Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.75

Савик
Константин Викторович

ИССЛЕДОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1 - 53 80 01 Автоматизация и управление технологическими процессами и производствами (по отраслям)

Научный руководитель

В. А. Захарьев,
кандидат технических наук,
доцент

Минск 2020

ВВЕДЕНИЕ

Надежность и безопасность сети крайне важны в мире, где компьютерные сети являются ключевым элементом в коммуникациях и транзакциях между объектами. Сетевые администраторы, правительство, консультанты по безопасности и хакеры использовали различные инструменты для проверки уязвимостей целевых сетей, таких как, например, возможность удаленного доступа к компьютерам в сети и управления ими без авторизации. Благодаря этому интенсивному тестированию целевая сеть может быть «защищена» от распространенных уязвимостей и эзотерических атак. Однако существующие системы тестирования дают противоречивые результаты, используют недоказанные методы или наносят ущерб целевой сети, не реагируют на изменяющиеся сетевые среды или обнаруживают новые уязвимости и сообщают о результатах в трудных для понимания текстовых отчетах.

Цель исследования: сравнительный анализ и модернизация существующих методов и алгоритмов обнаружений уязвимостей. Для достижения поставленной цели в работе решались следующие задачи:

– определение характерных уязвимостей в распределенных системах, их классификация и анализ;

– анализ атак производимых в распределенных системах, исследование методов и систем обнаружения уязвимостей;

– разработка математической, функциональной модели распределенной системы на примере интернет вещей;

– разработка алгоритма и архитектуры системы обнаружения уязвимостей.

Предмет: исследование и анализ методов обнаружения уязвимостей для тестирования распределённой системы.

Объект: методы поиска уязвимостей, распределенная система.

Задачи: провести обзор источников по теме диссертационного исследования, ознакомиться с особенностями проведения тестирования систем на наличие уязвимостей, обозначит вектор исследуемых уязвимостей, выполнить сравнительный анализ существующих методов, алгоритмов реализации обнаружения уязвимостей, сформулировать и формализовать предложения по улучшению существующих методов, спроектировать и разработать прототип распределённой системы для тестирования метода обнаружения уязвимостей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования

С постоянно растущей технологической экспансией мира распределенные системы становятся все более распространенными. В тоже время компьютерные сети имеют огромные масштабы, это приводит и к увеличению количества уязвимостей в них, соответственно усложняется процесс анализа защищенности систем.

Актуальной задачей является исследование методов обнаружения уязвимостей в распределеных системах, классификация уязвимостей, анализ возможности универсального подхода к защите системы от попытки получения несанкционированного доступа.

Актуальность исследования

Целью диссертационной работы является сравнительный анализ и модернизация существующих методов и алгоритмов обнаружений уязвимостей.

Задачи исследования

– обзор источников по теме диссертационного исследования;

– ознакомиться с особенностями проведения тестирования системна наличие уязвимостей;

– обозначить вектор исследуемых уязвимостей;

– выполнить сравнительный анализ существующих методов, алгоритмов реализации обнаружения уязвимостей;

– сформулировать и формализовать предложения по улучшению существующих методов;

– спроектировать и разработать прототип распределённой системы для тестирования метода обна-ружения уязвимостей.

Новизна полученных результатов

Новизна данной работы заключается в исследовании и применении методов обнаружения уязвимостей одном из видов распределенной системы - сети интернет вещей.

Личный вклад соискателя

Соискателем выполнены все изложенные в работе разработки и исследования. Постановка задач и обсуждение результатов проводились совместно с научным руководителем, доцентом кафедры систем управления Белорусского государственного университета информатики и радиоэлектроники. Обработка, интерпретация данных, а также выводы сделаны автором самостоятельно.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались на следующих научных конференциях:

– 54-ая научная конференция аспирантов, магистрантов и студентов БГУИР;

– 55-я юбилейная научная конференция аспирантов, магистрантов и студентов учреждения образования "Белорусский государственный университет информатики и радиоэлектроники";

– Информационные технологии и системы 2019 (ИТС 2019) Information Technologies and Systems 2019 (ITS 2019).

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, сформулирована цель, определены основные задачи, научная новизна и практическая значимость полученных результатов, а также положения, выносимые на защиту.

В первой главе данной диссертационной работы была рассмотрена распределенная система, ее особенности и характеристики, даны ее основные понятия. Были проведен сравнительный анализ и классификация уязвмостей распроделенной системы, а также определены критические уязвимости. Были приведены примеры уязвимостей на всех уровнях модели OSI.

Во второй главе были рассмотрены методы обнаружения уязвимостей в распределенных системах, так же в частном случае распределенной системы - сети интрнет вещей, проведен анализ безопасности аспектов интернет вещей:

- безопасность связи;
- защита устройств;
- контроль взаимодействий в сети;
- контроль устройств.

Был произведен анализ атак, характерных для сетей IoT, также был проведен анализ уязвимостей характерных для TCP/IP стека на различных уровнях модели OSI и их характеристика. Исследованы методы обнаружения и защиты от уязвимостей на предложенном векторе сетевых атак. По итогам исследования атак и методов защиты были рассмотрены системы обнаружения уязвимостей - SIEM-системы и определены недостатки существующих решений, относительно применения их в сетях интернет вещей.

В третей главе была разработана математическая модель взаимодействия устройств в IoT, с использованием теории графов, функциональная модель предметной области IoT, которая позволила сформулировать требования к разработке SIEM-системы для выявления и анализа инцидентов безопасности в IoT, которые легли в основу построения архитектуры SIEM-системы и алгоритма распределения задач между узлами многопроцессороного кластера.

В четверой главе было проведено иммтирование атаки типа HTTP flood. Рассмотрены вопросы построения современных систем управления инцидентами безопасности (SIEM). Продемонстрированы возможности практического применения разработанной системы в условиях мониторинга безопасности защищаемых узлов.

ЗАКЛЮЧЕНИЕ

Согласно отчету Cisco Annual Internet Report (AIR), к 2023 году пользователями Интернета станут 66% населения Земли. Уже на данном этапе количество интрнет устройств превышает количество людей на землей. С развитием индустрии 4.0 и, интернет вещей интегрируется все с большим количеством областей человеческой деятельности, при этом растет количество угроз безопасности, обусловленных низкой защищенностью конечных устройств ИВ, проблемами безопасности сетей, на основе которых реализуются решения ИВ, отсутствием единого подхода к анализу безопасности ИВ и формализации понятия «событие безопасности» применительно к ИВ системам.

Наиболее перспективным решением для анализа безопасности в ИВ является подход SIEM-систем, предметом анализа которых являются события. Это особенно актуально для систем ИВ, в которых устройства управляют друг другом, обмениваясь сообщениями без влияния человека. Однако существующие SIEM-системы не могут быть применены для анализа безопасности в ИВ, в связи с этим была рассмотрена задача создания методологического и математического обеспечения SIEM-систем для ИВ. Исследованное обеспечение решает проблемы анализа безопасности в ИВ.

В рамках диссертационного исследования были рассмотрены следующие задачи: выполнена формализация понятия события безопасности в ИВ; исследована функциональная модель предметной области ИВ, описывающая уровни представления: конфигурации устройства ИВ, пространства сообщений, угроз и инцидентов безопасности; исследованы алгоритмы обнаружения уязвимостей; исследована архитектура системы анализа событий безпасности; спроектирована система обнаружения уязвимостей, произведено эксперементальное исследование предлагаемой системы, в рамках которого системы выявила угрозу безопасности 100-го запроса с одного ip-адреса в течение 1 секунды, по указанным в системе правилам.

Таким образом, в ходе диссертационного исследования был разработан подход, к оценке и управлению безопасностью ИВ на основе формализации инцидента безопасности в ИВ, методы предварительной обработки данных и математические модели показателей безопасности, а также, в ходе эксперимента была установлена эффективность использования принципа самоподобия для оценки безопасности ИВ. Все поставленные задачи были решены, желаемая цель достигнута.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Савик, К. В. Сравнительный анализ быстродействия публичных DNS-серверов / К. В. Савик, П. А. Рубель // Информационные технологии и управление: материалы 54-й научной конференции аспирантов, магистрантов и студентов, Минск, 23 – 27 апреля 2018 г. – Минск: БГУИР, 2018. – С. 22 – 23.

2. Савик, К. В. Методы обнаружения уязвимостей в распределенных системах / К. В. Савик // 55-я юбилейная научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»: материалы конференции по направлению 2: Информационные технологии и управление, Минск, 22–26 апреля 2019 г. / редкол.: Л. Ю. Шилин [и др.]. – Минск: БГУИР, 2019. – С. 32-33.

3. Савик, К. В. Анализ метода сканирования ЛВС / Савик К. В. // Информационные технологии и системы 2019 (ИТС 2019) = Information Technologies and Systems 2019 (ITS 2019) : материалы международной научной конференции, Минск, 30 октября 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2019. – С. 84 – 85.