ВВЕДЕНИЕ В АНОМАЛЬНЫЕ ТРАФИКИ: ОБЪЯСНЕНИЕ ПОНЯТИЯ АНОМАЛЬНЫХ ТРАФИКОВ В КОНТЕКСТЕ СЕТЕВОЙ БЕЗОПАСНОСТИ И АНАЛИЗА ДАННЫХ

Нилуфар Кахрамоновна Абдулхамидова

Ферганский филиал Ташкентского университета информационных технологий, студент магистратуры, Ферганский область, г.Кувасай, ул.А.Наваи 128-45
softmint27@gmail.com

Сугдиёна Илхомжон кизи Мамадалиева

Ферганский филиал Ташкентского университета информационных технологий, студент магистратуры, Ферганский область, район Бувайда, ул.Сой-Буйи 4
ibrohimovasugdiyona98@gmail.com

Тураева Дилфузахан Салижановна

Аспирант Ферганского филиала Ташкентского университета информационных технологий, г.Фергана, ул. Нурли, дом 56.

dilfuzaturayeva42@gmail.com

Аннотация: Статья представляет введение в аномальные трафики в контексте сетевой безопасности и анализа данных. В ней объясняется понятие аномальных трафиков, их причины и последствия. Рассматривается важность обнаружения и анализа аномальных трафиков для обеспечения безопасности сетей.

Ключевые слова: Аномальные трафики, сетевая безопасность, анализ данных, обнаружение аномалий.

Введение

В современном цифровом мире обеспечение безопасности сетей становится все более важным. Аномальные трафики, которые могут указывать на наличие вредоносных активностей или необычных сетевых событий, являются одним из ключевых аспектов сетевой безопасности. В данной статье мы рассмотрим понятие аномальных трафиков, их причины и последствия, а также важность обнаружения и анализа таких трафиков для обеспечения безопасности сетей.

Основная часть

Аномальные трафики в сетевой безопасности относятся к необычным или отклоняющимся от нормы сетевым активностям. Они могут включать в себя атаки, вирусы, вредоносные программы, нежелательную почту, а также другие необычные сетевые события. Аномальные трафики могут возникать из-за различных причин, включая злонамеренные действия хакеров, системные сбои, ошибки в конфигурации сети или некорректное поведение пользователей.

Аномальные трафики могут быть вызваны различными причинами. Одной из причин является наличие вредоносных активностей, таких как атаки на сетевую инфраструктуру или компьютеры. Некорректная конфигурация сети или программного обеспечения также может привести к возникновению аномальных трафиков. Кроме

того, ошибки пользователя, такие как некорректное использование сетевых ресурсов или подозрительное поведение, могут также вызвать аномальные трафики.

Аномальные трафики могут иметь серьезные последствия для сетевой безопасности и функционирования сети в целом. Они могут привести к утечке конфиденциальных данных, нарушению целостности системы, отказу в обслуживании (DoS) или повреждению ресурсов сети. Атаки, осуществляемые через аномальные трафики, могут привести к финансовым потерям, потере репутации и нарушению доверия клиентов.

Важность обнаружения и анализа аномальных трафиков: Обнаружение и анализ аномальных трафиков играют ключевую роль в обеспечении безопасности сетей. Раннее обнаружение таких трафиков позволяет принять меры по предотвращению возможных атак или нарушений безопасности. Анализ аномальных трафиков позволяет выявить паттерны и характеристики необычной активности, что в свою очередь помогает в построении более эффективных стратегий защиты и принятии соответствующих мер по обеспечению безопасности.

Существуют различные методы и технологии для обнаружения и анализа аномальных трафиков. Это включает использование систем обнаружения вторжений (IDS), систем анализа потока данных (DPI), машинного обучения и статистического анализа данных. Эти инструменты позволяют автоматически обнаруживать и классифицировать аномальные трафики, а также идентифицировать новые и ранее неизвестные угрозы.

Однако, необходимо учитывать, что обнаружение аномальных трафиков часто сопровождается ложными срабатываниями. Некорректная классификация нормальной активности как аномальной может привести к проблемам и снижению производительности сети. Поэтому важно применять методы и технологии анализа, которые максимально снижают количество ложных срабатываний и обеспечивают высокую точность обнаружения.

Заключение

Аномальные трафики представляют собой важный аспект сетевой безопасности. Их обнаружение и анализ позволяют предотвратить потенциальные атаки, защитить конфиденциальные данные и обеспечить надежную работу сети. Применение современных методов анализа данных и технологий искусственного интеллекта позволяет эффективно обнаруживать аномальные трафики и принимать соответствующие меры по обеспечению безопасности. Развитие и совершенствование этих методов будет продолжаться, чтобы бороться с постоянно изменяющимися угрозами и обеспечивать безопасность в сетевой среде.

Список использованных литературы

1. Mukhtarov, F. . (2023). IMPROVING THE METHODOLOGY OF TEACHING THE SCIENCE OF "CYBERSECURITY FUNDAMENTALS" IN THE CONDITIONS OF IDEOLOGICAL THREATS. International Bulletin of Engineering and Technology, 3(9), 38–44. Retrieved from https://internationalbulletins.com/intjour/index.php/ibet/article/view/1030
2. Mukhtarov, F. M. (2023). THE POWER OF CYBERSECURITY EDUCATION: DEFENDING AGAINST DIGITAL THREATS. *GOLDEN BRAIN*, *1*(26), 63–66. Retrieved from https://researchedu.org/index.php/goldenbrain/article/view/4816

3. Хусанова, М., Мухториддинов, М., & Ганиева, Ш. (2023). AN OVERVIEW OF NETWORK SECURITY AND MONITORING TECHNIQUES. *Conference on Digital Innovation : "Modern Problems and Solutions"*. извлечено от https://fer-teach.uz/index.php/codimpas/article/view/1359
4. Садирова, Х., Хусанова, М., & Акбаров, Н. (2023). INTRUSION DETECTION AND PREVENTION SYSTEMS FOR NETWORK SECURITY. *Conference on Digital Innovation : "Modern Problems and Solutions"*. извлечено от https://fer-teach.uz/index.php/codimpas/article/view/1360
5. Muxtarov, F. (2023). AXBOROT XAVFSIZLIGIDA VEB-FILTRLASHNING VAZIFALARI VA MUAMMOLARI. *Research and Implementation*. извлечено от https://fer-teach.uz/index.php/rai/article/view/1008
6. Рахматов, Р., Умаров, А., & Хусанова, М. (2023). NETWORK TRAFFIC ANALYSIS FOR SECURITY MONITORING. *Conference on Digital Innovation : "Modern Problems and Solutions"*. извлечено от https://fer-teach.uz/index.php/codimpas/article/view/1361