М.И. Маннанов

ПРЕДОТВРАЩЕНИЕ СЕТЕВЫХ АТАК: ТЕХНОЛОГИИ И РЕШЕНИЯ

(Ферганский филиал Ташкентский университет информационных технологий, Узбекистан)

Системы предотвращения атак (IPS) сегодня очень популярны. Они объединяют целый ряд технологий безопасности и достаточно далеко шагнули от своих предков - систем обнаружения вторжений. Тем не менее, некоторые аналитики критикуют IPS за объективные недостатки и даже предсказывают скорую смерть таких систем. Рассмотрению современных технологий предотвращения атак, анализу их сильных и слабых сторон, а также перспектив их существования посвящена данная статья

Раньше было всего два класса защитных средств, устанавливаемых на периметре, - межсетевые экраны (firewall) и системы обнаружения вторжений (IDS). Межсетевые экраны (далее МСЭ) пропускали трафик через себя, но не "заглядывали" внутрь пересыла емых данных, фокусируясь только на заголовке IP-пакета. Системы IDS (Intrusion Detection System), напротив, анализировали то, что упускалось из виду межсетевыми экранами, но не были способны блокировать атаки, так как трафик через них не проходил. Поэтому на стыке двух технологий родился новый класс защитных средств - системы предотвращения вторжений (IPS).

Четыре к одному

Современные системы IPS развивались в нескольких направлениях. Некоторые производители развили имеющиеся у них IDS, оснастив их гораздо более эффективными механизмами предотвращения атак. Например, в системах IDS использовалась простая посылка TCP-пакетов с флагом RST или реконфигурация МСЭ и сетевого оборудования. Эффективность этой "защиты" для классических IDS составляет всего около 30% - ведь трафик через устройство не проходит и о реагировании в реальном времени говорить не приходится (существует хоть и минимальная, но задержка). Однако было найдено простое решение: поместить систему IDS между защищаемыми и незащищаемыми ресурсами (весь трафик между ними проходит через IDS). Так появились системы под названием inline-IDS, позже переименованные в IPS. По этому пути пошли компании ISS, Cisco, NFR и Sourcefire.

Варианты внедрения

Обычно при упоминании систем IPS в голову приходят выделенные устройства, которые могут быть установлены на периметре корпоративной сети и, в ряде случаев, внутри нее. Внедрение в качестве систем защиты таких аппаратных устройств (security appliance) - наиболее распространенный вариант, но далеко не единственный. Такие шлюзы безопасности, несмотря на хорошую краткосрочную и среднесрочную перспективу, в дальнейшем постепенно уйдут

в тень, и их место займут решения, интегрированные в инфраструктуру, что гораздо эффективнее со многих точек зрения.

Во-первых, стоимость интегрированного решения ниже стоимости автономного (stand-alone) устройства. Во-вторых, ниже и стоимость внедрения (финансовая и временная) такого решения - можно не менять топологию сети. В-третьих, надежность выше, так как в цепочке прохождения трафика отсутствует дополнительное звено, подверженное отказам. Наконец, в-четвертых, интегрированные решения предоставляют более высокий уровень защиты за счет более тесного взаимодействия с защищаемыми ресурсами.

Для решения этой проблемы применяются системы корреляции событий, которые в состоянии определить, что скрывается за атаку емыми IP-адресами, и сделать вывод, подвержена ли цель такой атаке. Если нет, то событием можно пренебречь и оставить его <на потом>. Однако, чтобы принять решение о реальности атаки, необходимо знать, какие ОС и ПО установлены на атакуемом узле. Если, например, червь SQL Slammer атакует Linux-сервер, то последнему ничего не угрожает, так как SQL Slammer наносит ущерб только серверам с СУБД MS SQL Server без соответствующих заплаток. Информация о ПО и ОС может быть добыта двумя путями (ручное задание этих параметров для всех атакуемых узлов вряд ли можно рассматривать как перспективный способ). Например, с помощью дистанционного сканирования и получения необходимой информации от самого атакуемого узла. Этот способ наиболее прост в реализации - достаточно просканировать сеть и связать информацию об атаках с конкретными версиями ОС, ПО и уязвимостями (это и есть процесс корреляции). Однако у данного метода есть серьезное ограничение - системы корреляции стоят немалых денег.

Решение указанной проблемы заключается в использовании облегченных и интегрированных в системы предотвращения атак подсистем корреляции. Такая система регулярно проводит сканирование сети и запоминает состояние составляющих ее узлов. В момент атаки происходит связывание сведений об атаке с информацией об атакуемом узле. Если связь есть, то атака не ложная; если связь не обнаружена, то приоритет атаки снижается и администратор не тратит на нее время и энергию. Этот способ отсеивания ложных срабатываний появился недавно и пока не получил широкого распространения. В принципе, установленная на узле система персональной защиты (например, HIPS) сама сигнализирует сетевому сенсору, какая атака может нанести ущерб, а какая нет.

Мы рассмотрели современные технологии и решения в области предотвращения сетевых атак. Из обзора становится понятно, что до предрекаемой смерти систем IPS еще очень много времени. Разумеется, если их развитие продолжится вместе с информационными технологиями. Сама по себе технология IPS не является панацеей, и ее эффективность зависит от грамотного применения имеющихся инструментов и их интеграции с другими защитными и сетевыми технологиями. Только в случае построения комплексной инфраструктуры защиты системы IPS будут надежным кирпичиком в неприступной стене, опоясывающей вашу организацию.