УДК 004.056.53

ОСОБЕННОСТИ СОВРЕМЕННЫХ СРЕДСТВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

В.И. ГРИЦКЕВИЧ, С.Н. ПЕТРОВ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 10 ноября 2018

Аннотация. Проведен обзор разновидностей существующих систем обнаружения вторжений. Проанализированы особенности функционирования таких систем.

Ключевые слова: система обнаружения вторжений, сигнатура, аномальное поведение, сетевой трафик.

Введение

Средства обнаружения вторжений представляют собой программные или аппаратно-программные решения, автоматизирующие процессы сбора, хранения и анализа событий, происходящих в компьютерной системе, а также самостоятельно анализирующие эти события с целью выявления признаков нарушения информационной безопасности. Значительное увеличение количества различных типов и способов организации несанкционированного доступа к компьютерным сетям и системам приводят к тому, что средства обнаружения вторжений становятся одним из наиболее важных компонентов инфраструктуры безопасности.

Основная часть

Современные системы обнаружения вторжений (СОВ) имеют различную архитектуру (рис. 1).

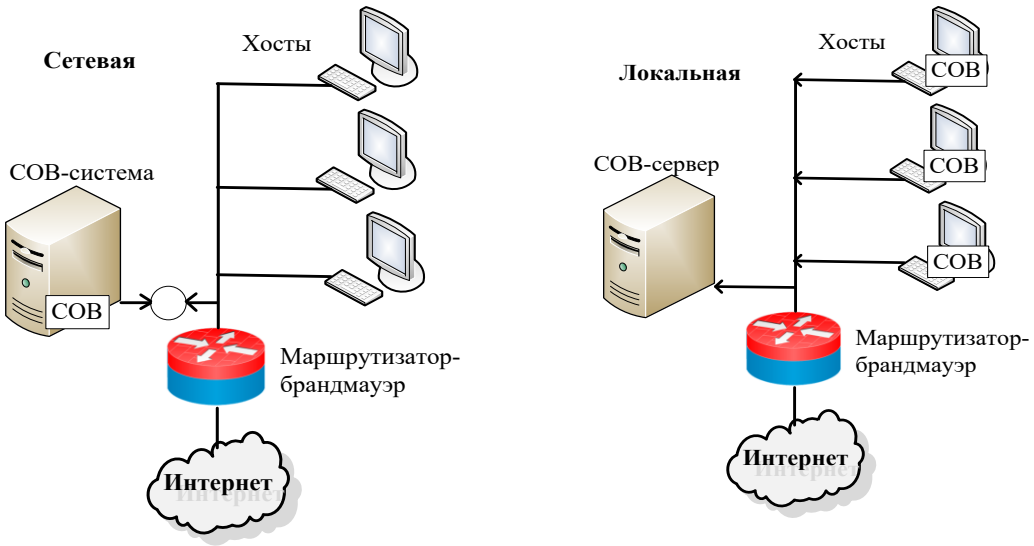

Рис. 1. Схемы сетевой и локальной СОВ

Сетевые СОВ располагаются в локальной сети предприятия и осуществляют мониторинг внутрисетевого трафика в режиме реального времени на предмет соответствия происходящих процессов заранее определенным сигнатурам атак. Признаки известных атак хранятся в базе данных системы и регулярно обновляются. Проблема такого подхода заключается в том, что постоянный мониторинг трафика серьезно снижает пропускную способность локальной сети

и производительность маршрутизатора. Тем не менее, пограничные маршрутизаторы (расположенные на стыке внутренних и публичных сетей) предоставляют отличную возможность для распознавания и пресечения атак до того, как они попадут во внутреннюю корпоративную сеть [1].

Локальные (хостовые) СОВ выполняют мониторинг и обработку событий, происходящих внутри хоста. Это отличает их от сетевых СОВ, которые отслеживают сетевой трафик. На функционирование локальных СОВ не влияет наличие в сети коммутаторов. Локальные СОВ более трудны в управлении, т. к. должны быть сконфигурированы на каждом узле локальной сети. Помимо этого, они используют вычислительные ресурсы узлов, за которыми наблюдают, что также понижает производительность системы [2].

Технологии по которым строятся СОВ делятся на две категории: обнаружение аномального поведения и обнаружение злоупотреблений.

Аномальное поведение пользователя определяется как отклонение от нормального поведения. Примером такого отклонения может служить большое число соединений за короткий промежуток времени либо высокая загрузка центрального процессора. Важной задачей является выявление среди всех подобных отклонений именно тех, которые свидетельствуют об атаке, т. к. не все аномальные отклонения являются ее следствием. Таким образом, возможны случаи, когда аномальное поведение, не являющееся атакой, определяется как атака и когда реальная атака не вызывает аномальных событий в системе. По сути, это означает, что системы обнаружения аномального поведения подвержены ошибкам первого и второго родов. Поэтому для построения профиля поведения системы следует привлекать администраторов, имеющих высокий уровень компетенций.

Детектирование атаки заключается в описании ее в виде сигнатуры и дальнейшем поиске этой сигнатуры в сетевом трафике. Сигнатурой может быть как шаблон действий, так и строка символов, которая определена как признак аномальной деятельности. Данная технология обнаружения атак похожа на технологию обнаружения вирусов. Такая система, хотя и справляется с обнаружением известных атак, не решает задачу определения неизвестных атак. Помимо этого, существует проблема описания атаки таким образом, который позволил бы в будущем зафиксировать ее возможные модификации [3].

В большинстве современных СОВ используется только сигнатурный метод распознавания атак или только поиск аномального поведения. В настоящее время существует недостаточное количество СОВ, которые реализуют сразу несколько подходов, т. е. гибридных систем. Помимо этого в системах обнаружения вторжений зачастую отсутствует встроенный имитатор атак, который проверяет корректность развернутой и эксплуатируемой системы, а также обеспечивает возможность тестирования конфигурационных параметров.

Еще одним распространенным недостатком СОВ является их низкое быстродействие и высокая степень нагрузки на локальную сеть и хосты в ней. Современные СОВ должны предусматривать возможность резервирование рубежей обороны сетевого периметра.

Заключение

Существующие СОВ отличаются используемыми методами обнаружения и их реализацией, архитектурой, уровнем детализации и типами обнаруживаемых атак. У каждой из этих систем есть свои достоинства и недостатки. Несмотря на постоянное развитие технологий, применяемых при разработке СОВ, все решения по реализации последних постоянно усложняются.

Так как алгоритмы совершения атак непрерывно совершенствуются, то к современным СОВ предъявляются все более жесткие и сильные требования. Негативным следствием этого является усложнение их развертывания и эксплуатации. В связи с вышеизложенным можно заключить, что в настоящее время представляется актуальной разработка гибридных СОВ, сочетающих в себе разные подходы к обнаружению атак.

FEATURES OF MODERN INTRUSIONS DETECTION MEANS

V.I. GRITSKEVICH, S.N. PETROV

Abstract. The review of existing intrusion detection systems is carried out. Operating features of such systems are analyzed.

Keywords: intrusion detection system, signature, anomalous behavior, network traffic

Список литературы

1. Сетевые IDS-системы. [Электронный ресурс]. URL: http://www.cnews.ru/reviews/free/oldcom/ security/ ids.shtml. (дата обращения: 22.10.2018).
2. HIDS (Host-Based Intrusion Detection System). [Электронный ресурс]. URL: https://ru.bmstu.wiki/HIDS_(Host-Based_Intrusion_Detection_System). (дата обращения: 22.10.2018).
3. Классификация систем обнаружения атак. [Электронный ресурс]. URL: http://libraryno.ru/9-3-1-klassifikaciya-sistem-obnaruzheniya-atak-shcelkunova/. (дата обращения: 22.10.2018).