УДК 004.056

М. КАРАПЕТЬЯНЦ

Национальный исследовательский ядерный университет «МИФИ», Москва

ВИРТУАЛЬНЫЙ ИСПЫТАТЕЛЬНЫЙ СТЕНД ДЛЯ СБОРА, ХРАНЕНИЯ И АНАЛИЗА ДАННЫХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В докладе представлена разработка виртуального испытательного стенда для сбора, хранения, а также анализа данных в области информационной безопасности. Определен перечень элементов стека технологий, позволяющих обеспечить автоматизированное развертывание предлагаемого виртуального испытательного стенда с возможностью его повторного воспроизведения.

Разработка новых алгоритмов, методов, методик и средств защиты информации в области информационной безопасности требует проведения эксперимента для подтверждения выдвинутой гипотезы. Одним из важных требований к виртуальному испытательному стенду является обеспечение достоверности и воспроизводимости научно-практических изысканий [1]. Это требование может быть обеспечено за счет использования программного обеспечения с открытым исходным кодом, средств автоматизации, базирующихся на принципе «Инфраструктура как код» (англ. IaC, «Infrastructure as Code»), и средств виртуализации.

В качестве средства виртуализации, обеспечивающего запуск и выполнение системного программного обеспечения, может быть использован VirtualBox, поскольку он распространяется с открытым исходным кодом и поддерживается большинством операционных систем на архитектуре X86, таких как Windows и Linux. Преимуществом использования VirtualBox также является возможность запуска практически любой операционной системы, начиная с Windows и заканчивая дистрибутивами на базе BSD. Воспроизводимость виртуальной среды на базе гипервизора VirtualBox может обеспечить программное обеспечение Vagrant. Это программное обеспечение используется для создания и конфигурирования виртуальной среды и по своей сути представляет собой универсальный интерфейс для управления разными видами систем виртуализации, включая и облачные системы. Конфигурирование самих виртуальных машин может осуществляться совместно с использованием инструментов автоматизации, таких как Bash, Ansible, Chef, Salt и Puppet. Наиболее подходящим инструментом автоматизации в данном случае является Ansible, позволяющий

обеспечить идемпотентность в рамках декларативной модели выполнения задач автоматизации с помощью только подключения по протоколу SSH. Эти свойства позволяют добиться желаемого состояния виртуального испытательного стенда и входящих в него инструментов сбора, анализа и хранения. Автоматизация процесса развертывания инструментов сбора, хранения и обработки данных в среде виртуальных машин требует применения средства контейнеризации Docker, которое может быть использовано вместе с инструментами Ansible для предварительной настройки среды контейнеров.

Обеспечить централизованный сбор, хранение и обработку данных в рамках виртуального испытательного стенда предлагается с помощью стека ELK [2], в состав которого входят Logstash, Elasticsearch, Kibana. Logstash осуществляет сбор и предварительную обработку данных, Elasticsearch – их индексацию и хранение, а Kibana предоставляет визуализацию полученных данных. В случае, если необходимо реализовать распределенную обработку данных, можно использовать Apache Spark, который поддерживает разные виды источников данных, таких как стек ELK, PostgreSQL, Apache Kafka, Apache Cassandra и другие виды хранилищ. Хранение данных в формате, отличном от стека ELK, может быть обеспечено за счет использования специализированных систем управления базами данных (СУБД): Neo4j, Redis, PostgreSQL, MongoDB. Или с использованием мультимодельных баз данных [3]. Каждая из СУБД может быть развернута с использованием контейнеров Docker.

В рамках исследования был разработан виртуальный испытательный стенд для сбора, обработки и анализа данных в области информационной безопасности. Результаты исследования могут быть использованы для проведения репрезентативных научно-практических исследований.

Список литературы

1. Басыня Е.А., Малышев Е.А. Обеспечение достоверности результатов научно-практических изысканий с применением программной инженерии // ЗАЩИТА ИНФОРМАЦИИ. ИНСАЙД. – 2023. – Т. 112 – №. 4. – С. 14–21.

2. Стрельцов А.С., Французова Г.А., Басыня Е.А. Разработка системы сбора, обработки, анализа, идентификации корреляции событий информационной инфраструктуры предприятия //Системы анализа и обработки данных. – 2023. – № 1 (89). – С. 101–113.

3. Басыня Е.А., Карапетьянц Н., Карапетьянц М. Исследование существующих подходов к анализу транзакций в сети Bitcoin // Программная инженерия. 2023. Т. 14, № 10. С. 493–501. DOI: 10.17587/prin.14.493-501.