Использование брандмауэра и IDS для обнаружения и предотвращение сетевых атак

Чернышов Н.А.

Научный руководитель: Головкина М.В.

Поволжский государственный университет телекоммуникаций и информатики.

Using a firewall and IDS to detect and prevent network attacks

Chernyshov N.A.

Scientific adviser: Golovkina M.V.

Volga State University of Telecommunications and informatics.

Аннотация

Благодаря быстрому росту использования компьютеров и Интернета, человечество вступило в эпоху, где доступно огромное количество информации, которая имеет важную ценность, и которая становится доступной через Интернет. Несомненно, что такая информация делает жизнь людей более быстрой и удобной. Однако, различные вредоносные материалы, такие как вирусы, нежелательный контент и т.д., наносят большой вред не только отдельным людям, но и всему обществу.

Брандмауэры и системы обнаружения вторжений являются двумя наиболее известными и важными инструментами для обеспечения безопасности. Брандмауэр действует как первая линия обороны против сетевых атак, контролируя сетевой трафик, чтобы предотвратить

несанкционированный доступ. Хотя брандмауэры могут контролировать сетевой трафик, но на них нельзя полностью полагаться в обеспечении безопасности. Система обнаружения вторжений (IDS) уменьшает пробелы в безопасности и укрепляет безопасность сети, анализируя сетевые ресурсы на предмет аномального поведения и неправомерного использования в режиме реального времени.

Использование систем обнаружения и предотвращения вторжений (IDPS) позволяет вывести сетевую безопасность на новый уровень. В данном контексте мы рассмотрим два важных инструмента сетевой безопасности, такие как брандмауэры и системы предотвращения вторжений. Мы рассмотрим их классификацию, недостатки и важность для обеспечения сетевой безопасности.

Введение

Существует множество различных типов устройств и механизмов в области безопасности, которые обеспечивают многоуровневый подход к защите. Если злоумышленник способен обойти один уровень, другой уровень встаёт на пути защиты сети. Два наиболее популярных и значимых инструмента, используемых для защиты сетей, это межсетевые экраны и системы обнаружения вторжений. Основная функция брандмауэра - экранирование сетевого трафика для предотвращения несанкционированного доступа между компьютерными сетями.

В данной статье мы рассмотрим использование брандмауэров и систем обнаружения вторжений, а также разберёмся в архитектуре этих технологий. Мы коснёмся признаков атак и контрмер, необходимых для защиты сети от взлома. Данная работа описывает важность брандмауэра и системы обнаружения вторжений, и почему они должны быть частью плана защиты каждого администратора сетевой безопасности. Брандмауэр эффективно обеспечивает безопасность сети в организации. Мы также обсудим возможности использования брандмауэра с системой обнаружения вторжений

для обнаружения и предотвращения сетевых атак и создания безопасной архитектуры для организации, где передача файлов может быть полезной. Брандмауэры стали более важными элементами защиты, чем когда-либо для любого типа сети, в связи с большим количеством угроз сетевых атак. Они идеально разработаны для фильтрации и блокирования атак. История событий вторжения доказала, что только обнаружение недостаточно для блокирования атак злоумышленников на сети, что привело к появлению системы обнаружения и предотвращения вторжений (IDPS). IDPS не только сообщает об атаках администратору, но и мгновенно блокирует их.

Решения для обеспечения сетевой безопасности

Ко Количество пользователей Интернета растёт очень быстро благодаря его простоте использования и возможности подключения к сети. Интернет очень полезен, однако риски, связанные с ним, и вредоносные вторжения также увеличиваются каждый день. Эксплуатация компьютерных сетей становится все более распространённой, и для коммерческих организаций и частных лиц важно защитить свои данные от серьёзных угроз, направленных на кражу информации. На рынке существует множество решений по обеспечению безопасности, включая такие, как брандмауэр и система обнаружения вторжений (IDS), которые будут описаны далее.

Брандмауэр - это устройство, установленное между внутренней сетью организации и остальной сетью, предназначенное для пересылки одних пакетов и фильтрации других. Например, брандмауэр может фильтровать все входящие пакеты, предназначенные для определённого хоста или определённого сервера, такого как HTTP, или его можно использовать для отказа в доступе к определённому хосту или службе в организации.

Основная технология межсетевых экранов - это брандмауэр с фильтрацией пакетов. Пакетная фильтрация брандмауэра фильтрует на сетевом или транспортном уровне. Он обеспечивает сетевую безопасность, фильтруя сеть на основе информации, содержащейся в заголовке TCP/IP

каждого пакета. Брандмауэр проверяет эти заголовки, чтобы решить, следует ли принимать и маршрутизировать пакеты по их адресатам или отклонить пакет, отбросив их. Брандмауэр Packet-Filter - это маршрутизатор, который использует таблицу фильтрации, чтобы решить, какие пакеты должны быть отброшены.

Для работы с ИТ существует четыре основных типа IDS

- **Сетевая система обнаружения вторжений (NIDS)**

Это независимая платформа, которая идентифицирует вторжения путем анализа сетевого трафика и мониторинга нескольких хостов. Для получения доступа к сетевому трафику системы обнаружения вторжений подключаются к сетевому коммутатору, настроенному на экранирование портов, или к сетевому разветвителю. Датчики NIDS размещаются в узловых точках сети для мониторинга, обычно в демилитаризованной зоне (DMZ) или на границах сети. Датчики перехватывают весь сетевой трафик и анализируют содержимое отдельных пакетов на предмет вредоносного трафика. Примером NIDS является Snort.

- **Система обнаружения вторжений на базе хоста (HIDS)**

состоит из агента на хосте, который идентифицирует вторжения путем анализа системных вызовов, журналов приложений, модификаций файловой системы (двоичные файлы, файлы паролей), баз данных возможностей, списков контроля доступа и других действий и состояний хоста. В HIDS датчики обычно состоят из программного агента. Некоторые IDS на основе приложений также относятся к этой категории. Примером HIDS является OSSEC. Системы обнаружения вторжений могут также быть специфичными для конкретной системы, используя пользовательские инструменты. В случае физической безопасности здания, IDS определяется как система сигнализации, предназначенная для обнаружения несанкционированного проникновения.

- **Система обнаружения вторжений по периметру (PIDS)**

Обнаруживает и точно определяет местоположение попыток вторжения на периметре ограждения критических инфраструктур. PIDS использует более современную технологию волоконно-оптического кабеля, установленного на ограждении периметра. Система PIDS обнаруживает нарушения на ограждении и, если это нарушение расценено системой как попытка вторжения, включается сигнал тревоги.

Сравнение с межсетевыми экранами и идентификаторами

Хотя обе системы относятся к сетевой безопасности, система обнаружения вторжений (IDS) отличается от брандмауэра тем, что последний ищет вторжения снаружи сети, в то время как IDS следит за нарушениями безопасности как извне, так и изнутри сети.

IDS использует сетевой трафик и сигнатуры распространенных компьютерных атак для обнаружения потенциальных нарушений безопасности и оповещения операторов. Если система прерывает соединения, то она называется системой предотвращения вторжений и представляет собой другую форму межсетевого экрана прикладного уровня.

Заключение

В этой статье мы представили подробный обзор брандмауэров и систем обнаружения вторжений (IDS), а также их роли в защите корпоративных сетей. Несмотря на то, что некоторые предсказывают конец брандмауэра, его стратегическое расположение в сети делает его незаменимым инструментом для защиты сети. Надлежащие методы обеспечения безопасности требуют развертывания брандмауэров между любыми двумя сетями с различными требованиями безопасности. В данной статье иллюстрируется важность систем обнаружения вторжений (IDS) и их различных типов. IDS отслеживает хосты, изменения системы или прослушивания сетевых пакетов в поисках вредоносного содержимого. Администраторы безопасности должны рассмотреть возможность использования комбинации хост-ориентированных

и сетевых систем обнаружения вторжений, основанных на сигнатурах и аномалиях. IDS можно настроить исключительно как устройства мониторинга и обнаружения, или он может участвовать в качестве встроенного устройства и предотвращать угрозы. Его слабыми сторонами являются большое количество ложных срабатываний и усилия, необходимые для поддержания актуальности сигнатур.

Список литературы:

1. М. А. Полтавцева, "Высокопроизводительные системы обнаружения вторжений", Инфра-Инженерия, 2023 г., стр. 24-35.
2. Ю. Диогенес, Э. Озкайя, "Кибербезопасность: стратегии атак и обороны", ДМК Пресс, 2020 г., стр. 186-244.
3. K. Scarfone и P. Mell, "Руководство по системам обнаружения и предотвращения вторжений (IDPS)", Gaithersburg, MD, Специальная публикация NIST 800-94, февраль 2007 г.
4. S. Nassar, A.E. Sayed, N. Aiad, "Улучшение производительности сети с помощью параллельных брандмауэров", в Proc. 6th International Conference on Networked Computing, May 2010 г., стр. 1-5.
5. S. Ioannidisи др., "Реализация распределенного брандмауэра", в Трудах конференции ACM Computer and Communication Security (CCS), pp. 190-199, 2000.
6. W. Stallings, Криптография,принципы и практика сетевой безопасности. 4-е изд., Prentice Hall, 2005 г.
7. X. Jhang, C. Li, W. Zheng, “Intrusion Prevention System Design.” in Proc. of 4th International Conference on Computer and Information Technology, стр.386-390, сентябрь 2004 г.
8. Samrah, "Системы обнаружения вторжений; определение, необходимость и проблемы". 2003 г.
9. Firewall Technology, 0278-6648/02/$17.00 © 2002 IEEE