УДК 004

Д. І. Чубенко
Г. Б. Ракитянська

РОЗРОБКА СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Вінницький національний технічний університет;

Анотація

У роботі розглянуто проблему забезпечення безпеки інформаційних мереж та запропоновано архітектуру системи виявлення мережевих вторгнень (IDS) із застосуванням алгоритмів машинного навчання. Запропоноване рішення використовує інтелектуальні технології аналізу мережевого трафіку для виявлення аномалій та класифікації кібератак у режимі реального часу.

Ключові слова: система виявлення вторгнень, кібербезпека, машинне навчання, мережевий трафік, аналіз аномалій, класифікація атак, нейронні мережі.

Abstract

The paper addresses the problem of information network security and proposes the architecture of a network intrusion detection system (IDS) using machine learning algorithms. The proposed solution uses intelligent network traffic analysis technologies to detect anomalies and classify cyberattacks in real-time.

Keywords: intrusion detection system, cybersecurity, machine learning, network traffic, anomaly analysis, attack classification, neural networks.

Вступ

Сучасний етап розвитку цифрового суспільства характеризується стрімким зростанням обсягів передачі даних та, відповідно, збільшенням кількості кіберзагроз. Значна частина сучасних кібератак має модифікований характер, що формує об'єктивний бар'єр для їх своєчасного блокування. Академічні дослідження підтверджують, що використання традиційних сигнатурних методів виявлення вторгнень є недостатнім, оскільки вони не здатні ефективно протистояти атакам нульового дня (zero-day) [1].

Водночас, концепція інтелектуального аналізу даних доводить необхідність створення адаптивних інструментів для безперервного моніторингу мережевої безпеки [2]. Традиційні підходи до аналізу трафіку часто вимагають постійного оновлення баз правил і генерують велику кількість хибнопозитивних спрацювань. Існуючі програмні рішення або аналізують лише базові заголовки пакетів, або вимагають значних обчислювальних потужностей для глибокого інспектування. Рішенням проблеми є розробка системи виявлення мережевих вторгнень, яка забезпечує перехоплення трафіку з функцією його локального аналізу моделями машинного навчання.

Основна частина

Аналіз сучасних засобів кіберзахисту виявив низку суттєвих недоліків у контексті розпізнавання нових патернів атак. Популярні IDS (наприклад, Snort або Suricata) пропонують потужні механізми парсингу, проте ця функція є абсолютно залежною від попередньо написаних правил і погано працює з невідомими аномаліями [3]. З іншого боку, системи на базі статистичного аналізу забезпечують виявлення відхилень, але часто не здатні точно класифікувати тип загрози [4]. У цих системах відсутні вбудовані алгоритми розпізнавання прихованих залежностей у багатовимірних даних.

Для вирішення цих проблем запропоновано комплексну архітектурну модель автономної системи виявлення вторгнень, розроблену сучасними засобами мови програмування Python. Модуль збору даних реалізує гібридний підхід: для обробки мережевих інтерфейсів застосовується сучасна бібліотека Scapy, а для агрегації потоків — спеціалізовані інструменти захоплення пакетів. За точну

підготовку даних відповідає модуль попередньої обробки, який здійснює нормалізацію ознак та конвертує категоріальні змінні мережевих протоколів у числові вектори.

Ключовою особливістю розробленої системи є модуль інтелектуального аналізу, який здійснює класифікацію на базі ансамблевих методів (Random Forest) або глибоких нейронних мереж [5]. Використання інструментарію Scikit-learn та TensorFlow забезпечує виконання інференсу безпосередньо на сервері організації, усуваючи необхідність передачі чутливих даних у зовнішні хмарні сервіси. Для забезпечення безперебійності роботи системи процеси перехоплення пакетів та їх класифікації виконуються в окремих фонових потоках асинхронно. Крім того, з метою оптимізації ресурсів реалізовано механізм збереження історії інцидентів у локальну базу даних для подальшого донавчання моделі.

Висновки

Розроблена система ефективно вирішує проблему виявлення невідомих кіберзагроз в умовах динамічної зміни характеристик мережевого трафіку. Завдяки використанню оптимізованих алгоритмів вилучення ознак та ансамблевого підходу до класифікації можливо досягнути високої точності розпізнавання атак при зниженні рівня хибних спрацювань. Запропонований програмний продукт не лише оптимізує процес моніторингу безпеки, але й виступає потужним інструментом для проактивного захисту інформаційних систем завдяки функціям самонавчання та виявлення аномалій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019. Vol. 2, No. 1. P. 1-22.

2. Ferrag M. A., Maglaras L., Moschoyiannis S., Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications. 2020. Vol. 50. P. 102419.

3. Sarker I. H. CyberSecurity Data Science: An Overview from Machine Learning Perspective. Journal of Big Data. 2021. Vol. 8, No. 1. P. 1-29.

4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. /В.Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа /. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. –К. : ПВП «Задруга», 2014. – 320 с.

5. Носко П. М. Використання методів машинного навчання для виявлення мережевих загроз [Текст] / П. М. Носко – К.: НТУУ КПІ ім. Ігоря Сікорського, 2021. – С. 383–385.

Чубенко Денис Ігорович — студент групи 4ПІ-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: deniscubenko82@gmail.com.

Ракитянська Ганна Борисівна — *доцент кафедри програмного забезпечення Вінницького національного технічного університету, Вінниця, e-mail: rakit@vntu.edu.ua.*

Chubenko Denys — student of group 4PI-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: deniscubenko82@gmail.com.

Rakityanska Anna — *Associate Professor in the Department of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: rakit@vntu.edu.ua*