METHODS OF THE NETWORK TRAFFIC ANALYSIS AS A BASIS FOR DESIGNING THE INTRUSION DETECTION SYSTEM

Kusakina N.M. (Russian Federation) Email: Kusakina543@scientifictext.ru

Kusakina Nadezhda Mikhailovna - Postgraduate,
COMPUTER ENGINEERING DEPARTMENT,
SAMARA STATE TECHNICAL UNIVERSITY (SAMARA POLYTECH),
ENGINEER
SC INFORMATION SECURITY,
INFORMATION INFRASTRUCTURE MONITORING DEPARTMENT,
PAO SBERBANK,
SAMARA

Abstract: *the article analyzes the methods of classifying the detection network traffic anomalies as the basis for developing intrusion detection systems. Such systems have significant differences depending on the method used to detect anomalies: the dependence of the speed of work on the signature base, the number of false positives. It is considered the possibility of circumventing the work of IDS during a network attack with the help of intentionally generated parasitic traffic. Examples of new models based on artificial neural networks are given to analyze incomplete input data when network anomalies are detected.*
Keywords: *computer networks, network traffic, analysis methods, network traffic anomalies, classification of network traffic anomalies, network intrusions.*

МЕТОДЫ АНАЛИЗА СЕТЕВОГО ТРАФИКА КАК ОСНОВА ПРОЕКТИРОВАНИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Кусакина Н.М. (Российская Федерация)

Кусакина Надежда Михайловна – аспирант,
кафедра вычислительной техники,
Самарский государственный технический университет,
инженер
СЦ Информационная безопасность,
отдел мониторинга информационной инфраструктуры,
ПАО Сбербанк,
г. Самара

Аннотация: *в настоящей статье приводится анализ методов классификации выявленных аномалий сетевого трафика как основы построения систем обнаружения вторжений. Подобные системы имеют существенные различия в зависимости от используемого метода обнаружения аномалий: зависимость скорости работы от базы сигнатур, количество ложных срабатываний. Рассматривается возможность обхода работы IDS при проведении сетевой атаки с помощью преднамеренно сгенерированного паразитного трафика. Приводятся примеры новых моделей на основе искусственных нейронных сетей для проведения анализа неполных входных данных при обнаружении сетевых аномалий.*
Ключевые слова: *компьютерные сети, сетевой трафик, методы анализа, аномалии сетевого трафика, классификация аномалий сетевого трафика, сетевые вторжения.*

Разработка новых моделей функционирования компьютерных систем, а также методов прогнозирования их работы в настоящее время является актуальным направлением научных исследований. Особое внимание уделяется исследованиям по оценке функционирования информационной инфраструктуры при стороннем информационно-техническом воздействии. Становятся актуальными выявление и классификация аномалий сетевого трафика с последующим выделением из их числа особого подмножества аномалий - внешних воздействий. Результаты подобных исследований становятся полезными при создании модели работы систем и сетей связи, оптимизации настроек сетевого оборудования, а также составлении методологии поддержания заданного параметра QoS и противоборству внешним воздействиям на сеть, в том числе проектировании новых средств обнаружения вторжений.

Аномалии сетевого трафика на основании источника её возникновения могут быть разделены на два типа: преднамеренное информационно-техническое воздействие на компьютерную сеть и случайное отклонение от штатного режима работы (нарушение работоспособности сетевого оборудования, авария на линии передачи). Анализ экспериментальных данных позволяет сделать вывод, что интенсивность трафика компьютерной сети при различном преднамеренном воздействии на неё существенно

отличается от интенсивности штатного функционирования сети, что делает возможным определение не только наличия аномалии сетевого трафика, но и распознавание конкретного её типа.

В настоящее время идентификация и распознавание воздействия на сети связи на основании анализа циркулирующего в них трафика является наиболее актуальным направлением научных исследований. Так для выявления аномалии сетевого трафика, обусловленной фактом наличия преднамеренного внешнего воздействия на сеть, используется следующие методы:

1. Трендовый анализ [3, 4];
2. Корреляционный анализ [5, 6];
3. Методы на основе вейвлет-анализа [7];
4. Методы классификаторов с использованием теории нечетких множеств;
5. Методы фрактального анализа [8];
6. Анализ трафика на основе нейронных сетей [9];
7. Методы конечных автоматов на основе генетических алгоритмов [10];
8. Методы на основе бионических подходов [11];
9. Гибридные подходы.

Воспользуемся классификацией аномалии сетевого трафика типа «удаленная сетевая атака» на основе анализа материалов [12, 13], представленной на рис. 1.

Упомянутые методы обнаружения и классификации аномалий и их комбинации используются при проектировании программно-аппаратных комплексов/систем обнаружения вторжений – IDS (от английского термина Intrusion Detection System). 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.

Рис. 1. Классификация аномалий сетевого трафика типа удаленная сетевая атака

Анализ предустановленных сигнатур стал первым методом, примененным при проектировании IDS. Согласно статистике более 75% аномалий сетевого трафика типа «информационно-техническое вторжение» происходит по известным сценариям. Хотя правила достаточно часто обновляются и

дополняются, системы на базе только сигнатурного метода не получили широкого распространения по причине наличия ряда недостатков.

При использовании сигнатурного метода проходящий через IDS трафик разбивается на транспортные потоки, далее они маркируются и в случае необходимости нормализуются парсерами. Итоговые декодированные поля заголовков, например, TCP-пакета проверяются наборами сигнатур на предмет наличия попыток сетевых вторжений или пакетов, соответствующих деятельности вредоносных объектов. Система проводит сравнение списка имеющихся сигнатур с данными очередного пакета, соответственно, она выявляет только известные ей аномалии. Рост числа сигнатур приводит к замедлению работы самой системы из-за обработки «медленных» правил, например, содержащих в себе проверку подстроки пакета регулярным выражением, и порождает ситуации обхода самих сигнатур. А если нагрузка на ядро IDS начинает превышать 80%, то IDS начинает выборочно пропускать проверку пакетов.

Получаем возможность ситуации использования преднамеренно сгенированного трафика, содержащего в себе модифицированную подстроку, совпадающую с подстрокой сигнатуры лишь частично. Наличие таких подстрок многократно увеличивает время проверки поля пакета. А после того, как буфер IDS переполнится, пакеты будут проходить сквозь неё без проверки. Использование «медленных» сигнатур при проведении вторжения в компьютерную сеть не может быть выявлено механизмами самой системы обнаружения вторжений в то время, когда злоумышленник может послать массив подобных пакетов и обезоружить систему.

На первый взгляд системы обнаружения вторжений, на основе статистического анализа, (выявления аномалий) работают медленнее, чем системы на основе сигнатуры. Во-вторых – основной проблемой их использования можно считать частоту ложных срабатываний.

С целью улучшения сложившейся ситуации в данной области исследования проводится поиск новых методов обнаружения аномалий сетевого трафика и построения новых систем обнаружения вторжений. Например, системы на основе анализа соединений удаленных хостов [14] или на основе искусственных нейронных сетей. Одним из определяющих преимуществ нейронных моделей является возможность анализа неполных входных данных или сигнала с какими-либо помехами, а также проведение нелинейного анализа произошедших событий (в случае распределённого внешнего воздействия на сеть). В этом случае каждое событие в сети будет иметь собственный вес, что важно так как, в реальном сетевом трафике пакет может искажаться как умышленно, так и в результате непреднамеренного сбоя работы системы.

Наиболее важным качеством нейронных сетей является способность прогнозировать дальнейшие события, поведение системы, возможные аномалии. Так в ходе самообучения система, система обнаружения вторжения на основе искусственных нейронных сетей улучшает свои способности по выявлению закономерностей между отдельными событиями, их последовательностью, какими-либо связками, что позволяет либо в более короткие сроки локализовать проблему, либо заранее предпринять защитные меры и полностью отразить нападение без вреда [15].

В настоящее время распространены два вида реализации систем обнаружения вторжений на базе искусственных нейронных сетей. Первый представляет собой комбинацию экспертной системы и нейросетевого метода, является системой двухступенчатого анализа: при обнаружении в проходящем через IDS трафике вероятной угрозы, информация о зафиксированном инциденте передаётся для анализа экспертной системе, которая уже принимает решение о сигнализации об атаке. Преимущество подобной реализации заключается в повышении чувствительности анализатора, поскольку он получает данные о вероятных угрозах. Недостаток - необходимость постоянного обновления баз сигнатур, иначе новые виды вторжений, фиксируемые с помощью нейронных сетей, не смогут быть распознаны.

Вторая реализация системы обнаружения вторжений на основе искусственных нейронных сетей в качестве автономной системы. Такие системы обладают высокой скоростью работы и не требуют постоянного обновления сигнатур, так как используют свойство самообучения. Этот подход позволяет, как минимизировать время реакции системы на аномалию сетевого трафика, так и увеличить объемы пропускаемого трафика, что является актуальной задачей в условиях роста компьютерных сетей.

В заключении можно сделать вывод о том, что развитие методов выявления аномалий сетевого трафика является основой развития программно-аппаратных средств обеспечения стабильной работы компьютерных сетей. Полнота и точность используемых методов анализа трафика влияет на соотношение числа ложных срабатываний и распознанных раннее неизвестных типов аномалий, так как не каждое аномальное поведение пакета сетевого трафика является преднамеренным вторжением в сеть.

Список литературы / References

1. *Park K.* Self-Similar Network Traffic: An Overview. [Электронный ресурс], 2003. Режим доступа: http://pi.314159.ru/park1.pdf/ (дата обращения 15.01.2018).

2. *Willinger W., Taqqu M.S., Errimilli A.* A bibliographical guide to self-similar traffic and performance modeling for modern high-speed networks. [Электронный ресурс], 2001. Режим доступа: http://linkage.rockefeller.edu/wli/reading/taqqu96.pdf/ (дата обращения 15.01.2018).
3. *Ажмухамедов И.М., Марьенков А.Н.* Поиск и оценка аномалий сетевого трафика на основе циклического анализа // Инженерный вестник Дона, 2012. Т. 20. № 2. С. 17-26.
4. *Ажмухамедов И.М., Марьенков А.Н.* Выявление аномалий в вычислительных сетях общего пользования на основе прогнозирования объема сетевого трафика // Проблемы информационной безопасности. Компьютерные системы, 2012. № 3. С. 35-39.
5. *Шелухин О.И., Судариков Р.А.* Анализ информативных признаков в задачах обнаружения аномалий трафика статистическими методами // T-Comm: Телекоммуникации и транспорт, 2014. Т. 8. № 3. С. 14-18.
6. *Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М.* Распределенная система защиты облачных вычислений от сетевых атак // Вестник СибГУТИ, 2013. № 3. С. 46-62.
7. *Шелухин О.И., Гармашев А.В.* Обнаружение DOS и DDOS-атак методом дискретного вейвлет-анализа // T-Comm: Телекоммуникации и транспорт, 2011. № 1. С. 44-46.
8. *Басараб М.А., Строганов И.С.* Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности, 2014. № 4 (7). С. 30-40.
9. *Фраленко В.П.* Обнаружение сетевых атак с помощью генетически создаваемых конечных автоматов // Вестник РУДН. Серия Математика. Информатика. Физика, 2012. № 4. С. 92-1-2.
10. *Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М.* Эксперименты по нейросетевому мониторингу и распознаванию сетевых атак // Информационное противодействие угрозам терроризма, 2010. № 15. С. 81-86.
11. *Браницкий А.А., Котенко И.В.* Обнаружение сетевых атак на основе комплексирования нейронных, иммуннх и нейронечетких классификаторов // Информационно-управляющие системы, 2015. № 4. С. 69-76.
12. *Микова С.Ю., Оладько В.С., Нестеренко М.А.* Подход к классификации аномалий сетевого трафика // Инновационная наука, 2015. № 11. С. 78-80.
13. *Багров Е.В.* Мониторинг и аудит информационной безопасности на предприятии // Вестник Волгоградского государственного университета. Серия 10. Инновационная деятельность, 2011. № 5. С. 54-56.
14. *Явтуховский Е.Ю.* Анализ систем обнаружения вторжений на основе интеллектуальных технологий [Текст] // Технические науки: теория и практика: материалы III Междунар. науч. конф. (г. Чита, апрель 2016 г.). Чита: Издательство Молодой ученый, 2016. С. 27-30. Режим доступа https://moluch.ru/conf/tech/archive/165/10049/ (дата обращения: 17.01.2018).
15. *Макаренко С.И., Михайлов Р.Л.* Информационные конфликты – анализ работ и методологии исследования // Системы управления, связи и безопасности, 2016. № 3. С. 95-178. Режим доступа: http://sccs.intelgr.com/archive/2016-03/04-Makarenko.pdf/ (дата обращения 15.01.2018).
16. *Макаренко С.И., Чукляев И.И.* Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. № 1 (2), 2014. С. 13-21.