обход брандмауэров снаружи и изнутри

крис касперски ака мыщъх no-email

большинство (если не все) корпоративных сетей ограждены по периметру недемократично настроенными брандмауэрами, защищающих внутренних пользователей от самих себя и отпугивающих начинающих хакеров вместе с кучей воинствующих малолеток. между тем, для опытного взломщика даже качественный и грамотно настроенный брандмауэр – не преграда.

введение в брандмауэры

Брандмауэр (он же *firewall*) в общем случае представляет собой совокупность систем, обеспечивающих надлежащий уровень разграничения доступа, достигаемый путем управления проходящим трафиком по более или менее гибкому набору критериев (правил поведения). Короче говоря, брандмауэр пропускает только ту часть трафика, которая явно разрешена администратором и блокирует все остальное.

На рынке доминируют два типа брандмауэров – ***пакетные фильтры***, так же называемые шлюзами фильтрации пакетов (packet filter gateway), и ***программные прокси*** (application proxy). Примером первого их них является Firewall от компании Check Point, а второго – Microsoft Proxy Server.

Пакетные фильтры полностью прозрачны для пользователей и весьма производительны, однако, недостаточно надежны. Фактически, они представляют собой разновидность маршрутизатора, принимающего пакеты как извне, так и изнутри сети, и решающего как с ними поступить – пропустить дальше или уничтожить, при необходимости уведомив отправителя, что его пакет сдох. Большинство брандмауэров этого типа работает на IP-уровне, причем полнота поддержки IP-протокола и качество фильтрации оставляют желать лучшего, поэтому атакующий может легко их обмануть. На домашних компьютерах такие брандмауэры еще имеют смысл, но при наличии даже плохонького маршрутизатора они лишь удорожают систему, ничего не давая взамен, т. к. те же самые правила фильтрации пакетов можно задать и на маршрутизаторе!

Программные прокси представляют собой обычные прокси-сервера, прослушивающие заданные порты (например, 25, 110, 80) и поддерживающие взаимодействие с заранее оговоренным перечнем сетевых сервисов. В отличии от фильтров, передающих IP-пакеты "как есть", прокси самостоятельно собирают TCP-пакеты, выкусывают из них пользовательские данные, наклеивают на них новый заголовок, и вновь разбирают полученный пакет на IP, при необходимости осуществляя трансляцию адресов. Если брандмауэр не содержит ошибок, обмануть его на сетевом уровне уже не удастся, к тому же он скрывает от атакующего структуру внутренней сети – снаружи остается лишь брандмауэр. А для достижения наивысшей защищенности, администратор может организовать на брандмауэре дополнительные процедуры авторизации и аутентификации, набрасывающиеся на противника еще на дальних рубежах обороны. Это были достоинства. А теперь поговорим о недостатках. Программные прокси крайне неудобны, поскольку ограничивают пользователей в выборе приложений. Они работают намного медленнее пакетных фильтров и здорово снижают производительность (особенно на быстрых каналах). Поэтому, главным образом мы будем говорить о пакетных фильтрах, оставив программные прокси в стороне.

Брандмауэры обоих типов обычно включают в себя более или менее кастрированную версию ***системы определения вторжений*** (***I****ntruder* ***D****etection* ***S****ystem* или сокращенно *IDS*), анализирующую характер сетевых запросов и выявляющую потенциально опасные действия – обращение к несуществующим портам (характерно для сканирования), пакеты с TTL равным единице (характерно для трассировки) и т. д. Все это существенно затрудняет атаку и хакеру приходится действовать очень осторожно, поскольку любой неверный шаг тут же выдаст его с головой. Однако, интеллектуальность интегрированных систем распознавания достаточна невелика и большинство уважающих себя администраторов перекладывает эту задачу на плечи специализированных пакетов, таких например, как Real Secure от Internet Security System.

В зависимости от конфигурации сети, брандмауэр может быть установлен как на выделенный компьютер, так и делить системные ресурсы с кем-нибудь еще. Персональные брандмауэры, широко распространенные в мире Windows, в подавляющем большинстве случаев устанавливаются непосредственно на сам защищаемый компьютер. Если это пакетный фильтр,

реализованный без ошибок, то защищенность системы ничуть не страдает и атаковать ее так же просто/сложно, как и на выделенном брандмауэре. Локальные программные прокси защищают компьютер лишь он некоторых типов атак (например, блокируют засылку троянов через IE), оставляя систему полностью открытой. В UNIX-подобных системах пакетный фильтры присутствует изначально, а в штатный комплект поставки входит большое количество разнообразных прокси-серверов, поэтому, озабочиваться приобретением дополнительного программного обеспечения ненужно.

Рисунок 1 узел, защищенный брандмауэром, чувствует себя словно за кирпичной стеной

отчего защищает и не защищает брандмауэр

Пакетные фильтры в общем случае позволяют закрывать все входящие/исходящие TCP-порты, полностью или частично блокировать некоторые протоколы (например, ICMP), препятствовать установке соединений с данными IP-адресами и т. д. Правильно сконфигурированная сеть должна состоять по меньшей мере из двух зон: а) внутренней корпоративной сети (corporative network), огражденной брандмауэром и населенной рабочими станциями, сетевыми принтерами, intranet-серверами, серверами баз данных и прочими ресурсами подобного типа; б) демилитаризованной зоны (demilitarized zone или сокращенно DMZ), в которой расположены публичные сервера, которые должны быть доступны из Интернет (см. рис. 2). Брандмаузер, настроенный на наиболее драконический уровень защищенности, должен:

- закрывать все порты, кроме тех, что принадлежат публичным сетевым службам (HTTP, FTP, SMTP и т. д.);
- пакеты, приходящие на заданный порт, отправлять тем и только тем узлам, на которых установлены соответствующие службы (например, WWW-сервер расположен на узле A, а FTP-сервер на узле B, то пакет, направленный на 80 порт узла B должен блокироваться брандмауэром);
- блокировать входящие соединения из внешней сети, направленные в корпоративную сеть (правда, в этом случае пользователи сети не смогут работать с внешними FTP-серверами в активном режиме);
- блокировать исходящие соединения из DMZ-зоны, направленные во внутреннюю сеть (исключая FTP- и DNS-сервера, которым исходящие соединения необходимы);
- блокировать входящие соединения из DMZ-зоны, направленные во внутреннюю сеть (если этого не сделать, то атакующий, захвативший управление одним из публичных серверов, беспрепятственно проникнет и в корпоративную сеть);
- блокировать входящие соединения в DMZ-зону из внешней сети по служебным протоколам, часто использующимся для атаки (например, ICMP, правда, полное блокирование ICMP создает большие проблемы, в частности, перестает работать ping и становится невозможным автоматическое определение наиболее предпочтительного MTU);
- блокировать входящие/исходящие соединения с портами и/или IP-адресами внешней сети, заданными администратором;

Рисунок 2 типичная структура локальной сети

Фактически роль брандмауэра сводится к ограждению корпоративной сети от всяких любопытствующих идиотов, блуждающих по просторам Интернет. Тем не менее, прочность этого ограждения только кажущаяся. Если клиент корпоративной сети использует уязвимую версию браузера или клиента электронной почты (а большинство программного обеспечения уязвимо!), атакующему достаточно заманить его на троянизированную WEB-страничку или послать ему письмо с вирусом внутри и через короткое время локальная сеть окажется поражена. Даже если исходящие соединения из корпоративной сети запрещены (а как же тогда бедным пользователям шариться по Интернету?), shell-код сможет воспользоваться уже установленным TCP-соединением, через которое он и был заброшен на атакованный узел, передавая хакеру бразды удаленного управления системой.

Брандмауэр может и сам является объектом атаки, ведь он как и всякая сложная программа, не обходится без дыр и уязвимостей. Дыры в брандмауэрах обнаруживаются практически каждый год и далеко не сразу затыкаются (особенно если брандмауэр реализован на "железном" уровне). Забавно, но плохой брандмауэр не только не увеличивает, но даже ухудшает защищенность системы (в первую очередь это относится к персональным брандмауэрам, популярность которых в последнее время необычайно высока).

обнаружение и идентификация брандмауэра

Залогом успешной атаки является своевременное обнаружение и идентификация брандмауэра (или в большее общем случае – системы обнаружения вторжений, но в контексте настоящей статьи мы будем исходить из того, что она совмещена с брандмауэром).

Большинство брандмауэров отбрасывают пакеты с истечением TTL (Time To Live – время жизни), блокируя тем самым трассировку маршрута, чем и разоблачают себя. Аналогичным образом поступают и некоторые маршрутизаторы, однако, как уже говорилось выше, между маршрутизатором и пакетным фильтром нем принципиальной разницы.

Отслеживание маршрута обычно осуществляется утилитой traceroute, поддерживающий трассировку через протоколы ICMP и UDP, причем ICMP блокируется гораздо чаще. Выбрав узел, заведомо защищенный брандмауэром (например, www.intel.ru), попробуем отследить к нему маршрут:

```
$traceroute –I wwww.intel.ru
Трассировка маршрута к bouncer.glb.intel.com [198.175.98.50]
с максимальным числом прыжков 30:

  1  1352 ms   150 ms   150 ms  62.183.0.180
  2   140 ms   150 ms   140 ms  62.183.0.220
  3   140 ms   140 ms   130 ms  217.106.16.52
  4   200 ms   190 ms   191 ms  aksai-bbn0-po2-2.rt-comm.ru [217.106.7.25]
  5   190 ms   211 ms   210 ms  msk-bbn0-po1-3.rt-comm.ru [217.106.7.93]
  6   200 ms   190 ms   210 ms  spb-bbn0-po8-1.rt-comm.ru [217.106.6.230]
  7   190 ms   180 ms   201 ms  stockholm-bgw0-po0-3-0-0.rt-comm.ru [217.106.7.30]
  8   180 ms   191 ms   190 ms  POS4-0.GW7.STK3.ALTER.NET [146.188.68.149]
  9   190 ms   191 ms   190 ms  146.188.5.33
 10   190 ms   190 ms   200 ms  146.188.11.230
 11   311 ms   310 ms   311 ms  146.188.5.197
 12   291 ms   310 ms   301 ms  so-0-0-0.IL1.DCA6.ALTER.NET [146.188.13.33]
 13   381 ms   370 ms   371 ms  152.63.1.137
 14   371 ms   450 ms   451 ms  152.63.107.150
 15   381 ms   451 ms   450 ms  152.63.107.105
 16   370 ms   461 ms   451 ms  152.63.106.33
 17   361 ms   380 ms   371 ms  157.130.180.186
 18   370 ms   381 ms   441 ms  192.198.138.68
 19     *        *        *     Превышен интервал ожидания для запроса.
 20     *        *        *     Превышен интервал ожидания для запроса.
```

Листинг 1 трассировка маршрута, умирающая на брандмауэре (маршрутизаторе)

Смотрите, трассировка доходит до узла 192.198.138.68, а затем умирает, что указывает либо на брандмауэр, либо на недемократичный маршрутизатор. Чуть позже мы покажем как можно проникнуть сквозь него, а пока выберем для трассировки другой узел, например, www.zenon.ru

```
$traceroute –I wwww.intel.ru
Трассировка маршрута к distributed.zenon.net [195.2.91.103]
с максимальным числом прыжков 30:

  1  2444 ms  1632 ms  1642 ms  62.183.0.180
  2  1923 ms  1632 ms  1823 ms  62.183.0.220
  3  1632 ms  1603 ms  1852 ms  217.106.16.52
  4  1693 ms  1532 ms  1302 ms  aksai-bbn0-po2-2.rt-comm.ru [217.106.7.25]
  5  1642 ms  1603 ms  1642 ms  217.106.7.93
  6  1562 ms  1853 ms  1762 ms  msk-bgw1-ge0-3-0-0.rt-comm.ru [217.106.7.194]
  7  1462 ms   411 ms   180 ms  mow-b1-pos1-2.telia.net [213.248.99.89]
  8   170 ms   180 ms   160 ms  mow-b2-geth2-0.telia.net [213.248.101.18]
  9   160 ms   160 ms   170 ms  213.248.78.178
 10   160 ms   151 ms   180 ms  62.113.112.67
 11   181 ms   160 ms   170 ms  css-rus2.zenon.net [195.2.91.103]
Трассировка завершена.
```

Листинг 2 успешное завершение трассировки еще не есть свидетельство отсутствия брандмауэра

На этот раз трассировка проходит нормально. Выходит, что никакого брандмауэра вокруг zenon'a нет? Что ж! Очень может быть, но для уверенного ответа нам требуется дополнительная информация. Узел 195.2.91.193 принадлежит сети класса C (три старших бита IP-адреса равны 110) и, если эта сеть не защищена брандмауэром, большинство ее узлов должны откликаться на ping, что в данном случае и происходит. Сканирование выявляет 65 открытых адресов. Следовательно, либо маршрутизатора здесь нет, либо он беспрепятственно пропускает наш ping.

При желании можно попробовать просканировать порты, однако, во-первых, наличие открытых портов еще ни о чем не говорит (быть может брандмаузер блокирует лишь один порт, но самый нужный, например, защищает дырявый RPC от посягательств извне), а во-вторых, при сканировании хакеру будет трудно остаться незамеченным. С другой стороны, порты сканируют все кто не лень и администраторы уже давно не обращают на это внимания.

Утилита **nmap** (популярный сканер портов такой) позволяет обнаруживать некоторые из брандмауэров, устанавливая статут порта во "firewalled". Такое происходит всякий раз, когда в ответ на SYN, удаленный узел возвращает ICMP пакет типа 3 с кодом 13 (Admin Prohibited Filter) с действительным IP-адресом брандмауэра в заголовке (nmap его не отображает, пишите собственный сканер или используя любой снифак самостоятельно проанализируйте возвращаемый пакет). Если возвратится SYN/ACK – сканируемый порт отрыт. RST/ACK указывает на закрытый или заблокированный брандмауэром порт. Не все брандмауэры генерируют RST/ACK при попытке подключения к заблокированным портам (Check Point Firewall – генерирует), некоторые отсылают ICMP сообщение, как было показано выше, или ни хрена не посылают вообще.

Рисунок 3 внешний вид утилиты nmap

Большинство брандмауэров поддерживают удаленное управление через Интернет, открывая один или несколько TCP-портов, уникальных для каждого брандмауэра. Так например, Check Point Firewall открывает 256, 257 и 258 порты, а Microsoft Proxy – 1080. Некоторые брандмауэры явным образом сообщают свое имя и версию программного продукта при подключении к ним по netcat (или telnet), в особенности этим грешат Proxy-сервера. Последовательно опрашивая все узлы, расположенные впереди исследуемого хоста, на предмет прослушивания характерных для брандмауэров портов, мы в большинстве случаев сможет не только выявить их присутствие, но и определить IP-адрес! Разумеется, эти порты могут быть закрыты как на самом брандмауэре (правда, не все брандмауэры это позволяют), так и на предшествующем ему маршрутизаторе (но тогда брандмауэром будет нельзя управлять через Интернет).

Рисунок 4 структура IP-пакета

сканирование и трассировка через брандмауэр

Прямая трассировка через брандмауэр чаще всего оказывается невозможной (какому администратору приятно раскрывать интимные подробности топологии своих сетей) и атакующему приходится прибегать ко всевозможным ухищрениям.

Утилита **Firewalk** представляет собой классический трассер, посылающий TCP или UDP пакеты, с таким расчетом, чтобы на узле, следующим непосредственно за брандмауэром их TTL обращался в ноль, заставляя систему генерировать сообщение ICMP_TIME_EXCEEDED, благодаря чему firewalk уверенно работает даже там, где штатные средства уже не справляются, хотя крепко защищенный брандмауэр ей конечно не пробить и атакующему приходится использовать более продвинутые алгоритмы.

Будем исходить из того, что с каждым отправляемым IP-пакетом, система увеличивает его ID на единицу (как это чаще всего и случается). С другой стороны, согласно спецификации RFC-793, описывающей TCP протокол, всякий хост, получивший посторонний пакет, не относящийся к установленным TCP-соединениям, должен реагировать на него посылкой RST. Для реализации атаки нам понадобиться удаленный узел, не обрабатывающий в данный момент

никакого постороннего трафика и генерирующий предсказуемую последовательность ID. В хакерских кулуарах такой узел называется **немым** (*dump*). Обнаружить немой хост очень просто – достаточно лишь отправить ему серию IP-пакетов и проанализировать ID, возвращенный в заголовках. Запомним (запишем на бумажку) ID последнего пакета. Затем, выбрав жертву, подходящую для атаки, отправим ей SYN-пакет, указав в обратном адресе IP немного узла. Атакуемый узел, думая, что немой хост хочет установить с ним TCP-соединение, ответит: SYN/ACK. Немой хост, словив посторонний SYN/ACK, возвратит RST, увеличивая свой счетчик ID на единицу. Отправив немому хосту еще один IP-пакет, хакер, сравнив проанализировав возвращенный ID, сможет узнать – посылал ли немой хост жертве RST-пакет или нет. Если посылал, значит, атакуемый хост активен и подтверждает установку TCP-соединения на заданный порт. При желании, хакер может просканировать все интересующие его порты, не рискуя оказаться замеченным, ведь вычислить его IP практически невозможно – сканирование осуществляется "руками" немого узла и с точки зрения атакуемого выглядит как обычное SYN-сканирование.

Предположим, что немой хост расположен внутри DMZ, а жертва находится внутри корпоративной сети. Тогда, отправив немому хосту SYN-пакет от имени жертвы, мы сможем проникнуть через брандмауэр, поскольку он будем думать, что с ним устанавливает соединение внутренний хост, а соединения этого типа в 99,9% случаях разрешены (если их запретить, пользователи корпоративной сети не смогут работать со своим же собственными публичными серверами). Естественно, все маршрутизаторы на пути от хакера к немому хосту, не должны блокировать пакет с поддельным обратным адресом, в противном случае пакет умрет задолго до того, как доберется до места назначения.

Утилита **hping** как раз и реализует сценарий сканирования данного типа, что делает ее основным орудием злоумышленника для исследования корпоративных сетей, огражденных брандмауэром.

Как вариант, хакер может захватить один из узлов, расположенных внутри DMZ, используя их как плацдарм для дальнейших атак.

Рисунок 5 структура TCP-пакета

проникновение через брандмауэр

Сборку фрагментированных TCP-пакетов поддерживают только самые качественные из брандмауэров, а все остальные анализируют лишь первый фрагмент, беспрепятственно пропуская все остальные. Послав сильно фрагментированный TCP-пакет, "размазывающий" TCP-заголовок по нескольким IP-пакетам, хакер скроет от брандмауэра Acknowledgment Number и он не сможет определить принадлежность TCP-пакета к соответствующей ему TCP-сессии (быть может он относится к легальному соединению, установленным корпоративным пользователям). Если только на брандмауэре не активирована опция "резать фрагментированные пакеты", успех хакерской операции гарантирован. Блокирование фрагментированных пакетов создает множество проблем и препятствует нормальной работе сети. Теоретически возможно блокировать лишь пакеты с фрагментированным TCP-заголовком, однако, это далеко не всякий брандмауэр поддерживает столь гибкую политику настройки. Атаки данного типа, кстати говоря, называемые Tiny Fragment Attack, обладают чрезвычайно мощной проникающей способностью и потому являются излюбленным приемом всех хакеров.

Рисунок 6 фрагментация TCP-пакетов как способ обхода брандмауэров

Атаки с использованием внутренней маршрутизации (она же маршрутизация от источника или source routing) намного менее актуальны, тем не менее мы все же их рассмотрим. Как известно IP-протокол позволяет включать в пакет информацию о маршрутизации. При отправке IP-пакета жертве, навязанная хакером маршрутизация чаще всего игнорируется и траектория перемещения пакета определяется исключительно промежуточными маршрутизаторами, но ответные пакеты возвращаются по маршруту обратному, указанному в IP-заголовке, что создает благоприятные условия для его подмены. Более упрощенный варит атаки ограничивается одной лишь подменой IP-адреса отправителя, посылая пакет от имени одного их внутренних узлов. Грамотно настроенные маршрутизаторы (и большинство клонов

UNIX) блокируют пакеты с внутренней маршрутизацией. Пакеты с поддельными IP-адресами представляют несколько большую проблему, однако, качественный брандмауэр позволяет отсеивать и их.

Таблицы маршрутизации могут быть динамически изменены посылкой сообщения ICMP Redirect, позволяя (по крайней мере теоретически) направить хакерский трафик в обход брандмауэра (см. так же ARP spoofing), однако, в реальной жизни такие безнадежно инсекьюрные системы практически никогда не встречаются, во всяком случае сейчас.

побег из-за брандмауэра

Пользователи внутренней сети, огражденной по периметру недемократичным брандмауэром, серьезно ограничены в своих возможностях (про невозможность работы с FTP-серверами в активном режиме мы уже говорили). Так же могут быть запрещены некоторые протоколы и закрыты необходимые вам порты. В клинических случаях администраторы ведут списки "черных" IP-адресов, блокируя доступ к сайтам "нецелесообразной" тематики.

Поскольку брандмауэры рассчитаны на защиту извне, а не изнутри, вырваться из-за их застенков очень просто, достаточно лишь воспользоваться любым подходящим Proxy-сервером, находящимся во внешней сети и еще не занесенным администратором в "черный список". В частности, популярный клиент ICQ позволяет обмениваться сообщениями не напрямую, а через сервер (не обязательно сервер компании-разработчика). Существуют тысячи серверов, поддерживающих работу ICQ. Одни существуют в более или менее неизменном виде уже несколько лет, другие динамически то появляются, то исчезают. И если "долгожителей" еще реально занести в стоп-лист, то уследить за серверами-однодневками администратор просто не в состоянии!

Так же, вы можете воспользоваться протоколом SSH (Secure Shell), изначально спроектированным для работы через брандмауэр и поддерживающим шифрование трафика (на тот случай, если брандмауэр вздумает искать в нем "запрещенные" слова типа "sex", "hack" и т.д.). SSH-протокол может работать по любому доступному порту, например, 80, и тогда с точки зрения брандмауэра все будет выглядеть как легальная работа с WEB-сервером. Между тем, SSH является лишь фундаментом для остальных протоколов, из которых в первую очередь хотелось бы отметить протокол telnet, обеспечивающий взаимодействие с удаленными терминалами. Заплатив порядка 20$ за хостиг любому провайдеру вы получите аккаунт, поддерживающий SSH и позволяющий устанавливать соединения с другими узлами сети (бесплатные хостинги этой возможности чаще всего лишены или накладывают на нее жесткие ограничения).

Наконец, можно воспользоваться сотовой телефонией, прямым модемным подключением и прочими коммуникационными средствами, устанавливающих соединение с провайдером, в обход брандмауэра.

>>>> ссылки по теме

nmap

Популярный сканер портов, позволяющий обнаруживать некоторые типы брандмауэров. Бесплатен. Исходные тексты доступны. На сайте море технической информации по проблеме. http://www.insecure.org/nmap/

FireWalk

Утилита для трассировки сети через брандмауэр, работающая на TCP/UDP протоколах и основанная на TTL. Бесплатна. http://www.packetfactory.net/firewalk. Перед использованием рекомендуется ознакомится с документацией http://www.packetfactory.net/firewalk/firewalk-final.pdf.

HPING

Утилита, реализующая сканирование через немой хост. Мощное оружие для исследования внутренней сети по-за брандмауэром. Бесплатна и хорошо документирована http://www.hping.org/papers.html

SSH-клиент

Secure Shell клиент, используемый пользователями внутренней сети для преодоления запретов и ограничений, наложенных брандмауэром. Бесплатен. Распространяется вместе с исходными текстами. http://www.openssh.com.

Fuck You

Подробный FAQ по брандмауэрам английском языке www.interhack.net/pubs/fwfaq/firewalls-faq.pdf. Его русский перевод, не отличающейся особой свежестью, лежит на ln.com.ua/~openxs/articles/fwfaq.html.

Firewalls

Конспект лекций по брандмауэрам от тайваньского профессора Yeali S. Sun (на английском языке). http://www.im.ntu.edu.tw/~sunny/pdf/IS/Firewall.pdf

OpenNet

Огромный портал по сетевой безопасности, содержащей в том числе и информацию о дырах в популярных брандмауэрах (на русском и английском языке) http://www.opennet.ru

заключение

Технологии построения брандмауэров не стоят на месте и специалисты по информационной безопасности не дремлют. С каждым днем хакерствовать становится все труднее и труднее, однако, полностью хакерство не исчезнет никогда. Ведь на смену заткнутым дырам приходят другие. Главное – не сидеть сложа руки, а творчески экспериментировать с брандмауэрами, изучать стандарты и спецификации, изучать дизассемблерные листинги и искать, искать и еще раз искать…

>>>> *вноски*

- брандмауэры подвержены большому количеству DoS атак, таких, например как, эхо-шторм или SYN-flood, которым они в принципе неспособны противостоять;
- брандмауэр это – маршрутизатор, проски-север и система обнаружения вторжений в одном флаконе;
- брандмауэры не защищают от атак, а лишь ограждают локальную сеть кирпичным забором, через который легко перелезть;
- в большинстве случаев через кирпичную стену брандмауэра можно пробить ICMP-тоннель, обернув передаваемые данные ICMP-заголовком;
- брандмауэр можно атаковать не только извне, но и изнутри корпоративной сети;
- различные брандмауэры по разному реагируют на нестандартные TCP-пакеты, позволяя идентифицировать себя;
- брандмаузеры, открывающие 53 порт (служба DNS) не только на приемнике (например, Check Point Firewall), но и на источнике, позволяют хакеру просканировать всю внутреннею сеть;
- уязвимость программных прокси в общем случае невелика и в основном они атакуются через ошибки переполнения буфера;
- некоторые брандмауэры подвержены несанкционированному просмотру файлов через порт 8010 и запросы типа http://www.host.com::8010/c:/ или http://www.host.com::8010//
- служба DCOM нуждается в широком диапазоне открытых портов, что существенно снижает степень защищенности системы, обессмысливая брандмауэр.