Архітектура програмного комплексу забезпечення безпеки виявлення і протидії DDoS-атакам

Савіцька О.О., Джулій В.М., Муляр І.В.
Хмельницький національний університет

Програмний комплекс виявлення початку атаки в режимі реального часу розраховує середньоквадратичне відхилення з урахуванням актуальних сезонних періодів за кількістю запитів до мережного ресурсу в кожному періоді. Програмний комплекс дає можливість задати розмірність розглянутих періодів: 1 хвилина, 15 хвилин, 1 годину і т.д. А також вести моніторинг відразу по декількох періодів. На підставі розрахованого середньоквадратичного відхилення задається верхня межа кількості запитів до мережного ресурсу відповідного періоду.

Програмний комплекс виявлення початку атаки має гнучкі налаштування, що дозволяють задати чутливість до можливої атаки (лістинг 1). Конфігураційні дані виділені в окремий php-файл, що дає додаткові можливості як з точки зору зручності, так і з точки зору безпеки. Чутливість варіюється за допомогою корекції границі, а також порушенням границі відразу в декількох періодах різного розміру. Наприклад, при порушенні границі на хвилинних інтервалах засіб може тільки сповістити зацікавлених осіб про збільшення активності. У разі порушення границі також на п'ятихвилинному інтервалі відбувається повне включення механізму захисту.

Лістинг 1 - Фрагмент конфігураційного файлу

```
//час періоду мережевої активності в секундах, 86400 добу, 604800 тиждень
    $Loop = 40400;
//період для дослідження в секундах
```

```
$User_per = 300;
//кількість періодів для аналізу
$Count_user_per = 100;
//період, який необхідно відступити від початку атаки для позначки
//легітивного трафіку
$Safe_per = 600;
//число в процентах, на яке благополучний трафік повинен відрізнятися від
//шкідливого
$Pogresnost = 10.
```

У разі виявлення початку атаки виконуються наступні дії:

1. Розсилка повідомлень. В автоматичному режимі відбувається розсилка повідомлень електронною поштою.

2. Виконання скриптів. Запускаються скрипти або сторонні програми, підготовлені для виконання системним адміністратором. Це можуть бути як скрипти, що включають додаткові рівні кешування або ж відключають модулі web-ресурсу, що генерують підвищене навантаження, так і системні скрипти та програми.

3. Активація засобів фільтрації трафіка.

Засіб фільтрації трафіка. На підставі розробленого алгоритму засіб фільтрації трафіку проводить первинну кластеризацію. В результаті первинної кластеризації в базі даних створюються дві таблиці, що характеризують шкідливий і легітивний трафік. Отримані таблиці використовуються в якості навчальних вибірок при класифікації запитів, що надходять. В процесі роботи таблиці уточнюються і доповнюються.

Дані, які містяться в таблиці, що характеризує шкідливий трафік, використовуються для блокування трафіку. У розробляємому програмному засобі передбачена можливість вилучення з таблиці, відповідно шкідливому трафіку, клієнтських IP адрес і створення на їх основі заборонних правил. Крім цього, на підставі даних про шкідливий трафік можливо реалізувати додаткові механізми захисту. Наприклад, при надходженні шкідливих запитів до конкретної сторінки можна в автоматичному режимі тимчасово заблокувати цю сторінку або ж підмінити її статичної або кеш-версією. В цьому випадку шкідливий трафік, який був некоректно класифікований і не був заблокований на попередньому рівні, завдасть меншої шкоди.

Блокування шкідливих запитів. Для блокування шкідливих запитів передбачено два варіанти. В першому варіанті блокування здійснюється за допомогою створення відповідних забороняючих правил для iptables. Другий варіант буде актуальний якщо засіб функціонує у вузьких рамках віртуального хостингу, в цьому випадку блокування шкідливого трафіку здійснюється за допомогою заборонних правил, зазначених у файлі .htaccess (Лістинг 2).

В обох випадках блокування трафіку здійснюється повністю в автоматичному режимі. Також передбачений механізм експорту даних про

шкідливий трафік для блокування його в різних програмних файерволах або ж на вищих мережевих вузлах.

Лістинг 2 - Приклад блокування IP-адрес у файлі .htaccess

```
order allow, deny
deny from 192.168.0.1
deny from 192.168.0.2
allow from all
```

Архітектура програмного комплексу представлена на рис. 1.

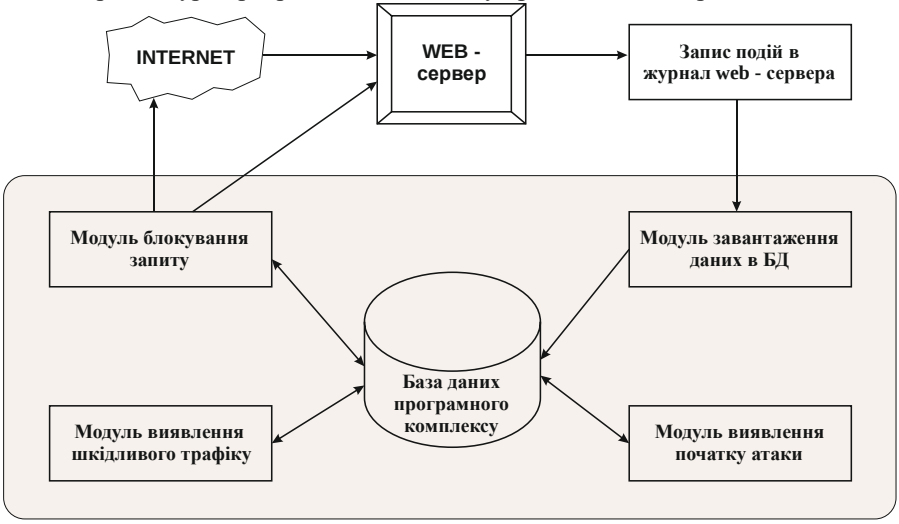

Рисунок 1 - Архітектура програмного комплексу

Взаємодія модулів програмного комплексу, один з одним і з WEB-сервером, відбувається за наступною схемою:

1. В результаті обробки запитів, що приходять до WEB-сервера з мережі інтернет, в журнал WEB-сервера додаються відповідні події.

2. Модуль завантаження даних з заданим інтервалом часу зчитує нові дані з журналу і завантажує їх в базу даних.

3. Модуль виявлення початку атаки, аналізує дані про запити, що містяться в базі даних. У разі виявлення початку атаки, цей модуль створює в базі даних дві порожні таблиці. Одну для легітимних запитів, другу для шкідливих.

4. Модуль виявлення шкідливого трафіку відстежує появу і стан зазначених вище таблиць БД. Якщо таблиці незаповнені, модуль проводить кластеризацію і первинне заповнення таблиць. Якщо в таблицях вже є дані, модуль аналізує запити, шо надійшли на предмет приналежності до груп легітивних або шкідливих запитів, і додає дані про запит в відповідну таблицю.

5. Модуль блокування запиту отримує список IP-адрес з таблиці, що містить шкідливі запити і вносить їх в «чорні списки» брандмауера або передає для блокування на вищестоящий мережевий сегмент.

Розроблений програмний засіб повністю відповідає поставленим завданням. Основні риси створеного програмного комплексу для виявлення і протидії DDoS-атакам це кроссплатформенність, універсальність і масштабованість.

Програмний комплекс може застосовуватися в якості засобу забезпечення безпеки так званої «останньої милі». Основною спеціалізацією комплексу є забезпечення безпеки web-серверів від DDoS-атак типу http-flood. Програмний комплекс підтримує різні операційні системи, він може бути використаний з більшістю сучасних web-серверів. При цьому інсталяція комплексу може здійснюватися як в рамках фізичного сервера, так і в рамках віртуального хостингу.

Універсальність програмного комплексу виявлення і протидії DDoS-атакам полягає в можливості його використання не тільки для виявлення http-flood'a, а й інших DDoS - атак різних типів. При незначних змінах, що не відносяться до основного модуля, програмний засіб може аналізувати різні дані, що містяться в log-файлах різних мережевих сервісах, або ж використовувати дані, отримані від мережевих локаторів.

У даній реалізації весь програмний комплекс, що складається з трьох модулів, розміщується на кінцевому мережевому ресурсі. В разі необхідності, модулі програми можуть бути розміщені в різних місцях мережі. Так, наприклад, на кінцевому сервері може знаходитися тільки засіб завантаження даних. Засоби виявлення атаки і фільтрації трафіку можуть бути встановлені на окремому сервері, недоступному для атаки з зовнішньої мережі. При такій установці програмний засіб зможе нормально функціонувати і проводити класифікацію трафіку навіть в випадку відмови атакуємого сервера.

Можливий варіант інсталяції, коли на вузлі, безпеку якого потрібно підтримувати, взагалі не встановлено ніяких модулів програмного засобу. У цьому випадку дані для аналізу можуть бути отримані від мережевих локаторів або вищестоящих маршрутизаторів. Блокування трафіку може бути здійснена на вищому вузлі.

Також програмний комплекс підтримує мультиінсталляцію при одночасному запуску декількох однойменних модулів. Так наприклад, дані для аналізу можуть надходити в базу даних з декількох джерел. Дані про шкідливий трафік можуть бути передані для блокування на різні рівні.

Література

1. Бабаш, А.В. Криптографические методы защиты информации: учебник / А. В. Бабаш, Е. К. Баранова. - М. : КНОРУС, 2016. - 190 с.

2. Батурин, Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзинский. – М.: Юридическая литература, 2006. – 160 с.

3. Борисов, М.А. Основы программно-аппаратной защиты информации: учеб. пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов. - 4-е изд., перераб. и доп. - М. : ЛЕНАНД, 2016. - 416 с.

4. Васильева, И.Н. Криптографические методы защиты информации : учебник и практикум для академ. бакалавриата / И. Н. Васильева. - Санкт-Петерб. гос. эконом. ун-т . - М. : Юрайт, 2017. - 349 с.

5. Нестеров, С.А. Основы информационной безопасности : учебник / С. А. Нестеров. - СПб. : Лань, 2017. – 423 с.