Разработка IDS-системы на основе технологии множественных временных окон

П.А. Серов, Д.А. Панов, С.С. Иванов, К.В. Садова

Филиал Самарского государственного технического университета в г. Сызрани, Россия

Обоснование. Современные информационные системы используют технологию удаленного доступа. Одним из видов мошеннических действий в информационной сети является организация сетевой атаки на ресурс, доступный в этой сети. Наиболее распространенным типом атаки является DoS-атака (Denial of Service) — это атака, целью которой является перегрузка подсистемы сервиса запросами на предоставление ресурса [1–3]. В результате атаки сетевой ресурс оказывается недоступен для использования легитимными пользователями. Различают следующие разновидности атак. DoS-атака характеризуется использованием одиночного потока запросов. DDoS (Distributed Denial of Service) связана с использованием многопоточных запросов, которые генерируются несколькими сетевыми источниками. Ранняя и достоверная идентификация начала сетевой атаки является одной из наиболее актуальных задач при обеспечении бесперебойного легитимного доступа к ресурсу, разделяемому между сетевыми пользователями.

Цель — создание метода раннего детектирования DoS и DDoS-атак, разработка программного обеспечения.

Методы. Современные методы детектирования используют анализ статистики потока запросов: сетевая атака характеризуется возрастанием плотности потока. Основная сложность использования современных методов определяется необходимостью детектирования атаки в условиях возможного применения различных сценариев атакующей стороной. Использование отдельного временного окна [2–4], характерное для современных методов обнаружения атаки, ограничивает чувствительность системы детектирования вследствие неопределенности сценария, используемого атакующей стороной. Неопределенность временных характеристик атаки (плавное, скачкообразное, ступенчатое и т.д. изменение потока запросов) приводит к невозможности оптимального выбора ширины окна. В свою очередь это вызывает невозможность отделения атаки от возникновения внезапного повышения спроса к ресурсу. Предлагаемый метод анализа использует двухэтапный подход. Метод идентификации степени опасности основан на одновременном анализе статистики в нескольких временных окнах, каждое из которых имеет уникальное значение ширины. Степень опасности определяется на основе характеристик программно-аппаратных средств, использующихся для доступа к ресурсу. При возникновении угрозы используется метод глубокого анализа. Целью анализа является идентификация причин повышенного спроса к ресурсу [1]. На этом этапе происходит обработка полей заголовков IP-пакетов с использованием локально хранимых списков, характеризующих историю доступа к ресурсу. IP-адрес и порт получателя используются для идентификации жертвы атаки. IP-адрес, порт источника и значения флагов позволяют отделить атаку от возникновения повышенного спроса к ресурсу. В случае если детектирована атака, эти поля заголовка позволяют также определить тип сетевой атаки.

Результаты. Предложен метод двухэтапного анализа потока запросов на предоставление сетевого ресурса. Разработан метод решения задачи детектирования изменения статистического распределения, основанный на использовании набора временных окон. Использование метода позволяет проводить анализ степени опасности ситуации с точки зрения доступности сетевого ресурса. Предложен метод анализа потока запросов к ресурсу в ситуации возникновения риска атаки. Разработано программное обеспечение, реализующее функции предлагаемых численных методов. Проведены численные исследования с использованием набора данных [5].

Выводы. К преимуществам использования предложенного метода можно отнести раннее определение атак и возможность детализации картины событий в информационной сети. Присутствует возможность использования программного обеспечения как отдельно, так и совместно с другими средствами защиты информации. Перспективы разработки связаны с реализацией методов глубокого машинного обучения при построении систем мониторинга. Масштабируемость решения позволяет использовать метод

при построении как систем мониторинга конкретного сетевого ресурса, так и распределенных системы контроля. Актуальность использования метода связана с развитием новых сетевых технологий (Internet of Things, Internet everywhere) и технологий, архитектура которых включает сетевые решения («умные» технологии, наземные транспортные системы нового поколения, технологии автономных интеллектуальных агентов).

Ключевые слова: запрос на предоставление ресурса; сетевая атака; статистический анализ; временное окно; мониторинг; IDS; средства защиты информации.

Список литературы

1. Фаткиева Р.Р. Разработка метрик для обнаружения атак на основе анализа сетевого трафика // Вестник Бурятского государственного университета. Математика, информатика. 2013. № 9. С. 81–86.
2. Терновой О.С. Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности в результате ddos атак // Известия Алтайского государственного университета. 2013. Т. 2, № 1. С. 123–125. DOI: 10.14258/izvasu(2013)1.2-24
3. Zhou Z., Gaurav A., Gupta B.B., et al. A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic // Neural Comput Appl. 2021. P. 1–14. DOI: 10.1007/s00521-021-06389-6
4. Gavrilis D., Dermatas E. Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features // Comput Networks. 2005. Vol. 48, No. 2. P. 235–245. DOI: 10.1016/j.comnet.2004.08.014
5. Erhan D., Anarım E. Boğaziçi University distributed denial of service dataset // Data in brief. 2020. Vol. 32. ID 106187. DOI: 10.1016/j.dib.2020.106187

Сведения об авторах:

Павел Александрович Серов — студент, группа ЭИЗ-19(с); филиал Самарского государственного технического университет в г. Сызрани, Россия. E-mail: serov.archer@gmail.com

Дмитрий Алексеевич Панов — студент, группа ЭИ-20; филиал Самарского государственного технического университет в г. Сызрани, Россия. E-mail: dimapanov571@gmail.com

Сергей Сергеевич Иванов — студент, группа ЭИЗ-19(с); филиал Самарского государственного технического университет в г. Сызрани, Россия. E-mail: teamparker17@gmail.com

Кристина Владимировна Садова — научный руководитель; старший преподаватель кафедры «Информатика и системы управления»; филиал Самарского государственного технического университет в г. Сызрани, Россия. E-mail: crazyojj@mail.ru