УДК 004.056

**ИЗУЧЕНИЕ ИНСТРУМЕНТА VELOCIRAPTOR**

**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*](mailto:2003.06.10kr@gmail.com)

**Статья "Velociraptor" посвящена новейшим достижениям в области информационной безопасности, фокусируясь на инструменте Velociraptor для проведения активного мониторинга и анализа систем. Автор исследует функциональные возможности этого мощного средства, его применение для выявления угроз, анализа инцидентов и оптимизации защиты от атак. Обсуждаются особенности установки и настройки Velociraptor, его интеграция с другими системами безопасности и практические примеры использования в реальных сценариях. Статья предоставляет полезную информацию для специалистов по безопасности, стремящихся улучшить свои навыки и повысить уровень защиты информационных систем.**

Ключевые слова: Velociraptor, информационная безопасность, мониторинг систем, анализ инцидентов, защита от атак, инструменты безопасности, интеграция систем, обнаружение угроз.

**LEARNING THE VELOCIRAPTOR TOOL**

**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*](mailto:2003.06.10kr@gmail.com)

**The article "Velociraptor" is devoted to the latest achievements in the field of information security, focusing on the Velociraptor tool for active monitoring and analysis of systems. The author explores the functionality of this powerful tool, its application to identify threats, analyze incidents and optimize protection against attacks. The features of installing and configuring Velociraptor, its integration with other security systems, and practical examples of use in real-world scenarios are discussed. The article provides useful information for security professionals seeking to improve their skills and increase the level of protection of information systems.**

Keywords: Velociraptor, information security, system monitoring, incident analysis, attack protection, security tools, system integration, threat detection.

В условиях постоянно развивающихся киберугроз и возрастания сложности информационных систем, обеспечение надежной защиты данных и систем становится одной из приоритетных задач в области информационной безопасности. Одним из ключевых аспектов успешной защиты является способность оперативно обнаруживать и анализировать потенциальные угрозы, а также эффективно реагировать на инциденты. В этой связи инструменты, позволяющие осуществлять активный мониторинг и глубокий анализ систем, играют критически важную роль.

Одним из таких инструментов является Velociraptor, который привлек внимание специалистов своей функциональностью и гибкостью. Velociraptor представляет собой современное решение для мониторинга систем, которое позволяет проводить детальный анализ инцидентов, выявлять угрозы и оптимизировать процессы защиты. Этот инструмент предоставляет широкие возможности для сбора и обработки данных, выполнения запросов по анализу, а также для интеграции с другими системами безопасности.[1]

Цель данной статьи – предоставить обзор возможностей Velociraptor, рассмотреть его ключевые функции и преимущества, а также продемонстрировать его практическое применение в реальных условиях. В статье будут освещены основные аспекты установки и настройки инструмента, его использование для обнаружения угроз и анализа инцидентов, а также предложены рекомендации по эффективной интеграции Velociraptor в существующую инфраструктуру безопасности. Таким образом, данная работа направлена на помощь специалистам по информационной безопасности в улучшении их практических навыков и повышении уровня защиты информационных систем.

Velociraptor — это современный инструмент для мониторинга и анализа информационных систем, разработанный с целью упрощения процесса обнаружения угроз и анализа инцидентов. Он обеспечивает гибкие возможности для сбора и обработки данных, что позволяет специалистам по информационной безопасности эффективно реагировать на возникающие угрозы и улучшать защиту своих систем.

Velociraptor предлагает ряд ключевых функций, которые делают его ценным инструментом в арсенале профессионалов по информационной безопасности:[2]

Сбор и анализ данных: Velociraptor позволяет собирать данные из различных источников, включая файлы, реестры, процессы и сетевые соединения. Этот инструмент поддерживает мощные запросы на основе языка запросов, что упрощает анализ больших объемов данных.[3]

Гибкость запросов: Один из наиболее значимых аспектов Velociraptor — это возможность создавать сложные запросы для выявления специфических паттернов и аномалий в системе. Это позволяет детализировать анализ и быстро реагировать на потенциальные угрозы.

Реальное время и исторические данные: Velociraptor поддерживает как мониторинг в реальном времени, так и анализ исторических данных, что позволяет отслеживать и анализировать события, произошедшие в системе в прошлом.

Автоматизация задач: Инструмент позволяет автоматизировать многие задачи, такие как сбор данных и выполнение запросов, что снижает нагрузку на специалистов и повышает эффективность работы.[4]

Установка Velociraptor относительно проста и может быть выполнена на различных платформах. Процесс включает следующие этапы:

Загрузка и установка: Сначала необходимо загрузить актуальную версию Velociraptor с официального сайта проекта и следовать инструкциям по установке.

Настройка агента: После установки требуется настроить агентов Velociraptor на целевых системах. Агенты будут выполнять запросы и собирать данные в соответствии с заданными правилами.

Конфигурация сервера: Важным этапом является настройка сервера Velociraptor, который будет обрабатывать запросы и хранить результаты анализа. Сервер должен быть настроен в соответствии с требованиями организации и объемом обрабатываемых данных.

Velociraptor легко интегрируется с различными системами и инструментами безопасности, такими как SIEM-системы и системы управления инцидентами. Это позволяет объединить данные из различных источников и получить более полное представление о состоянии безопасности системы.

Интеграция с SIEM: Velociraptor может передавать данные и события в SIEM-системы для более глубокого анализа и корреляции.

API и сценарии: Инструмент поддерживает API и возможность создания пользовательских сценариев для интеграции с другими системами и автоматизации рабочих процессов.[5]

Примеры использования Velociraptor в реальных условиях подчеркивают его эффективность и универсальность:

Обнаружение вредоносного ПО: Velociraptor можно использовать для поиска следов вредоносного ПО на системах, включая выявление подозрительных файлов и процессов.

Анализ инцидентов: В случае инцидентов безопасности инструмент помогает проводить детальный анализ, включая восстановление истории изменений и выявление точек компрометации.

Мониторинг систем: Velociraptor обеспечивает постоянный мониторинг системы и помогает обнаруживать аномалии, которые могут указывать на потенциальные угрозы.

Velociraptor представляет собой мощный инструмент для мониторинга и анализа систем безопасности, предлагающий широкий спектр функций для обнаружения угроз и управления инцидентами. Его гибкость, возможности автоматизации и интеграции делают его ценным ресурсом для специалистов по информационной безопасности. Эффективное использование Velociraptor может значительно повысить уровень защиты информационных систем и улучшить способность реагировать на киберугрозы.

**Список литературы**

1. 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.

2. Штеренберг С. И. Анализ работы алгоритмов защиты информации на основе самомодифицирующегося кода с применением стеговложения //Наукоемкие технологии в космических исследованиях Земли. – 2016. – Т. 8. – №. 2. – С. 86-90.

3. 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.

4. Виткова Л. А., Ахрамеева К. А., Грузинский Б. А. Использование геометрических хеш-функций в информационной безопасности //Известия высших учебных заведений. Технология легкой промышленности. – 2017. – Т. 37. – №. 3. – С. 5-9.

5. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 111-114.

**References**

1. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A.V. Krasov, A. Yu. Tsvetkov. Volume Part 1. – St. Petersburg : St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2015. – 63 p. – EDN CMMEML.

2. Shterenberg S. I. Analysis of the work of information security algorithms based on self-modifying code using a stack //High–tech technologies in space exploration of the Earth. - 2016. – Vol. 8. – No. 2. – pp. 86-90.

3. 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.

4. Vitkova L. A., Akhrameeva K. A., Gruzinsky B. A. The use of geometric hash functions in information security //News of higher educational institutions. Light industry technology. - 2017. – vol. 37. – No. 3. – pp. 5-9.

5. Birikh E. V., Ferapontova S. S. On the issue of personal data audit //Actual problems of infotelecommunications in science and education (APINO 2018). – 2018. – pp. 111-114.