Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 654.01

ГРИБОВИЧ
Александр Александрович

ИССЛЕДОВАНИЕ СУЩЕСТВУЮЩИХ АЛГОРИТМОВ ПО КОНТРОЛЮ И ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА

Автореферат
на соискание степени магистра
по специальности 1–45 80 01 Системы и сети инфокоммуникаций

_____

Научный руководитель
кандидат технических наук, доцент
МЕДВЕДЕВ Сергей Александрович

_____

Минск 2024

ВВЕДЕНИЕ

В современном мире обеспечение безопасности сетей становится всё более актуальным, особенно на фоне растущих угроз в интернете. С увеличением количества кибератак и совершенствованием методов злоумышленников, предприятия и организации вынуждены уделять больше внимания защите своих сетей и данных. Эффективная защита сети требует комплексного подхода, который включает в себя как превентивные меры, так и оперативное реагирование на инциденты безопасности.

Концепция сетевого мониторинга безопасности (NSM) заключается в сборе, анализе и реагировании на признаки вторжений и аномальной активности в сети. Этот процесс позволяет своевременно выявлять и нейтрализовать угрозы, минимизируя потенциальный ущерб. NSM включает несколько ключевых фаз: планирование, сопротивление, обнаружение и реагирование. В каждой из этих фаз применяются различные методы и инструменты, которые помогают специалистам по безопасности контролировать и защищать сетевую инфраструктуру.

Для эффективного сетевого мониторинга используются различные инструменты, такие как Nmap для генерации трафика и имитации атак, BurpSuite для анализа веб-приложений и выполнения атак, а также Wireshark, Fiddler и Microsoft Network Monitor для мониторинга и анализа сетевого трафика. Каждый из этих инструментов обладает своими уникальными возможностями и подходит для различных сценариев использования.

Цель данного исследования — оценить и сравнить возможности этих инструментов, выявить их сильные и слабые стороны, а также предложить рекомендации по их применению в различных условиях.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 6 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «Обеспечение безопасности человека, общества, государства». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной является выяснение эффективности работы популярных бесплатных программных средств по мониторингу и фильтрации сетевого трафика. Проработать критерии привлекательности для потенциального заказчика программного средства

Для достижения поставленной цели в диссертации решены следующие задачи:

1 В подходящей сетевой среде провести исследование и сравнение выбранных программных средств,

2 Выделить их преимущества и недостатки.

Личный вклад соискателя ученой степени

Содержание диссертации отображает личный вклад автора. Он заключается в научном исследовании методов по мониторингу и контролю трафика, выбора программных средств для исследования, постановке и проведении экспериментов по исследованию характеристик, оценке эффективности исследуемых алгоритмов, обработке и анализе полученных результатов, формулировке выводов.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем кандидатом технических наук, доцентом Медведевым Сергеем Александровичем

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на: 60-й научной конференции аспирантов, магистрантов и студентов учреждения образования «БГУИР»

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 3 печатных работы, в том числе: 3 статей и тезисов в сборниках и материалах конференций.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трех глав с выводами по каждой главе, заключения, библиографического списка, восьми приложений.

Общий объем диссертационной работы составляет 61 страниц, из них 50 страниц текста, 9 рисунков на 9 страницах, 2 таблиц на 2 страницах, список использованных библиографических источников (13 наименований), список публикаций автора по теме диссертации (3 наименования на 6 страницах), графический материал на 11 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Грибовича Александра Александровича «Исследование существующих алгоритмов по контролю и фильтрации сетевого трафика» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 28.06.2024 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 97й %).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В современном мире обеспечение безопасности сетей становится всё более актуальным, особенно на фоне растущих угроз в интернете. Концепция сетевого мониторинга безопасности (NSM) заключается в сборе, анализе и реагировании на признаки вторжений, что позволяет эффективно выявлять аномалии и вредоносную активность. Процесс сетевого мониторинга безопасности включает несколько ключевых фаз: планирование, сопротивление, обнаружение и реагирование. На этапе планирования IT-команды и специалисты по безопасности анализируют текущую ситуацию, разрабатывают меры защиты, проводят тестирование на проникновение и симуляции атак. В фазе сопротивления применяются автоматизированные средства защиты, такие как брандмауэры и антивирусы, а также проводится обучение и управление конфигурациями.

Фазы обнаружения и реагирования включают сбор и анализ данных для выявления аномалий. Сбор данных осуществляется с помощью различных методов, таких как захват пакетов, анализ сетевых потоков, системы обнаружения вторжений (IDS), управление информацией и событиями безопасности (SIEM), журналирование DNS и DHCP серверов, и мониторинг конечных точек (EDR). Существует несколько методов сбора данных, каждый из которых имеет свои преимущества и недостатки. Например, захват пакетов позволяет детально анализировать сетевой трафик, но неэффективен против шифрованных данных. Анализ сетевых потоков предоставляет информацию о сетевых соединениях, но требует специальных сенсоров и систем для обработки данных.

Для эффективного управления безопасностью сети важно постоянно обновлять политики безопасности и тщательно проверять конфигурации конечных точек. Организации могут быть на разных стадиях внедрения инфраструктуры NSM, от начального этапа определения потребностей до активного анализа и совершенствования стратегий сбора данных. Собранные сетевые данные помогают выявлять закономерности и аномалии, предоставляя ценную информацию для улучшения диагностики и устранения угроз. Таким образом, мониторинг сетевых данных и активности пользователей играет ключевую роль в защите сети от вредоносных атак.

Wireshark, Fiddler и Microsoft Network Monitor показали различные сильные и слабые стороны в процессе мониторинга сетевого трафика, сгенерированного Nmap и BurpSuite. Wireshark отличается глубоким анализом пакетов, широкими возможностями фильтрации и декодирования, а также

удобным графическим интерфейсом, но имеет меньшую производительность при высоких нагрузках по сравнению с Fiddler. Fiddler специализируется на HTTP/HTTPS трафике, обеспечивает удобный анализ веб-трафика, поддержку скриптов и расшифровки HTTPS, но ограничен только HTTP/HTTPS трафиком и требует больше ресурсов памяти. Microsoft Network Monitor хорошо поддерживает анализ всего сетевого трафика, интегрируется с Windows и имеет удобный интерфейс, но обладает меньшим количеством функций по сравнению с Wireshark и устаревшим интерфейсом по сравнению с современными инструментами.

Общий вывод заключается в том, что Wireshark является наиболее мощным и универсальным инструментом для анализа сетевого трафика, обеспечивая глубокий анализ и детальную визуализацию. Fiddler отлично подходит для анализа веб-трафика (HTTP/HTTPS) и выполнения задач, связанных с тестированием веб-приложений. Microsoft Network Monitor предоставляет хорошую поддержку анализа сетевого трафика, но уступает по функциональности и интерфейсу современным инструментам.

ЗАКЛЮЧЕНИЕ

Обеспечение безопасности сетей становится всё более актуальным из-за растущих угроз в интернете. Концепция сетевого мониторинга безопасности (NSM) играет ключевую роль в защите сетей, обеспечивая сбор, анализ и реагирование на признаки вторжений. Основные фазы NSM включают планирование, сопротивление, обнаружение и реагирование. На каждом этапе применяются различные методы и инструменты для выявления аномалий и предотвращения вредоносной активности.

Эффективный сетевой мониторинг включает использование различных методов сбора данных, таких как захват пакетов, анализ сетевых потоков и системы обнаружения вторжений. Каждый метод имеет свои преимущества и ограничения, что требует комплексного подхода и использования мультиаспектной методологии для оценки инструментов сетевого контроля. Важно учитывать сценарии использования, размер сети и уникальные особенности каждого инструмента, такие как Wireshark, Fiddler и Microsoft Network Monitor.

Wireshark выделяется своей универсальностью и глубиной анализа пакетов, хотя при высоких нагрузках его производительность может снижаться. Fiddler специализируется на анализе веб-трафика (HTTP/HTTPS) и предлагает удобный интерфейс и поддержку скриптов, однако ограничен только этими типами трафика и требует больше ресурсов памяти. Microsoft Network Monitor хорошо интегрирован с Windows и поддерживает анализ всего сетевого трафика, но уступает Wireshark по количеству функций и имеет устаревший интерфейс.

Выбор подходящих инструментов и методов для сетевого мониторинга зависит от конкретных потребностей и условий эксплуатации. Комплексный подход к оценке инструментов сетевого контроля, учитывающий различные аспекты и критерии, позволяет обеспечивать достоверные результаты и улучшать стратегии сетевой безопасности.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1–А. Грибович, А. А. Сравнительный анализ протоколов передачи данных LORAWANи SIGFOX/ Клепцов Ю.В., Грищук А.А., Грибович А.А.// 60-я научная конференция аспирантов, магистрантов и студентов: тезисы докладов 60-ой научной конференции аспирантов, магистрантов и студентов БГУИР. Минск, 21-24 апреля 2024 г. / редкол.: В. Ю. Цветков [и др.]. – Минск: БГУИР, 2024. –С.__.

2–А. Грибович, А. А. Система автоматической идентификации объектов/ Клепцов Ю.В., Грищук А.А., Грибович А.А.// 60-я научная конференция аспирантов, магистрантов и студентов: тезисы докладов 60-ой научной конференции аспирантов, магистрантов и студентов БГУИР. Минск, 21-24 апреля 2024 г. / редкол.: В. Ю. Цветков [и др.]. – Минск: БГУИР, 2024. –С.__.

3–А. Грибович, А. А. Анализ сетевого трафика. Методы сбора сетевых признаков и предложений для обнаружения вторжений/ Клепцов Ю.В., Грибович А.А., Грищук А.А.// 60-я научная конференция аспирантов, магистрантов и студентов: тезисы докладов 60-ой научной конференции аспирантов, магистрантов и студентов БГУИР. Минск, 21-24 апреля 2024 г. / редкол.: В. Ю. Цветков [и др.]. – Минск: БГУИР, 2024. –С.__.