Виявлення DDoS атак статистичними методами

Радівілова Тамара Анатоліївна,
Тавалбех Максим Хаджем,
Глушаєв Денис Ярославович,
Заіка Максим Володимирович

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
tamara.radivilova@nure.ua, tavalbeh@icloud.com,
denys.hlushaiev@nure.ua, maksym.zaika@nure.ua

Анотація. *Запропоновано алгоритм виявлення вторгнень заснований на статистичних методах аналізу аномалій. Перевагою алгоритму є раннє виявлення вторгнень, за рахунок швидкого обчислення ентропії із застосуванням методу рухомого вікна. Запропонований алгоритм було програмно реалізовано та проведено експерименти на тестових даних, які було взято з датасетів.*

Ключові слова: *системи виявлення вторгнень, атаки, ентропія, аналіз аномалій, трафік.*

I. Вступ

Постійне збільшення використання мережевої зв'язку в останні роки призвело до збільшення ризику компрометації інформації. Методи вторгнень розвиваються і стають більш витонченими. Отже, класичні системи виявлення вторгнень показують зниження продуктивності при виявленні нових атак. [1]

Системи виявлення вторгнень класифікуються за методиками аналізу на сигнатурні, статистичні (аномальні) і гібридні. Статистичні методи створюють статистичну модель, що описує нормальний мережевий трафік, і ідентифікують будь-яку ненормальну поведінку, що відхиляється від моделі. Основною проблемою аномальних методів є складність в налаштуванні і велика кількість хибнопозитивних тривог в разі некоректно заданих правил [2]. У даній роботі основна увага приділяється системам виявлення вторгнень на основі аномалій, зокрема, щодо виявлення мережевих атак.

Статистичні методи виявлення аномалій створюють статистичну модель, що описує нормальний мережевий трафік та поведінку мережі, і ідентифікують будь-яку ненормальну поведінку, що відхиляється від моделі. На відміну від сигнатурних методів, методи на основі аномалій мають ту перевагу, що вони можуть виявляти атаки з нульовим днем, так як нові атаки можуть бути виявлені, як тільки вони відбудуться. Основною проблемою методів на основі аномалій є складність в налаштуванні і велика кількість хибнопозитивних тривог в разі некоректно заданих правил [2]. У даній роботі основна увага приділяється системам на основі статистичного виявлення аномалій, зокрема, щодо виявлення DDoS атак.

II. Статистичний метод виявлення DDoS атак

У зв'язку з цим запропоновано алгоритм виявлення та захисту від DDoS атак (таких як UDP-flood, потоків TCP SYN, Ping of Death атак та HTTP flood). Запропонований алгоритм зосереджується на трьох важливих частинах, а саме виявленні, захисті і повідомленні про напади. Запропонований алгоритм виявлення буде перевіряти вхідний трафік, будь то трафік DDoS або звичайний трафік. Якщо вхідний трафік є DDoS-трафіком, то запропонований алгоритм виявлення буде визначати типи DDoS-атак, такі як UDP-flood, потоків TCP SYN, Ping of Death та HTTP flood, засновані на поведінці атаки. Наш алгоритм виявлення вторгнень вимірює статистичні властивості конкретних полів в заголовках пакетів. Наприклад, якщо детектор захоплює 1000 послідовних пакетів в точці пірингу і обчислює частоту зустрічі кожної унікальної IP-адреси джерела в цих 1000 пакетах, то детектор буде мати модель розподілу адреси джерела. Подальші обчислення з цим розподілом дозволяють виміряти випадковість або однорідність адрес, а також «добротність» розподілу по відношенню до попередніх вимірювань. Далі застосовується умовна ентропія для виявлення відмінностей між розподілом класів пакетів в поточному трафіку в порівнянні з розподілом, знайденим в результаті методу максимуму. [2]

Ентропія трафіку залежить від ймовірностей p_i появи пакетів і-го типу при їх передачі $H = -\sum_{i=1}^{n} p_i \log_2 p_i$, де p_i – ймовірність появи пакету і-го типу, яка може виступати його частотою $f_i = n_i / N$; n_i – кількість пакетів і-го типу; N – загальна кількість пакетів трафіку. Для збільшення швидкості обчислень ентропії використовувався метод рухомого вікна.

Якщо кількість отриманих пакетів нижче значення ентропії в 0.3, пакет автоматично видаляється за допомогою алгоритму захисту. Алгоритм захисту забезпечить можливість проходження в мережі тільки легітимного трафіку.

Для аналізу роботи запропонованого алгоритму проводився аналіз трафіку з датасету [3]. Датасет містив нормальний трафік та атаки DDoS, UDP-flood, потоків TCP SYN, Ping of Death та HTTP flood.

III. Висновки

Запропонований алгоритм виявлення вторгнень на основі статистичних методів аналізу аномалій показав високі значення точності виявлення атак (близько 94%) та низькі значення помилкового позитивного показника (близько 16%).

Список літератури

[1] Gupta, N., Srivastava, K., Sharma, A.: Reducing False Positive in Intrusion Detection System: A Survey. International Journal of Computer Science and Information Technologies 7 (3), 1600-1603 (2016)

[2] Vytalii Bulakh, Lyudmyla Kirichenko, Tamara Radivilova. Classification of Multifractal Time Series by Decision Tree Methods. 14th International Conference ICTERI 2018 ICT in Education, Research, and Industrial Applications, 2018, p.1-4.

[3] Al-kasassbeh, M.; Al-Naymat, G.; Al-Hawari, E. Towards Generating Realistic SNMP-MIB Dataset for Network Anomaly Detection. Int. J. Comput. Sci. Inf. Secur. 2016, 14, 1162–1185.