УДК 004.056:004.738.5

ЕКСПЕРИМЕНТАЛЬНА УСТАНОВКА ДЛЯ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ ВІД DOS-АТАК НА ВЕБСИСТЕМИ НА БАЗІ APACHE WEB SERVER

Василенко І.О., Марчук А.В.
e-mail: ivan.vasylenko@nure.ua, artem.marchuk@nure.ua
Науковий керівник – к.т.н., ст. викл. Марчук А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

An experimental setup is proposed for reproducible research of DoS attacks on a web system at the application level. The setup is designed for local deployment in an isolated environment using Apache Web Server as the target research object. The architecture of the stand, scenarios of legitimate load and attack impact are proposed. The proposed setup can be used as a basis for Master's research and educational laboratory work, ensuring the repeatability of experiments and the possibility of comparing the results obtained.

Порушення доступності вебсервісів унаслідок атак типу Denial of Service залишається однією з найбільш поширених загроз для сучасних інформаційних систем. Особливу небезпеку становлять атаки прикладного рівня, які імітують нормальну поведінку клієнтів, але створюють надмірне навантаження на вебсервер, пул робочих процесів, точки входу застосунку. У таких умовах навіть відносно проста атака може спричинити істотне зниження продуктивності, зростання затримок або повну недоступність сервісу для легітимних користувачів.

На практиці механізми захисту вебсерверів часто налаштовуються за типовими рекомендаціями без глибокої експериментальної перевірки їхньої ефективності в умовах конкретного навантаження та конкретної архітектури. Це призводить до двох проблем. По-перше, окремі механізми можуть виявитися малоефективними проти певного класу атак, зокрема slow HTTP. По-друге, надмірно жорсткі обмеження можуть негативно впливати на легітимний трафік, збільшуючи затримки та кількість хибних блокувань.

У зв’язку з цим актуальним є створення експериментальної установки, яка дозволяє у відтворюваних умовах досліджувати поведінку вебсервера під час DoS-впливу, порівнювати методи захисту та оцінювати механізми виявлення атак на основі кількісних показників.

Метою запропонованої установки є створення контрольованого середовища для дослідження ефективності засобів захисту й виявлення DoS-атак у вебсистемі на базі Apache. Установка передбачає локальне розгортання в межах ізольованої інфраструктури, наприклад на віртуальних машинах або в контейнерах, що забезпечує безпечне проведення експериментів та повторюваність результатів.

Структурно установка містить чотири основні компоненти:

– цільовий сервер, на якому розгортається Apache HTTP Server та тестовий вебзастосунок із кількома точками доступу різної складності обробки. Доцільно використовувати щонайменше три типи кінцевих точок (endpoint): для легких службових запитів перевірки доступності, для стандартного запиту середньої складності та ресурсоємного запиту, який моделює складнішу бізнес-логіку або інтенсивне використання ресурсів;

– генератор легітимного трафіку, який імітує звичайних користувачів системи. Він створює фонове навантаження з контрольованою інтенсивністю, що дозволяє оцінювати доступність сервісу, затримки відповіді та якість обслуговування в умовах одночасної присутності атаки;

– генератор атакувального трафіку, який формує DoS-вплив. На відміну від легітимного трафіку, цей потік спрямований на перевантаження вебсервера, виснаження його ресурсів або блокування можливості обслуговування нормальних клієнтів;

– підсистема моніторингу та журналювання, що забезпечує збір показників роботи сервера, стану з’єднань, завантаження ресурсів, коду відповідей, швидкості обробки запитів і параметрів спрацювання захисних механізмів. Саме ця підсистема є основою для кількісного порівняння різних конфігурацій захисту.

Для забезпечення репрезентативності результатів до експериментів було включено кілька типових сценаріїв DoS-атак прикладного рівня.

Перший сценарій – HTTP flood, за якого на сервер надходить велика кількість коротких HTTP GET-запитів. Такий тип атаки дозволяє оцінити ефективність механізмів обмеження частоти запитів і базових антифлудових налаштувань.

Другий сценарій – атака на ресурсоємний endpoint, коли значний потік запитів спрямовується саме до тих точок застосунку, які потребують більших витрат CPU, пам’яті або часу обробки. У цьому випадку доцільно досліджувати, наскільки ефективно захисні механізми запобігають деградації сервісу в умовах асиметричного навантаження.

Третій сценарій – slow HTTP або slowloris-подібна атака, що полягає в утриманні великої кількості повільних з’єднань. На відміну від класичного flood, такий вплив може мати відносно невелику інтенсивність за кількістю запитів, але при цьому виснажувати доступні робочі процеси чи сокети сервера.

У межах запропонованої установки виконано порівняння кілька конфігурацій захисту вебсервера Apache.

Базовою була конфігурація без спеціальних засобів захисту, яка використовувалась як контрольний варіант для подальшого порівняння.

В наступній конфігурації було передбачене обмеження частоти запитів та антифлудових механізмів, таких як mod_evasive.

Окремо досліджена конфігурація з посиленим керуванням таймаутами та з'єднаннями, що включала використання mod_reqtimeout, налаштування KeepAliveTimeout, Timeout та суміжних параметрів.

Третій експеримент було виконано з використанням Web Application Firewall, зокрема ModSecurity.

В результаті проведення експериментів було встановлено:

– використання механізмів обмеження частоти запитів та антифлудового механізму mod_evasive дозволило зменшити рівень HTTP flood атак;

– застосування керування таймаутами та з'єднаннями за допомогою mod_reqtimeout та засобів налаштування KeepAliveTimeout, Timeout та суміжних параметрів зменшило рівень slow HTTP-атак;

– використання Web Application Firewall, зокрема ModSecurity дозволило зменшити кількість небажаних запитів, а також виявляти аномальну активність трафіку.

Висновки

У роботі запропоновано концепцію експериментальної установки для дослідження ефективності методів захисту та виявлення DoS-атак у вебсистемі на базі Apache. Перевагою установки є її відтворюваність, ізольованість, можливість одночасного моделювання легітимного й атакувального трафіку, а також наявність системи кількісних метрик для об'єктивного порівняння різних конфігурацій захисту.

Список використаних джерел:

1. Protect Apache using Mod_security and Mod_evasive on RHEL/CentOS & Fedora. URL: https://client.connectindo.com/knowledgebase/2/Protect-Apache-using-Mod_security-and-Mod_evasive-on-RHELorCentOS-and-Fedora.html

2. Apache Module mod_reqtimeout. URL: https://httpd.apache.org/docs/current/mod/mod_reqtimeout.html

3. How to secure Apache with ModSecurity? URL: https://help.time4vps.com/en/articles/377603-how-to-secure-apache-with-modsecurity