Петляк Н.С., асистент,
Кльоц Ю.П., к.т.н., доцент
Хмельницький національний університет

ПІДХІД ДО АНАЛІЗУ ВИХІДНОГО ТРАФІКУ НА ОСНОВІ СИГНАТУР

Цифровізація суспільства призводить до стрімкого збільшення кібератак. Одним із джерел забезпечення потреб в інформаційних технологіях є використання загальнодоступних комп'ютерних мереж. Проте такі мережі є привабливими для порушників за рахунок підключення без ідентифікації.

Наявні IPS/IDS системи розраховані на захист корпоративних мереж, їх налаштування вимагає профільних фахівців та додаткових затрат на обладнання, а поточні дослідження у даній предметній області орієнтовані на вирішення вузьких задач [1-3].

Пропонуємо підхід до аналізу вихідного мережевого трафіку, що складається з кількох методів задля максимальної ефективності та без перевантаження мережевого обладнання.

Аналіз моделей поведінки порушників при найпоширеніших типах атак дозволяє зробити висновок щодо того з яких елементів пакету трафіку слід формувати сигнатуру пакету для визначення зловмисного трафіка. Задля зменшення часової затримки при передачі даних та ефективного використання мережевих ресурсів проведено оптимізацію визначених елементів та обрано найбільш значущі відповідно до [4].

Під час роботи даної системи формується сигнатура з пакета трафіку та передається на етап виконання методу виявлення зловмисного вихідного трафіку на основі сигнатур. Даний метод працює наступним чином:

Крок 1. Якщо сформована сигнатура пакету належать множині дозволених сигнатур, то з'єднання дозволяється та відбувається перехід до кроку 4.

Крок 2. Якщо сформована сигнатура пакету належать множині заборонених сигнатур, то з'єднання забороняється та відбувається перехід до кроку 4.

Крок 3. Якщо сформована сигнатура пакету не належать множині дозволених сигнатур та не належать множині заборонених сигнатур, то відбувається перехід до методу виявлення зловмисного вихідного трафіку заснованого на нечіткому логічному висновку.

Крок 4. Завершення обробки пакету.

Метод виявлення зловмисного вихідного трафіку заснований на нечіткому логічному висновку містить набори правил, що дозволяють чи забороняють з'єднання. Даний метод працює наступним чином:

Крок 1. Якщо сформована сигнатура пакета належить до одного з правил, що задовольняють вимогу дозволеного трафіку, то пакету дозволено з'єднання та відбувається перехід до кроку 2. В іншому випадку перехід до кроку 3.

Крок 2: Сигнатура пакета записується в множину дозволених з'єднань. Перехід до кроку 6.

Крок 3. Якщо сформована сигнатура пакета належить до одного з правил, які задовольняють вимогу щодо забороненого трафіку, то з'єднання та користувач блокуються, відбувається перехід до кроку 4. В іншому випадку перехід до кроку 5.

Крок 4. Сигнатура пакета записується в множину заборонених з'єднань. Перехід до кроку 6.

Крок 5: Сигнатура пакета записується в множину невизначених з'єднань, після чого пакет отримує дозвіл на передачу.

Крок 6: Завершення обробки пакета.

Під час роботи даного методу також відслідковується рівень завантаженості процесора маршрутизатора, оскільки це один із ключових параметрів завантаженості мережі. Якщо рівень сягає максимальних значень, то відбувається перехід від методу заснованого на нечіткому логічному висновку до адаптивного методу виявлення зловмисного вихідного трафіку.

Він відрізняється від попереднього скороченим набором правил які забезпечують зменшення навантаження на маршрутизатор на достатню точність виявлення вихідного зловмисного трафіку.

Запропонований підхід дозволить класифікувати вихідний трафік з метою дозволу безпечних з'єднань чи блокування зловмисних.

Список використаних джерел

1. M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani. CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques. IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, 1 March1, 2021, doi: 10.1109/JIOT.2020.3002255.
2. Mansoor Farooq, "Supervised Learning Techniques for Intrusion Detection System based on Multi-layer Classification Approach" International Journal of Advanced Computer Science and Applications(IJACSA), 13(3), 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130338
3. Amrutha Muralidharan Nair and R Santhosh, "Mitigation of DDoS Attack in Cloud Computing Domain by Integrating the DCLB Algorithm with Fuzzy Logic" International Journal of Advanced Computer Science and Applications(IJACSA), 13(10), 2022. http://dx.doi.org/10.14569/IJACSA.2022.0131059
4. Творошенко І.С. Технології прийняття рішень в інформаційних системах: навч. посібник. – Харків: ХНУРЕ, 2021. – 120 с.