Н.М. Кусакина

КЛАССИФИКАЦИОННЫЙ ПОДХОД К АНОМАЛИЯМ СЕТЕВОГО ТРАФИКА ПРИ ПРОЕКТИРОВАНИИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

(Самарский государственный технический университет)

Обеспечение стабильной работы компьютерных сетей предприятия в современной реальности становится основной целью деятельности различных его подразделений. Оптимизация затрат на поддержание требуемого уровня качества работы компьютерных сетей обуславливает необходимость постоянного технологического роста, использования новых методов и алгоритмов работы.

Развитие программно-аппаратных средств обнаружения вторжений (Intrusion Detection System - IDS) основывается на эволюции методов обнаружения аномалий сетевого трафика. В последнее время тема классификации срабатываний правил IDS стала площадкой глубоких исследований, где основное внимание уделено определению реальных угроз от ложноположительных срабатываний и их дальнейших их классификации. [1, 2]

Различают несколько типов систем обнаружения вторжения в зависимости от типа используемого сенсора, его расположения и методов подсистемы анализа (характеристики анализатора). Если IDS при анализе трафика использует шаблон штатного функционирования системы, она называется поведенческой (контролируются частота событий, объем переданных пакетов и другие статистические характеристики); если IDS работает с информацией об выявленных вторжениях, она является интеллектуальной.

Системы обнаружения вторжений на основе анализа поведения сетевого трафика, так называемые A-IDS, и обнаружения его аномалий считается лучшем вариантом по сравнению с системами на основе сигнатурного метода обнаружения аномалий – S-IDS, так как не требуют предварительного знания самой сигнатуры. Однако определение типа зафиксированной атаки представляет собой трудную задачу по причине того, что A-IDS не может соотносить обнаруженную активность с классом атаки. [3]

Можно сказать, что любое срабатывание подобной системы должно проходить ручную обработку администратором безопасности либо лицом, осуществляющим мониторинг событий A-IDS. Это, в свою очередь, увеличивает как нагрузку персонала, так и время реагирования на возникающие инциденты безопасности. Также необходимо помнить о том, что сложность и динамическое изменение статистических свойств трафика может ввести дополнительные ошибки обработки зафиксированного события.

В исследовании рассмотрены несколько методов для анализа событий срабатывания A-IDS, основанные на различных алгоритмах классификации и наборах свойств сетевого трафика: в частности, энтропийный анализ на основе энтропии Шаннона. Рассмотрены сценарии атак с помощью мониторинга ста-

тистических свойств сетевого трафика. Сетевой трафик собирается либо на основе пакетных данных, либо сущности потока. Каждое из этих представлений обеспечивает различный вид, а в совокупности они могут обеспечить полное представление о сетевой деятельности. По мере того, как потоки данных проходили по сети, сетевой пакетный сниффер захватывал каждый пакет и декодировал необработанные данные пакета, показывая значения различных полей в пакете. По данным анализа экспериментальных данных были сформированы подмножества признаков сетевых атак и их влияния на потоки трафика.

Например, важные свойства сетевого трафика при наблюдении атаки типа отказ в обслуживании (Denial of Service – DOS):

- общее количество байт, полученных за период наблюдения;
- общее количество байт, отправленных за период наблюдения;
- общее количество пакетов, отправленных в течение периода наблюдения;
- общее количество пакетов, полученных за период наблюдения;
- общее количество пакетов, полученных в течение периода наблюдения от разных IP-адресов;
- общее количество различных номеров портов TCP и UDP, используемых источником;
- общее количество различных номеров портов TCP и UDP, используемых хостом назначения;
- общее количество соединений TCP за период наблюдения;
- общее количество соединений UDP за период наблюдения;
- общее количество открытых соединений;
- общее количество установленных соединений, которое представляет открытое соединение;
- общее количество отправленных запросов на соединение;
- общее количество подтвержденных завершений соединения.

При фиксировании атаки типа IP-спуфинг или ARP-спуфинг набор выбранных свойств трафика будет несколько иным:

- общее количество пакетов, полученных в течение периода наблюдения от разных IP-адресов;
- общее количество пакетов, отправленных в течение периода наблюдения, на разные IP;
- количество номеров привилегированных портов, используемых в течение периода наблюдения;
- количество различных номеров привилегированных портов, используемых в течение периода наблюдения;
- количество зарегистрированных портов, используемых в течение периода наблюдения;
- количество различных номеров зарегистрированных номеров портов;
- общее количество различных номеров портов TCP и UDP, используемых источником;

- общее количество различных номеров портов TCP и UDP, используемых хостом назначения;
- количество TCP-запросов для передачи;
- количество полуоткрытых соединений;
- количество установленных соединений, которые представляют собой открытое соединение;
- количество отправленных запросов на соединение;
- количество подтвержденных завершений соединения.

Эта работа является важной частью построения системы обнаружения вторжений и конструирования модуля анализатора. На данном этапе выбираются атрибуты сетевого трафика, которые считаются максимально полезными во время обработки определенного события для установления его класса. Благодаря уменьшению количества таких атрибутов скорость выполнения вычислений классификатора повышается, соответственно, увеличивается и общая производительность системы.

Также выбор данных характеристик влияет на классификацию и точность работы A-IDS. Поэтому, анализируя известные атаки и их влияние на сетевой трафик корпоративной сети, уделялось особое внимание релевантности использования значения каждого свойства зафиксированного события.

При использовании классификатора сетевых аномалий на основе машинного обучения можно повысить точность классификации атак в случае представления сетевого трафика в виде потоков, их извлечении из общего массива передаваемых данных во время проведения определенной атаки, путем сравнения этих последовательностей с ранее собранными.

Литература

1. Rodas O., A study on network security monitoring for the hybrid classification-based intrusion prevention systems [Текст] / O. Rodas, M. A. To // International Journal of Space-Based and Situated Computing. – 2015. vol. 5, no. 2. - pp. 115.

2. Кусакина, Н.М. Методы анализа сетевого трафика как основа проектирования системы обнаружения атак. [Текст] / Н.М. Кусакина // International scientific review. – 2018. № 1 (42). – С. 28-32.

3. Aghdam, J.Y., Feature selection for intrusion detection system using ant colony optimization. [Текст] / J.Y. Aghdam, P. Kabiri // International Journal of Network Security. – 2016. vol. 18, no. 3. - pp. 420-432.

4. Willinger W., A bibliographical guide to self-similar traffic and performance modeling for modern high-speed networks. [Электронный ресурс], 2001. – URL Режим доступа: http://linkage.rockefeller.edu/wli/reading/taqqu96.pdf (дата обращения 15.03.2018).