СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ МЕТОДІВ ГЛИБИННОГО НАВЧАННЯ

Попович І.Д.
Науковий керівник – к.т.н., доцент Мазурова О.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Програмної інженерії, тел. (057) 702-14-46)

Security of cloud based servers is one of the most important aspects of modern web-applications. Intrusion detection systems are effective instruments to detect incoming threats to be able to react in a proper way. Rapid artificial intelligence technology growing provides a great opportunity to make Intrusion detection systems more efficient. In order to analyze the effectiveness of different deep learning approaches, created a web tool that used pretrained models to solve intrusion detection system task.

Безпека хмарних додатків є одним з найважливіших завдань, яке розв'язується у ході проектування сучасних веб-систем. В найкращому варіанті необхідно розробити систему, яка повністю захищена від зловмисників. Але в реальному випадку це неможливо. Тому, щоб своєчасно реагувати, потрібно якнайшвидше визначити загрозу.

Система виявлення вторгнень (англ. Intrusion detection system – IDS) – це тип програмного забезпечення, призначеного для автоматичного сповіщення адміністраторів, коли хтось чи щось намагається порушити інформаційну систему через зловмисні дії або через порушення правил безпеки [1].

IDS може містити один або обидва типи виявлення вторгнень: на основі визначення підписів та на основі визначення аномалій [2]. IDS на основі підписів відстежує мережевий трафік на предмет підозрілих зразків у пакетах даних, підписів відомих вторгнень у мережу, щоб виявити та усунути напади та компроміси [2]. Це досягається за допомогою використання бази даних відомих типів вторгнень та шаблонів даних, що дозволяє IDS на основі підписів швидко ідентифікувати вторгнення та розпочати відповідний хід дій.

В свою чергу IDS на основі аномалії використовує властивості системи у звичайному стані, щоб відстежувати, чи відбувається незвична чи підозріла діяльність [2]. Цей метод вимагає підготовки, оскільки для базової підготовки моделі потрібно, щоб IDS дізнався про ваші схеми використання, і це робить його органічним, евристичним підходом до виявлення вторгнень. Перевага IDS на основі аномалії полягає в тому, що він є більш гнучким та потужним, ніж IDS на основі підписів, для якої необхідна існуюча база даних зловмисного трафіку.

Отже, була поставлена задача дослідити підходи, які можна використати для створення системи виявлення вторгнень на основі аномалії, побудувати модель, яка базується на обраних підходах та

програмно реалізувати її в складі прикладного додатку, призначеного для виявлення аномальної активності в мережі у реальному часі.

Дослідження проводилися в області штучного інтелекту. Досягнення у цьому напрямку активно застосовуються у багатьох галузях, у тому числі і в галузі безпеки програмного забезпечення. Для розв'язання задачі визначення аномалій існує багато методів класичного машинного навчання, такі як нейронні мережі (ANN), Support vector machines (SVM), Naive-Bayesian (NB), Random Forests (RF), Self-Organized Maps (SOM) . Наразі активно використовують більш ефективний підхід глибинного навчання. Зокрема, звичайні рекурентні нейронні мережі (RNN), а також більш специфічні Long short-term memory(LSTM) та Gated recurrent unit (GRU) [3].

Головна перевага архітектури LSTM над звичайними рекурентними нейронними мережами в тому, що вона може обробляти довготривалі залежності у даних. Це стало можливим завдяки додаванню до одиниці мережі додаткових шарів, які регулюють потік інформації до мережевої клітини.

GRU створений для вирішення тієї ж проблеми, що LSTM, але її одиниця мережі має на один шар менше. Крім того, GRU має можливість повторювати останні вихідні дані при переході до наступної ітерації мережі. Це робить її більш ефективною, ніж LSTM, в деяких випадках, зокрема, на датасетах малого розміру.

У даній роботі проаналізовано методи Long short-term memory та Gated recurrent unit у контексті задачі навчання для побудови IDS на основі аномалій та реалізовано демонстраційну систему виявлення вторгнень, яка базується на натренованих моделях, побудованих за допомогою обраних методів: перегляд підозрілих подій у системі; відображення статусу підозрілих на аномалію подій; сортування подій за різними критеріями; будування графіків аномалій у залежності від часу.

У якості технології для тренування моделей було використано мову Python та фреймворк для глибинного навчання TensorFlow. Для написання прикладного додатку було використано Python-фреймворк aiohttp на базі asyncio для написання API для натренованих моделей та нереляційну базу даних MongoDB у якості базового сховища даних. Також було використано Vue.js для побудови веб-клієнту системи моніторингу.

Запропоновані моделі може бути використано для побудови IDS або різноманітних аналізаторів мережі. Розроблений прикладний додаток може бути використано для моніторінгу мережі різних хмарних серверів, кластерів, або локальних мереж та виявлення різноманітних кібератак.

Список використаних джерел:

1. Michael Sikorski, Andrew Hoing. Practical Malware Analysis. – No Strach Press, 2018. – 802 с. 2. Stefan Axelsson. Intrusion Detection Systems: A Survey and Taxonomy. – Department of Computer Engineering Chalmers University of Technology G¨oteborg, Sweden, 2015. – 27 с. 3. Raghavendra Chalapathy, Sanjay Chawla. Deep Learning for Anomaly Detection: A Survey. – University of Sydney, 2019. – 48 с.