УДК 004

Фирсова А.А.
Магистрант
2 курс, Факультет оптических и квантовых коммуникаций
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»

ПОИСК ПРОТОКОЛОВ С ПРИМЕНЕНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ И АЛГОРИТМОВ НЕЧЕТКОЙ ЛОГИКИ В СИСТЕМАХ АНАЛИЗА ТРАФИКА

Аннотация: *в работе рассматривается новый эффективный подход к анализу сетевого трафика с целью определения протокола информационного обмена прикладного уровня. Дается краткое описание структуры алгоритма классификации сетевых пакетов на принадлежность к одному из известных сетевых протоколов (TLS v1, TLS v1.2, HTTP, SSH v2, DNS, DHCP v6 и др).*

Ключевые слова: *межсетевой экран, антивирус, DDoS-атака, IDS, IPS.*

Abstract: *the paper considers a new effective approach to the analysis of network traffic in order to determine the protocol of information exchange at the application level. A brief description of the structure of the algorithm for classifying network packets as belonging to one of the well-known network protocols (TLS v1, TLS v1.2, HTTP, SSH v2, DNS, DHCP v6, etc.) is given.*

Keywords: *firewall, antivirus, DDoS attack, IDS, IPS.*

В последнее время не ослабевает интерес операторов телекоммуникационного рынка к системам анализа сетевого трафика network traffic analysis (NTA), глубокой инспекции пакетов (DPI) и к системам обеспечения комплексной информационной безопасности [1]. Полагаем, что и в дальнейшем его рост будет продолжаться, особенно для систем обеспечения

информационной безопасности, использующих современные интеллектуальные математические модели и методы.

Анализ трафика в течение многих лет остается актуальным направлением исследований. Этому способствуют две основные причины: рост трафика, в том числе вредоносного, появление новых технологий.

Разработано и эксплуатируется множество систем обеспечения информационной безопасности. К таким системам можно отнести:

1. Системы управление правами доступа (IDM – Identity Management);
2. Системы контроля действий администраторов (PAM – Privelege Accounts Management);
3. Развитые межсетевые экраны (NGFW – Next Generation Firewalls);
4. Средства анализа защищенности (SIEM – Security Information and Event Management);
5. Антивирусные решения (AV – Antivirus, Antibot, Malware Protection);
6. Системы обнаружения вторжений и аномалий (IDS – Intrusion Detection System, APIDS – Application protocol-based IDS);
7. Системы предотвращения атак (IPS – Intrusion Prevention System);
8. Системы аудита и мониторинга средств безопасности (NMS – Security Information and Event Management);
9. Системы защиты от атак класса «Отказ в обслуживании» (DDoS PS – DDoS Protection Systems);
10. Системы управления политиками сетевого трафика (PCEF – Policy and Charging Enforcement Function, PCRF – Policy and Charging Rules Function, NAC – Network Access Control);
11. Другие системы.

Системы анализа трафика NTA являются необходимым инструментом многих представленных классов других систем обеспечения информационной безопасности, таких как IDS, IPS, NMS, DDoS PS и др.

Идентификация протоколов инфокоммуникационного обмена позволяет решать следующие типы задач:

1. Разработка датчиков обнаружения атак;
2. Идентификация типов устройства, задействованных в информационном обмене;
3. Определение типовых приложений, запущенных на устройствах, задействованных в процессе информационного обмена;
4. Создание датчиков обнаружения аномального или поддельного трафика (в случае выдачи одного протокола за другой протокол);
5. классификация сетевых приложений прикладного уровня вплоть до седьмого уровня модели OSI (SKYPE, Facebook и др.) [2].

Вместе с тем классификатор сетевых пакетов (КСП) прикладного уровня может быть очень полезен при распознавании внутреннего состояния, в котором может находиться тот или иной протокол в процессе информационного обмена на этапе handshake (рукопожатия), что является важным элементом поведенческого анализа. Классификация трафика может быть осуществлена на основе:

1. Использования традиционных подходов к анализу трафика (сигнатурный и поведенческий) в зависимости от того, зашифрован трафик или нет. Основан на анализе номеров портов пакетов, сигнатуры протокола (payload-based). Поведенческий (статистический) анализ характеристик обмена (statistical analysis) пакетами между абонентами и статистических свойств сетевого трафика основан на исследовании последовательности размеров пакетов, временных интервалов между пакетами и т. д.;
2. Разработки и применения математических методов:

a) Базовые статические алгоритмы;

b) Machine leaning (метод опорных векторов);

c) Алгоритмы нечеткой логики;

d) Методы теории нейронных сетей.

Качественная классификация сетевых пакетов приложений прикладного уровня, как в плане характеристик классификации (точность, время, надежность и др.), так и в плане уменьшения требований к вычислительной мощности, оказывает важное влияние на функ ционирование систем NTA, анализ трафика DPI, IDS/IPS, DDoS PS и др. Как на весь технологический процесс, так и на качество анализа. По уровню классификации сетевых пакетов различают: «поверхностный» анализ пакетов (SPI – Shallow Packet Inspection), «средний» анализ пакетов (MPI – Medium Packet Inspection) и «глубокий» анализ пакетов (DPI – Deep Packet Inspection) [3]. Анализаторы «поверхностного» уровня функционируют в простейших межсетевых экранах, где решение о блокировании того или иного пакета обычно принимается в соответствии со списком запрещенных IP-адресов и номеров портов. Программные средства анализа трафика, относящиеся к «среднему» уровню, позволяют проводить фильтрацию трафика с использованием информации о формате передаваемых данных, а также более полной локализации отправителя. Эти инструменты обычно выступают в роли посредника (proxy) между провайдером доступа к сети Интернет и внутренней сетью. Системы «глубокого» анализа пакетов предназначены для идентификации приложений, участвующих в сетевых взаимодействиях. Поэтому «углубленный» разбор предполагает анализ содержимого сетевых пакетов всех уровней и назначение подобных систем – это обеспечение информационной безопасности и мониторинг качества каналов связи.

Как правило, для анализа сетевого трафика исследователи в своих работах определяют протокол прикладного уровня с использованием алгоритмов машинного обучения «с учителем».

Разработка КСП состоит из четырех этапов: (1) мониторинг и сбор пакетной статистической информации наиболее известных протоколов сетевого трафика, (2) предобработка первичной пакетной статистической информации, (3) построение КСП и (4) тестирование [4].

Представленная в данной работе методика распознавания сетевых протоколов информационного обмена иллюстрирует развитие систем анализа трафика (NTA) и других систем обеспечения информационной безопасности, таких как IDS, IPS, NMS, DDoS PS и т.п., в условиях действия программ импортозамещения с применением нового подхода анализа трафика, в основе которого лежит использование алгоритмов машинного обучения, алгоритмов нечеткой логики, позволяющих проводить классификацию сетевых пакетов приложений прикладного уровня.

Существует перспектива появления нейросетевого КСП промышленного уровня с показателями не уступающими известным DPI-решениям, но работающего на совершенно другом уровне.

В данной работе приводится попытка перехода от простого логического КСП на правилах, главным недостатком которого является трудоемкость и рутинность формирования правил, к современному высокотехнологичному нейросетевому классификатору, базирующемуся на методах машинного обучения и интеллектуальной обработке данных. Идея совместного использования нейросетевого подхода классификации сетевых пакетов и DPI, NTA и др. сейчас обсуждаемая.

Список литературы:

1. Лось А.Б., Даниелян Ю.Ю. Сравнительный анализ систем обнаружения вторжений, представленных на отечественном рынке. Вестник МФЮА /2014. – №3. С.181 – 187.

2. Kawai H., Ata S., Nakamura N., Oka I. Identification of Communication Devices from Analysis of Traffic. Patterns. Electric Industry Co., Ltd. Japan, 2018. С 27 – 31.

3. Агеев С.А., Саенко И.Б., Котенко И.В. Метод и алгоритмы обнаружения аномалий в трафике. – №3. 2021. С 54 – 58.

4. Хазов В. 2016.Введение в DPI: Аналитика, обстановка на рынке и тренды. – URL: https://vasexperts.ru/blog/privet-mir.