УДК 004.681

Чернышев А.Н.

ПРОТИВОДЕЙСТВИЕ СЕТЕВЫМ АТАКАМ

Одной из движущих сил и главным объектом всех отраслей современной человеческой деятельности становится информация, и состояние каналов, сетей и безопасность серверов становятся основой экономического развития. Сложные сетевые технологии достаточно уязвимы для целенаправленных атак. Причем такие атаки могут производиться удаленно, в том числе и из-за пределов государства. Все это ставит новые проблемы перед разработчиками и строителями информационной инфраструктуры. Современные формы бизнеса в основном базируются на сетевых технологиях, а некоторые из них полностью зависимы от сетей (электронная торговля, IP-телефония, сетевое провайдерство и т.д.) и по этой причине особенно уязвимы. Производится модифицирование с учетом требований безопасности некоторых протоколов и программ.

Постоянно растет число ЭВМ, подключенных в Интернет. Сегодня трудно представить себе фирму, организацию или учреждение, где бы для обработки документов, ведения бухгалтерии, учета, обмена сообщениями, доступа к информационным и поисковым серверам и так далее не использовали машин, подключенных к сети. Но преимущества доступа к информации через сеть все чаще омрачается атаками вирусов, червей, троянских коней, spyware и хакеров.

Рассмотрим некоторые наиболее опасные виды сетевых атак. Некоторые классы атак, например, использующие переполнение буферов, являются составной частью многих видов вредоносных атак. Одна из наиболее опасных разновидностей предполагает ввод в диалоговое окно помимо текста присоединенного к нему исполняемого кода, что может привести к записи этого кода поверх исполняемой программы и его исполнение.

Вирусы - вредоносные программы, способные к самокопированию и к саморассылке.

Phishing - получение паролей, PIN-кодов и пр. (последующая кража информации). Этот вид атаки начинается с рассылки почтовых сообщений, содержащих ссылку на известный ресурс (или имитирующий такую ссылку).

Троянский конь (Spyware) - программа, записывающая все нажатия клавиш на терминале или мышке, способна записывать screenshot'ы и передавать эти данные удаленному хозяину. Если на ЭВМ оказался установленным общеизвестный троянский конь, машина становится уязвимой. Именно с этим связано сканирование хакерами номеров портов известных троянских коней.

SPAM составляет до 90% полного объема почтовых сообщений. Сопряжено это с тем, что рассылка SPAM стала достаточно доходной частью полукриминального бизнеса.

Не менее опасны такие сетевые атаки как: угадывание паролей, репликационный код, взлом паролей, использование известных уязвимых мест, отключение/обход систем аудита, back doors (специальные входы в программу, возникающие из-за ошибок при ее написании или оставленные программистами для отладки), использование снифферов и sweepers (систем контроля содержимого), использование программ диагностики сети для получения необходимых данных, использование автоматизированных сканеров уязвимостей, подмена данных в IP-пакетах, атаки типа "отказ в обслуживании" (DoS), атаки на Web-серверы (CGI-скрипты), технологии скрытого сканирования, распределенные средства атаки.

Наибольшую долю рынка информационной безопасности составляют межсетевые экраны, системы обнаружения атак (Intrusion Detection Systems - IDS) и антивирусные системы. Однако эти средства перестают удовлетворять современным требованиям, предъявляемым к защитным системам. IDS всего лишь обнаруживают компьютерные атаки.

Существуют две технологии обнаружения атак: технология сигнатурного анализа и так называемая технология выявления аномальной деятельности. IDS, основанные на первой из них, обнаруживают далеко не все атаки, а лишь те, которые уже описаны в сигнатурах (образец IP-пакета данных, характерного для какой-либо определенной атаки). Иными

словами, они реагируют только на известные атаки и беззащитны перед новыми, неизвестными. Такие IDS работают по тому же принципу, что и антивирусные программы: известные вирусы ловятся, неизвестные - нет. Появление новой сигнатуры всегда обусловлено анализом механизма уже прошедшей атаки и ее воздействия на какую-либо информационную систему. Система, ориентированная на выявление новых типов атак, - это система выявления «аномального» поведения, которая отслеживает в сетевом трафике, в работе приложений и в других процессах все отклонения от нормы, контролирует частоту событий и обнаруживает статистические аномалии. Основанная на анализе поведения, такая система может остановить как известные, так и не встречавшиеся ранее виды несанкционированной деятельности. Однако и у нее есть существенный недостаток - трудности с формулировкой эффективных критериев того, что считать аномальным поведением, а что не считать.

В первую очередь в IDS используются различные способы определения несанкционированной активности. Хорошо известны проблемы, связанные с атаками через межсетевой экран (брандмауэр). Межсетевой экран разрешает или запрещает доступ к определенным сервисам (портам), но не проверяет поток информации, проходящий через открытый порт. IDS, в свою очередь, пытается обнаружить атаку на систему или на сеть в целом и предупредить об этом администратора безопасности, в то время как атакующий полагает, что он остался незамеченным.

Наиболее популярна классификация IDS по способу сбора информации об атаке: network-based, host-based, application-based. Система первого типа работает по типу сниффера, "прослушивая" трафик в сети и определяя возможные действия злоумышленников. Поиск атаки идет по принципу "от хоста до хоста". Системы второго типа, host-based,предназначены для мониторинга, детектирования и реагирования на действия злоумышленников на определенном хосте. Система, располагаясь на защищаемом хосте, проверяет и выявляет направленные против него действия. Третий тип IDS, application-based, основан на поиске проблем в определенном приложении. Существуют также гибридные IDS, представляющие собой комбинацию различных типов систем.

Общая схема функционирования IDS приведена на рис. 1. В последнее время появилось много публикаций о системах, называемых distributed IDS (dIDS). dIDS состоит из множества IDS, которые расположены в различных участках большой сети и связаны между собой и с центральным управляющим сервером. Такая система усиливает защищенность корпоративной подсети благодаря централизации информации об атаке от различных IDS. dIDS состоит из следующих подсистем: центральный анализирующий сервер, агенты сети, сервер сбора информации об атаке.

Центральный анализирующий сервер обычно состоит из базы данных и Web-сервера, что позволяет сохранять информацию об атаках и манипулировать данными с помощью удобного Web-интерфейса.

Агент сети - один из наиболее важных компонентов dIDS. Он представляет собой небольшую программу, цель которой - сообщать об атаке на центральный анализирующий сервер.

Сервер сбора информации об атаке - часть системы dIDS, логически базирующаяся на центральном анализирующем сервере. Сервер определяет параметры, по которым группируется информация, полученная от агентов сети.

Несмотря на многочисленные упреки и сомнения в работоспособности IDS, пользователи уже широко применяют как коммерческие средства, так и свободно распространяемые. Разработчики оснащают свои продукты возможностями активного реагирования на атаку. Система не только определяет, но и пытается остановить атаку, а также может провести ответное нападение на атакующего. Наиболее распространенные типы активного реагирования - прерывание сессии и переконфигурирование межсетевого экрана.

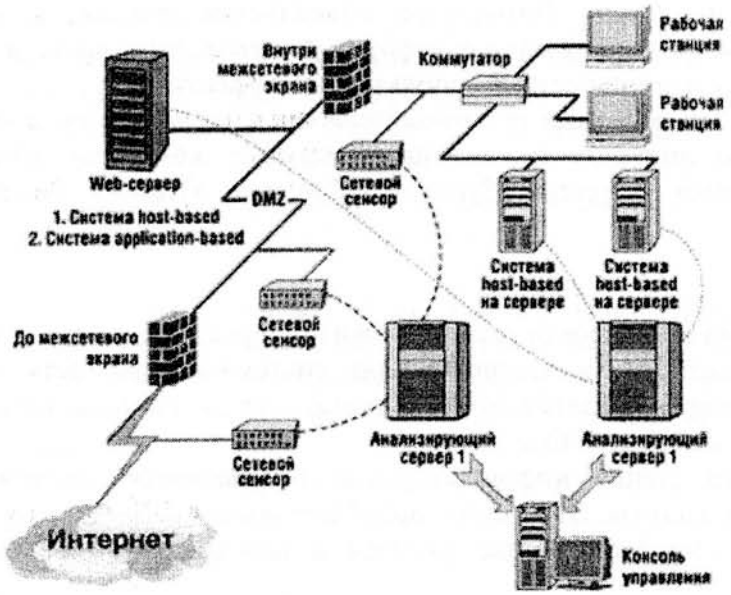

Рис. 1. Общая схема функционирования IDS.

Прерывание сессии наиболее популярно, потому что для этого не используются драйверы внешних устройств, таких, как межсетевой экран. В оба конца соединения, например, просто посылаются пакеты TCP RESET (с корректным номером sequence/acknowledgement).

Так как необходимо не только обнаружение, но и блокирование вредоносных воздействий - переход к проактивной защите. Обнаружение вторжений без противодействия нельзя считать эффективным средством защиты. Приобретая систему информационной безопасности, пользователь преследует цель гарантированно защитить свои информационные ресурсы от злонамеренных действий. Поэтому на очередном витке развития информационных технологий, сталкиваясь с постоянной эволюцией угроз и следуя пожеланиям пользователей, разработчики средств информационной защиты предложили на смену IDS системы предотвращения компьютерных атак (Intrusion Prevention Systems - IPS).

Основа функционирования IPS - интеграция IDS с межсетевыми экранами. Кроме того обязательным условием эффективной работы IPS является установка системы «в разрыв» сети. Система IPS не только определяет, но и пытается остановить атаку, и даже может провести ответное нападение на атакующего. Наиболее распространенные типы реагирования - прерывание сессии и переконфигурирование межсетевого экрана.

Сегодня IPS - уже превалирующая технология, реализованная в продуктах практически всех известных производителей средств информационной защиты. Некоторые вендоры идут дальше и пытаются дополнить системы предотвращения атак уникальными разработками.

В подходах ведущих производителей средств информационной безопасности в настоящее время доминирует принцип эшелонированной защиты. Вместо отдельных межсетевых экранов, устройств организации виртуальных частных сетей (VPN), антивирусных систем, систем обнаружения и предотвращения вторжений на рынок поставляются комплексные решения, в том числе и на программно-аппаратной основе (security appliance), интегрируемые в инфраструктуру компании для обеспечения информационной защиты на всех уровнях. Переход к объединению в одном продукте основных средств информационной защиты не только дает возможность упростить сетевую инфраструктуру, но и обеспечивает многоуровневую защиту с более эффективным управлением. Подобная интеграция позволила значительно снизить общую стоимость владения средствами защиты информации, упростить процесс установки и администрирования и в тоже время повысить уровень безопасности защищаемых

информационных ресурсов. Физическое объединение влияет, в первую очередь, на стоимость системы, поскольку одна платформа дешевле нескольких, а технические ресурсы в такой консолидированной системе используются эффективнее.

Практически все основные производители средств защиты предлагают свои решения в этом сегменте, но лидирующие позиции занимают компании Internet Security System (продуктовая линейка Proventia), Symantec (Symantec Gateway Security) и Cisco Systems (Cisco ASA 5500).

Выводы

Полная защита целостности сети возможна при реализации таких компонентов защиты: политика безопасности интрасети организации, система защиты хостов в сети, сетевой аудит, защита на основе маршрутизаторов, межсетевые экраны, системы обнаружения вторжений, план реагирования на выявленные атаки.

Тенденции на рынке информационной безопасности, стремятся к объединению различных средств защиты. Это делает подобные объединенные устройства более гибкими при внедрении в информационные системы и намного упрощает процесс установки и эксплуатации.

Одной из основных наиболее эффективных схем защиты на данном уровне развития технологий информационной безопасности, является схема, сочетающая в себе интеграцию аппаратной платформы, межсетевого экрана и системы обнаружения и предотвращения вторжений, использующей сигнатурный и поведенческий анализ.

Поступила 29.03.2007 г.

УДК 681.14

Мухин В.Е., Стретович Е.Н.

АДАПТИВНОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ

Введение

Современные компьютерные сети (КС) – разнообразная и весьма сложная совокупность устройств, телекоммуникационных технологий, программного обеспечения и высокоэффективных средств его проектирования. Развитие компьютерных информационных технологий приводит к тому, что все более критичными становятся надежность и безопасность ресурсов сетей, выполняющих сбор, накопление, обработку, передачу и хранение данных. В последнее время появились новые проблемы обеспечения безопасности компьютерных сетей, которые в значительной степени определяют эффективность создаваемых компьютерных сетей.

Реализация средств защиты информации в КС требует дополнительных аппаратных, программных и, как следствие, временных затрат на обработку информации. Повышение уровня защищенности КС вызывает рост удельного объема дополнительной (служебной) информации передаваемой и обрабатываемой в компьютерных сетях, что обуславливает снижение пропускной способности сети по передаче полезной (пользовательской) информации. С другой стороны, в общем случае оказывается, что нет необходимости поддерживать уровень защищенности КС постоянно максимально высоким. В те периоды времени, когда в сети обрабатываются менее критичные данные, вполне допустимо снизить уровень ее защищенности, что обеспечит снижение объема служебной информации и повышение пропускной способности сети по передаче пользовательских данных. Таким