УДК 004.056

Беляев П.А.

магистрант

Научный руководитель: Макаров И.С., к.т.н

Поволжский государственный университет телекоммуникаций и информатики

МЕТОДИКИ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО И ЗЛОУМЫШЛЕННОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ, ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ АНОМАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: научная статья посвящена системам обнаружения аномального и злоумышленного поведения. Рассмотрены технологии обнаружения аномальной активности. Представлены достоинства и недостатки этих систем.

Ключевые слова: методики, аномалия, технологии, атака, сеть

Belyaev P.A.

undergraduate

Methods for detecting anomalous and malicious user behavior, abnormal activity detection technologies

Abstract: The scientific article is devoted to systems for detecting anomalous and malicious behavior. Technologies for detecting anomalous activity are considered. The advantages and disadvantages of these systems are presented.

Keywords: techniques, anomaly, technology, attack, network

Систему обнаружения вторжений (СОВ) можно разделить на 2 методики: часть из них ищет аномальное поведение, другая – злоумышленное.

Системы обнаружения аномального поведения (от англ. anomaly detection) основаны на том, что СОВ известны признаки, характеризующие

правильное или допустимое поведение объекта наблюдения. Под «нормальным» или «правильным» поведением понимаются действия, выполняемые объектом и не противоречащие политике безопасности.

Системы обнаружения злоумышленного поведения (misuse detection) основаны на том, что заранее известны признаки, характеризующие поведение
злоумышленника. Наиболее распространенной реализацией технологии обнаружения злоумышленного поведения являются экспертные системы (например, системы Snort, RealSecure IDS, Enterasys Advanced Dragon IDS)[1-3].

Рассмотрим более подробно технологии, используемые в данных системах (рисунок 1).

Рисунок 1 – Существующие технологии СОВ

Технологии обнаружения аномальной деятельности

Датчики-сенсоры аномалий идентифицируют необычное поведение, так
называемые аномалии, в функционировании отдельного объекта. Поэтому главная трудность в применении их на практике связана с нестабильностью

самих защищаемых объектов, а также и взаимодействующих с ними внешних объектов. В качестве объекта наблюдения может выступать сеть в целом, отдельный компьютер, сетевая служба (например, файловый сервер FTP), пользователь и так далее Датчики срабатывают при условии, что нападения отличаются от «обычной» (законной) деятельности. Тут стоить отметить, что в разных реализациях свое определение допустимого отклонения для наблюдаемого поведения от разрешенного и свое определение для «порога срабатывания» сенсора наблюдения.

Меры и методы, обычно используемые в обнаружении аномалии, включают в себя следующие:

− пороговые значения: наблюдения за объектом выражаются в виде числовых интервалов. Выход за пределы этих интервалов считается аномальным поведением. В качестве наблюдаемых параметров могут быть, например: количество файлов, к которым обращается пользователь в данный период времени, число неудачных попыток входа в систему, загрузка центрального процессора и тому подобное. Пороги могут быть статическими и динамическими (то есть изменяться, подстраиваясь под конкретную систему);

− параметрические: для выявления атак строится специальный «профиль нормальной системы» на основе шаблонов (то есть некоторой политики, которой обычно должен придерживаться данный объект);

− непараметрические: профиль строится на основе наблюдения за объектом в период обучения;

− статистические меры: решение о наличии атаки делается по большому
количеству собранных данных путем их статистической предобработки;

− меры на основе правил (сигнатур): они очень похожи на непараметрические статистические меры. В период обучения составляется представление о нормальном поведении объекта, которое записывается в виде

специальных «правил». Получаются сигнатуры «хорошего» поведения объекта;

− другие меры: нейронные сети, генетические алгоритмы, позволяющие
классифицировать некоторый набор видимых сенсору-датчику признаков.

В современных системах обнаружения аномалий в основном используют первые два метода. Следует заметить, что существуют две крайности при использовании данной технологии:

− обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак (ошибка второго рода);

− пропуск атаки, которая не подпадает под определение аномального поведения (ошибка первого рода). Этот случай гораздо более опасен, чем ложное причисление аномального поведения к классу атак.

Поэтому при установке и эксплуатации систем такой категории обычные
пользователи и специалисты сталкиваются с двумя довольно нетривиальными
задачами:

− определение граничных значений характеристик поведения субъекта для снижения вероятности появления одного из двух вышеописанных крайних
случаев;

− построение профиля объекта – это трудно формализуемая и затратная по времени задача, требующая от специалиста безопасности большой предварительной работы, высокой квалификации и опыта.

Как правило, системы обнаружения аномальной активности используют
журналы регистрации и текущую деятельность пользователя в качестве источника данных для анализа. К достоинствам систем обнаружения атак на основе технологии выявления аномального поведения можно отнести то, что

они:

− не нуждаются в обновлении сигнатур и правил обнаружения атак;

− способны обнаруживать новые типы атак, сигнатуры для которых еще

не разработаны;

− генерируют информацию, которая может быть использована в системах обнаружения злоумышленного поведения.

Недостатками этих систем является следующее:

− генерируют много ошибок второго рода;

− требуют длительного и качественного обучения;

− обычно слишком медленны в работе и требуют большого количества вычислительных ресурсов[4].

Использованные источники

1. Анализ угроз сетевой безопасности [Электронный ресурс]: статья // Лаборатория Сетевой Безопасности. – 2016. – Режим доступа: http://ypn.ru/138/analysis-of-threats-to-network-security/.

2. Басараб, М. А. Анализ сетевого трафика корпоративной сети университета методами нелинейной динамики [Электронный ресурс]: статья / М. А. Басараб, А. В. Колесников, И. П. Иванов // Наука и образование: научное издание / МГТУ им. Н. Э. Баумана. – 2013. – Режим доступа: http://technomag.bmstu.ru/doc/587054.html.

3. Лукацкий, А. Предотвращение сетевых атак: технологии и решения [Электронный ресурс]: статья / А. Лукацкий // IT-портал. – 2006. – Режим доступа: http://citforum.ru/security/articles/ips/.

4. Маркин, Ю. В. Обзор современных инструментов анализа сетевого трафика [Электронный ресурс]: статья / Ю. В. Маркин, А. С Санаров // сборники трудов Института системного программирования Российской академии наук. – 2014. – Режим доступа: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf.