Анализ уязвимостей операционной системы РЕД ОС

Д.К. Рябцев, А.Д. Родикова

Поволжский Государственный университет телекоммуникаций и информатики, Самара, Россия

Обоснование. В современном мире одним из ключевых направлений в области защиты информации является поиск, анализ и разработка методов по устранению потенциальных угроз. Каждый день информационные системы подвергаются различным рискам: кибератаки, мошенничество, кража личных данных. Атака на операционные системы является одним из самых распространенных видов киберпреступности. Это приводит к нарушению доступности, потере целостности и конфиденциальности обрабатываемой информации.

Цель — разработка системы, способной проводить комплексный анализ уязвимостей операционной системы РЕД ОС. Система будет представлять инструменты для выявления, классификации и устранения уязвимостей, а также для мониторинга безопасности операционной системы. Мы стремимся создать инструмент, который будет удобен в использовании не только для специалистов в области информационной безопасности, но и для обычных пользователей.

Методы.

1. Анализ официальной документации операционной системы РЕД ОС на сайте разработчика. Мы провели тщательный анализ системных утилит, которые предоставляет операционная система. В процессе поисков была обнаружена утилита OpenSCAP. OpenSCAP — это набор инструментов для проверки соответствия систем различным стандартам.
2. Выбор языка программирования. Для разработки программы был выбран объектно-ориентированный язык программирования Java. Java-программы могут компилироваться в байт-коды без сторонних ПО с помощью Java Virtual Machine (JVM). Это означает, что одно и то же приложение может работать на различных версиях операционной системы.
3. Разработка программного обеспечения. В процессе разработки нашего проекта мы написали ПО, которое запускается с помощью исполняемого файла java — jar. Для полного функционирования программы из-под программного кода java в терминал РЕД ОС вызываются команды для установки и работы OpenSCAP, для сохранения и открытия отчета об уязвимостях в нужном пользователю формате.
4. Анализ результатов и проверка соответствия. Мы удостоверились, соответствует ли система требованиям, и приняли меры по устранению обнаруженных проблем.
5. Написание документации нашего продукта для пользователей. Мы составили подробную инструкцию, как запустить нашу программу в среде операционной системы РЕД ОС.

Результаты. В результате нашего исследования мы разработали собственное программное обеспечение, способное сканировать и оценивать уязвимость операционной системы РЕД ОС на базе встроенной утилиты — сканера уязвимостей OpenSCAP.

Выводы. Проведя исследование РЕД ОС, а также создав проект, осуществляющий нахождение уязвимостей в этой системе, мы сделали вывод о необходимости анализа уязвимостей ОС, служащего основой для разработки новых методов защиты и улучшения общей стратегии информационной безопасности. Применение современных технологий машинного обучения может значительно улучшить процесс обеспечения информационной безопасности, делая его более систематизированным и эффективным.

Ключевые слова: РЕД ОС; анализ уязвимостей; кибератака; угроза операционной системе.

Список литературы

1. scap-security-guide [Электронный ресурс]. SCAP security guide documentation [дата обращения: 25.02.2024]. Режим доступа: https://github.com/ComplianceAsCode/content
2. OpenSCAP [Электронный ресурс]. The OpenSCAP Project [дата обращения: 25.02.2024]. Режим доступа: https://www.open-scap.org
3. redos.red-soft.ru [Электронный ресурс]. Документация РЕД ОС [дата обращения: 25.02.2024]. Режим доступа: https://redos.red-soft.ru/product/docs/

Сведения об авторах:

Даниил Константинович Рябцев — студент, группа ПрИ-23, факультет кибербезопасности и управления (факультет №1); Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: daniil.riabtcev@gmail.com

Анна Дмитриевна Родикова — студентка, группа ИБТС-22, факультет кибербезопасности и управления (факультет №1); Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: rodikova.anechka@mail.ru

Сведения о научном руководителе:

Игорь Сергеевич Макаров — кандидат технических наук, доцент; заведующий кафедрой «Программная инженерия»; Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: i.makarov@psuti.ru