математичної статистики, та має чудові можливості для пошуку колізій у хеш-функціях, а з розвитком технологій може збільшити свою актуальність.

Список використаної літератури:

1. *Birthday problem URL: https://en.wikipedia.org/wiki/Birthday_problem*
2. *Answering the Birthday Problem in Statistics URL: https://statisticsbyjim.com/fun/birthday-problem/*
3. *What is the birthday paradox and how we can use it in cryptography?https://justcryptography.com/the-birthday-paradox/*

УДК 004.056

Саган М.Я. студент 2 курсу СО «Магістр»
спеціальності 122 «Комп'ютерні науки»
Антонов Ю.С. к. фіз.-мат. н., доцент кафедри інформаційних технологій

ПРОБЛЕМА ЗАХИСТУ NGINX СЕРВЕРІВ ВІД ВІД DDoS АТАК

Донецький національний університет імені Василя Стуса, м Вінниця

Сфера IT розвивається надзвичайно швидкими темпами, нові проекти з'являються кожного дня. Завдяки хмарним провайдерам, кожен може отримати можливість створювати та розгортати свої рішення в короткий час та за розумні гроші. Хмарні сервіси звільняють користувачів від необхідності обслуговування власної інфраструктури, необхідності оплати роботи спеціалістів, адміністраторів, та позбавляють необхідності вивчати предмет самостійно. Все сказане вище значно знижує поріг входу. Хмарні рішення надають надзвичайну гнучкість при виборі ресурсів, але іноді, через це страждають характеристики компонентів. Так диски, які надає амазон, мають дуже низький показник IOPS (операції введення/виведення за секунду).

Разом із цим доволі гостро стає проблема захисту хмарних та класичних ресурсів від зовнішніх атак, які використовують як специфічні дефекти системи для атаки так і більш прості, але не менш дієві DoS\DDoS атаки [1-3].

В представленій роботі пропонується програмне рішення, що дозволяє ефективно обробляти логи веб-сервера NGINX та реагувати на загрози. Продукт мінімально впливає на роботу сервера, в плані споживання його ресурсів та створення затримок. Спроєктовано продукт таким чином, щоб він міг ефективно працювати із повільними дисками, аби уникнути їх використання взагалі. Джерелом логів є веб сервер NGINX [4], так як він являє собою швидкий і максимально продуктивний програмний продукт, який прекрасно працює на широкому спектрі засобів, та може обробляти великі

обсяги трафіку. Даний веб сервер широко використовується у високонавантажених системах для роздачі корисного трафіку, або як проксі.

Додаток складається із трьох структурних модулів:

- ***модуль даних*** – включає в себе функціонал читання файлу з диску, та його парсингом, тобто передає підготовлені дані на вхід програми.
- ***модель*** – аналізує дані та на основі проведеного аналізу робить запит до модуля блокування на, власне, блокування адреси
- ***модуль блокування*** – отримує запити від моделі, та проводить блокування адрес

Взаємодію користувача з програмою зображено на рис. 1 а діаграму потоків даних, що відображає взаємодію програмного продукту, як з користувачем, так із зовнішнім комплексом (веб-сервером) на рис. 2.

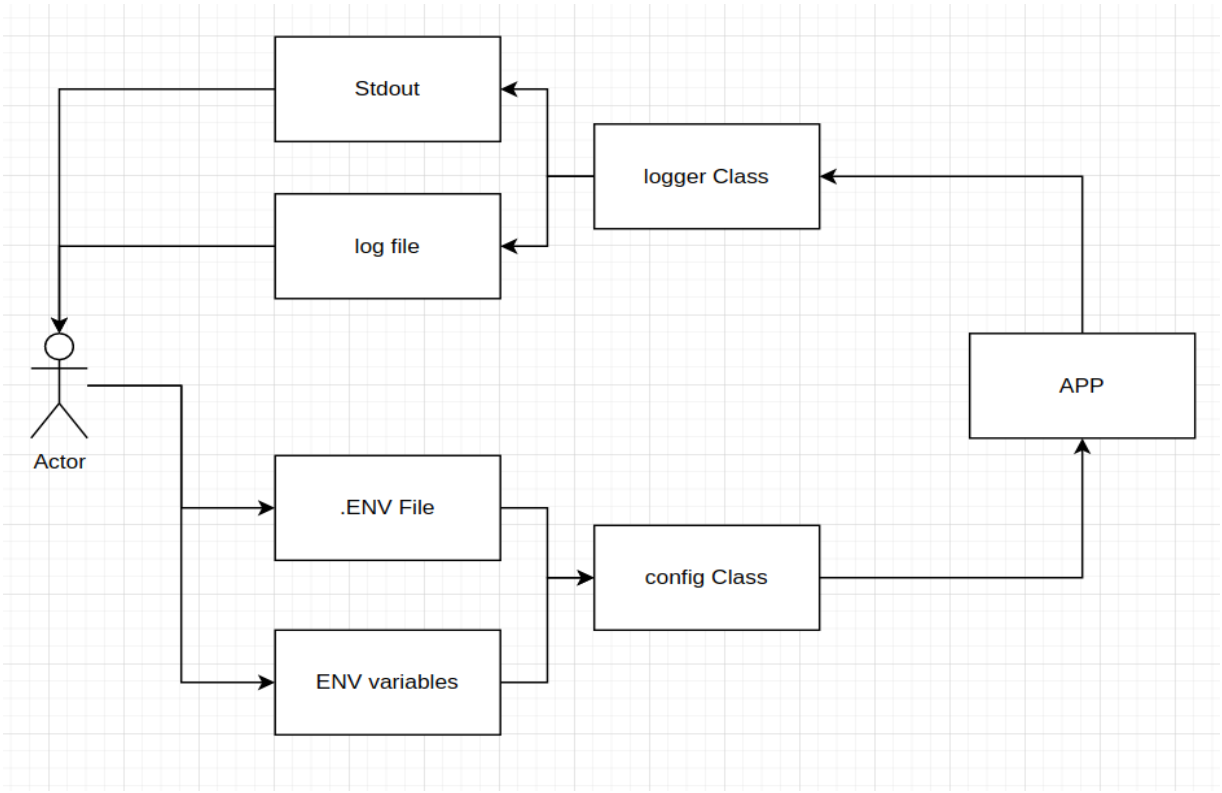

Рисунок 1. взаємодія користувача з програмою

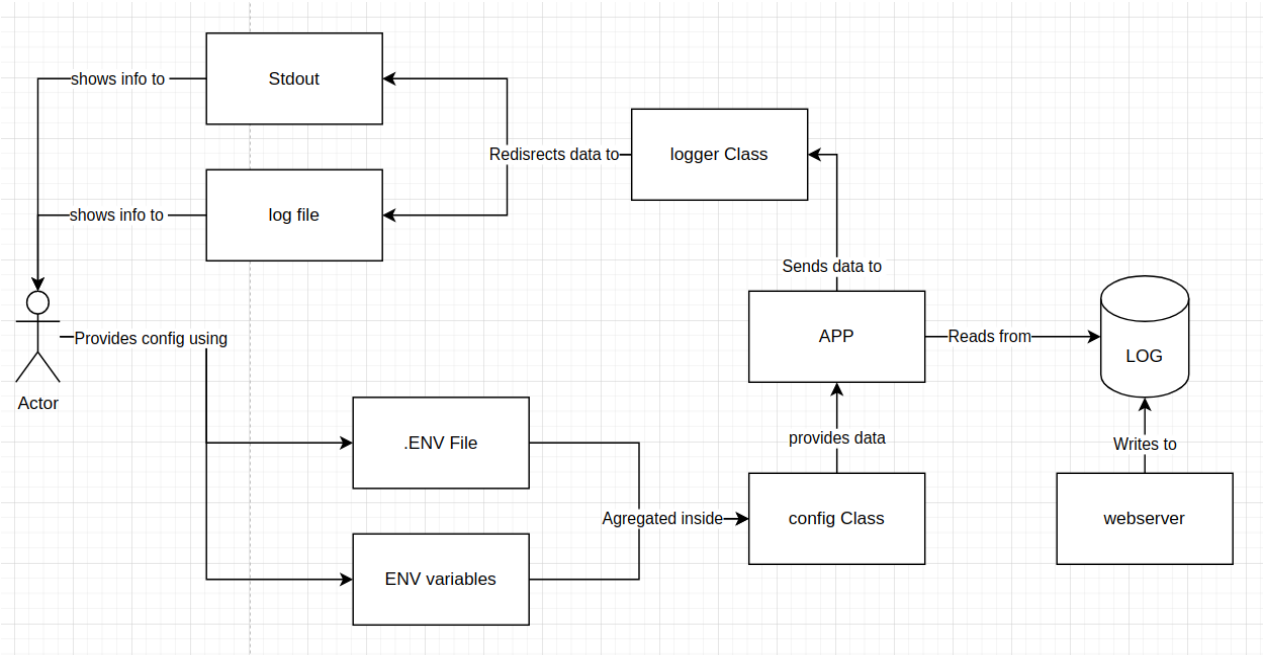

Рисунок 2. Діаграма потоків даних

Для перевірки роботи програми, було обрано примітивний сценарій з двома атакуючими машинами із адресами 172.17.0.1 та 172.17.0.1, вони являють собою віртуальні машини, встановлені на тій же фізичній машині що сервіс. Сценарій відповідає типовому в такій ситуації, тобто, ми маємо певний об'єм логів, який був накопичений до запуску даного програмного продукту, а також ми маємо ситуацію, коли користувач проводить атаку під час роботи продукту та веб-сервера. За сценарієм 172.17.0.1 почав атаку ще до того як аналізатор було запущено, а 172.17.0.2 емулює звичайні неагресивні запити. Хост 172.17.0.1 було заблоковано ще в першому проході, а 172.17.0.2 хоч і був замічений в обох проходах, не був заблокований, оскільки не проводив агресивних запитів.

Список використаних джерел

1. *Антонов Ю.С., Римар П.В., Антонова О.Г. Проблема DoS/DDoS атак навчальних ресурсів студентами. Сучасний захист інформації. 2019. N4(40). С. 52-62*
2. *А.О. Олійник, Ю.С. Антонов. Програмний аналіз журналів веб серверів Apache з метою запобігання мережевим атакам. Матеріали другої всеукраїнської наукової конференції Комп'ютерні технології обробки даних https://jktod.donnu.edu.ua/article/view/11715*
3. *Fail2ban URL: https://www.fail2ban.org/wiki/index.php/Main_Page*
4. *Nginx URL: https://www.nginx.com/resources/glossary/nginx/*