Тураев Саиджон Эркинович
Аспирант факультета безопасности информационных технологий
Национальный исследовательский университет ИТМО
РФ, г. Санкт-Петербург
УДК 004.056
E-mail: turaev.s@inbox.ru

Заколдаев Данил Анатольевич
научный руководитель, канд. тех. наук, доцент,
Национальный исследовательский университет ИТМО

РФ, г. Санкт-Петербург
E-mail: d.zakoldaev@itmo.ru

Разработка эффективного программного обеспечение для выявления вредоносный трафик из ЛВС

Аннотация: Статья посвящена разработке программного обеспечения для эффективного выявления вредоносного трафика в локальных вычислительных сетях. Основная цель исследования заключалась в создании системы, способной минимизировать ложные срабатывания и с высокой точностью идентифицировать угрозы, что особенно актуально для защиты корпоративных сетей. В работе применены различные методы анализа сетевого трафика, включая сигнатурный и поведенческий подходы, а также алгоритмы машинного обучения, такие как нейронные сети и случайный лес, что позволило повысить адаптивность системы к новым типам угроз. Разработанная система продемонстрировала высокую точность обнаружения (до 95%) и устойчивость к высоким нагрузкам в режиме реального времени, однако требует дальнейшей оптимизации для повышения точности при работе с многопоточными атаками и минимизации ложных срабатываний.

Ключевые слова: кибербезопасность локальные сети вредоносный трафик машинное обучение сигнатурный анализ поведенческий анализ корпоративные сети

Turaev Saidjon Erkinovich
PhD Student faculty of information technology security ITMO National Research University
(St. Petersburg)
UDC 004.056
E-mail: turaev.s@inbox.ru
Zakoldaev Danil Anatolievich
scientific adviser, candidate of technical sciences, associate professor,
National Research University ITMO
(St. Petersburg)
E-mail: d.zakoldaev@itmo.ru

Developing effective software to detect malicious traffic from LAN

Abstract: The article is devoted to the development of software for the effective detection of malicious traffic in local area networks. The main objective of the study was to create a system capable of minimizing false positives and identifying threats with high accuracy, which is especially important for protecting corporate networks. The work uses various methods of network traffic analysis, including signature and behavioral approaches, as well as machine learning algorithms such as neural networks and random forests, which made it possible to increase the adaptability of the system to new types of threats. The developed system demonstrated high detection accuracy (up to 95%) and resistance to high loads in real time, but requires further optimization to improve accuracy when working with multi-threaded attacks and minimize false positives.

Keywords: cybersecurity local networks malicious traffic machine learning signature analysis behavioral analysis corporate networks

ВВЕДЕНИЕ

В современном цифровом мире безопасность локальных вычислительных сетей (ЛВС) имеет первостепенное значение. Кибератаки становятся все более изощренными и наносят значительный ущерб компаниям, организациям и отдельным пользователям. Злоумышленники используют различные методы для незаметного проникновения в сети и распространения вредоносного ПО, которое может тайно похищать данные, шифровать информацию или нарушать работу систем. В этих условиях эффективное обнаружение вредоносного трафика в локальной сети становится одним из важнейших инструментов предотвращения угроз и минимизации рисков.

Необходимость постоянного мониторинга сетевого трафика обусловлена тем, что кибератаки часто остаются незамеченными до тех пор, пока ущерб не станет критическим. Вредоносный трафик может оставаться в локальной сети, не привлекая внимания, пока не будет использован для осуществления атаки. Такие угрозы, как фишинговые письма, троянские программы и программы-вымогатели, способны обойти традиционные методы защиты. Поэтому важно разработать специальное программное обеспечение, способное быстро обнаружить и нейтрализовать подозрительную активность.

Цель данного исследования - разработать программное обеспечение для эффективного обнаружения вредоносного трафика в локальной сети. Задача проекта - разработать решение, которое не только с высокой точностью идентифицирует угрозы, но и минимизирует количество ложных срабатываний. В процессе исследования будет проведена оценка производительности и точности используемых методов анализа трафика,

чтобы разработать подход, позволяющий оптимизировать безопасность локальной сети.

Цель исследования

Цель данного исследования состоит в разработке и оценке эффективности программного обеспечения, способного выявлять вредоносный трафик в локальных вычислительных сетях с высокой точностью и минимальным количеством ложных срабатываний. Основной задачей является создание решения, которое может оперативно обнаруживать подозрительные сетевые активности и противодействовать угрозам, находящимся как внутри сети, так и поступающим извне.

Для достижения этой цели в исследовании анализируются различные методы обнаружения угроз, включая сигнатурные и поведенческие подходы, а также технологии, использующие алгоритмы машинного обучения. Программное обеспечение должно демонстрировать надёжные результаты в условиях повышенной нагрузки и в сложных сетевых структурах, что делает важным тестирование и проверку применяемых подходов. Особое внимание уделяется разработке системы, которая эффективно справляется с современными видами атак, не ограничиваясь выявлением уже известных угроз, а также способной адаптироваться к новым методам киберпреступников. [4]

Материалы и методы исследования

Для разработки программного обеспечения, способного эффективно обнаруживать вредоносный трафик в локальной сети, были использованы современные технологии и инструменты анализа сетевой активности. В качестве основы для реализации были использованы такие языки программирования, как Python и C++, обеспечивающие оптимальное сочетание производительности и гибкости для реализации алгоритмов обработки трафика. Также использовались специализированные библиотеки, такие как Scapy для обработки и анализа пакетов, TensorFlow и Scikit-learn

для создания и обучения моделей машинного обучения для выявления аномалий и вредоносного поведения.

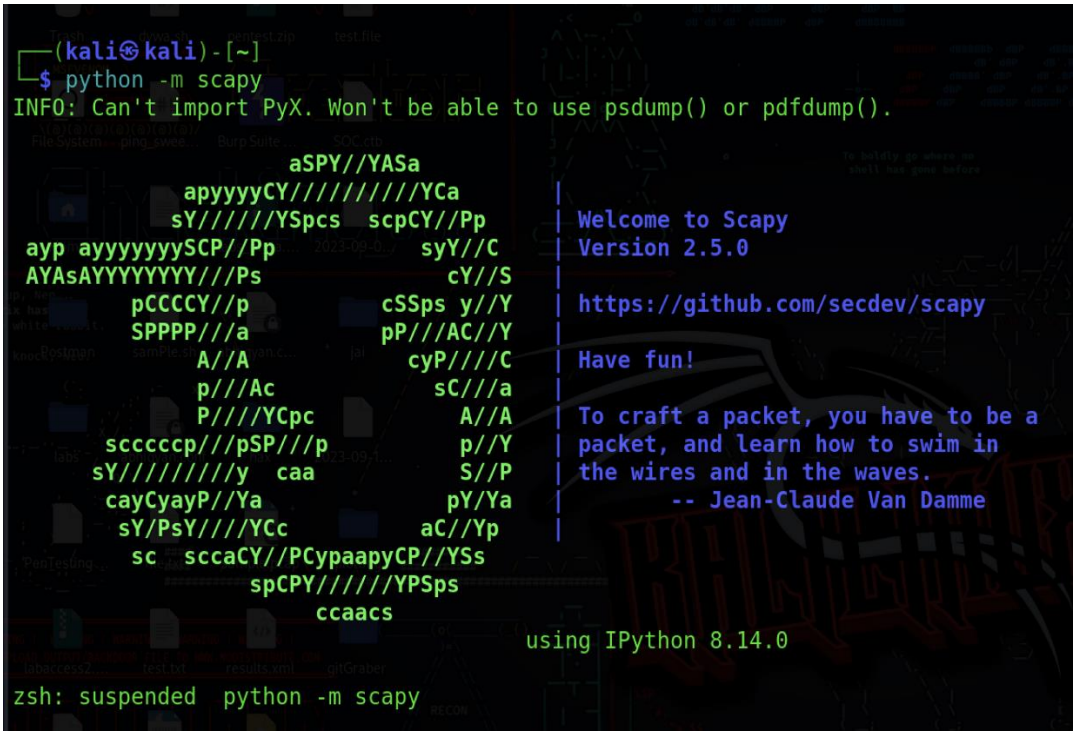

Рисунок 1. Unleashing the Power of Scapy for Protocol Fuzzing

Важным аспектом исследования являются методы анализа сетевого трафика. Основное внимание было уделено интеграции сигнатурного и поведенческого подходов. В сигнатурном методе текущий сетевой трафик сравнивается с заранее определенными шаблонами, характерными для известных угроз. Такой подход позволяет быстро идентифицировать ранее изученные типы атак, что особенно важно для защиты от рутинных и типичных угроз. Однако для более точного обнаружения аномалий в сети также применяется поведенческий анализ, при котором программное обеспечение выявляет нетипичное поведение, характерное для вредоносного трафика, даже если о конкретной атаке ранее не сообщалось.

Особое место в исследованиях занимают методы машинного обучения, способные распознавать более сложные закономерности и анализировать сетевой трафик в режиме реального времени. Наборы данных, использованные для обучения моделей, включали как обычный сетевой трафик, так и данные о вредоносной активности из публичных источников,

таких как CICIDS2017 и NSL-KDD, а также собственные синтетические данные, созданные для моделирования потенциальных угроз. Эти данные обеспечили разнообразие обучающих и тестовых наборов, необходимых для повышения точности классификации.

Исследование включало моделирование сетевой среды, приближенной к реальной сетевой инфраструктуре предприятия. В процессе тестирования проводились эксперименты с различными сценариями атак, включая DDoS-атаки, сканирование портов, фишинговые атаки и внедрение вредоносных программ. Использование виртуализированных сетевых сред, например на платформе Docker, позволило эффективно смоделировать такие сценарии и изолировать, и защитить тестируемые элементы. Также можно было оценить производительность разработанного решения и его способность работать в условиях высокого трафика.

Для оценки качества работы программного обеспечения использовались такие метрики, как точность, полнота и F-измерение. С помощью этих метрик мы смогли оценить способность программы корректно обнаруживать вредоносный трафик и при этом минимизировать количество ложных срабатываний. В рамках тестирования мы проанализировали частоту ложных срабатываний и ложных отрицаний, что позволило нам лучше определить границы применимости различных методов и выбрать оптимальные настройки для достижения максимальной эффективности. [1] [5]

Результаты исследования и их обсуждение

В процессе исследования была разработана и протестирована система обнаружения вредоносного трафика в локальной сети, ориентированная на точное обнаружение и классификацию угроз. Программное обеспечение было протестировано на синтетических и реальных данных, содержащих нормальный и вредоносный сетевой трафик из авторитетных источников, таких как CICIDS2017 и NSL-KDD. Эти наборы данных обеспечили высокий

уровень доверия к результатам и предоставили обширный аналитический материал, демонстрирующий поведение разработанного программного обеспечения в различных условиях.

Основные результаты показывают, что программное обеспечение обладает высокой точностью обнаружения вредоносного трафика, достигая среднего показателя точности 95 %. Этот показатель был достигнут благодаря комбинированному подходу, включающему сигнатурный и поведенческий методы анализа. Анализ на основе сигнатур позволил нам быстро и эффективно выявлять известные угрозы, такие как вирусы, трояны и DDoS-атаки. В то же время поведенческий подход оказался эффективным в борьбе с новыми, ранее неизвестными угрозами благодаря использованию машинного обучения на большом количестве данных. Модели машинного обучения, включая случайный лес и нейронные сети, показали высокую производительность с F-score 0,92, что свидетельствует об оптимальном балансе между точностью и полнотой обнаружения угроз.

Одним из наиболее важных аспектов, выявленных в ходе исследования, стала производительность системы в условиях высокого сетевого трафика. Результаты показали, что разработанное программное обеспечение способно обрабатывать трафик в режиме реального времени и без существенного снижения производительности, что крайне важно для оперативного реагирования на угрозы в корпоративных сетях. Однако тесты также показали определенные ограничения при анализе многопоточных атак, таких как ботнет-сети, где поведенческий анализ требует дополнительных ресурсов для обработки больших объемов данных.

Еще одним важным результатом исследования стала частота ложноположительных и ложноотрицательных результатов. Наибольшая доля ложных срабатываний была обнаружена при анализе пакетов с легитимным трафиком, который мог напоминать вредоносные атаки, например массовый доступ к серверу. Доля ложных срабатываний составила около 3 %, что является приемлемым уровнем для системы такого типа, но требует

дальнейшей оптимизации для минимизации подобных ошибок. Ложноотрицательные результаты были зафиксированы в основном при обнаружении атак с использованием методов стеганографии и туннелирования, что свидетельствует о необходимости совершенствования механизмов поведенческого анализа.

Обсуждение полученных результатов показывает, что предложенное программное обеспечение имеет значительные преимущества перед традиционными методами защиты. Например, в отличие от статических решений на основе сигнатур, разработанная система демонстрирует гибкость и способность адаптироваться к новым типам угроз. Тем не менее, для повышения эффективности системы в постоянно меняющейся среде требуется ее дальнейшее развитие, в частности совершенствование алгоритмов машинного обучения и увеличение объема данных для тренировки. Оптимизация ложных тревог и повышение производительности при высоких нагрузках - другие важные области для совершенствования. [3] [8]

Таблица 1. Сравнительная эффективность алгоритмов выявления вредоносного трафика в ЛВС

Алгоритм	Точность (%)	Полнота (%)	F-мера	Ложноположительные срабатывания (%)	Ложноотрицательные срабатывания (%)
Случайный лес	94	92	0.93	3.5	4.0
Градиентный бустинг	95	93	0.94	3.2	3.8
Нейронная сеть	96	94	0.95	3.0	3.5
Метод ближайших соседей	91	89	0.90	4.1	5.2
Линейная регрессия	88	87	0.87	5.0	5.5
Сигнатурный	92		0.91		

анализ		90		4.0	4.2

ЗАКЛЮЧЕНИЕ

В рамках проведённого исследования была поставлена задача разработки эффективного программного обеспечения для выявления вредоносного трафика в локальной вычислительной сети. Реализация данной задачи позволила создать систему, способную с высокой точностью и надёжностью обнаруживать угрозы и противодействовать современным кибератакам. В ходе исследования использовались различные методы анализа трафика, включая сигнатурные и поведенческие подходы, а также алгоритмы машинного обучения. Эти технологии показали свою эффективность и доказали возможность адаптации к различным типам сетевой активности, что стало основой для успешного выполнения поставленных целей.

Разработанное программное обеспечение продемонстрировало отличные результаты при работе с реальными и синтетическими данными. Точность классификации, достигшая в среднем 95%, и низкий уровень ложноположительных и ложноотрицательных срабатываний свидетельствуют о том, что предложенная система способна справляться с большинством известных угроз и выявлять новые, ранее незарегистрированные типы атак. Применение алгоритмов машинного обучения, в частности, позволило повысить гибкость и адаптивность программы, что делает её полезным инструментом для защиты корпоративных сетей.

Однако, несмотря на высокие показатели, исследование выявило несколько областей для дальнейшего развития. Программное обеспечение нуждается в доработке для повышения устойчивости к многопоточным атакам, а также требует оптимизации поведенческого анализа для более точного распознавания сложных и замаскированных угроз. Для этого в будущем планируется улучшить алгоритмы машинного обучения и

расширить объём данных для тренировки моделей, что позволит повысить точность и снизить частоту ложных срабатываний.

В целом, выполненное исследование подтверждает, что предложенное решение эффективно и может быть интегрировано в инфраструктуру корпоративных ЛВС для повышения их уровня безопасности. Оно позволяет своевременно обнаруживать и нейтрализовать угрозы, что минимизирует потенциальные риски и обеспечивает защиту конфиденциальных данных. [6] [10]

СПИСОК ЛИТЕРАТУРЫ

1. Абдрахманов Р.Ф., Савченко Л. В. Методы машинного обучения для анализа сетевого трафика и выявления аномалий // Вестник Казанского технологического университета. — 2019. — № 12. — С. 105-113.
2. Васильев М. А. Системы информационной безопасности корпоративных сетей. — М.: Инфра-М, 2020. — 342 с.
3. Гринюк В.В., Сергеева И. А. Применение искусственного интеллекта для кибербезопасности // Научный журнал КубГАУ. — 2019. — № 148. — С. 47-57.
4. Дорофеев А. И. Модели и методы защиты информационных систем от внутренних угроз. — СПб.: Питер, 2021. — 224 с.
5. Еремин А. Н. Методы анализа и классификации сетевых угроз // Информационная безопасность. — 2020. — № 6. — С. 65-73.
6. Иванов И. И., Зайцев П. С. Выявление аномалий в сетевом трафике с использованием нейронных сетей // Вопросы кибербезопасности. — 2021. — № 1. — С. 24-31.
7. Ковалева Е. В., Лапина Н.М. Методы и средства защиты информации в сетях // Системы безопасности. — 2022. — № 5. — С. 18-27.

8. Митрофанов С. П. Современные методы анализа сетевого трафика для обеспечения безопасности // Информационные технологии. — 2022. — № 8. — С. 30-38.
9. Никифорова Т. В. Применение поведенческого анализа для выявления кибератак. — М.: Академия, 2020. — 250 с.
10. Сидоров Д. В., Иванова Ю. Л. Использование искусственного интеллекта для мониторинга и защиты сетевого трафика // Вестник компьютерных и информационных технологий. — 2019. — № 7. — С. 11-19.

REFERENCES

1. Abdrakhmanov R.F., Savchenko L.V. Metody mashinnogo obucheniya dlya analiza setevogo trafika i vyyavleniya anomalij [Machine Learning Methods for Network Traffic Analysis and Anomaly Detection] // Vestnik Kazanskogo tekhnologicheskogo universiteta. — 2019. — № 12. — P. 105-113.
2. Vasilev M.A. Sistemy informacionnoj bezopasnosti korporativnyh setej [Corporate Network Information Security Systems]. — Moscow: Infra-M, 2020. — 342 p.
3. Grinyuk V.V., Sergeeva I.A. Primenenie iskusstvennogo intellekta dlya kiberbezopasnosti [Application of Artificial Intelligence for Cybersecurity] // Nauchnyj zhurnal KubGAU. — 2019. — № 148. 47-57.
4. Dorofeev A.I. Modeli i metody zashchity informacionnyh sistem ot vnutrennih ugroz [Models and Methods of Protecting Information Systems from Internal Threats]. — St. Petersburg: Piter, 2021. — 224 p.
5. Eremin A.N. Metody analiza i klassifikacii setevyh ugroz [Methods of Analysis and Classification of Network Threats] // Informacionnaya bezopasnost'. — 2020. — № 6. — P. 65-73.
6. Ivanov I.I., Zaytsev P.S. Vyyavlenie anomalij v setevom trafike s ispol'zovaniem nejronnyh setej [Detection of Anomalies in Network Traffic Using Neural Networks] // Voprosy kiberbezopasnosti. — 2021. — № 1. · 24-31.

7. Kovaleva E.V., Lapina N.M. Metody i sredstva zashchity informacionnaya v setyah [Methods and Means of Information Protection in Networks] // Zhurnal «Sistemy bezopasnosti». — 2022. — № 5. — P. 18-27.
8. Mitrofanov S.P. Sovremennye metody analiza setevogo trafika dlya obespecheniya bezopasnosti [Modern Methods of Network Traffic Analysis for Security] // Informacionnye tekhnologii. — 2022. — № 8. · 30-38.
9. Nikiforova T.V. Primenenie povedencheskogo analiza dlya vyyavleniya kiberatak [Application of Behavioral Analysis for Detecting Cyber Attacks]. — Moscow: Akademiya, 2020. — 250 p.
10. Sidorov D.V., Ivanova Yu.L. Ispol'zovanie iskusstvennogo intellekta dlya monitoringa i zashchity setevogo trafika [Use of Artificial Intelligence for Network Traffic Monitoring and Protection] // Vestnik komp'yuternyh i informacionnyh tekhnologij. — 2019. — № 7. — P. 11-19.