УДК 004.056

Анализ недостатков современных систем обнаружения вторжений

Юмашева Елена Сергеевна (Санкт-Петербургский национально исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург)

Гатчин Юрий Арменакович (Санкт-Петербургский национально исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург)

На данный момент не существует единого метода по решению проблем обнаружения аномальных ситуаций во время обработки информации компьютерными системами и информационными сетями. Однако в условиях постоянного развития и создания новых ИТ и постоянного усовершенствования аппаратной части компьютеров, нынешние решения поиска аномалий не дают нужного уровня безопасности системы. Методы обнаружения аномалий выбираются применительно к определенному набору параметров системы, и будут эффективно функционировать только для данного набора [1].

Рассмотрим некоторые методы.

Сигнатурный метод – метод обнаружения вторжений в систему, которые содержат сигнатуры типовых атак. Метод является затратным с точки зрения вычислений из-за большого числа сигнатур. Что-бы снизить данные затраты мощностей был разработан новый метод, который совмещал в себе поиск только в определенных частях пакетов с традиционным сопоставлением сигнатур. Преимущества метода заключаются в эффективном определении атак и маленькому числу ложных срабатываний. Недостатки метода заключаются в частом обновлении баз сигнатур и не возможности выявления атак, не описанных в сигнатурах.

Поведенческий метод – метод в основе которого лежат модели (нормального) функционирования информационной системы (ИС). Принцип работы метода заключается в сравнении эталонной работы системы с тем как система работает в данный момент. Несоответствия считаются вторжениями или аномалиями. Преимущества метода заключаются в определении атак без сигнатур, а также в высокой чувствительности к изменениям в ИС. Недостатки метода заключаются в большом количестве ложных срабатываний и большим затратам на обучение системы.

Комбинированный метод [2]:

1. База правил. Определяется взаимодействие между узлами ИС, всегда следующими определённым протоколам. Появлении неизвестной команды во время обмена информацией между узлами, является признаком начала атаки.
2. Метод имитации биологических систем. Данный метод построен на основе данных о биологических объектах таких как: генетические алгоритмы, искусственные нейронные сети используя алгоритм создает имитацию поведения биологических систем. Метод считается одним из самых перспективных из-за саморазвития и адаптации.
3. Метод продукционных правил. Описывает модели атак на естественном языке. Системы использующие данную методику состоят из двух баз данных: факты и правила. Факты это входные данные, а правила – алгоритмы для логических решений о факте нападения на основе входящего набора фактов. Такая система описывает характеристики атак, которые должна обнаружить система обнаружения вторжения.

На этапе вторжения можно обнаружить атаку как сигнатурным, так и поведенческим методом. Любое вторжение можно охарактеризовать определенными особенностями: можно представить в виде сигнатур или отклонение от эталона. Но наиболее эффективным методом является их комбинация с применением любых (сетевых или узловых) датчиков.

Список литературы:

1. Тишина, Н.А. Тенденции развития технологии обнаружения аномалий сетевого трафика (статья) / Н.А. Тишина // Современные информационные технологии в науке, образовании и практике. Материалы XI всероссийской научно-практической конференции. – Оренбург: ООО ИПК«Университет», 2014. – С. 99 – 101. 1
2. Cannady J. Artificial Neural Networks for Misuse Detection. [Электронный Ресурс] — Режим доступа.URL: [http://csrc.nist.gov/nissc/1998/proceedings/paperF13.pdf].