Критерії виявлення повільних DDoS-атак

УДК 004.21.1(043.2)

Петро Поночовний[1], Ігор Аверічев[2]

Державний університет інформаційно-комунікаційних технологій,
[1]petja91@ukr.net, [2]iaverichev19@gmail.com

В TCP/IP-мережах при передачі даних можуть виникати шкідливі повільні DDoS-атаки [1], які призводять до перевантажень і відмови в обслуговуванні, при яких передача даних унеможливлюється.

На сьогодні не має чітких правил, які дозволяють виявити такі види атак. Деякими вченими запропоновані нечіткі алгоритми [2], ефективність яких варіюється від виду переданої інформації та від кількості фактичних запитів до серверу, однак і вони не дають чітку відповідь, як можна виявити повільну DDoS-атаку і як їй протидіяти.

Сформулюємо вимоги для аналізу повільних DDoS-атак.

1. Аналіз тривалості з'єднання.

Під час нормальної роботи мережі ці значення коливаються від дуже малих до великих. Необхідно знайти середнє арифметичне значення цієї множини.

2. Аналіз кількості байтів і потоків в секунду.

Під час повільної DDoS-атаки цей показник повинен бути дуже малий, тому що пакети між атакуючим хостом та сервером майже не відправляються, а сервер знаходиться в режимі очікування, не розриваючи з'єднання. Необхідно знайти медіану кожної з двох вибірок.

3. Аналіз кількості пакетів, відправлених з хоста.

Визначається кількість переданих даних відправником за одну секунду. Знаходимо медіану вибірки для всіх сеансів і визначаємо яку саме кількість даних клієнт може відправити в середньому на сервер.

4. Аналіз кількості пакетів, відправлених на сервер.

Це кількість переданих даних назад з сервера до відправника за одну секунду. Знаходимо медіану вибірки, враховуючи дані всіх сеансів.

5. Аналіз мінімального значення підключень з однієї IP-адреси, створених за одну хвилину.

Потрібно розбити вибірку на класи, групуючи значення по IP-адресам джерела і визначати кількість підключень протягом кожної хвилини. З даної вибірки обираємо середнє значення. Мінімальним значення з якого почнеться спостереження – одне підключення на секунду, тобто шістдесят підключень на хвилину. Менша кількість підключень у вибірку входити не буде.

6. Аналіз мінімального коефіцієнту варіації для вибірки із кількості переданих байтів в потоці з кожної IP-адреси.

Необхідно розбити всю вибірку відправлених байтів на класи по IP-адресам джерел. Фіксуються значення кількості байт для кожного підключення з конкретної IP-адреси, потім для кожного класу розраховується дисперсія та середнє значення. Далі знаходяться коефіцієнти варіації для кожної IP-адреси, серед яких обираються два мінімальних значення і знаходиться серед них середнє. Це значення і буде складовою критерія.

Сформулюємо основні критерії для визначення шкідливих з'єднань.

Критерій 1 – залежність тривалості сеансу від кількості переданої інформації.

Під час повільної DDoS-атаки на відмову в обслуговуванні, тобто при великій тривалості з'єднання маємо дуже малу кількість переданих пакетів. Таке з'єднання вважається підозрілим по першому критерію, якщо відповідає наступним умовам: 1) тривалість TCP сеансу більша за граничну; 2) кількість переданої інформації менша за граничну;

Критерій 2 – однорідність множин переданої інформації та тривалості.

При нормальній роботі мережі множини значень кількості байт в секунду можуть суттєво відрізнятися від сеанса до сеансу, створених з однієї IP-адреси, тому вони вважаються неоднорідними, як і значення тривалості сеансу.

Тривалість з'єднання буде вважатися однорідною, тому що під час атаки зловмисник намагається якомога довше зайняти сервер. Тобто єдине, що може скинути з'єднання – це часовий ліміт сервера, тому тривалість буде варіюватися навколо конкретного значення. Підключення вважається підозрілим, якщо з'єднання з однієї IP-адреси будуть відповідати таким вимогам: 1) коефіцієнт варіації кількості переданих байтів даних з даної IP-адреси менший, ніж значення, що визнані граничними у даній мережі; 2) значення тривалості підключень з даної IP-адреси є однорідною множиною, тобто її коефіцієнт варіації приймає значення менше на 30%.

Критерій 3 – велика кількість підключень за хвилину.

При атаці на відмову в обслуговуванні спостерігається велика кількість з'єднань з IP-адреси атакуючого. Після того, як кількість підключень за хвилину прийме значення більше, ніж зазначено у файлі з границями, підключення буде вважатися підозрілим по другому критерію.

Приведені критерії були сформовані виходячи із практичних спостережень, якими можна оперувати при аналізі мережевого трафіку представленого у вигляді двонаправлених TCP потоків.

На основі кожного з критеріїв не можна робити висновки щодо шкідливості програм, тому що їм можуть відповідати і легітимним з'єднанням, що викличе хибні спрацювання. Однак співпадіння по комбінації двох критеріїв підвищує ймовірність того, що сеанс виявиться шкідливим і з даної IP-адреси відбувається повільна DDoS-атака. Якщо TCP потік відповідає трьом критеріям одночасно, то висновок однозначний, що саме з цієї IP-адреси відбувається атака, а з'єднання є шкідливим і його необхідно перервати чи заблокувати.

1. Collection and Analysis of Slow Denial of Service Attacks Using Machine Learning Algorithms. – Режим доступу до ресурсу: https://www.proquest.com/openview/c5edb8073f8b9e10eb12c9c6e588d92e/1?pqorigsite=gscholar&cbl=18750&diss=y (дата звернення: 10.04.2024).
2. Лаптєв О.А., Бучик С.С., Савченко В.А., Наконечний В.С., Михальчук І.І., Шестак Я.В. Виявлення та блокування повільних DDOS-атак за допомогою прогнозування поведінки користувача // Наукоємні технології, 2022. – № 3(55). – С.184-192.