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

УДК 004.056.5

Мурашко
Евгений Андреевич

Методика детектирования сетевых атак с использованием устройств мониторинга и контроля транзитного трафика

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

Научный руководитель

Петров Сергей Николаевич
Кандидат технических наук,
доцент

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время отсутствует общий подход к решению проблемы обнаружения аномальных ситуаций во время обработки информации компьютерными системами и информационными сетями. Методы обнаружения аномалий часто применяются для решения задач обнаружения атак на вычислительные системы и информационные сети. Они выбираются применительно к определенному набору параметров системы, и их эффективность зависит только для этого набора параметров.

На сегодняшний день системы обнаружения вторжений и атак обычно представляют собой программные или аппаратно-программные комплексы, которые автоматизируют процесс контроля событий, протекающих в компьютерной системе или сети, а также анализируют эти события в поисках уязвимостей. Поскольку количество различных типов и способов организации несанкционированных проникновений в чужие сети за последние годы значительно увеличилось, системы обнаружения атак (СОА) стали необходимым компонентом инфраструктуры безопасности большинства организаций.

Методика детектирования атак с использованием программно-аппаратных средств защиты информации способствуют своевременному обнаружению проблем, которые могут привести к успешным противозаконным действиям со стороны злоумышленника. Другими словами, обнаружение уязвимости на этапе разработки методики позволяет разработчикам систем защиты информации заблокировать все возможные варианты незаконных действий злоумышленника для получения выгоды.

Целью диссертации разработка методики детектирования сетевых атак, позволяющей разработать систему защиты информации в корпоративной сети и провести испытания любого устройства или программного решения, используемого в инфокоммуникационных сетях. Данная методика позволит определить верность отношения этих средств к определенной категории продуктов сетевой инфраструктуры, целевую аудиторию покупателя (малые, средние или большие сети передачи данных), функциональные возможности передачи и защиты данных от несанкционированного доступа, а также безопасность использования для различных типов предприятий.

В диссертации будет проведен анализ классических и современных методов атак, методов тестирования, обзор средств защиты от сетевых атак, выбрано необходимое оборудование и приведены его характеристики, которое в дальнейшем будет использовано для разработки методики детектирования атак и проведения испытаний программно-аппаратных средств защиты информации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке методики детектирования сетевых атак с использованием устройств мониторинга и контроля транзитного трафика и программно-аппаратного комплекса для реализации данной методики.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1 Произвести анализ классических и современных методов атаки на вычислительные сети.

2 Сравнить и подобрать средства защиты вычислительной сети.

3 Разработать методику детектирования сетевых атак с использованием устройств мониторинга и контроля транзитного трафика и протестировать её с помощью программно-аппаратного комплекса сетевой защиты.

Апробация результатов диссертации

Основные результаты диссертации докладывались и обсуждались на 56-й научной конференции аспирантов, магистрантов и студентов БГУИР (г. Минск, 21-24 апреля 2020 г.) и XVIII белорусско-российской научно-технической конференции «Технические средства защиты информации» (г. Минск, 9 июня 2020 г.).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 2 тезиса докладов в сборниках материалов конференции.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе диссертации кратко рассматриваются типы атак, которые обычно применяются против сетей IP, и перечисляются способы борьбы с ними. Рассматриваются классические виды атак, такие как перехват пакетов, спуфинг, DOS-атаки, парольные атаки, MITM-атаки, сетевая разведка, переадресация портов и заражение вредоносным ПО типа Trojan, а также современные виды атак, такие как злоупотребление «доверием», Mailbombing, переполнение буфера, SQL-инъекции, PHP-инъекции, межсайтовый скриптинг, XPath-инъекции, заражение Ransomware и социальная инженерия. В конце главы даются выводы об опасности перечисленных атак и об эффективности способов борьбы с ними.

Во второй главе диссертации производится обзор и сравнение средств защиты от атак. Даётся описание алгоритма выявления аномалий и отображается классификация методов обнаружения атак. Далее рассматриваются средства межсетевого экранирования, приведён их сравнительный анализ и требования СТБ. В обзоре отхватываются такие линейки устройств как межсетевые экраны Cisco ASA, шлюз безопасности Check Point, многофункциональные устройства FortiGate, межсетевые экраны Palo Alto Networks, межсетевые экраны веб-приложений Imperva SecureSphere и программно-аппаратные комплексы Blue Coat Proxy SG. Также производится анализ существующих средств защиты от вторжений, описана архитектура и классификация IDS, а также приводятся требования СТБ. Рассматриваются такие IDS/IPS как IDS Bro, IDS/IPS Snort, Suricata IDS/IPS и система обнаружения вторжений на рабочие станции OSSEC HIDS. В конце главы даются выводы о применении межсетевых экранов и систем обнаружения/предотвращения вторжений в вычислительных сетях.

В третьей главе диссертации описывается процесс разработки методики детектирования сетевых атак. Определяются угрозы информационной безопасности и задачи, которые должны выполняться средствами защиты информации. Далее производится проектирование модели сети предприятия с применением как физических устройств, так и с использованием виртуальной инфраструктуры. Данная модель используется в испытаниях средств защиты информации. По результатам испытаний производится сравнение эффективности средств защиты информации. В конце главы даются выводы о произведённых испытаниях и об эффективности разработанной методики.

Все использованные при подготовке диссертации источники приведены в библиографическом списке.

ЗАКЛЮЧЕНИЕ

В данной диссертации была разработана методика детектирования сетевых атак с использованием устройств мониторинга и контроля транзитного трафика.

Была проанализирована необходимость и целесообразность разработки системы, соответствующей всем требованиям, которая может использоваться для испытаний любого типа и категории программно-аппаратных СЗИ.

В диссертации были рассмотрены следующие вопросы: анализ способов атаки на сетевые ресурсы, применение классических и современных видов атак; обзор и сравнение средств защиты; определение угроз и задач для построения системы защиты информации, разработка модели сети предприятия, построение испытательного стенда на основе виртуальной и физической сетевой инфраструктуры; выделение преимуществ и недостатков средств защиты при проектировании данной методики.

Данная методика несет в себе цель оценки соответствия, поиска недостатков программно-аппаратных СЗИ, что необходимо для усовершенствования разработок производителей в области защиты информации.

Получение подробных данных о продукте помогает потенциальному покупателю системы быть уверенным в безопасности данного устройства, а также в безопасности передачи данных, которое данное устройство обеспечивает.

Соответственно разработка методики испытаний является неотъемлемой частью разработки функционального продукта, а результат разработки методики – гарантом реализации трех основных постулатов информационной безопасности: конфиденциальности, целостности и доступности данных

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Мурашко, Е. А. Особенности применения программно-аппаратных средств защиты информации для обнаружения сетевых атак в корпоративных сетях/ Е.А. Мурашко, С.Н. Петров // Технические средства защиты информации : тез. докл. XVIII Белорусско-российской науч.-техн. конф. Минск, 9 июня 2020 г. / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2020.

2–А. Мурашко, Е. А. Детектирование сетевых атак с использованием устройств мониторинга и контроля транзитного трафика/ Мурашко Е. А., Марычев Д.В. // 56-я научная конференция аспирантов, магистрантов и студентов БГУИР : тезисы докладов 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР. Минск, 21-24 апреля 2020 г. / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2020.