УДК 004.42

А. А. Цыганков[1]✉

Виртуальный стенд для проведения экспериментального сравнительного исследования методов активного анализа информационных систем

[1]Национальный исследовательский ядерный университет «МИФИ»,
г. Москва,Российская Федерация
e-mail: aatsygankov@mephi.ru

Аннотация. Сбор информации об атакуемой сетевой инфраструктуре и активное сканирование являются техниками атак на корпоративную инфраструктуру. Некорректная конфигурация сетевого и серверного оборудования может стать точкой входа атакующих в информационную систему. Для оценки защищенности системы используются сетевые сканеры. В работе рассматривается виртуальный стенд для проведения экспериментального сравнительного исследования методов активного анализа информационных систем. Целью исследования является разработка платформы для анализа поведения сетевых сканеров. В рамках исследования проанализированы сценарии использования и приведены рекомендации по автоматизации установки и конфигурирования виртуального стенда. На обзор вынесена архитектура платформы, а также изложен подход к ее разработке. Результаты исследования могут использоваться для построения ряда виртуальных стендов, исследующих поведение методов активного анализа информационных систем. Область применимости включает инфраструктуру, функционирующую на базе стека протоколов TCP/IP.

Ключевые слова: виртуальный стенд, сетевая безопасность, сетевые сканеры, TCP/IP

A. A. Tsygankov[1]✉

Virtual stand for experimental comparative study of active analysis methods for information systems

[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Moscow, Russian Federation
e-mail: aatsygankov@mephi.ru

Abstract. Gathering information about the targeted network infrastructure and active scanning are common attack techniques against corporate systems. Misconfigured network and server equipment can serve as an entry point for attackers into an information system. Network scanners are widely used to assess system security. This study presents a virtual testbed for conducting experimental comparative research on active analysis methods for information systems. The research aims to develop a platform for analyzing the behavior of network scanners. The study examines usage scenarios and provides recommendations for automating the deployment and configuration of the virtual testbed. The paper reviews the platform's architecture and outlines the development approach. The findings can be applied to construct a range of virtual testbeds for studying the behavior of active analysis methods in information systems. The proposed solution is applicable to infrastructures operating on the TCP/IP protocol stack.

Keywords: virtual stand, network security, network scanners, TCP/IP

Введение

Активное развитие информационных технологий способствует расширению собственной информационной инфраструктуры государственных учреждений и частных компаний, что не только расширяет поверхность потенциальной атаки, но и увеличивает влияние человеческого фактора на безопасность сетевого и серверного оборудования. Согласно исследованиям Лаборатории Касперского, одного из ведущих вендоров в области информационной безопасности в Российской Федерации, 12 % срабатываний антивирусного оборудования в день приходится на сканирование UDP (англ. User Datagram Protocol) портов, 13 % – на атаки, использующие уязвимости TCP (англ. Transmission Control Protocol, Internet Protocol). Однако методы активного анализа информационных систем используются не только злоумышленниками, но и специалистами информационной безопасности для поддержания актуальных данных о состоянии корпоративной инфраструктуры, инвентаризации активов и проверки соответствия узлов сети требованиям безопасности [1–3].

На стандартизацию обеспечения сетевой информационной безопасности также направлены ряд нормативно-правовых актов, в частности Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и Приказом Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств». Актуальность исследования также подтверждается Концепцией государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий, утвержденной Правительством Российской Федерации.

Исследованиями в области методов активного анализа занимается ряд научных школ, в частности Zakir Durumeric, Eric Wustrow и J. Alex Halderman (университет Мичигана). В своих работах научная группа выносит на обзор сетевой сканер Zmap, а также производит сравнительный анализ собственного решения с актуальными аналогами [4]. Поиск оптимального решения позволяет минимизировать не только риски ложноположительных срабатываний систем мониторинга состояния корпоративной инфраструктуры, но и затраченное на исследование время и ресурсы. Приведенные данные свидетельствуют об актуальности темы исследования и указывают на растущую потребность в разработке решений для анализа сканеров сети.

Моделирование предметной области

Методы активного анализа, используемые для исследования информационной системы, функционируют идентичным образом и эксплуатируют уязвимости стека протоколов TCP/IP. Для разработки виртуального стенда для проведения сравнительного анализа сетевых сканеров была разработана UML-диаграмма (англ. Unified

Modeling Language) последовательности взаимодействия (рис. 1), демонстрирующий процесс взаимодействия модулей виртуального стенда на примере исследования порта на доступность [5].

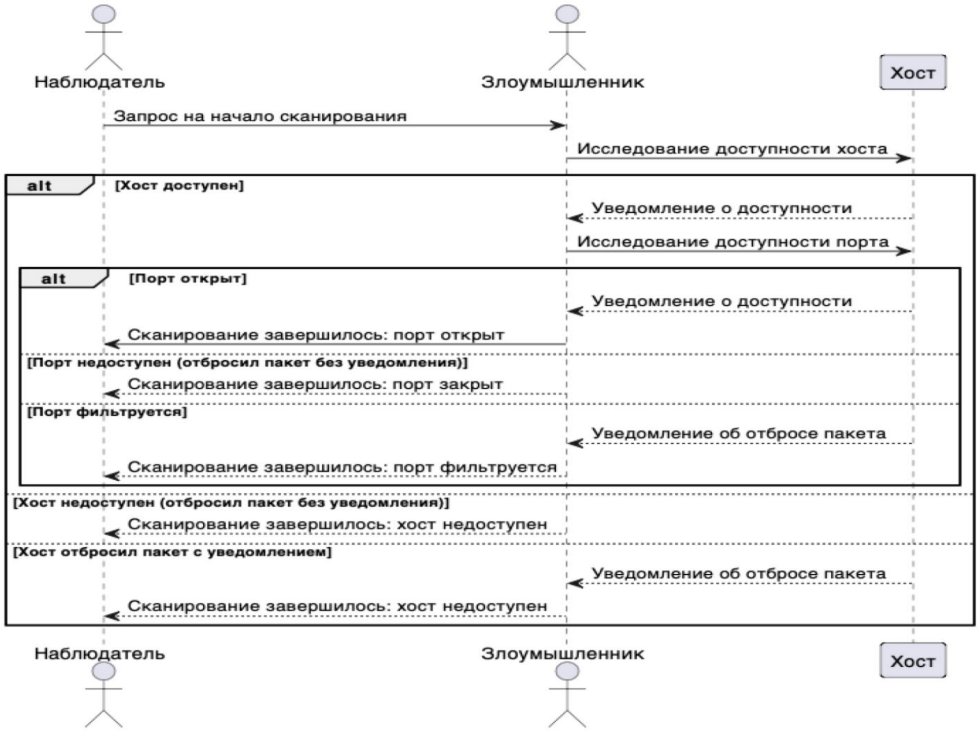

Рис. 1. UML-диаграмма последовательности взаимодействия с виртуальным лабораторным стендом

Предусматривается три участника сетевого взаимодействия: наблюдатель, инициирующий процесс сканирования; злоумышленник, выполняющий непосредственное взаимодействие с хостом для получения информации; хост, объект сканирования.

Постановка задачи

Целью исследования является разработка платформы для сравнительного анализа поведения сетевых сканеров. В рамках декомпозиции цели выделены следующие задачи:

1) определение требований к системе;
2) моделирование топологии сети виртуального стенда;
3) выбор стека технологий.

Результатом работы является описание функциональности, архитектуры и стека технологий выносимого на обзор виртуального стенда для проведения экспериментального сравнительного исследования методов активного анализа информационных систем. Топология сети и сама платформа удовлетворяют установленным в рамках исследования критериям с целью имитации корпоративной инфраструктуры предприятия.

Требования к виртуальному стенду

Топология сети виртуального стенда для имитации корпоративной инфраструктуры должна удовлетворять требованиям [6]:

1) должна содержать демилитаризованную зону с помещенными в нее виртуальными машинами, имитирующими вычислительные мощности;

2) должна удовлетворять трехуровневой иерархической модели построения сети и содержать объекты на всех трех уровнях: доступа, распределения и ядра;

3) в топологии сети должны быть созданы оптимальные условия для скоростного обмена информацией между хостами (в том числе с использованием технологии связующего древа);

4) наборы хостов сети виртуального стенда должны быть логически разделены;

5) топология сети не должна содержать единой точки отказа;

6) любое взаимодействие объектов локальной сети с глобальной сетью должно происходить через межсетевой экран.

Выполнение требований к топологии сети виртуального стенда обеспечивает корректные выходные данные сравнительного анализа сетевых сканеров, сопоставимые с реальной корпоративной инфраструктурой предприятия [7].

Виртуальный лабораторный стенд также должен удовлетворять ряду требований [8, 9]:

1) установка и конфигурирование каждого модуля стенда должна происходить автоматически;

2) в составе стенда должен быть определен механизм поддержания декларируемого состояния модулей;

3) в составе стенда должен быть определен механизм централизованного сбора и хранения системных журналов модулей.

Важным аспектом также является возможность установки виртуального стенда на различные платформы, операционные системы и гипервизоры.

Топология сети виртуального стенда

Учитывая требования, описанные в предыдущей главе, была разработана топология сети виртуального стенда (рис. 2).

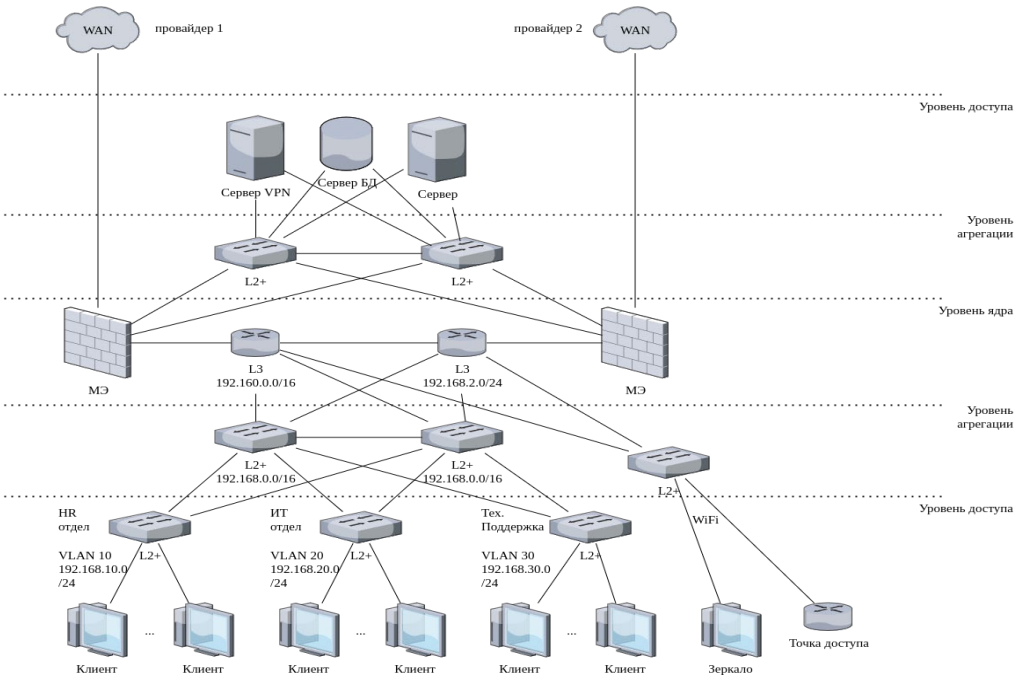

Рис. 2. Топология сети виртуального стенда

На рис. 2 представлена топология сети, построенная с учетом трехуровневой иерархической модели построения сети. На уровне доступа располагаются виртуальные машины, имитирующие хосты сотрудников. Стоит отметить, что предложенная топология содержит логическое разделение конечных хостов на группы с использованием технологии виртуальных локальных сетей VLAN (англ. Virtual Local Area Network). Также на уровне доступа располагаются виртуальные машины, имитирующие сервера (в рамках примера сервер VPN (англ. Virtual Private Network), баз данных) [10–12].

На уровне агрегации находятся виртуальные коммутаторы. Отказоустойчивость оборудования на этом уровне обеспечивается использованием технологии связующего древа.

На уровне ядра расположены два межсетевых экрана, ограничивающие трафик между локальной сетью предприятия, глобальной сетью и демилитаризованной зоной.

Предложенная в рамках исследования топология полностью удовлетворяет поставленным целям построения виртуального стенда и определенным требованиям.

Стек технологий

Важными аспектами при выборе технологий виртуального лабораторного стенда является воспроизводимость, масштабируемость и точность конечных измерений. Стек технологий, основываясь на предложенных требованиях, содержит:

1) систему управления конфигурациями;

2) систему мониторинга;

3) систему агрегации журналов событий.

Основу управления конфигурациями составляет Ansible, выбранный в силу его агент-независимой архитектуры, поддержки декларативного подхода через YAML-сценарии (англ. YAML Ain't Markup Language) и кроссплатформенной совместимости. Важным преимуществом решения является минимизация вмешательства в тестовую среду в связи с архитектурой системы. Для обеспечения идемпотентности конфигураций применяются модули Terraform, позволяющие программно определять топологию сети и виртуальные машины в гипервизорах [13].

Мониторинг сетевой активности предлагается выстраивать на базе Prometheus – системы сбора временных рядов, обладающей высокой производительностью при обработке потоковых данных. Prometheus интегрирован с экспортерами для сбора метрик сетевых интерфейсов, состояния сервисов и трафика межсетевых экранов. Визуализация данных осуществляется через Grafana, предоставляющую гибкие инструменты построения дашбордов на основе запросов к PromQL [14].

Для централизованного сбора и анализа журналов событий предлагается платформа Loki, отличающаяся от традиционных решений низкими накладными расходами на хранение и возможностью использования меток для индексации логов [15].

Виртуальный лабораторный стенд, предложенный в рамках настоящего исследования, возможно реализовать в рамках программных эмуляторов, симуляторов, гипервизоров 1-го и 2-го типа.

Заключение и обсуждение

В ходе научно-практических изысканий была предложена топология сети и стек технологий виртуального стенда для проведения экспериментального сравнительного исследования методов активного анализа информационных систем. Архитектура стенда основана на трехуровневой модели сети, включающей зоны доступа, агрегации и ядра, что обеспечивает соответствие реальным корпоративным инфраструктурам. Применение технологий автоматизации развертывания, мониторинга и агрегации журналов позволяет создать воспроизводимую среду, пригодную для многократного тестирования сетевых сканеров. Область применения полученного решения включает информационные системы, функционирующие на базе стека протоколов TCP/IP.

Практическая значимость исследования заключается в возможности использования разработанного стенда для валидации сетевых сканеров, обучения специалистов по информационной безопасности и тестирования систем обнаружения вторжений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия //Безопасность информационных технологий. – 2018. – Т. 25. – №. 4. – С. 42-51.

2. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия //Защита информации. Инсайд. – 2021. – №. 5. – С. 101.

3. 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.

4. Durumeric Z., Wustrow E., Halderman J. A. {ZMap}: Fast internet-wide scanning and its security applications //22nd USENIX Security Symposium (USENIX Security 13). – 2013. – С. 605-620.

5. Wang Y. et al. A Unified Modeling Framework for Automated Penetration Testing //arXiv preprint arXiv:2502.11588. – 2025.

6. Bringhenti D. et al. Automation for network security configuration: State of the art and research trends //ACM Computing Surveys. – 2023. – Т. 56. – №. 3. – С. 1-37.

7. Медведев Ю. С., Терехов В. В. Особенности построения распределенной корпоративной сети предприятия для обеспечения информационными и вычислительными ресурсами //Научные чтения имени профессора НЕ Жуковского. – 2022. – С. 258-260.

8. Врублевский Д. Н. Разработка лабораторных работ для изучения средств защиты компьютерных сетей //Молодость. Интеллект. Инициатива. – 2016. – С. 10-10.

9. Кукушкина Н. В., Новохрёстов А. К. Разработка лабораторного стенда для изучения систем обнаружения вторжений //Безопасность цифровых технологий. – 2021. – №. 4 (103). – С. 37.

10. Lavrov E. A. et al. Analysis of information security issues in corporate computer networks //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2021. – Т. 1047. – №. 1. – С. 012117.

11. Varadharajan V. et al. A policy-based security architecture for software-defined networks //IEEE Transactions on Information Forensics and Security. – 2018. – Т. 14. – №. 4. – С. 897-912.

12. Добрышин М. М. Иерархическая модель изменения уровня информационной безопасности в условиях компьютерных атак на корпоративную сеть связи //Экономика и качество систем связи. – 2024. – №. 3 (33). – С. 108-119.

13. Opdebeeck R., Zerouali A., De Roover C. Smelly variables in ansible infrastructure code: Detection, prevalence, and lifetime //Proceedings of the 19th international conference on mining software repositories. – 2022. – С. 61-72.

14. An S. Y. et al. A pre-study on the open source prometheus monitoring system //Smart Media Journal. – 2021. – Т. 10. – №. 2. – С. 110-118.

15. Pai K., Srinivas B. K. Enhanced Visibility for Real-time Monitoring and Alerting in Kubernetes by Integrating Prometheus, Grafana, Loki, and Alerta //International Journal of Scientific Research in Engineering and Management. – 2024.