МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ПЕТРА МОГИЛИ

Смирнова Аріна Ігоревна

УДК 004.9

Система виявлення мережевих атак з використанням алгоритмів кластеризації

Галузь знань 12 «Інформаційні технології» за спеціальністю
122 «Комп’ютерні науки»
122 - ДР.А - 403.10790569

Автореферат
дипломної роботи на здобуття освітньої кваліфікації
«Бакалавр комп’ютерних наук»

Миколаїв – 2020

Дипломна робота є рукопис.

Робота виконана в Чорноморському національному університеті імені Петра Могили Міністерства освіти і науки України на кафедрі Інтелектуальних інформаційних систем

Науковий керівник: к.т.н., доцент
кафедри інтелектуальних
інформаційних систем
Сіденко Євген Вікторович

Рецензент: к.т.н., доцент
завідувач кафедри інженерії
програмного забезпечення
Дворник Ольга Василівна

Захист відбудеться «25» червня 2020 р. о $14^{\underline{30}}$ год. на засіданні екзаменаційної комісії (ауд. 2-403) у Чорноморському національному університеті імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

З дипломною роботою можна ознайомитися в бібліотеці Чорноморського національного університету імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

Автореферат представлений «20» червня 2020 р.

Секретар
екзаменаційної комісії,
викладач кафедри ІІС О. С. Скакодуб

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

У зв'язку з широким розповсюдженням глобальної інформаційної мережі Інтернет та розвитком комп'ютерних мереж, виникла реальна потреба в їх захисту від зовнішніх впливів з боку зловмисників. Наприклад, здійснення атак через мережу Інтернет стає способом проведення інформаційних операцій, а також вчинення злочинів у фінансовій та інших сферах, в тому числі членами терористичних організацій.

Комп'ютерні мережі протягом усієї своєї історії розвитку містили потенційну небезпеку порушення конфіденційності оброблюваної чи переданої інформації. Останнім часом, коли більшість державних і комерційних організацій мають власні мережі, а також вихід в глобальну мережу, вірогідність несанкціонованого доступу до закритих для сторонніх осіб відомостями значно зростає і виникає нагальна потреба своєчасного вжиття спеціальних заходів захисту, зокрема, використання систем виявлення вторгнень.

Робота присвячена розробці проекту виявлення мережевих атак з використанням алгоритмів кластеризації.

Метою роботи є виявлення вторгнень (атак) на мережевому або транспортному рівнях.

Об'єктом дослідження є система виявлення шкідливих дій і аномальних явищ на основі аналізу трафіку в комп'ютерній мережі.

Предметом дослідження є набір моделей, евристичних методів і алгоритмів, що навчаються на позитивному і / або змішаному трафіку мережі та призначених для виявлення вторгнень і аномальних явищ в комп'ютерних мережах.

Дипломна робота складається зі вступу, 4 розділів, висновків, переліку джерел посилання та додатків. Загальний обсяг роботи складає 62 сторінки (без додатків), 25 рис., 1 табл., 1 додаток та 20 джерел посилання на літературні джерела.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі дипломної роботи обґрунтовано актуальність обраної теми, сформульовано мету і задачі дослідження, визначено предмет та об'єкт дослідження.

У першому розділі проводиться аналіз предметної сфери, проводиться постановка задачі, аналіз існуючих аналогів.

Чітко сформована предметна сфера, об'єкт та предмет дослідження. Були розгянуті приклади самих популярних мережевих систем виявлення вторгнень, такі як Snort та Suricata, також ці системи були оцінені за різними критеріями. Під час опису процесу діяльності можна зробити висновок, що досліджувана сфера має досить багато недоліків, таких як незручність, вірогідність помилки під час виявлення вторження, та інші програмні поломки.

Також було наведено обґрунтування доцільності розробки, шляхом здійснення аналізу предметної області, етапів проектування архітектури додатку та аналізу методів розв'язання задачі. Також наведено техніко-економічне обґрунтування доцільності розробки. Результатом стала постановка задачі розробки.

У другому розділі виконано ґрунтовний аналіз засобів розробки , вибору математічної моделі, наведено порівняння сучасних технологій для розробки веб-ресурсів, проаналізовано основні плюси та мінуси базових підходів. Результатом стало обрання середовища розробки та стеку технологій.

Такоє було обґрунтовано вибір програмного забезпечення так і вибір технології для розробки вебзастосунку.

Для розробки серверної частини було обрано наступні інструменти, а саме CLion як середовище програмування, PGAdmin4 як графічне представлення бази даних.

База даних є PostgreSQL, вибір був обраний із за її масштабованості, безпечності, та підтримка транзакції.

У третьому розділі була описана програмна реалізація системи і описана інструкція з експлуатування для адміністратора серверної частини і методиста, який заповнює розклад.

Весь проект, дуже просто розгортається завдяки Ansible Playbook і легко масштабується. Щоб розгорнути всі микросервери у проекту потрібно ввести всього одну команду у терміналі.

Завдяки мікросервісної структурі у проекті легко замінити кожну частину, наприклад, якщо у проекті є фронтенд мікросервіс частину написаний за допомогою мови Angular, то її легко підмінити на сервіс написаний на любої іншої мові.

Результатом роботи є аналітичний сервер на хмарному сервісі, який управляється за допомогою консолі користувача. Користувач може в інтерфейсі дивитися, фільтрувати дані про мережеві вторгнення. Результати фільтрування показані на головної таблиці огляду. Також на цієї консолі є додаткові віджети, на яких можна побачити інформацію о попередженнях за рівнями мережі та по сенсорам встановленним у розгядаємих мережах.

У розділі з охорони праці було вивчено проблеми, пов'язані із забезпеченням здорових та безпечних умов, в яких відбувається праця людини, є одним із найважливіших завдань у розробці нових технологій та виробничих систем. Дослідження та виявлення можливих причин нещасних випадків на виробництві, професійних захворювань, аварій, вибухів, пожеж, а також розробка заходів та вимог, спрямованих на усунення цих причин, може створити безпечні та сприятливі умови для праці людини. Комфортні та безпечні умови праці – один з основних факторів, що впливають на продуктивність та безпеку, здоров'я працівників.

ЗАГАЛЬНІ ВИСНОВКИ

Виявлення мережевих атак є в даний момент однією з найбільш гострих проблем мережевих технологій. В даної дипломної роботі були наведені основні визначення що стосуються систем виявлення вторгнень. Перераховані складові елементи з яких побудовано систему виявлення вторгнень.

У результаті даної дипломної роботи було виконано

1. Класифікацію та аналіз архітектур сучасних систем виявлення вторгнень;

2. Дослідження та аналіз існуючих моделей, методів і систем евристичного виявлення вторгнень, вибір основних критеріїв оцінки евристичних методів виявлення вторгнень, оцінка існуючих методів і систем виявлення вторжень, були виділені їх недоліки, був виділений об'єкт дослідження, проаналізована предметна область, визначено мету і завдання роботи.

3. Розробка представлення трафіку у вигляді простору векторів; розробка набору швидких алгоритмів, що реалізує таке перетворення;

4. Дослідження та вибір чисельних методів скорочення розмірності отриманого простору;

5. Вибір і налаштування методу вилучення знань і формування бази знань про трафік цільової мережі;

6. Розробка моделі евристичної системи виявлення вторгнень на основі отриманих алгоритмів і вибраних методів;

7. Дослідження та оцінка отриманої моделі;

8. Розробка комплексу програм реалізують модель і дослідження його працездатності в реальних мережах.

В ході виконання роботи реалізовані такі функції, як: перегляд попереджень про мережеві вторгення, фільтрація, классифікація вторгнень, було розроблено математичне забезпечення системи, у якому було визначено,

якими алгоритмами можна рішити виникненні проблеми, та була розроблена система виявлення вторгнень методом кластеризації.

Всі сервіси спроектовані таким чином, щоб легко було підтримувати і додавати новий функціонал до нього.

Під час роботи над дипломним проектом не виявлено порушень щодо охорони праці. Робоче місце було належним чином обладнане. Технічний стан обладнання відповідав нормам техніки безпеки та нормам охорони праці, під час роботи не виявлено дефектів обладнання.

В результаті написання спеціальної частини з охорони праці була досягнута мета, а саме створення безпечних та здорових умов праці на робочому місці.

Анотація

Робота присвячена розробці проекту виявлення мережевих атак з використанням алгоритмів кластеризації.

Мета роботи – розробка моделі виявлення вторгнень на мережевому / транспортному рівнях і побудова евристичної мережевої системи виявлення вторгнень на основі отриманої моделі.

У роботі виконано аналіз предметної області, розроблено концепцію системи, сформульовано постановку задачі. Розглянуто приклади та недоліки існуючих інформаційних систем виявлення мережевих атак, які допоможуть зрозуміти можливі проблеми, які можуть виникнути, при проектуванні системи.

Також було виконано розділ з охорони праці.

Робота викладена на ___ сторінках друкованого тексту, містить 1 таблицю, 25 рисунків, та 2 додатка.

Summary

The work is devoted to the development of a project to detect network attacks using clustering algorithms.

The purpose of the work is to develop a model of intrusion detection at the network / transport levels and to build a heuristic network intrusion detection system based on the obtained model.

The analysis of the subject area is performed in the work, the concept of the system is developed, the problem statement is formulated. Examples and shortcomings of existing network attack detection information systems are considered, which will help to understand possible problems that may arise when designing a system.

A section on labor protection was also completed.

The work is presented on ___ pages of printed text, contains 1 table, 25 figures, and 2 appendices.