Удальцов К.Р. Исследование системы анализа сетевого трафика ZEEK // Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 11(49) с. 33–36

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ИССЛЕДОВАНИЕ СИСТЕМЫ АНАЛИЗА СЕТЕВОГО ТРАФИКА ZEEK

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

Статья представляет собой глубокое исследование системы анализа сетевого трафика Zeek (ранее известной как Bro). Zeek - это мощный инструмент для мониторинга сетевой активности и выявления угроз в реальном времени. В статье рассматриваются основные функции и возможности Zeek, включая его способность обнаруживать сложные атаки, обеспечивать детализированный анализ сетевого трафика и интегрироваться с другими системами безопасности. Также обсуждаются примеры использования Zeek в реальных сценариях и его роль в современных системах информационной безопасности.

Ключевые слова: Zeek, сетевой мониторинг, анализ трафика, безопасность сети, обнаружение угроз, системный анализ, информационная безопасность, интеграция безопасности.

INVESTIGATION OF THE ZEEK NETWORK TRAFFIC ANALYSIS SYSTEM

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

The article is an in-depth study of the Zeek network traffic analysis system (formerly known as Bro). Zeek is a powerful tool for monitoring network activity and detecting threats in real time. The article discusses the main functions and capabilities of Zeek, including its ability to detect complex attacks, provide detailed analysis of network traffic and integrate with other security systems. Examples of using Zeek in real-world scenarios and its role in modern information security systems are also discussed.

Keywords: Zeek, network monitoring, traffic analysis, network security, threat detection, system analysis, information security, security integration.

В условиях современного цифрового мира обеспечение информационной безопасности стало одной из ключевых задач для организаций всех размеров. С ростом сложности и частоты кибератак возрастает необходимость в эффективных и надежных средствах мониторинга и анализа сетевого трафика. Одним из таких инструментов является Zeek (ранее известный как Bro), который предоставляет мощные возможности для мониторинга и анализа сетевых данных.

Zeek представляет собой открытое программное обеспечение, которое используется для детектирования и анализа сетевых угроз в реальном времени. Он предлагает не только базовые функции мониторинга, но и продвинутые механизмы для обнаружения сложных атак и аномалий в сетевом трафике. Благодаря своей архитектуре и гибкости, Zeek может быть

настроен под конкретные нужды организации, обеспечивая глубокое понимание происходящих событий и потенциальных угроз.

В данной статье мы рассмотрим ключевые аспекты работы Zeek, включая его основные функции, архитектуру и принципы работы. Мы также проанализируем примеры использования Zeek в реальных сценариях, что позволит лучше понять его применение и преимущества. Основное внимание будет уделено тому, как Zeek может улучшить способность организаций выявлять и реагировать на киберугрозы, тем самым повышая общий уровень безопасности сетевой инфраструктуры.[1]

Zeek – это мощный инструмент для мониторинга сетевого трафика, который обеспечивает глубокий анализ сетевых данных и позволяет обнаруживать сложные атаки. Основные функции Zeek включают:

Анализ сетевых протоколов: Zeek способен анализировать широкий спектр сетевых протоколов, включая HTTP, DNS, SMTP и многие другие. Это позволяет ему выявлять аномалии и потенциальные угрозы, связанные с использованием различных протоколов.

Обнаружение атак: Zeek имеет встроенные скрипты и механизмы для обнаружения известных типов атак, таких как SQL-инъекции, XSS (межсайтовый скриптинг), и другие. Также он способен обнаруживать нетипичное поведение, которое может указывать на атаку.[2]

Логирование событий: Zeek записывает детализированные логи о сетевых событиях, что позволяет проводить ретроспективный анализ и исследовать инциденты безопасности. Эти логи включают информацию о сетевых соединениях, передачах данных и многом другом.

Гибкость и расширяемость: Zeek поддерживает использование скриптов на собственном языке сценариев, что позволяет пользователям создавать кастомизированные правила и расширять функциональность системы.[3]

Zeek имеет модульную архитектуру, которая состоит из нескольких ключевых компонентов:

Сборщик данных: Этот компонент отвечает за захват сетевого трафика и передачу его на анализ. Zeek может работать как с реальным сетевым трафиком, так и с заранее сохраненными пакетами.

Детектор протоколов: Этот модуль занимается анализом сетевых протоколов и выделением значимой информации из трафика. Он обрабатывает пакеты и извлекает данные, необходимые для дальнейшего анализа.

Скриптовый движок: Zeek использует собственный язык сценариев для написания правил и скриптов, которые позволяют пользователям настроить поведение системы в соответствии с конкретными требованиями. Скрипты могут включать правила обнаружения угроз, обработку событий и многое другое.

Модуль логирования: Этот компонент записывает информацию о сетевых событиях и действиях в лог-файлы. Логи могут быть использованы для анализа инцидентов и создания отчетов.[4]

Zeek применим в различных сценариях информационной безопасности:

Обнаружение и реагирование на атаки: В организациях Zeek используется для мониторинга сетевого трафика и выявления признаков атак, таких как сканирование портов или попытки эксплуатации уязвимостей.

Анализ инцидентов: После произошедшего инцидента Zeek предоставляет подробные логи и информацию, которые помогают в расследовании и устранении последствий атаки.

Мониторинг и аудит: Zeek позволяет организациям проводить регулярные проверки и аудит своей сетевой активности, обеспечивая постоянный мониторинг и обнаружение потенциальных угроз.

Zeek может быть интегрирован с различными системами и инструментами безопасности:

Системы управления инцидентами безопасности (SIEM): Zeek может передавать данные в SIEM-системы для централизованного анализа и корреляции событий безопасности.[5]

Системы обнаружения вторжений (IDS): В сочетании с IDS Zeek может улучшить обнаружение угроз и снижение ложных срабатываний.

Аналитические инструменты: Данные, собранные Zeek, могут быть переданы в аналитические платформы для создания отчетов и визуализации сетевой активности.

Zeek представляет собой мощный инструмент для анализа сетевого трафика и обеспечения безопасности сети. Его способность анализировать широкий спектр протоколов, обнаруживать сложные атаки и предоставлять детализированные логи делает его важной частью современного набора инструментов для защиты информационных систем. Гибкость и расширяемость Zeek позволяют адаптировать его под конкретные требования и сценарии использования, что делает его ценным активом для организаций, стремящихся повысить свою сетевую безопасность.

Список литературы

1. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.
2. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEML.
3. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.
4. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
5. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.

References

1. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation

in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 2. – pp. 50-56.

2. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A.V. Krasov, A. Y. Tsvetkov. Volume Part 1. – St. Petersburg : St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2015. – 63 p. – EDN CMMEML.
3. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.
4. Katasonov A. I., Tsvetkov A. Yu. Analysis of access control mechanisms in special purpose systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 563-568.
5. Orlov G. A., Krasov A.V., Gelfand A.M. Application of Big Data in the analysis of big data in computer networks //High-tech technologies in space exploration of the Earth. – 2020. – vol. 12. – No. 4. – pp. 76-84.