МЕТОДИ МІНІМІЗАЦІЇ ВПЛИВУ SLOWLORIS АТАК НА ВЕБСЕРВЕР

Ванца Віталій Іванович
здобувач другого (магістерського) рівня вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Тимощук Віталій Дмитрович
здобувач першого (бакалаврського) рівня вищої освіти
факультету прикладних інформаційних технологій та електроінженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Стебельський Максим Віталійович
здобувачка першого (бакалаврського) рівня вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Науковий керівник: Тимощук Дмитро Іванович
старший викладач кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Україна

У сучасному цифровому світі, вебсервери є невід'ємною складовою мережі Інтернет. Проте існують різноманітні загрози для цих серверів, включаючи атаки типу Slowloris, які можуть вразити навіть надійні системи.

Slowloris - це тип атаки на вебсервер, який полягає в тому, що зловмисник намагається зайняти всі доступні "слоти" з'єднання з сервером, не дозволяючи іншим легітимним користувачам отримати доступ до нього. Цей вид атаки використовується для переповнення ресурсів сервера за допомогою багатьох незавершених HTTP-запитів, що призводить до блокування доступу для інших користувачів [1].

Apache, який займає одне з провідних місць серед вебсерверів у світі, відомий своєю широкою популярністю та широким використанням для хостингу вебсайтів. Чимало компаній, незалежно від розміру, обирають Apache як свій основний вебсервер завдяки його надійності, гнучкості та підтримці спільноти.

Незважаючи на всі ці позитивні якості, потокова архітектура Apache має певні вразливості, зокрема до атаки Slowloris, що може стати викликом для цієї платформи [2].

Під час атаки, коли використовується багато джерел, застосування модулів для Apache, які спрямовані на пом'якшення атаки, може не принести очікуваного результату. Наприклад, модуль mod_reqtimeout, який відкидає повільні з’єднання, не зупиняє їх створення. Це може призвести до заповнення "слотів" підключення Apache під час періодів очікування.

Модуль mod_antiloris спрямований на обмеження великої кількості повільних з'єднань від одного клієнта. Це виправляє недоліки mod_reqtimeout, проте при використанні для атаки бот-мережі, такий метод також може бути неефективним.

Архітектура вебсервера Nginx є асинхронною і використовує неблокуючу модель обробки запитів. Це дозволяє серверу обробляти запити незалежно від

завершення попередніх операцій [3]. При належному налаштуванні, Nginx не схильний до вразливостей, пов'язаних з атаками типу Slowloris.

У дослідницькій роботі було розглянуто використання технік, пов'язаних зі змінами на рівні мережі, таких як використання систем, що можуть виявляти та блокувати підозрілі IP-адреси з аномально великою кількістю незавершених запитів до вебсервера.

Метою роботи було створення та оцінка ефективності програмного захисту для відновлення працездатності вебсерверів в операційні системі Linux, які піддаються атакам типу Slowloris. Це включало розробку методики виявлення атак, написання програми на мові програмування C, інтеграцію з брандмауером для блокування IP-адрес, які ініціюють атаки, налаштування програмного забезпечення як сервісу, систему логування та сповіщення про виявлені атаки.

Проведені дослідження підтверджують можливість успішного впровадження розробленого програмного захисту для вебсерверів. Ця реалізація сприятиме підвищенню стабільності та безпеки вебсерверів, а також підвищенню рівня захисту від кіберзагроз.

Список використаних джерел:

1. Slowloris DDoS attack [Електронний ресурс]. — URL: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/ (дата звернення: 30.10.2023).
2. Developer Documentation for the Apache HTTP Server 2.4 [Електронний ресурс]. — URL: https://httpd.apache.org/docs/2.4/developer/ (дата звернення: 30.10.2023).
3. Inside NGINX: How We Designed for Performance & Scale [Електронний ресурс]. — URL: https://www.nginx.com/blog/inside-nginx-how-we-designed-for-performance-scale/ (дата звернення: 30.10.2023).