ДЕТЕКТИРОВАНИЕ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ УСТРОЙСТВ МОНИТОРИНГА И КОНТРОЛЯ ТРАНЗИТНОГО ТРАФИКА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мурашко Е. А., Марычев Д.В.

Петров С.Н. – к.т.н., доцент

В настоящее время отсутствует общий подход к решению проблемы обнаружения аномальных ситуаций во время обработки информации компьютерными системами и информационными сетями. Однако в условиях активного развития информационных технологий и постоянной модернизации программного и аппаратного обеспечения компьютерных систем, решение задач обнаружения аномалий не может обеспечивать безопасность системы. 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.

Детектирование 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 тестирования позволяет разработчикам технических и программных продуктов заблокировать все возможные варианты незаконных действий злоумышленника для получения выгоды.

Методика детектирования атак позволяет определить, какое максимальное количество атак может обнаружить и предотвратить устройство без потери данных, что позволяет распределить все категории программно-аппаратных продуктов на определенные сценарии их использования, а также их пригодность для использования в сетях различных организаций. Результаты тестирования помогают увидеть, какими функциональными возможностями может обладать устройство, либо программный продукт, что позволит потенциальному покупателю, увидев заключения экспертов, определить, какое именное решение правильнее и выгоднее всего использовать в организации сетевой инфраструктуры компании либо предприятия.

Современные методы детектирования атак с использованием программно-аппаратных средств защиты информации имеют широкое распространение в жизни сообщества информационных технологий, но подразумевает собой засекречивание методик испытаний. Данный факт имеет место по причине того, что в ситуации, когда методика испытаний продукта находится в общем доступе, потенциальный злоумышленник может видеть места, через которые легче всего если не полностью перехватить информацию, то нанести ей вред.

Для проведения тестирования программно-аппаратных средств защиты информации необходимо соответствующее оборудование, средства соединения через каналы связи, соответствующие определенным требованиям и специализированное программное обеспечение.

Существует несколько основных типов реализации системы тестирования: система на основе аппаратного тестового стенда, система на основе виртуальной сетевой инфраструктуры, а также смешанный тип. Каждый из приведенных типов имеет преимущества при тестировании той или иной категории программных и программно-аппаратных средств защиты информации. Также определенные средства защиты информации возможно протестировать только лишь на определенном типе тестового стенда. Для проведения испытаний на ПЭВМ испытательного стенда устанавливается следующее ПО:

Таблица 1 – Перечень программного обеспечения

№п/п	ПЭВМ (ВМ)	Перечень программного обеспечения
1	ПЭВМ 1	ОС Microsoft Windows 7 Professional; утилита Wireshark версия 2.0.7; утилита Iperf; почтовый клиент Thunderbird версии 52.4.0; утилита Small HTTP Server 3.05.93;
2	ПЭВМ 2	ОС Kali Linux 2.0;
3	ПЭВМ 3	ОС Windows Server 2013; утилита Iperf; Small HTTP Server 3.05.93; VMware Workstation 12 Версия 12.5.2:

№п/п	ПЭВМ (ВМ)	Перечень программного обеспечения
4	ВМ 1	ОС Microsoft Windows 7; Courier Mail Server; RADIUS сервер.
5	ВМ 2	ОС Ubuntu 8.04; Web-приложение bWAPP v2.2 (приложение уязвимое к SQL инъекциям и межсайтовому выполнению сценариев XSS).

Персональные электронные вычислительные машины, коммутаторы и тестируемое программно-аппаратное СЗИ соединяются кабелями UTP категории 6 в соответствии со схемой, указанной на рисунке 1. При наличии разъемов для SFP/SFP+ модулей используются волоконно-оптические кабели.

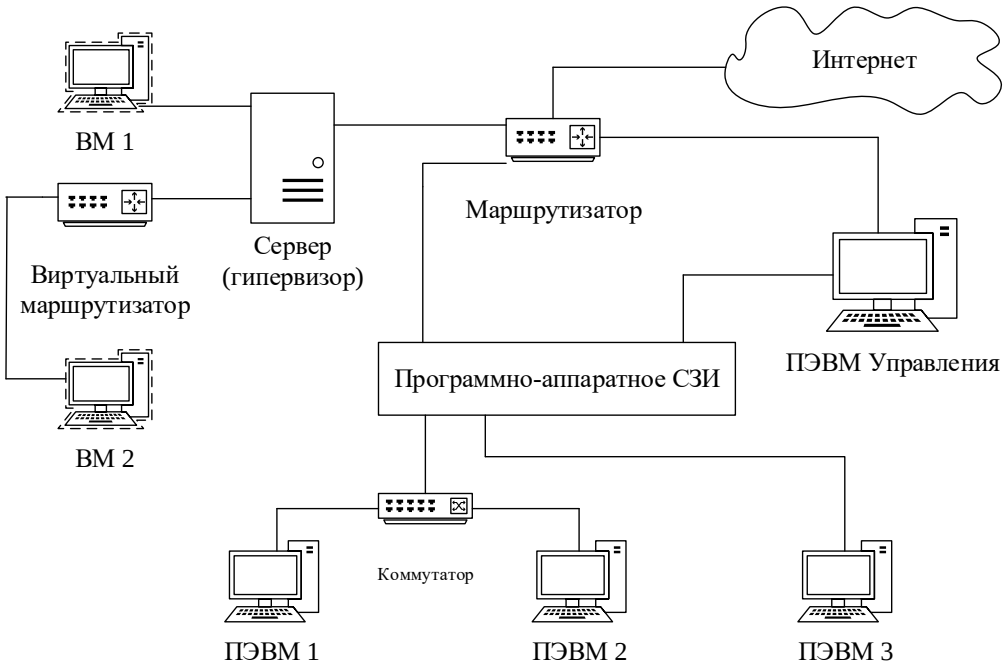

Рисунок 1 – Схема испытательного стенда

Рассмотренная система 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 и об обрабатываемым им атаках помогает потенциальному покупателю системы быть уверенным в безопасности данного устройства, а также в безопасности передачи данных, которое данное устройство обеспечивает. Соответственно тестирование согласно методике испытаний является неотъемлемой частью разработки функционального продукта, а результат тестирования на обнаружение сетевых атак – гарантом реализации трех основных постулатов информационной безопасности: конфиденциальности, целостности и доступности данных

Список использованных источников:

1 Компьютерные системы и сети [Электронный ресурс]. – Режим доступа : http://www.kcc.ru.

2 В.Г. Олифер, Н.А. Олифер. Компьютерные сети, принципы, технологии, протоколы (2-е издание) [Электронный ресурс]. – Режим доступа: https://www.bsuir.by/m/12_100229_1_85460.pdf.

3 Архитектура локальных сетей типа Ethernet [Электронный ресурс]. – Режим доступа http://sgpek.ru/files/electronbook/ISS/l9.html.

4 IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific [Электронный ресурс]. – Режим доступа : http://standards.ieee.org.

5 Ю.А. Родичев. Нормативная база и стандарты в области информационной безопасности [Учебное пособие]. – Режим доступа: https://search.rsl.ru/ru/record/01008599511.

6 Полторак А.А. Методы обнаружения сетевых аномалий в облачных средах [Электронный ресурс]. – Режим доступа: https://sibac.info/archive/meghdis/11(46).pdf (дата обращения: 01.07.2019)

7 С.Ю. Микова, В.С. Оладько, М.А. Нестеренко. Подход к классификации аномалий сетевого трафика [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/podhod-k-klassifikatsii-anomaliy-setevogo-trafika

8 Е.В. Ананьгин, И.С. Кожевникова, А.В. Лысенко, А.В. Никишова. Методы обнаружения аномалий и вторжений. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/metody-obnaruzheniya-anomaliy-i-vtorzheniy

9 А. А. Браницкий, И. В. Котенко, Анализ и классификация методов обнаружения сетевых атак, Тр. СПИИРАН, 2016, выпуск 45, 207–244 [Электронный ресурс]. – Режим доступа: http://www.mathnet.ru/links/1caa527ffecf29541261d48d0c84db5c/trspy873.pdf