обход IDS

крис касперски ака мыщъх (серый, пещерный), ака mezumi, aka souriz, aka elraton, no email

> **за несколько прошедших лет системы обнаружения вторжений выросли из ясельного возраста и уже не бьют хакеров совочком по голове, а мочат их вовсю, вцепляясь мертвой хваткой, словно трехглавый пес цербер. количество IDS все растет и уже шагу нельзя ступить, чтобы не вляпаться в какой-нибудь кал, и если мы не научимся летать ниже радаров, нас просто превратят в shit. как и любая другая сущность IDS имеет свои слабости, знание которых позволяет ее обходить**

введение или добро пожаловать в ад

Не так страшен черт, как его малюют, тем более, что попасть в его лапы не так-то просто, поскольку все подступы к аду контролирует злобный мифический (но от этого ничуть не менее кусючий) трехглавый пес Цербер, по научному называемый "системой обнаружения вторжений". Она же — Intrusion Detection System или, сокращенно, IDS.

В отличии от брандмауэров, наглухо закрывающих порты, чем и предотвращающих возможность атаки (ну, "предотвращающих" — это в идеале), IDS пытается распознать сам _факт_ атаки. Но, успешные атаки, как известно, не распознаются, поэтому, правильнее говорить о распознавании _попыток_ атаки.

Системы обнаружения вторжений распознают и отсекают (точнее, пресекают) большинство актов вандализма, захлестнувших Сеть в последнее время, когда любой мальчик, еще даже не трахавшийся, уже качает очередной сканер безопасности или нюкер и начинает типа атаковать. Такие "типа атаки" составляют свыше 99% от всех якобы зафиксированных атак на Пентагон, Мелкософт и другой ширпотреб, нанимающих мальчиков типа экспертов по безопасности. Такие с понтом "типа эксперты" в своей массе просто смотрят в лог IDS, и бьются в экстазе от радости, видя сколько мега-хакеров было остановлено на пути к информационной крепости. А что! Сканирование портов — это уже атака, а перебор параметров cgi-скриптов это вообще… Нет, ну чисто вообще конкретно! Какая хорошая IDS, без нее нам трынденц. Мысль о том, что правильно настроенная и заштопанная ось способа справиться с SYN/PING/UDP флудом и сама, просто не приходим им в голову, но зато создает вескую мотивацию, оправдывающую их килобаксовую зарплату. Встречаются, конечно, и нормальные администраторы, но мало… очень мало. И большинство из них не использует IDS, поскольку это кал и вообще на фиг.

Настоящего хакера, целенаправленно атакующего сервер через только ему одному известную ошибку переполнения, IDS не только не остановит, но даже не обнаружит. Кроме того, во многих случаях IDS сама может выступать объектом атаки, поэтому ее присутствие не только не усиливает безопасность, но даже ослабляет ее! (во всяком случае — потенциально. удаленных дыр в IDS зафиксировано мало, поскольку в них практически никто не ковырялся). К тому же, ошибочно распознанные атаки (процент которых достаточно велик) вкупе с активными действиями, предпринятыми со стороны IDS против "хакера", создают у легальных пользователей бааальшие проблемы, что не есть хорошо.

Но здесь мы не дискутируем "за" и "против" IDS, поскольку воздействовать на политику безопасности атакуемого сервера, хакер может только своим хвостом и головой, но никак не пропагандой против IDS (исключение составляют случаи, когда хакер атакует сервера своей же собственной компании и не хочет, чтобы каждый его шаг попадал в лог).

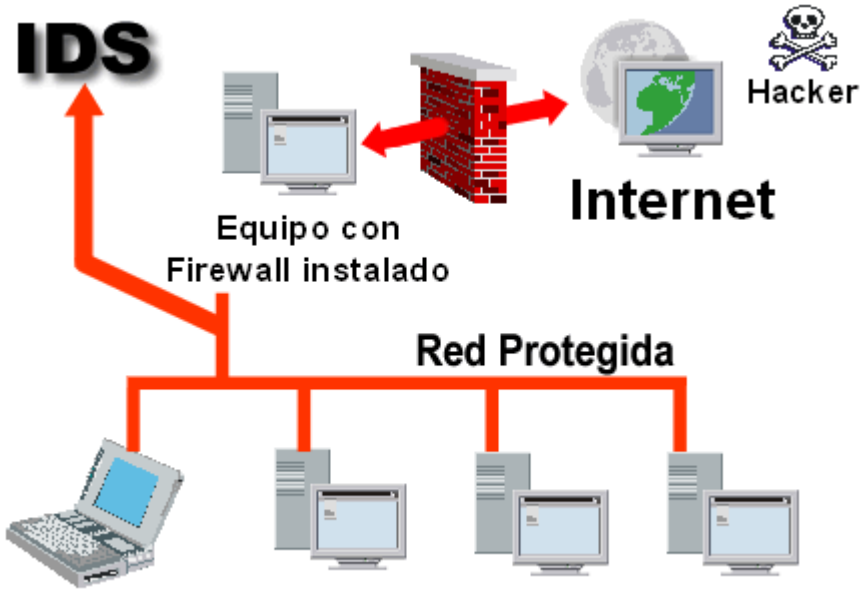

Рисунок 1 система обнаружения вторжений, ведущая мониторинг сетевой активности вверенных ей узлов

типы IDS

Развелось тут… Типов короче… Это раньше все было просто, сейчас же — хрен поймешь! По сектору охвата IDS делятся (условно) на сетевые и локальные. Сетевая IDS устанавливается на отдельном узле, контролирующим целую подсеть, и зачастую является аппаратным решением (т. е. "ящиком" в который вмонтирован процессор, память, сетевые адаптеры, встроенная операционная система, под которой вращается IDS). Сетевая IDS может располагаться как между внешней и внутренней сетью (наиболее типичная конфигурация), так и представлять отдельный узел внутри локальной сети, что (естественно) уменьшает возможности ее воздействия на атакующего, упрощает хакеру задачу распознания наличия IDS и ее обход.

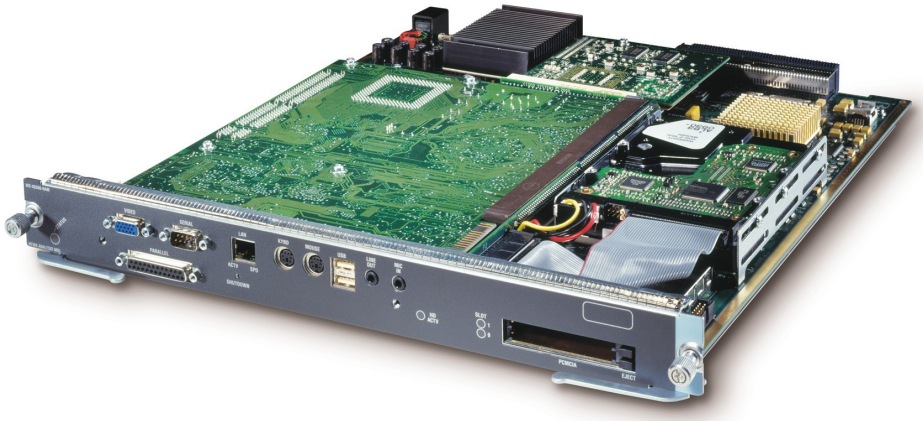

Рисунок 2 аппаратный IDS модуль для марштуизатора CISCO Catalyst 6000 Series

Локальные IDS устанавливаются непосредственно на тот узел, который они охраняют, и такие IDS часто являются частью персонального брандмауэра или антивируса. Разработчики ПО любят подобные комплексные решения, стремясь запихать в одну коробку как можно больше софта, но администраторы (я имею ввиду _нормальные_ администраторы) только морщатся при виде подобных "швейцарских ножей". Специализированные решения всегда имеют массу преимуществ перед универсальными, предъявляя при этом значительно меньше требования к аппаратным ресурсам, но… кого это вообще интересует?

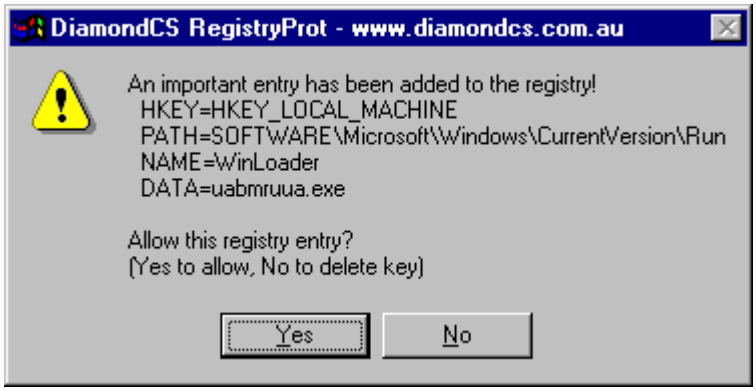

Рисунок 3 локальные IDS, обычно входящие в состав персональных брандмауэров и антивирусов, не только следят за сетевой активностью, но так же могут контролировать некоторые жизненно важные ветви реестра, выдавая предупреждение при попытке их изменения

По "следственным" методам IDS делятся на пассивные и активные. Пассивные ограничиваются мониторингом сетевой активности, записывая в лог подозрительные действия или явно выявленные атаки. Практически все IDS поддерживают гибко настраиваемую степень детализации лога (чем детальнее лог, тем больше информации он несет о сетевой активности, но тем труднее в нем вылавливать _реальные_ попытки атаки, к тому же большинство IDS кидают

всю информацию в один лог, устроенный по принципу кольцевого списка, что позволяет атакующему уничтожить следы атаки "тупыми" попытками проникновения типа сканирования портов, затирающих всю остальную информацию). Так же, практически все IDS предусматривают возможность оповещения администратора через почту, SMS или другие средства коммуникации, однако, далеко не каждый администратор спешит воспользоваться ими. Вот ему радость просыпаться от звонка сотового, радостного объявляющего об очередной выявленной псевдо-атаке!

Активные IDS не только собирают улики, но и предпринимают ответные действия против атакующего, пока администратор инсталлирует телку на топчан (сотовый как вибратор?! хм, оригинально!). Какие же это действия? Ну, например, занесение хакерского IP в black-лист до снятия его администратором или на некоторое время (скажем, шесть минут или целый час). Учитывая достаточно большое число ложных срабатывай, и частоту (не)посещения работы администратором, становится ясно, что "бан до помилования" отсекает большое количество честных пользователей и даже целые подсети, сам по себе являясь нехилой DoS атакой (а вы все черви, вирусы блин. установите себе активную IDS и почувствуйте насколько она круче всех их вместе взятых!). Менее жесткая мерка — посылка IDS'ом ответного TCP-пакета, инициирующего разрыв соединения (не работает с UDP и "сырыми" IP-пакетами, так же не работает против атак на переполняющиеся буфера и реально лишь ограничивает активность флудеров, да и то…)

архитектура и принципы работы IDS

Сетевая IDS конструктивно состоит из "сенсоров", собирающих информацию о сетевой активности (обычно, грабящих весь трафик), базы данных, описывающей известные типы атак, и "мозгов" которые все это обрабатывают. Начнем с сенсоров. Если IDS расположена между внешней и внутренней сетью (например, наглухо встроена в маршрутизатор), то она просто "хватает" трафик, физически проходящий через нее и с точки зрения хакера все выглядит так, как будто никакой IDS тут нет.

А вот если IDS расположена внутри сети, то единственный путь сбора информации — это перевод сетевой карты в "неразборчивый" режим и такая IDS элементарно обнаруживается, поскольку превращается в обыкновенный сниффер, методики выявления которых подробно рассмотрены в мыщъх'иной статье "рыбная ловля в локальной сети – sniffering", ранее опубликованной в "хакере". Так чего же повторяться? Достаточно отметить, что для обнаружения sniffer'a (которым в данном случае является IDS) хакеру уже необходимо находится внутри локальной сети, чтобы посылать ARP-запросы и делать другие дела. Извне сети, имя под хвостом один лишь TCP/IP, выявить sniffer'a очень сложно, а еще сложнее остаться при этом незамеченным и не привлечь к себе внимания IDS.

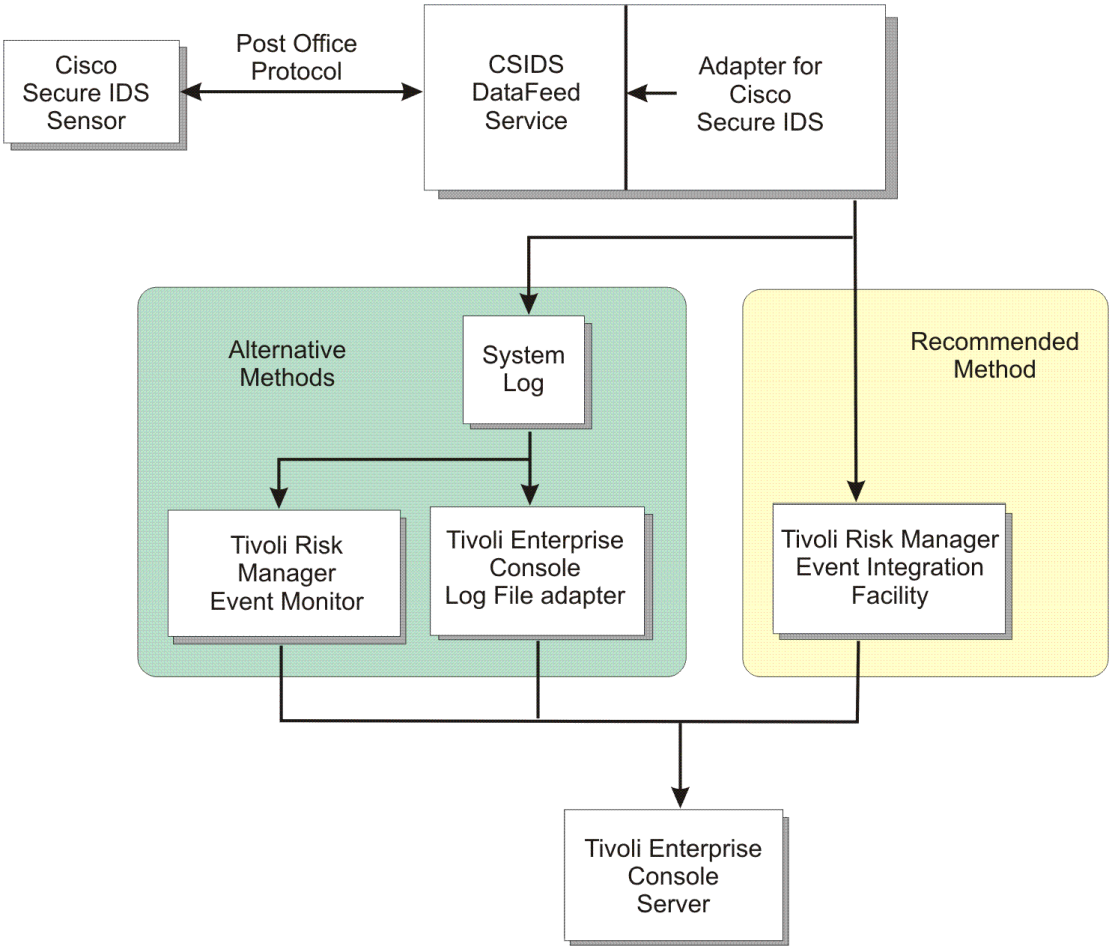

Рисунок 4 блок-схема аппаратного модуля обнаружения вторжений для марштутизаторов CISCO

База данных обычно описывает не только модели хакерского поведения (сканирование портов, подбор строк разной длины в попытке вызывать переполнение, перебор параметров cgi и т. д.), но так же содержит сигнатуры всех известных вирусов/червей и, — что самое главное, — сведения о всех дырах! То есть это что получается?! Допустим, внутри локальной сети находится не залатанный Microsoft IIS с ошибкой переполнения. Хакер разрабатывает свой собственный shell-код (сигнатура которого еще _никому_ не известна и который нельзя выявить эвристическими методами) и отправляет его серверу. Но! Между хакером и сервером находится IDS (установленная, например, на одном из промежуточных марштутизаторов, возможно, даже и не принадлежащем компании, чей сервер хакер хочет атаковать). IDS не знает, что делает этот shell-код, но видя, что он направляется прямо в дыру, говорит "ага!" и разрывает соединение (ставит хакеру бан). Вот так облом! Тупой администратор может не латать дырявый сервер годами, но если он подключен к правильному провайдеру и этот провайдер имеет правильную IDS, то задача атаки резко усложняется. Самое простое, но не самое правильное, что может предпринять хакер в этом случае — послать кому-нибудь из сотрудников атакуемой ограничении письмо с вложением (что находится во вложении объяснять, надеюсь, не надо?!), заманить их на web-сервер со страничкой, использующей одну из дыр в IE/FireFox'е ну и т. д. Короче захватить сеть изнутри.

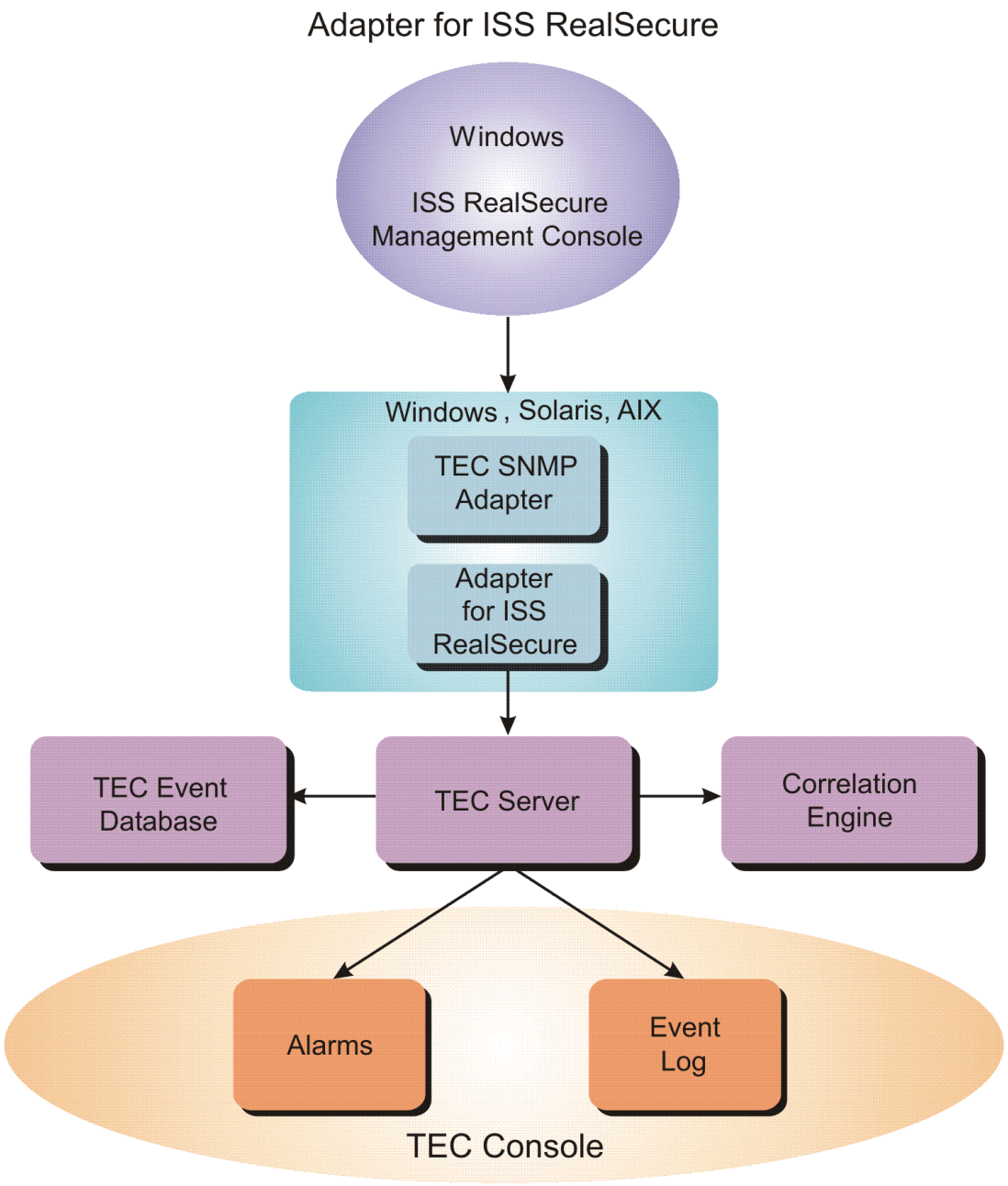

Рисунок 5 блок-схема системы обнаружения вторжений RealSecure от корпорации ISS

"Мозги", обрабатывающие всю информацию, далеко не всегда берутся с запасом и при интенсивном трафике время распознавания атаки резко возрастает! Некоторые IDS распознают атаку спустя пять и более минут от ее начала. Для разборок со флудом этого, обычно, оказывается вполне достаточно, но вот против ошибок переполнения тут уже сильно не повоюешь. За эти пять минут хакер вполне успевает овладеть сервером, установить rootkit последнего поколения, утащить массу конфиденциальных данных… Вот и лови его потом! А что?! Все логично. Обработка трафика требует времени и если пакеты сыплются как из ведра, то IDS начинает отчаянно буксовать. Хорошо если она вообще не выкидывает пакеты, которые не успевает анализировать — тогда атака вообще не будет обнаружена (не говоря уже о каком бы то ни было противодействии атакующему).

Локальные IDS ведут себя несколько не так и "задерживают" пакеты вплоть до полного выяснения личности. Однако, смысла в них немного. Если администратор (или пользователь рабочей станции) не устанавливает заплатки, то, с какой это радости он будет обновлять базу IDS?! А без базы IDS распознает только тупые акты вандализма, о которых мы уже говорили, но никак не целенаправленную атаку на переполнение!

Поэтому, дальше мы будет говорить исключительно про сетевые IDS, как представляющие наибольшую опасность для хакера.

методы обхода IDS

Никаких сканирований портов! Никаких сканеров безопасности! Никакой другой дури!!! Ясно?! Наслушались тут советов на форумах, мать! Как это так — не сканировать? Ведь это же главная разведывательная операция перед началом каждой атаки! Ну… во-первых, далеко не каждой. Если известно, что на узле стоит web-сервер, в котором (возможно) есть дыра, так зачем остальные порты сканировать?!

Собственно говоря, сканирование преследует цель получить перечень служб, установленных на сервере (в идеале — с определением их типа и версий), затем среди них ищутся уязвимые и атака переходит во вторую стадию. Распространенные утилиты по умолчанию сканируют порты достаточно агрессивно, причем с одного и того же IP-адреса. А факт сканирования распознается элементарно — по приходу пакетов, направленных на закрытые порты. При превышении определенного порога агрессивности сканирования (кол-во пакетов в ед. времени) IDS сигнализирует об атаке и, зачастую, блокирует этот IP на хрен, создавая иллюзию, что все остальные порты закрытые.

Неагрессивное сканирование, к сожалению, занимает слишком много времени (в среднем — несколько суток), но и в этом случае с большой степенью вероятности оно обнаруживаются. Выход — менять IP с каждым посылаемым пакетом. Для этого хорошо подходит методика сканирования с использованием молчаливого хвоста, поддерживаемая продвинутыми сканерами, в том числе и nmap, либо подогнать армию "дронов" (чужих компьютеров с внедренным back-door'ом) и сказать ей "фас!". Здесь агрессивность сканирования уже не играет никакой роли, поскольку, каждый порт сканируется с нового IP, адрес которого IDS предвидеть не может, а потому не может и заблокировать. Чисто теоретически, обнаружив атаку, администратор способен (технически) заблокировать все ресурсы, перерезать сетевой кабель, забаррикадировать дверь и выключить сервер, но… сканирование портов в реальности происходит так часто, что на него просто перестают обращать внимание.

Обойти сигнатурную защиту сложнее, но все-таки возможно! Прежде всего, не стоит использовать никаких готовых (и широко известных) shell-кодов, rootkit'ов и прочей хрени, особенно не полиморфной. IDS заматериться так, что админ с секретаршей превратятся в сиамских близнецов (с женщинами от перепугу это часто случается). Это уже не просто подозрение в атаке, это 100% _попытка_ атаки (неважно — успешная она или нет). Даже если атака действительно окажется успешной (сервер не латанный), и IDS "проснется" задолго после того, как rootkit будет установлен (для этого атаку проводить лучше в rush hours или, по нашему, в часы пик, когда сервер максимально загружен и через IDS несется лавина честного трафика), админ, поднятый по тревоге, либо обнаружит rootkit (если он не лох), либо просто возьмет бэкап и сделает откат к заведомо "стерильной" конфигурации. Либо же переустановит всю систему с нуля (лох полный и окончательный). Шансы на выживание у хакера минимальны, так что не стоит действовать по принципу: кинул back-door, а если все тихо через неделю решил его заюзать. Опытный хакер юзает сервер сразу и причем набирает буковки не руками, а запускает заранее разработанные программы, хакающие данные на форсаже — так быстро, как это только возможно.

Достаточно многие атакующие прибегают к следующей уловке: они устанавливают два rootkit'а. Один из которых простой как точка, находящаяся на пересечении двух прямых (женских ног) и легко обнаруживаемый даже лохом, ну то есть, явная подстава. А второй — по настоящему хорошо замаскированный и очень-очень трудно обнаруживаемый. Есть шанс, что обнаружив и удалив первый rootkit, админ успокоится и больше не будет предпринимать никаких действий, считая, что хакер уже раздавлен.

Но мы, похоже, отклонились от темы статьи, озаглавленной "как обойти IDS", а не как зачморить админа. Так, методы воздействия на саму IDS мы откинем, поскольку они практически не изменились со времен атак на первых, еще доисторических брандмауэров (хинт: практически всякая IDS поддерживает функции удаленного управления и конфигурирования, но далеко не всякий админ спешит тут же изменить пароль, установленный производителем по умолчанию или меняет его на что-то простое и легко предсказуемое. спрашиваете как распознать IDS и определить ее версию? а все через тоже сканирование портов, поскольку большинство IDS реализуют удаленное управление именно через TCP/UDP порты, обычно доступные извне сети — ну какой админ откажется от возможности контроля за IDS из своего дома — но при этом зачастую частично закрытые брандмауэром так, что "прямое" сканирование

ничего не дает, но попытка подключения тем не менее проходит успешно. номер(а) портов однозначно идентифицируют IDS, а во многих случаях она сама выписывает свое имя/версию в окно telnet или web-панель).

Еще несколько лет назад, большинство IDS распознавало только две формы запроса к HTTP-серверам: UTF и HEX. Обе стандартные. При этом сами серверы (и, в частности, MS IIS) поддерживают нестандартный Unicode/Wide-формат (типа %u), что позволило хакерам и червям (среди которых числится и нашумевший CodeRed) легко обходить IDS, стоящие на магистральных каналах, со всеми, вытекающими отсюда последствиями — миллионы не патченных серверов захачились по всему миру, вызвав переполох и слухи о близком конце света, тьфу, Интернета. Конец же, как выяснилось, находился в другом кармане и в очередной раз был перенесен на неопределенный срок. Тем временем, разработчики IDS поняли свою ошибку, и поддержали Unicode/Wide-формат по полной программе. Однако, куча аппаратных IDS так и осталась не обновленной и совершенно неосведомленной ни о каких там %u.

А Windows Vista это вообще прелесть! Настоящий подарок для хакеров! Прозрачная (читай "принудительная") поддержка протокола IPv6 в сетях, разделенных между собой IPv4, осуществляется за счет инкапсуляции IPv6 в IPv4/UDP, о котором существующие IDS не в курсе. То есть, если у жертвы стоит Windows Vista или Server Longhorn, подключенный к Инетернет-каналу по IPv4 (а IPv6 в народ еще не пришел), хакер может свободно посылать Pv6 пакеты, инкапсулированные в UDP (для этого ему так же придется установить у себя висту). С точки зрения IDS все будет OK, никакой известной ей сигнатуры она не увидит, пока не "догадается" распотрошить инкапсулированный UDP и посмотреть, что у него там внутри. А с учетом того, что виста допускает вложенную инкапсуляцию, распознать атаку сможет только слишком умная IDS и притом обновленная. Понятное дело, что разработчики IDS не сидят сложна руки, а висту себе ставят в основном геймеры, но никаких не серьезные предприятия, то неизвестно, что произойдет быстрее — массовая миграция на висту или обновление IDS. Тем не менее, у хакеров есть отличный шанс показать всему миру свой огромный серый хвост ну… или, если не сам хвост, то по крайней мере ту штуку, что находится под ним.

заключение

И все-таки, что же такое IDS? Чучело филина или зубастый цербер? Смотря для кого. Для слона например, что моська, что цербер — все едино, а для мыша и филин угроза. Правильно настроенная IDS хорошо справляется с "пионерскими" атаками, отекая всяких там флудеров и куль-хацкеров с exploit'ом вместо головы. Хакеры, ведущие поиск дыр самостоятельно, присутствие IDS просто не замечают, как IDS не замечает неизвестную атаку.

Короче — задача обхода IDS в общем случае сводится к тому, чтобы их не обходить, а двигаться своим путем по заранее намеченному маршруту сквозь тернии, избегая протоптанных дорог и магистралей.

Рисунок 6 системы обнаружения вторжений хватают начинающих хакеров и мотают их как трехглавый пес цербер, но опытные хакеры обходят его со стороны хвоста так, что он их просто не замечает

>>> врезка самые популярные

Среди множества IDS имеющихся на рынке, наибольшей популярностью пользуются следующие продукты: Cisco Secure IDS, ISS RealSecure, Enterasys IDS Dragon, CA eTrust Intrusion Detection Engine и Intrusion.com SecureNet PDS. Некоммерческих IDS просто море, но в большинстве своем они годятся лишь для решения ограниченного круга задач и за пределы локальных сеток не выходят. На магистральных канал они просто загнуться (особенно, это касается IDS, написанных на скриптовых языках) и тут без аппаратных решений уже не обойтись!

>>> врезка что читать

Подробнее об устройстве и методах, применяемых системами обнаружения вторжений для распознавания нарушителей, можно узнать из следующих книг, купив (купив?!) их по кредитке или скачав в парнокопытном:

- **Cisco Security Professional's Guide to Secure Intrusion Detection Systems**:
  - http://www.bookpool.com/sm/1932266690
- **Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems:**
  - http://www.amazon.com/gp/product/customer-reviews/0735712328;
- **Cisco Secure Intrusion Detection System**:
  - http://www.amazon.ca/gp/product/158705034X/ref=olp_product_details/701-5759191-0599541?ie=UTF8&seller=