Министерство высшего образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

РАБОТА ПРОВЕРЕНА
Директор ООО «ИТ Дистрибуция»
_____ М.А. Семёнов
_____ 2020 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2020 г.

Система обнаружения целевых атак на сетевую инфраструктуру коммерческой организации

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2020.455.ПЗ ВКР

Руководитель проекта,
специалист по ЗИ НОЦ
«Информационная
безопасность»
_____ А.Е. Баринов
_____ 2020 г.

Автор проекта,
студент группы КЭ-555
_____М.А. Борщевский
_____ 2020 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2020 г.

Челябинск 2020

АННОТАЦИЯ

Борщевский М.А. Система обнаружение целевых атак на сетевую инфраструктуру коммерческой организации – Челябинск: ЮУрГУ, КЭ-555, 60 с., 40 ил., 4 табл., библиогр. список – 15 наим., 2 прил.

Выпускная квалификационная работа выполнена с целью реализации системы обнаружения целевых атак на базе виртуального стенда.

В выпускной квалификационной работе отражены все этапы создания системы обнаружения целевых атак на базе виртуально стенда от общих сведений о системе управления событиями информационной безопасности до тестирования системы.

В процессе выполнения квалификационной работы был проведён анализ рынка систем управления событиями информационной безопасности, осуществлен выбор программного обеспечения, выполнено описание выбранного программного обеспечения, спроектирован и настроен виртуальный стенд. Проведена установка и конфигурирование программного обеспечения. Также было осуществлено проверочное тестирование системы обнаружения целевых атак на базе виртуального стенда.

ОГЛАВЛЕНИЕ

ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

ВКР – Выпускная квалификационная работа
ИБ – Информационная безопасность
ИС – Информационная система
ЛВС – Локальные вычислительные сети
ПО- Программное обеспечение
ППО- Проприетарное программное обеспечение
ОС – Операционная система
ФСТЭК – Федеральная служба по техническому и экспортному контролю
БД – База данных
АРМ – Автоматизированное рабочее место
ИТ – Информационные технологии
СУБД – Система управления базами данных
СУСИБ – Система управления событиями информационной безопасности

ВВЕДЕНИЕ

В современном мире увеличиваются объемы информации, циркулирующих в локальных вычислительных сетях, параллельно растёт и число угроз, которые связаны с обеспечением информационной безопасности и повышением уязвимости информационных систем.

Обеспечение работоспособности сети, а также её функционирование зависит не только от надёжности аппаратуры, но и от возможности противодействовать целевым атакам, способным нарушить работоспособность сети. В независимости от сферы деятельности бизнеса и его интересов, предприятие нуждается в защите информации, которая хранится в корпоративных сетях. Для достижения этой цели, требуется выполнение ряда процедур, в частности осуществления мониторинга событий и инцидентов в системе.

Безопасность — это не только состояние системы, но и процессы, неотъемлемой частью которых является мониторинг событий ИБ, рано или поздно появляется необходимость централизованного наблюдения и анализа логов, которые в огромном количестве могут генерироваться системами обнаружения вторжений и системами предотвращения вторжений. Практически у всех источников логов имеется собственный формат, также некоторые системы могут писать логи в нескольких разных форматах, которые отличаются своей информативностью. Большое разнообразие форматов и способов хранения логов может стать затруднительным процессом, что может усложнить анализ и предотвращение угроз в области ИБ. Для упрощения такой задачи существует специальный класс ПО - SIEM (Security Information and Event Management). Такое ПО представляет собой анализ событийной информации, поступающей из различных подсистем, в рамках всей системы информационной безопасности и дальнейшего выявления отклонений от норм по каким-либо заранее определённым критериям и правилам.

Основной целью выпускной квалификационной работы является реализация системы обнаружение целевых атак на базе виртуального стенда, с помощью которого можно будет проводить подготовку к внедрению в реальную среду, а также использовать при обучении студентов, системных администраторов, администраторов ИБ.

Для достижения цели следует выполнить следующие задачи:

1) Описать принцип работы SIEM – системы.
2) Проанализировать рынок SIEM – системы.
3) Сделать обзор на компоненты выбранной SIEM – системы.
4) Спроектировать виртуальный стенд, предварительно выбрав платформу виртуализации.
5) Выполнить установку и конфигурацию компонентов выбранной SIEM – системы.
6) Провести тестирование.