ребята-механизаторы и вышибали непрошенных гостей к чертовой бабушке. Мы жили в те времена. Мы расслабились и привыкли к спокойной и безопасной жизни, к тому, что калитки на участках открыты, а дома не запираются, окна распахнуты и цветочки, высаженные вдоль забора, не вытаптывает соседский молодняк. Прошло всего четыре года, и мы вдруг обнаружили, что половина окрестных полей застроена крепкими кирпичными коттеджиками, за нашим забором, где 40 хаток, раскинулся дачный поселок на 5000 трехэтажных домов и город, из которого мы бежали, пришел к нам вновь, со всеми своими проблемами. Хулиганство? Пожалуйста. Драка в переулке, кражи со взломом? Сколько угодно. Настала пора очнуться и осмотреться. И привыкать жить в новом, совсем уже не виртуальном мире. Русский Интернет стал совсем как настоящий мир - с заводами, магазинами и житейскими заботами.

Чем мы рискуем

Я не собираюсь рассматривать здесь проблемы защиты сетей крупных коммерческих фирм. Денег у них обычно хватает на то, чтобы купить себе надежный и дорогой файервол. Мне интереснее оценить наши с вами проблемы - проблемы простых пользователей Сети, администраторов веб-серверов и мелких провайдеров. Вряд ли при взломе нашей системы мы рискуем большими деньгами. Не думаю, что на нашем сервере хранится невосполнимая информация. Все проще и прозаичнее. Любой взлом обходится администратору в большие потери личного и рабочего времени. Взломанный сервер нельзя использовать дальше. Выловить все возможные хакерские закладки и троянских коней - дело нелегкое. А самое главное - нельзя быть стопроцентно уверенным в успехе. Поэтому после взлома дорога у нас одна - полная переинсталляция системы с нуля. Установка операционки и всего прикладного софта с дитрибутивов. А такого софта почти всегда - много. И настройка его под конкретное окружение тоже дело не мгновенное. По-другому не получится, а это несколько часов работы, а иногда - несколько дней.

Итак, потери от взлома для обычного некоммерческого сервера - это потраченное время и трата сил. Для коммерческого - это недовольство клиентов, удар по престижу, а может быть, даже и по карману. И конечно, опять лишния трата сил - ценные технические специалисты вместо решеняя плановых задач будут восстанавливать систему, получая за это свою отнюдь не маленькую зарплату.

Легенды и мифы

Перечислю несколько устойчивых заблуждений и мифов, бытующих в связи с Интернетом в головах рядовых пользователей.

Говорят, что в Интернете, кроме порнухи, ничего не найти. И только за эротическими картинками народ по Сети и шарится.

Говорить такую чепуху может только тот, кто никогда не пытался найти достойный и интересный порносервер. А кто пытался, тот уже знает - все, что угодно, кроме черта лысого, проще найти, чем сервер с картинками, а не сервер, где вам покажут тысячи дурацких баннеров и будут долго клянчить номер кредитки, которой у вас все равно нет.

Говорят, что с перепиской по email`у надо быть осторожным, ведь кто-нибудь может послать вашему другу от вашего имени всякие гадости, а его ответы перехватывать, чтоб не дать ему прояснить ситуацию.

Да, действительно, бытовая переписка передается по Интернету в незашифрованном виде, ее можно перехватить и подсмотреть на почтовом сервере и даже сфальсифицировать. Только для занятия этим нужна высокая квалификация и доступ к этому серверу. А его могут получить люди только трех профессий: сисадмин - который с гораздо большим интересом поиграет в свободное время в Quake, хакер - которому недосуг заниматься глупостями (ведь зарубку на клавиатуре ставят не за прочтенное письмо, а за взломанный сервер) и, наконец, те-кому-положено. Но вы ведь не академик Сахаров.

Еще говорят, по Сети крадутся хакеры, взламывая все подряд, выкрадывая из компьютеров деньги, билеты, телефоны любовниц и сталкивая с орбиты космические спутники.

Не верьте. Это поклеп. Деньги тратятся сами собой, билеты - просто теряются, а космические спутники по TCP/IP заваливать не обязательно - они и сами падают.

И, наконец, самое опасное заблуждение: говорят, интернетовский сервер можно сделать на базе Windows NT.

Опасно это заблуждение тем, что приносит проблем больше, чем все хакерские атаки, вместе взятые, и гарантирует все те же неприятности, что и от взлома системы: потеря работоспособности, отказы, зависания, и как следствие - сизифовы труды и пот, переинсталляция системы и потеря клиентов.

Опасности для безопасности

В реализации протоколов TCP/IP есть несколько довольно неприятных недоработок, которые влекут за собой дырки в безопасности интернет-хоста, причем есть среди них и такие, которые сложно или даже невозможно закрыть полностью.

Система DNS (определение IP-адреса по доменному имени компьютера) "верит" первому же откликнувшемуся на запрос name-серверу, и ее можно обмануть, ответ сфальсифицировав. Причем обмануть можно не только отдельно взятую клиентскую машину, но и сервер DNS, "накормив" его фальшивыми адресами. Обманутый сервер начнет передавать "фальшивую" информацию всем своим клиентам, что особенно болезненно, если это крупный провайдерский узел, которым пользуются клиенты этого провайдера.

Защиты от такого метода атаки нет, и его широко применяют для подмены популярных веб-серверов. Если вы встретите сообщение о том, что "головная страница сервера имярек заменена страницей с призывами (призывы не пропущены цензурой)" - то девять против одного за то, что это сделано подменой DNS. Единственное кардинальное лечение этой дыры - перевод всех DNS-серверов в мире на named версии 8. Это процесс длительный и болезненный, и конца ему пока не видно.

Ко многим серверам применим целый набор DoS-атак (Denial of Service) - образно говоря, это все равно как "закидать банановыми шкурками". Атакующий генерит большой поток запросов на сервер, сервер не успевает их обрабатывать и забивает свои входные очереди ответами-в-никуда, реальным же пользователям в очередях уже не остается места. Это может быть и SYN-атака, забивающая приемную очередь TCP-пакетов на низком уровне, а может банальное "задавливание" веб-сервера большим потоком простых HTTP-запросов.

С точки зрения определений заваливание сервера DoS-атакой или DNS-подменой нельзя назвать взломом в чистом виде. Но в том-то и беда, что для атакованного сайта результат один и тот же - что при взломе, что при завале, что при банальном отказе по причине ошибок самого администратора: сервер молчит, посетители не могут на него попасть, администратору - головная боль и борьба с неисправностями, а начальству - отмывание мундира и денежные проблемы, все это - с гарантией.

А раз так, то неспециалистам (то есть подавляющему большинству) можно не тратить время и не забивать себе голову изучением, какие типы, виды и подвиды взломов, атак и т. д. существуют. Неприятности во всех случаях получаются совершенно идентичные. Зато, пожалуй, стоит проклассифицировать причины отказа системы.

Злонамеренное внешнее вмешательство ("Хакер")
Злонамеренное внутреннее вмешательство ("Засланный казачок")
Непреднамеренное внутреннее головотяпство ("Акела промахнулся").
Программно-аппаратная неисправность ("Ломается все").
Как легко догадаться, от "казачка" защититься невозможно в принципе. Понизить вероятность "поломок" можно, вложив деньги в более дорогое и надежное оборудование. Отказы из-за ошибки обслуживающего персонала, администратора, программиста - неизбежны и регулярны, вероятность их, по сравнению со всеми остальными бедами, наиболее высокая.

В этом свете борьба с хакерами становится уже не столь актуальной, шум вокруг них кажется непропорционально громким, и покупка очень надежного (и очень дорогого) файервола, возможно, уже не покажется вам панацеей от всех бед. Конечно, приятно иметь в своем дачном домике стальную бронированную дверь. Но если стены - из фанеры, если окна закрыты на крючок из проволоки, если к чердаку приставлена лестница - то злодей все равно проникнет внутрь. Так не лучше ли вместо покупки стальной двери купить дверь деревянную, но с хорошим замком, а на сэкономленную сумму купить рамы с решеткой и замок для чердака? Воплощая аналогии - сэкономив деньги на файерволе (а цены на коммерческий файервол находятся в интервале от 10 до 30 тысяч долларов), можно их вложить с большей (для обеспечения надежности) отдачей - в оборудование, в обучение сотрудников, в повышенную зарплату, на которую можно будет нанять квалифицированного администратора, делающего меньше ошибок, чем новичок-самоучка.

Самое опасное в Интернете - не хакеры, а спаммеры

Спаммеры, рассылающие по всему свету свои рекламные письма, давно не пользуются своими собственными выделенными почтовыми серверами. Потому что их мгновенно засекают и отключают провайдеры. А провайдеры отключают спаммеров, чтоб самим не остаться в изоляции, потому что если они этого не сделают, то соседи перестанут принимать от провайдеров-нарушителей любую почту. Спрашивается - почему в Москве между некоторыми адресами не ходит почта? (Не буду уточнять, между кем и кем, чтоб не обвинить невиновных - но пользователи, конечно, знают эти непроходимые адреса.) Потому что кое-кто из наших провайдеров не в состоянии придавить заведшихся у них спаммеров. Современный спаммер находит чужой почтовый сервер, в котором (по недосмотру системного администратора) разрешен relaying (пересылка почты от "чужих" адресов на "чужие" адреса). Что позволяет спаммеру послать через эту машину спам по всему миру.

Задумаемся на секунду - что произойдет с машиной, которой поручили разослать письма по списку в несколько сотен тысяч адресов. В принципе, ничего особо страшного - письма осядут в очереди (немаленькой), и машина будет их потихоньку, по несколько десятков единовременно, рассылать - и так в течение нескольких дней. Грозить вам это будет сильной загрузкой процессора и выходного интернетовского канала, а также - баааальшим счетом от провайдера за зарубежный трафик. Но это только начало.

Среди сотен тысяч адресов процентов 20 являются устаревшими и недействительными. На каждое недоставленное письмо машина получит письмо от "демона-почтаря" (mailer-daemon) - о недоставке сообщения. И пойдут они сплошным потоком, тысячи запросов на соединение единовременно. Получаем классический DoS - на SMTP-шный порт сваливается огромное количество запросов, с которыми машина справиться не успевает. Unix-ы обычно это переносят с большим трудом, тратя ВСЕ свои силы на прием почты - при этом прекращая обслуживать обычных посетителей. Windows NT - гарантированно умирает. Усугубляет разницу то, что современные версии сетевых Unix - Linux и FreeBSD - по умолчанию ставятся с отключенным relayng`ом, а Windows NT - с разрешенным.

Печальная история: один мой знакомый провайдер жаловался, что клиенты, которых он подключал на этой неделе по выделенному каналу, достали его жалобами: "сломалась, не работает почта, помогите". Все пять клиентов, как один. Каждый перед этим решил поставить свой собственный почтовый сервер. На Windows NT.

Веб-мастер - бди, враг не дремлет

Не подумайте, что я непоследователен и призываю наплевать на безопасность, выкинуть файерволы и заниматься вместо этого административно-хозяйственными вопросами. Конечно нет. И файервол нужен, и о хакерах надо не забывать. Просто надо смотреть на проблему комплексно, сбалансированно распределять ресурсы и не забывать обо всех узких местах. И о хакерах - тоже.

Нынешний среднестатический взломщик хакером в большинстве своем называться не имеет права. Это обычный подросток или недоучившийся студент, места в жизни не нашедший. Для большинства

обнаруженных в операционных системах дыр уже написаны программы, которые сами прощупывают окружающие хосты, сами определяют в них наличие дырок, сами ломают, сами закидывают в проломанную дыру крючки и закладки. Чтоб стать "хакером" теперь, достаточно наковырять себе этих программ посвежее, а дальше остается просто их запускать и нажимать кнопку "OK".

Чтобы защититься от таких взломщиков, достаточно внимательно отслеживать листы-рассылки с оповещениями об обнаруженных дырках в своей операционной системе и затыкать их СРАЗУ. Обычно дырки, эксплойты (т.е. способы использования дырок) и заплатки для них же становятся известны практически одновременно, и если не тормозить и затыкать все по мере обнаружения, то на пролом через очередную дыру хакерам останется не так уж много времени.

Ставьте патчи-заплатки

Самое незащищенное состояние сервера - в момент его инсталляции и начальной конфигурации. ЛЮБАЯ свежепроинсталлированная операционная система имеет дырки в безопасности - поскольку дистрибутив был напечатан давно, а security-патчи, появившиеся с тех пор, надо ставить дополнительно.

На время инсталляции операционной системы на интернет-сервер ОБЯЗАТЕЛЬНО отключите его от Интернета.

Конфигурация по умолчанию свежепроинсталлированного юникс-сервера рассчитана на дружественное сетевое окружение. Многие сервисы находятся в открытом состоянии (т.е. в положении "всем можно") - что удобно в локальной корпоративной сети, но абсолютно неприемлемо в сети общего доступа. Необходимо ОБЯЗАТЕЛЬНО перевести машину из расслабленного режима по умолчанию в режим строгой безопасности (т. е. когда запрещено все и всем, кому это явно не разрешено). Это касается всех сетевых служб - начиная с удаленного логина и FTP и кончая принтером и командами talk, finger и т. п.

Ну и как прикажете выживать?

Получается, что хакеры бродят толпами, вооруженные программами-сканерами, ошибаться - нельзя, взломать или хотя бы завалить могут практически каждого, и нет защиты. Как же жить-то тогда?

Смотрите на жизнь проще. В конце концов - по реальным улицам нашего реального города ходят хулиганы и маньяки, ходят с дубинками и пистолетами. Каждый из нас может схлопотать по физиономии, да и просто зарезать могут в подворотне - или в квартире окна побить, и никакой защиты не будет. Не станешь ведь ходить всю жизнь в бронежилете и с двумя телохранителями за спиной. Однако же живем, не боимся. Не так страшен черт, как его малюют, нормальных людей - большинство, хулиганов на всех никак не хватит - нас спасает принцип "неуловимого Джо". А также - разумная осторожность и грамотные системные администраторы операционной системы Unix.

Автор: Артур Скальский © Вести СТРАНА, РОССИЯ 1990 12.01.2000, 21:55 205
URL: https://babr24.com/?ADE=52185 Bytes: 16117 / 15401 Версия для печати

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта