160 с.
2. Ощенко Игорь 1С:Предприятие. Торговля и склад для начинающих. –М.: БХВ-Петербург, 2013. – 256 с.
3. Каргина Е. Н. Учет бизнес-процессов в системе "1С:Бухгалтерия 8.1". – М.: Феникс, 2010. – 192 с.

УДК 004.4

Алексеев А.В.
студент 4 курса
факультет «Информационных систем и технологий»
Поволжский Государственный Университет
Телекоммуникаций и Информатики
Россия, г. Самара

Alexeev A.V.
Student
fourth-year, Faculty of Information Systems and Technologies
Volga State University of Telecommunications and Informatics
Russia, Samara

АНАЛИЗ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Аннотация. В данной статье рассмотрены виды систем обнаружения вторжений. Проведен обзор и классификация систем обнаружения вторжений, а также видов сетевых атак.

Ключевые слова: Компьютерная безопасность, сетевая безопасность, системы обнаружения вторжений .

ANALYSIS OF INTRODUCTION SYSTEMS

Annotation. In this article, we consider the types of intrusion detection systems. A review and classification of intrusion detection systems and types of network attacks was conducted.

Keywords: Computer security, network security, intrusion detection systems.

Системы обнаружения вторжений (Intrusion Detection System) — это совокупность программных и/или аппаратных средств, служащих для выявления фактов несанкционированного доступа в компьютер или компьютерную сеть, а также предотвращения неавторизованного управления ими.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и

червей)

В последнее время применение пользователями систем обнаружения вторжения активно набирает популярность. IDS — важнейший элемент информационной безопасности, необходимый каждому дальновидному пользователю. Система обнаружения вторжений позволит не только выявить компьютерную атаку и блокировать ее, но и выполнить это в удобном графическом интерфейсе — от пользователя не потребуется специальных знаний о сетевых протоколах и возможных уязвимостях.

Host-based IDS (хостовая, или локальная) хостовая IDS теоретически может работать с любым типом трафика, включая изначально зашифрованный. Network-based IDS (сетевая) сетевая IDS не использует ресурсы процессора и память защищаемого объекта.

На сегодняшний день IDS принято классифицировать по нескольким параметрам, к числу которых можно отнести способ сбора информации, метод анализа информации, способ реагирования на угрозы и способ реализации.

В сетевой СОВ, сенсоры расположены на важных для наблюдения точках сети, часто в демилитаризованной зоне, или на границе сети. Сенсор перехватывает весь сетевой трафик и анализирует содержимое каждого пакета на наличие вредоносных компонентов.

Протокольные СОВ используются для отслеживания трафика, нарушающего правила определенных протоколов либо синтаксис языка (например, SQL). В хостовых СОВ сенсор обычно является программным агентом, который ведет наблюдение за активностью хоста, на который установлен. Также существуют гибридные версии перечисленных видов СОВ.

Сетевая СОВ (Network-based IDS, NIDS) отслеживает вторжения, проверяя сетевой трафик и ведет наблюдение за несколькими хостами. Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к хабу или свитчу, настроенному на зеркалирование портов, либо сетевое TAP устройство. Примером сетевой СОВ является Snort. Основанная на протоколе СОВ (Protocol-based IDS, PIDS) представляет собой систему (либо агента), которая отслеживает и анализирует коммуникационные протоколы со связанными системами или пользователями. Для веб-сервера подобная СОВ обычно ведет наблюдение за HTTP и HTTPS протоколами. При использовании HTTPS СОВ должна располагаться на таком интерфейсе, чтобы просматривать HTTPS пакеты ещё до их шифрования и отправки в сеть.

Основанная на прикладных протоколах СОВ (Application Protocol-based IDS, APIDS) — это система (или агент), которая ведет наблюдение и анализ данных, передаваемых с использованием специфичных для определенных приложений протоколов. Например, на веб-сервере с SQL базой данных СОВ будет отслеживать содержимое SQL команд, передаваемых на сервер. Узловая СОВ (Host-based IDS, HIDS) — система

(или агент), расположенная на хосте, отслеживающая вторжения, используя анализ системных вызовов, логов приложений, модификаций файлов (исполняемых, файлов паролей, системных баз данных), состояния хоста и прочих источников. Примером является OSSEC.

Гибридная СОВ совмещает два и более подходов к разработке СОВ. Данные от агентов на хостах комбинируются с сетевой информацией для создания наиболее полного представления о безопасности сети. В качестве примера гибридной СОВ можно привести Prelude.

Исходя из того, что в гетерогенной сети с высокой вероятностью могут присутствовать клиенты с различными ОС, заметным минусом сетевой IDS становится потенциальная уязвимость к атакам, учитывающим особенности реализации различных TCP/IP-стеков, например, при обработке фрагментированного сетевого трафика.

Известно несколько разновидностей таких атак:

1) FragmentationReassemblyTimeoutattacks — это атаки, базирующиеся на различии временных интервалов («тайм-аутов») стеков TCP/IP разных ОС при сборке фрагментов. Если значения тайм-аутов дефрагментатора IDS отличаются от соответствующих значений на стороне атакуемой системы, для последующего анализа будет собран неправильный поток.

2) TTL Basedattacks — в основном такие атаки реализуются путем генерации ложных фрагментов, которые по замыслу не будут получены жертвой, но будут перехвачены и ошибочно учтены дефрагментатором IDS для текущей сессии. Ситуацию легко воспроизвести, если IDS и атакуемый объект расположены в разных сетевых сегментах.

3) OverlappingFragments — при такой атаке происходит (либо не происходит) перезапись уже полученных фрагментов вновь поступающими дубликатами, имеющими аналогичный порядковый номер. В результате сессия на стороне IDS может быть дефрагментирована иначе, чем на стороне жертвы атаки.

Сетевая система обнаружения вторжений может защитить от атак, которые проходят через межсетевой экран во внутреннюю ЛВС. Межсетевые экраны могут быть неправильно сконфигурированы, пропуская в сеть нежелательный трафик некоторых приложений, который может быть опасным. Порты часто переправляются с межсетевого экрана внутренним серверам с трафиком, предназначенным для почтового или другого общедоступного сервера. Сетевая система обнаружения вторжений может отслеживать этот трафик и сигнализировать о потенциально опасных пакетах. Правильно сконфигурированная сетевая система обнаружения вторжений может перепроверять правила межсетевого экрана и предоставлять дополнительную защиту для серверов приложений.

Сетевые системы обнаружения вторжений полезны при защите от внешних атак, однако одним из их главных достоинств является способность выявлять внутренние атаки и подозрительную активность пользователей.

Активные IDS, помимо всего вышеперечисленного, пытаются

противостоять вторжению. Их действия могут включать в себя как разрыв текущего злонамеренного соединения, так и полное блокирование атакующего путем изменения конфигурации межсетевого экрана или иным способом

Пассивные системы в случае идентификации вторжения обычно создают детальный отчет о произошедшем, включающий лог сетевой атаки, оповещают службу безопасности, например, по электронной почте, и предоставляют рекомендации по устранению выявленной уязвимости.

По способу реализации IDS можно разделить на программные и аппаратные. В настоящее время большинство производителей программных средств защиты для домашних и корпоративных пользователей предлагают интегрированные решения, куда включены такие компоненты, как антивирус, антиспам, проактивный модуль и межсетевой экран, в сочетании со встроенной системой обнаружения вторжений.

Подклассы сетевых систем обнаружения вторжений:

− Прозрачные сетевые IDS (Transparent Network IDS — TNIDS) устанавливаются в разрыв сетевого подключения.

− Сенсорные сетевые IDS (SensorNetwork IDS — SNIDS) подключаются к сегменту сети одним портом и прослушивают трафик, попадающий на этот порт. Если локальная сеть является коммутируемой, то подключение сенсорных IDS производят к зеркальным портам коммутаторов, на которые направляется необходимый для прослушивания трафик.

Системы обнаружения вторжений — эффективный инструмент защиты пользователя от разного рода несанкционированных атак, однако не стоит забывать, что, если мы говорим о полноценной безопасности, IDS — всего лишь элемент данной системы.

Использованные источники:

1. kompjuternye-terminologii https://elhow.ru/kompjutery/kompjuternye-terminologii/chto-takoeids?utm_source=users&utm_medium=ct&utm_campaign=ct
2. Виктор Сердюк “Вы атакованы — защищайтесь!” [HTML] (http://inform.p-stone.ru /libr/nets/security/data/public7/).
3. Проблема «нулевого дня» [HTML] (http://itc.ua/article.phtml?ID= 26845&IDw =38&pid =57).
4. Intrusion Detection Systems (IDS) Part 2 — Classification; methods; techniques [HTML] (http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html