МІНІСТРЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра кібербезпеки

«До захисту допущено»

Завідувач кафедри

_____ Володимир ЛЮБЧАК

(підпис)

«___» _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека та захист інформації, освітньо-професійної програми Кібербезпека та захист інформації

на тему: «Методи та технології захисту цифрових активів веб-додатків в умовах DDoS-атаки»

Здобувача(ки) групи КБ-01 Циганенка Дениса Павловича

(шифр групи) (прізвище, ім'я, по батькові)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і тестів інших авторів мають посилання на відповідне джерело.

_____ Денис ЦИГАНЕНКО

(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник Володимир ЛЮБЧАК _____

(посада, науковий ступінь, вчене звання Ім'я та ПРІЗВИЩЕ) (підпис)

Суми 2024

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра кібербезпеки

«Затверджую»
Завідувач кафедри

_____ Володимир ЛЮБЧАК
(підпис)

«___»_____ 20___ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ
на здобуття освітнього ступеня бакалавр
зі спеціальності 125 – Кібербезпека, освітньо-професійної програми «Кібербезпека та захист інформації»
здобувача групи КБ-01 Циганенка Денис Павловича

1. Тема роботи: «Методи та технології захисту цифрових активів веб-додатків в умовах DDoS-атаки».
затверджено наказом по СумДУ №0212-VI від 04.03.2024 р. зі змінами згідно Наказу №0566-VI від 21.05.2024 р.
2. Термін подання студентом роботи: «____» _____ 20 ___ р.
3. Вихідні дані до роботи: _____
4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити): _____
_____

5. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ Керівник _____
(підпис) (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	Визначення мети, об’єкту і предмету дослідження	29.04.2024 - 02.05.2024	
2	Збір, систематизація й узагальнення матеріалу	03.05.2024 - 09.05.2024	
3	Створення тестового полігону для моделювання DDoS атаки та захисту від неї	10.05.2024 - 16.05.2024	
4	Оформлення документу кваліфікаційної роботи	19.05.2024 - 30.05.2024	

Здобувач вищої освіти _____ Керівник _____
(підпис) (підпис)

АНОТАЦІЯ

Кваліфікаційна робота виконана на 44 аркушах та містить 19 рисунків, 5 таблиць, 2 додатки та 11 джерел.

Об’єкт дослідження: Методи та технології захисту цифрових активів веб-додатків в умовах DDoS-атаки.

Мета роботи: Моделювання DDoS атаки в тестовому полігоні, аналіз існуючих рішень та впровадження ефективних захисних заходів для забезпечення стабільної роботи веб-додатків під час DDoS атаки.

Метод дослідження: аналіз літератури, класифікація та моделювання DDoS-атаки, експериментальне впровадження захисних технологій та моніторинг їх ефективності.

Результати роботи: в роботі проведено огляд та класифікацію DDoS-атак, розглянуто основні механізми їх реалізації та існуючі методи захисту. Описані архітектурні рішення та мережеві технології для мінімізації впливу DDoS-атак. В практичній частині роботи створено тестовий полігон та проведено аналіз вразливостей веб-додатку, впроваджено захисні заходи та проведено моніторинг їх ефективності. Результати дослідження можуть бути використані для покращення захисту веб-додатків від DDoS-атак.

Ключові слова: DDoS-атаки, захист веб-додатків, інформаційна безпека, мережеві технології, архітектурні рішення.

ЗМІСТ

Вступ.....5

1. Інформаційний огляд.....7

2. Методи та технології захситу від DDoS атак.....11

2.1. Визначення та класифікація DDoS атак.....11

2.2. Основні механізми та методи реалізації DDoS атак….....13

2.3. Огляд існуючих методів захиству від DDoS атак…….....16

2.4. Архітектурні рішення для мінімізації впливу DDoS атак.....19

2.5. Використання мережевих технологій для запобігання DDoS атакам.....22

2.6. Сервіси для виявлення та реагування на DDoS атаки.....25

3. Практична реалізація та захист від DDoS атак.....30

3.1. Аналіз вразливостей веб-додатку до DDoS атак.....30

3.2. Впровадження захисних заходів та моніторинг їх ефективності.....33

Висновки.....40

Список використаних джерел.....41

Додаток А. Базова конфігурація Nginx.....43

Додаток Б. Код Python скрипту для відправки запитів.....44

ВСТУП

У сучасному цифровому світі веб-додатки стали невід'ємною частиною щоденного життя підприємств і окремих користувачів. Вони надають широкий спектр послуг — від електронної комерції та банкінгу до соціальних мереж і хмарних сервісів. Однак, з розвитком веб-технологій одночасно зростають і загрози кібербезпеки, які можуть серйозно вплинути на функціонування цих додатків. Однією з найбільш небезпечних і поширених загроз є атаки типу DDoS (Distributed Denial of Service), що можуть призвести до серйозних збоїв в роботі веб-додатків, фінансових втрат та втрати репутації.

DDoS-атаки є однією з найсерйозніших загроз для цифрових активів веб-додатків. Вони характеризуються великим обсягом шкідливого трафіку, що надходить до цільової системи з різних джерел одночасно, що ускладнює їх виявлення та нейтралізацію. Такі атаки можуть призвести до повної недоступності сервісу, що завдає значних фінансових збитків та шкоди репутації компанії.

У першій половині 2022 року було зареєстровано 6 мільйонів випадків DDoS-атак, причому найбільше їх сталося в європейських країнах. Відповідно до річного звіту Cisco про Інтернет за 2020 рік, дослідники на основі зібраних статистичних даних прогнозують, що загальна кількість розподілених атак на відмову в обслуговуванні зросте з 7,9 млн у 2018 році до 15,4 млн у 2023 році. Це означає, що середньорічний темп зростання (CAGR) кількості DDoS-атак становить 14%, що є дуже високим показником. Тому питання захисту від таких атак надзвичайно актуальне.

Метою роботи є дослідження методів і технологій захисту цифрових активів веб-додатків в умовах DDoS-атак. Для досягнення мети необхідно вирішити такі завдання:

1. Визначити та класифікувати основні типи DDoS-атак, зрозуміти їх вплив на підприємства та бізнес.
2. Дослідити механізми та методи реалізації DDoS-атак, що дозволить краще розуміти принципи їх роботи та вразливості.
3. Провести огляд існуючих методів захисту від DDoS-атак, зокрема архітектурних рішень та мережевих технологій.
4. Розглянути сервіси для виявлення та реагування на DDoS-атаки, оцінити їх ефективність.
5. Проаналізувати вразливості веб-додатків до DDoS-атак та запропонувати практичні заходи захисту, включаючи моніторинг їх ефективності.

Наукова новизна дослідження полягає у систематичному підході до вивчення захисту цифрових активів веб-додатків від DDoS-атак. В роботі представлено детальний аналіз методів захисту, включаючи новітні технології та підходи, що дозволяють ефективно протистояти DDoS-атакам. Особлива увага приділяється практичним аспектам впровадження захисних заходів та оцінки їх ефективності.

Методи дослідження включають аналіз наукових джерел, огляд сучасних технологій захисту, а також практичні експерименти з метою оцінки ефективності різних методів захисту від DDoS-атак. Для цього використовуються як теоретичні, так і емпіричні підходи, що дозволяє отримати комплексне розуміння проблеми та знайти оптимальні рішення.

1. ІНФОРМАЦІЙНИЙ ОГЛЯД

У сучасному світі безліч сфер людської діяльності залежать від якості та надійності програмного забезпечення, створених для їх потреб. Ці програми автоматизують значну частину щоденних завдань. Отже, в цій галузі надзвичайно важливо забезпечувати високу якість програмного забезпечення та гарантувати стабільну доступність сервісів.

В наш час кіберзагрози дуже різноманітні, існує багато їх видів і класифікацій, кожна з яких потребує спеціальних методів боротьби. Проте, всім цифровим загрозам спільне те, що вони здебільшого поширюються через Інтернет. Оскільки більшість сучасного програмного забезпечення взаємодіє з користувачами або іншими програмами через глобальну мережу, кібератаки залишаються актуальною проблемою. Серед найпоширеніших видів загроз виділяються віруси, DoS-атаки, експлойти, фішинг та інші. Однією з найрозповсюдженіших загроз є DDoS-атака, що є специфічним видом атак на доступність сервісів.

Пошириність DDoS атак та загроза від них активно збільшується щороку зі збільшенням користувачів мережі Інтернет. Це дуже гарно відслідковується, якщо поглянути на графік відношення нових інтернет-користувачів до DDoS атак. Графік зображено на рисунку 1.1.

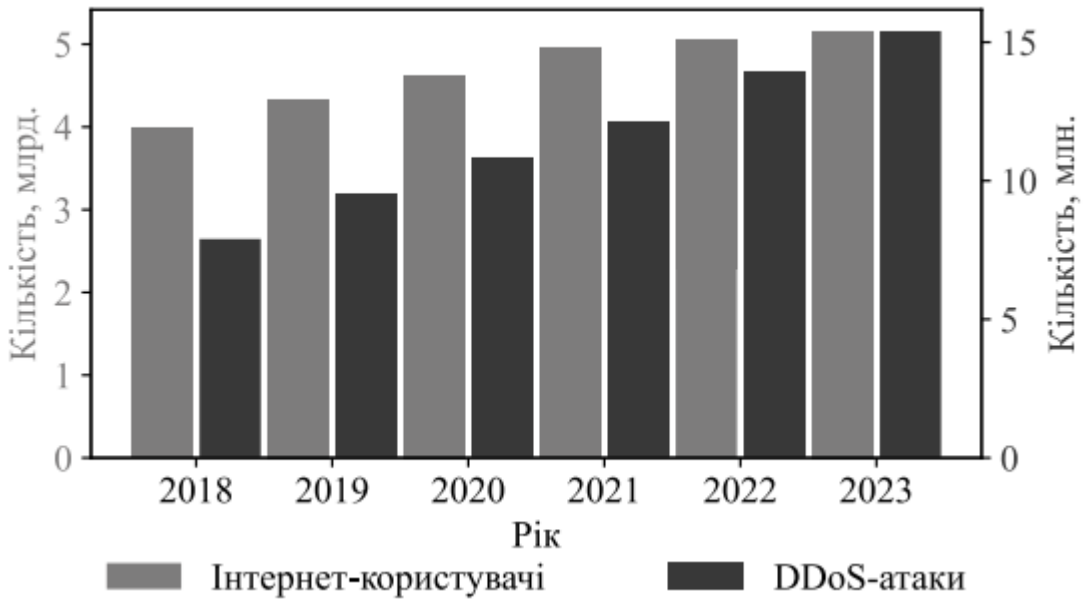


Рисунок 1.1 – Відношення росту користувачів інтенерту до DDoS атак

DDoS атаки є серйозною загрозою для бізнесу і організацій, оскільки можуть призвести до значних фінансових втрат, репутаційних збитків та порушення нормального функціонування послуг. Наприклад, атака на інтернет-магазин може зробити його недоступним для покупців, що призведе до втрати продажів. Але якщо розглянути вплив на бізнес більш детально то можна виділити наступні пункти:

- втрати компанії через простої атакованої системи, при цьому розмір втрачених прибутків значно перевищує витрати на організацію атаки;
- зниження продуктивності користувачів програмного забезпечення, оскільки під час перевантаження сервера шкідливим трафіком швидкість обробки запитів різко падає;

- витрати на відновлення нормальної роботи системи після атаки, оскільки, ймовірно, буде потрібно додатково перевірити інфраструктуру, перезапустити її компоненти, а також залучити фахівців з кібербезпеки та додаткових консультантів у службу підтримки;
- погіршення репутації бренду через невідповідність заявленим показникам доступності сервісу;
- зменшення клієнтів, які втратили довіру до компанії через неможливість задовольнити свої потреби, і, ймовірно, перейдуть до конкурентів, що пропонують аналогічні послуги.

Збільшення кількості підключених до мережі пристроїв, доступність потужних інструментів для проведення атак, а також зростання складності та цілеспрямованості DDoS атак створюють серйозні виклики для забезпечення кібербезпеки. Організації повинні впроваджувати сучасні методи захисту, постійно моніторити свою мережу та бути готовими до оперативного реагування на такі загрози, щоб мінімізувати їх вплив та забезпечити безперервність своїх бізнес-процесів. Нащастя деякі процеси можна автоматизувати та передати управління захистом на спеціальзовані сервіси.

Таким чином, питання виявлення DDoS-атак та захист від них є надзвичайно актуальним і вимагає розробки нових або вдосконалених методів ідентифікації. Це дозволить ефективніше захищатися від таких атак. Зважаючи на швидке зростання кількості атак на відмову в обслуговуванні, існуючі методи мають свої недоліки, особливо у класифікації кібератак на прикладному (програмному) рівні. Для вирішення цієї проблеми я застосовував програмні рішення для виявлення та блокування таких атак у автоматичному режимі, що дозволить бути не таким залежним від постійної аналітики та моніторингу мережевого трафіку.

Для демонстрації впливу DDoS атаки на систему я створив тествий веб-додаток з вбудованою вразливістю за допомогою мови програмування Python та фреймворку Django. Його розгорнув та запустив на VPS Digital Ocean з конфігурацією веб-сервера Nginx.

Також мною створено базовий скрипт на мові Python для відправлення HTTP GET запитів. За допомогою цього скрипту здійснено DDoS атаку з трьох різних віртуальних машин в тестовому середовищі.

2. МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ВІД DDOS АТАК

2.1 Визначення та класифікація DDoS атак

DDoS (Distributed Denial of Service) - це тип кібератаки, під час якої численні комп'ютери, інфіковані шкідливим програмним забезпеченням, одночасно надсилають запити на цільовий сервер або мережевий ресурс з метою перевантаження його можливостей і виведення з ладу. Такі атаки призводять до недоступності послуг для користувачів [1].

Цей тип атаки можна класифікувати за кількома ознаками, зокрема за типом вектору атаки, рівнем мережевої моделі (OSI) і методами виконання [2].

За типом вектору атаки:

1. Атаки на мережевому рівні (Network Layer Attacks):

- **UDP Flood**: Атака, яка засипає жертву великою кількістю UDP пакетів, що призводить до перевантаження її обробки.
- **ICMP Flood (Ping Flood):** Відправлення великої кількості ICMP запитів (наприклад, ping запити), що призводить до перевантаження мережевого каналу або сервера.

2. Атаки на транспортному рівні (Transport Layer Attacks):

- **SYN Flood:** Відправлення великої кількості SYN запитів з метою вичерпання ресурсів, необхідних для обробки нових з'єднань.
- **ACK Flood:** Відправлення великої кількості TCP ACK пакетів, що викликає перевантаження обробки ACK запитів.

3. Атаки на рівні додатків (Application Layer Attacks):

- **HTTP Flood:** Відправлення великої кількості HTTP запитів до веб-сервера, що перевантажує його обробку запитів і робить його недоступним для легітимних користувачів.
- **Slowloris:** Відправлення неповних HTTP запитів, змушуючи сервер тримати ці з'єднання відкритими і вичерпуючи доступні ресурси.

За рівнем моделі OSI:

1. **Мережевий рівень (Layer 3):** Атаки, спрямовані на перевантаження мережевого рівня, такі як ICMP Flood і UDP Flood.
2. **Транспортний рівень (Layer 4):** Атаки на транспортний рівень, наприклад, SYN Flood та ACK Flood.
3. **Сеансовий рівень (Layer 5):** Атаки, що експлуатують механізми управління сеансами, як наприклад, Slowloris.
4. **Рівень представлення (Layer 6) та рівень додатків (Layer 7):** Атаки на рівні додатків, такі як HTTP Flood, які спрямовані на специфічні сервіси або додатки.

За методами виконання:

1. **Атаки з використанням ботнетів:** Найпоширеніший метод, при якому велика кількість зламаних пристроїв (ботів) одночасно надсилають запити до цілі.
2. **Атаки за допомогою відбиття (Reflection Attacks):** Використання сторонніх серверів для відправки великої кількості відповідей на запити до жертви. Наприклад, DNS Amplification атаки.
3. **Атаки з посиленням (Amplification Attacks):** Використання сервісів, які відповідають на невеликий запит великою кількістю даних, спрямованих до жертви.

2.2 Основні механізми та методи реалізації DDoS атак

Існує чимало способів організації DDoS атак, але загалом їх можна розділити на дві основні групи: атаки на мережеву та програмну інфраструктури.

При атаці на мережеву частину хакер намагається перенаситити канал зв'язку сервера. Канал зв'язку визначається обсягом даних, який сервер може прийняти та обробити. Якщо трафік перевищує цей ліміт, сервер не встигає справлятися з потоком даних, і для користувачів веб-додаток стає недоступним [3]. Наприклад, якщо канал сервера може пропустити 1 Гб трафіку чи обслуговувати 10 000 користувачів одночасно, метою зловмисника є перевищити цей обсяг і утримувати таку ситуацію якомога довше, щоб реальні користувачі не могли зайти на сайт.

У випадку атаки на програмну частину зловмисник намагається вичерпати один із ресурсів сервера, таких як процесорні потужності, оперативну пам'ять, кількість допустимих процесів або підключень до бази даних. Коли один з цих ресурсів виснажується, сервер починає працювати повільніше або взагалі зависає. Сервер витрачає ці ресурси щоразу, коли користувач виконує будь-яку дію на сайті [4]. Наприклад, при введенні даних для входу в акаунт сервер перевіряє цю інформацію і повертає наступну сторінку або повідомлення про помилку. На різні запити потрібна різна кількість ресурсів. Метою зловмисника є знайти запит, який споживає найбільше ресурсів, і надіслати серверу максимальну кількість таких запитів, доки той не перестане працювати. Оскільки для цього потрібна велика кількість запитів, зловмисники створюють потужні ботнети для реалізації DDoS атак.

Ботнет (botnet) – мережа з ботів. Ботами називають пристрої, що виконують команди зловмисника в атаках на жертву [5]. Ботом може бути будь-який пристрій, що має доступ до інтернету, але зазвичай більшість ботів – це пристрої

IoT (Internet of Things). Це дуже великий спектр різноманітних “розумних” речей як електричні замки з віддаленим управлінням, камери відеоспостереження, кавові машини, принтери, тощо. Відношення збільшення саме IoT пристроїв до DDoS атак та інших пристроїв у мережі Інтернет показує актуальність використання цих пристроїв для таких атак. На рисунку 2.1 зображено графік відношення IoT пристроїв до інших девайсів що використовують всесвітню мережу Інтернет та DDoS атак.

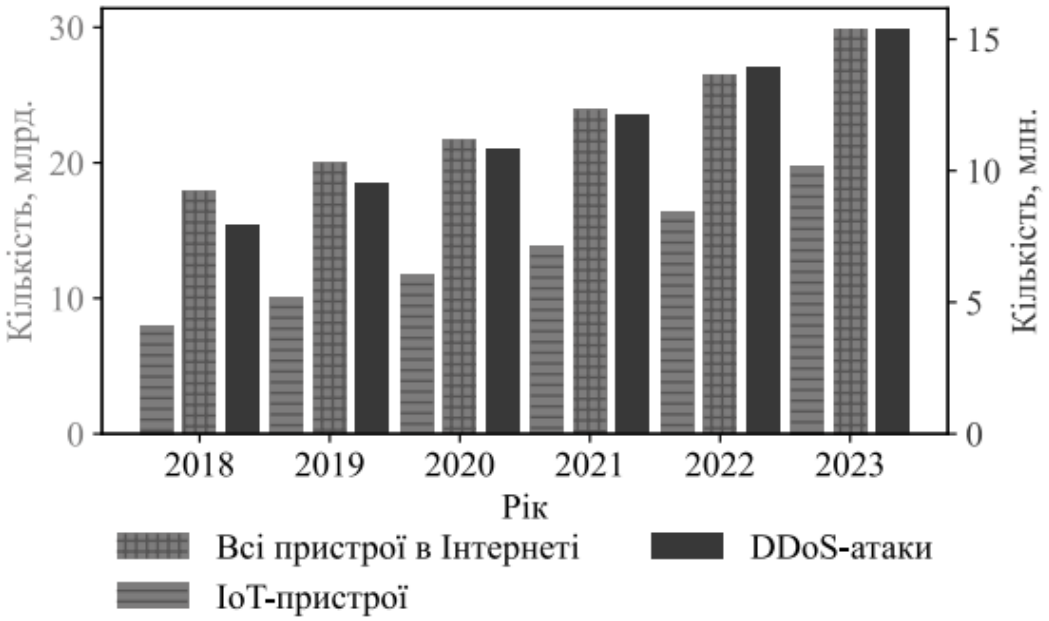


Рисунок 2.1 – Відношення IoT пристроїв у порівнянні з іншими девайсами до збільшення DDoS атак з плином часу

IoT досить слабкі за потужністю пристрої, але чому саме вони складають найбільшу частину пристроїв в мережі з ботів? Відповідь на це питання досить проста і знаходиться на поверхні. Власники таких пристроїв зазвичай не замислюються над безпекою, адже пристрій знаходиться вдома і виконує свою

роботу, а керувати наприклад світлом дистанційно досить зручно. Начебто нічого не наштовхує на небезпеку, але пристрій працює через мережу інтернет і має IP адресу, отже кожен хто її знає може спробувати під'єднатись до нього. Для підключення потрібен логін і пароль від панелі керування, але власники дуже рідко його змінюють з міркувань безпеки. Структура ботнет мережі для DDoS атаки з IoT девайсів наведено на рис.2.2.

Таким чином зловмисники методом перебору знаходять активні пристрої та за допомогою брутфорсу та спеціальних програм з легкістю підбирають стандартні логін та пароль за лічені секунди.

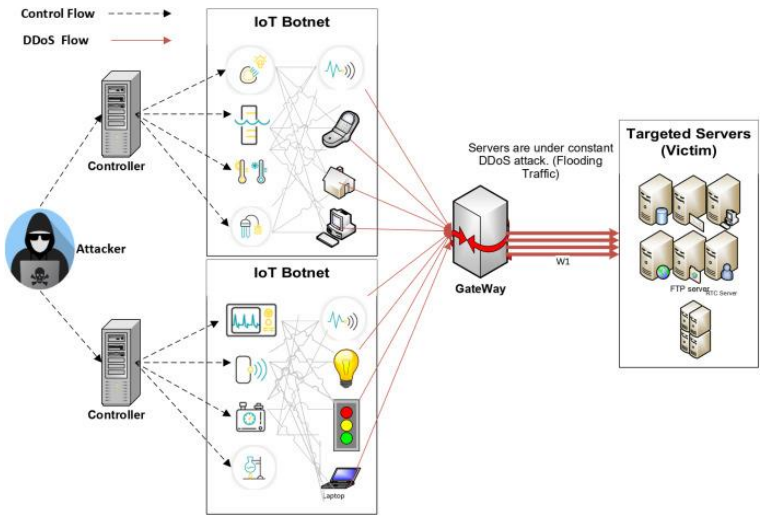


Рисунок 2.2 – Структура ботнет мережі для DDoS атаки з IoT девайсів

Для керування такими мережами зазвичай використовують сервери-контроллери. Вони створюють додатковий шар пристроїв між зловмисником та ботами. Головна їх мета – зручність групування ботів та керування ними. Таким чином правильно налаштовані контроллери мають у своєму розпорядженні тисячі ботів, яким вони можуть надіслати команду атаки чи зупинки. В свою

чергу зловмисник віддає команди лише контроллерам, що допомогає керувати потужностями атаки [6].

2.3 Огляд існуючих методів захисту від DDoS атак

Існує декілька принципів захисту від DDoS атак. Одні спрямовані на обмеження запитів, інші на блокування підозрілих запитів, тощо. Але цей вид атак досить складний для захисту, тому потребує комплексного рішення. Для захисту можуть бути вжиті наступні методи [7]:

1. Превентивні заходи:

1.1 Архітектурні рішення

Одним з перших кроків у захисті від DDoS атак є правильне проектування інфраструктури. Це включає в себе:

- **Розподілені мережі**: Використання розподіленої мережевої архітектури, де ресурси розташовані в різних географічних точках, допомагає знизити ризик однієї точки відмови. Це забезпечує можливість перенаправлення трафіку на менш завантажені сервери у разі атаки.
- **Балансувальники навантаження**: Вони дозволяють розподіляти вхідний трафік між кількома серверами, що запобігає перевантаженню одного сервера і допомагає зберігати працездатність сервісу під час атаки.

1.2 Аутентифікація та авторизація

Використання методів аутентифікації та авторизації може значно знизити ризик успішної DDoS атаки:

- **CAPTCHA**: Впровадження CAPTCHA на веб-формах допомагає відсіяти автоматизовані запити, роблячи атаку дорожчою та менш ефективною для зловмисників.

2. Активні методи захисту

2.1 Мережеві фільтри та брандмауери

Активні методи захисту включають фільтрацію трафіку на різних рівнях мережевої моделі:

- **Брандмауери**: Використання брандмауерів допомагає блокувати небажаний трафік на основі заданих правил. Це можуть бути як апаратні, так і програмні рішення.
- **Інтелектуальні системи виявлення загроз (IDS/IPS)**: Вони дозволяють виявляти та блокувати підозрілий трафік у реальному часі. Інтеграція таких систем з іншими компонентами мережевої інфраструктури підвищує ефективність захисту.

3. Міграція та пом'якшення атак

3.1 Використання CDN

Мережі доставки контенту (CDN) грають важливу роль у захисті від DDoS атак:

- **Розподіл трафіку**: CDN дозволяють розподіляти трафік між численними вузлами, що знижує навантаження на окремі сервери.
- **Кешування контенту**: Кешування статичного контенту допомагає зменшити кількість запитів до основного сервера, знижуючи ризик перевантаження.

3.2 Хмарні рішення

Використання хмарних сервісів для захисту від DDoS атак стає все більш популярним:

- **Хмарні брандмауери**: Вони забезпечують додатковий рівень захисту, дозволяючи відфільтровувати шкідливий трафік до того, як він досягне основної інфраструктури.

4. Резервні заходи та планування

4.1 Планування відновлення

Розробка планів відновлення після атак є важливим аспектом захисту:

- **Резервне копіювання**: Регулярне створення резервних копій даних дозволяє швидко відновити роботу після атаки.
- **Плани дій у надзвичайних ситуаціях**: Розробка та тестування планів дій у разі атаки допомагає мінімізувати простої та втрати.

4.2 Тренування та обізнаність

Підвищення обізнаності працівників щодо DDoS атак та їх наслідків сприяє ефективнішій протидії:

- **Навчання персоналу**: Регулярні тренування та навчальні програми для працівників допомагають їм розуміти, як реагувати на атаки та мінімізувати їх вплив.
- **Симуляції атак**: Проведення симуляцій атак дозволяє перевірити готовність організації до реальних загроз та вдосконалити існуючі плани захисту.

5. Використання сторонніх сервісів

5.1 Захист від DDoS як послуга

Існують спеціалізовані компанії, які надають послуги захисту від DDoS атак:

- **Спеціалізовані рішення**: Використання сервісів від компаній, що спеціалізуються на захисті від DDoS, може значно підвищити рівень безпеки.
- **Мережеві операційні центри (NOC)**: Деякі компанії пропонують цілодобовий моніторинг та реагування на атаки через свої NOC, що дозволяє швидко виявляти та зупиняти атаки.

5.2 Використання службової безпеки

Інтеграція з іншими службами безпеки може забезпечити додаткові рівні захисту:

- **Засоби моніторингу безпеки**: Використання сучасних засобів моніторингу дозволяє виявляти підозрілу активність та приймати відповідні заходи.
- **Інтеграція з SIEM**: Системи управління інформацією та подіями безпеки (SIEM) допомагають аналізувати великі обсяги даних та виявляти аномалії, що можуть свідчити про DDoS атаки.

Важливо розробити ефективні стратегії захисту, інтегрувати сучасні технології та постійно вдосконалювати підходи до безпеки, щоб забезпечити надійний захист від цього типу загроз.

2.4 Архітектурні рішення для мінімізації впливу DDoS атак

Головна мета використання архітектурних рішень для запобігання DDoS атакам та захисту від них полягає у забезпеченні доступності та безперебійної роботи веб-додатків навіть під час атак. Ця мета досягається шляхом таких основних завдань:

- Розподіл навантаження,
- Стабільність та відмовостійкість,
- Зниження вразливості,
- Швидке виявлення та реагування,
- Мінімізація втрат [8].

В цілому, метою є створення такої архітектури системи, яка забезпечить високий рівень доступності, надійності та безпеки цифрових активів веб-додатків, незважаючи на можливі спроби злочинців порушити їх роботу. Отже на основі списку завдань маємо наступні архітектурні рішення:

1. Використання хмарних послуг та CDN:

- Хмарні постачальники, такі як AWS, Google Cloud, Azure, пропонують інструменти для захисту від DDoS атак, які використовують великі можливості розподілу трафіку і масштабування. Наприклад, AWS Shield і Google Cloud Armor пропонують розширені функції захисту від DDoS.
- CDN, такі як Cloudflare, Akamai, і Fastly, можуть поглинути великий обсяг шкідливого трафіку і розподілити його по глобальній мережі серверів, зменшуючи навантаження на оригінальний сервер. Вони також забезпечують кешування контенту, що зменшує кількість запитів до основного серверу.

Схема роботи CDN зображена на рис. 2.3.

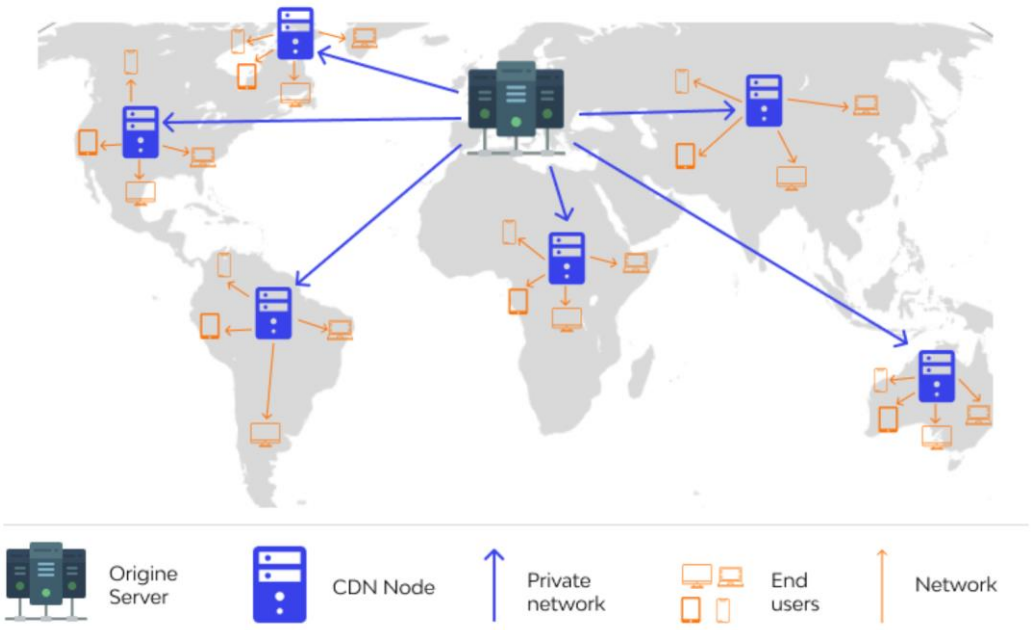


Рисунок 2.3 – Схема роботи CDN

2. Відмовостійка архітектура:

- Розподіл навантаження: Використання балансувальників навантаження (load balancers), таких як в Nginx, допомагає розподілити трафік між кількома серверами, зменшуючи навантаження на окремий сервер і підвищуючи відмовостійкість системи.
- Мікросервісна архітектура: Мікросервіси дозволяють розділити додаток на дрібні компоненти, кожен з яких може масштабуватися незалежно. Це підвищує стійкість додатку до атак, оскільки атака на один мікросервіс не обов'язково призведе до збою всього додатку.

Відмінності монолітної та мікросервісної архітектури наведено на рис.2.4.

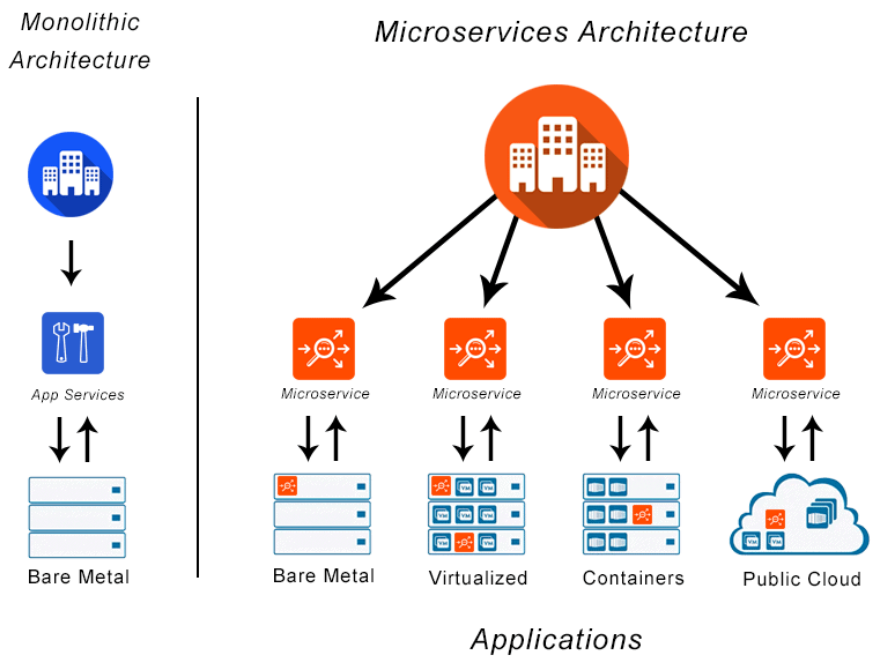


Рисунок 2.4 – Відмінності монолітної та мікросервісної архітектури

3. Захист на рівні додатку:

- WAF (Web Application Firewall): WAF, такі як ModSecurity, Imperva або AWS WAF, захищає веб-додатки від атак, аналізуючи HTTP-запити і блокуючи підозрілі. Вони здатні фільтрувати трафік, захищаючи від SQL-ін'єкцій, XSS та інших загроз (рис.2.5).
- Rate Limiting: Встановлення обмежень на кількість запитів від одного клієнта допомагає запобігти перевантаженню сервера. Це можна реалізувати на рівні веб-сервера або додатку.

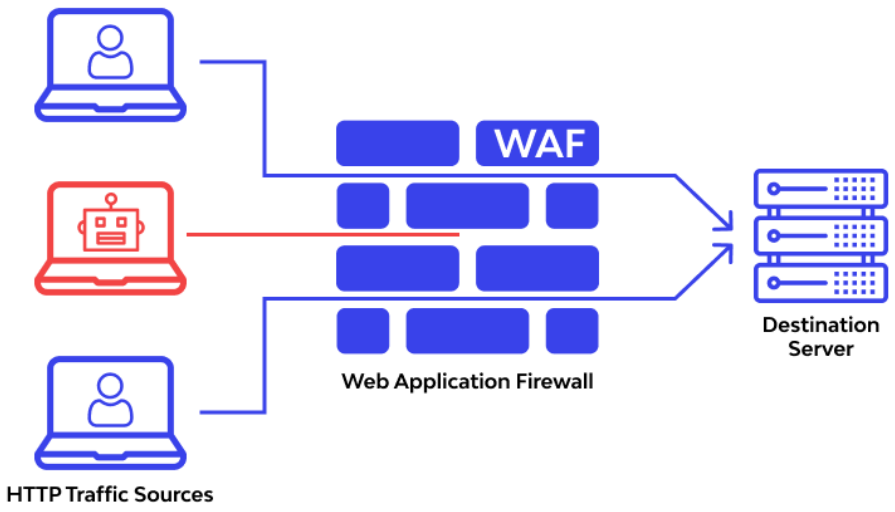


Рисунок 2.5 – Схема роботи WAF

2.5 Використання мережевих технологій для запобігання DDoS атакам

Мережеві технології в умовах DDoS атаки відіграють не менш важливу роль, так як канал зв’язку одна з цілей зловмисників при таких атаках. Значно покращити та збалансувати канал зв’язку можна наступними методами:

1. Anycast:

Anycast — це мережевий метод, який дозволяє одноій IP-адресі відповідати кільком вузлам у різних фізичних локаціях. Запити користувачів автоматично спрямовуються до найближчого або найменш завантаженого вузла, що розподіляє трафік і зменшує ймовірність перевантаження.

Переваги:

- Розподіл трафіку по кількох географічно розподілених точках.
- Зменшення затримок для кінцевих користувачів.
- Підвищення стійкості до атак на конкретні регіони або вузли.

2. Інтелектуальні балансувальники навантаження:

Інтелектуальні балансувальники навантаження, такі як F5 Networks, HAProxy, і Nginx, можуть аналізувати трафік у режимі реального часу і перенаправляти його до найменш завантажених або найбільш підходящих серверів.

Переваги:

- Розподіл навантаження між кількома серверами.
- Виявлення аномалій в трафіку і блокування шкідливих запитів.
- Зменшення ризику перевантаження одного серверу.

3. Мережеві шлюзи та фільтрація трафіку:

Мережеві шлюзи і фільтруючі пристрої, такі як Cisco ASA, Palo Alto Networks, і Fortinet, можуть фільтрувати трафік на основі попередньо визначених правил і блокувати підозрілий трафік до того, як він досягне внутрішньої мережі.

Переваги:

- Глибока інспекція пакетів (DPI) для виявлення і блокування шкідливих запитів.
- Захист на мережевому рівні, що дозволяє відсівати трафік до його обробки додатком.

- Можливість налаштування правил для специфічних типів атак.

4. Захист на рівні DNS:

Захист на рівні DNS, включаючи використання DNSSEC (DNS Security Extensions) і DNS-фаєрволів, допомагає захистити систему від атак, які націлені на DNS-сервери, таких як DNS Amplification атаки.

Переваги:

- Запобігання підробці DNS-записів і захист від DNS спуфінгу.
- Розподіл DNS-запитів для зменшення навантаження на окремі сервери.
- Додатковий рівень захисту для мережевої інфраструктури.

5. Мережеві анти-DDoS платформи:

Анти-DDoS платформи, такі як Arbor Networks, Radware, і A10 Networks, спеціалізуються на виявленні та блокуванні DDoS атак у реальному часі. Вони використовують різні методи для аналізу трафіку і визначення шкідливих запитів.

Переваги:

- Висока точність виявлення DDoS атак.
- Можливість автоматичного блокування атак.
- Підтримка великих обсягів трафіку і масштабованість.

Інтеграція Anycast, інтелектуальних балансувальників навантаження, мережевих шлюзів, захисту на рівні DNS та спеціалізованих анти-DDoS платформ дозволяє ефективно розподілити трафік, виявити і заблокувати шкідливі запити, а також забезпечити стабільну роботу додатків навіть під час атак. Ці технології є ключовими інструментами для створення стійкої до DDoS атак архітектури веб-додатків.

2.6 Сервіси для виявлення та реагування на DDoS атаки

Більшість налаштувань, як мережевої так і програмної частини, потребують специфічних знань на досить глибокому рівні, отже, підприємству може знадобитись фахівець який зможе налаштувати правильну інфраструктуру для їх веб-додатку та серверів. На сьогоднішній день це не обов'язково, так як декілька провідних сервісів дають можливість забезпечити безпеку від DDoS атак для будь-якого веб-додатку чи іншого веб-сервісу буквально в два натискання на клавіші. Далі наведено провідні сервіси які пропонують готові рішення для захисту веб-додатків [9].

1. Cloudflare

Основний функціонал:

- Захист від DDoS атак на рівні мережі, транспортного і прикладного рівнів.
- Використання глобальної мережі Anycast для розподілу трафіку.
- WAF для захисту від різних веб-загроз.
- Аналітика і моніторинг трафіку в реальному часі.

Переваги та недоліки Cloudflare представлено у таблиці 2.1.

Таблиця 2.1 – Переваги та недоліки Cloudflare

Переваги	**Недоліки**
• Легке налаштування і інтеграція з існуючими веб-додатками. • Потужна інфраструктура з великою кількістю точок присутності (PoPs) по всьому світу. • Висока ефективність в захисті від широкого спектру атак.	• Можливі проблеми з латентністю через маршрутизацію трафіку через мережу Cloudflare. • Обмежена можливість налаштування правил для окремих випадків. • Деякі функції доступні тільки у преміум-версіях.

2. AWS Shield

Основний функціонал:

- Захист від DDoS атак для додатків, розміщених в AWS.
- Інтеграція з іншими сервісами AWS, такими як Amazon CloudFront і AWS WAF.
- Автоматичне виявлення та реагування на DDoS атаки.
- Детальні звіти і аналітика по атакам.

Переваги та недоліки AWS Shield наведено у таблиці 2.2.

Таблиця 2.2 – Переваги та недоліки AWS Shield

Переваги	**Недоліки**
• Глибока інтеграція з екосистемою AWS, що спрощує налаштування для користувачів AWS. • Автоматичне масштабування для обробки великих обсягів трафіку. • Ефективний захист без додаткових налаштувань для базового рівня захисту (AWS Shield Standard).	• Додаткові витрати на використання преміум-версії (AWS Shield Advanced). • Обмеження в захисті для ресурсів, які не розміщені в AWS. • Можливість залежності від однієї хмарної платформи.

3. Akamai Kona Site Defender

Основний функціонал:

- Захист від DDoS атак і WAF.
- Глобальна мережа CDN для розподілу трафіку і зниження навантаження на оригінальний сервер.
- Аналітика в реальному часі і деталізовані звіти по атаках.

- Підтримка налаштувань політик безпеки для конкретних додатків.

Переваги та недоліки Akamai Kona Site Defender наведено у таблиці 2.3.

Таблиця 2.3 – Переваги та недоліки Akamai Kona Site Defender

Переваги	**Недоліки**
• Висока продуктивність завдяки глобальній мережі PoPs.	• Висока вартість, що може бути проблемою для малих і середніх бізнесів.
• Можливість налаштування захисту для різних типів додатків і бізнес-вимог. • Надійний захист від складних і багатоступеневих атак.	• Складність налаштування і управління без належного досвіду. • Потреба в інтеграції з іншими сервісами для повного захисту

4. Imperva Incapsula

Основний функціонал:

- Захист від DDoS атак на мережевому і прикладному рівнях.
- WAF для захисту від веб-атак, таких як SQL-ін'єкції і XSS.
- Розподілена мережа для поглинання трафіку і зниження навантаження.
- Моніторинг і звітність в реальному часі.

Переваги та недоліки Imperva Incapsula наведено в таблиці 2.4.

Таблиця 2.4 – Переваги та недоліки Imperva Incapsula

Переваги	**Недоліки**
• Простота у використанні і налаштуванні. • Висока ефективність в захисті від різних типів атак.	• Додаткові витрати на використання преміум-функцій. • Обмежені можливості налаштування для складних випадків.

• Гарна підтримка клієнтів і технічна допомога.	• Потенційні затримки через маршрутизацію трафіку через мережу Imperva.

5. Arbor Networks

Основний функціонал:

- Захист від DDoS атак на рівні мережі та додатків.
- Глибока інспекція пакетів (DPI) для виявлення аномалій в трафіку.
- Інтеграція з існуючими мережевими пристроями для розширення захисту.
- Моніторинг і аналітика в реальному часі.

Переваги та недоліки Arbor Networks наведено в таблиці 2.5.

Таблиця 2.5 – Переваги та недоліки Arbor Networks

Переваги	**Недоліки**
• Потужні можливості для виявлення і блокування складних DDoS атак. • Висока масштабованість і ефективність. • Добре підходить для великих підприємств і провайдерів послуг.	• Висока вартість, що може бути недоступною для малих бізнесів. • Складність налаштування і потреба в спеціалізованих знаннях. • Можливість затримок через глибоку інспекцію трафіку.

Рекомендація конкретного сервісу для виявлення та реагування на DDoS атаки залежить від кількох факторів, включаючи специфіку бізнесу, обсяг трафіку, технічні можливості команди та бюджет. Однак, зважаючи на загальну ефективність, простоту інтеграції та широкі можливості, я б порекомендував

Cloudflare. Мені довелось з ним працювати під час проходження переддипломної практики в АТ «Сумиобленерго» і вони активно використовують цей сервіс для захисту від DDoS атак. Панель керування WAF Cloudflare зображено на рис.2.6.

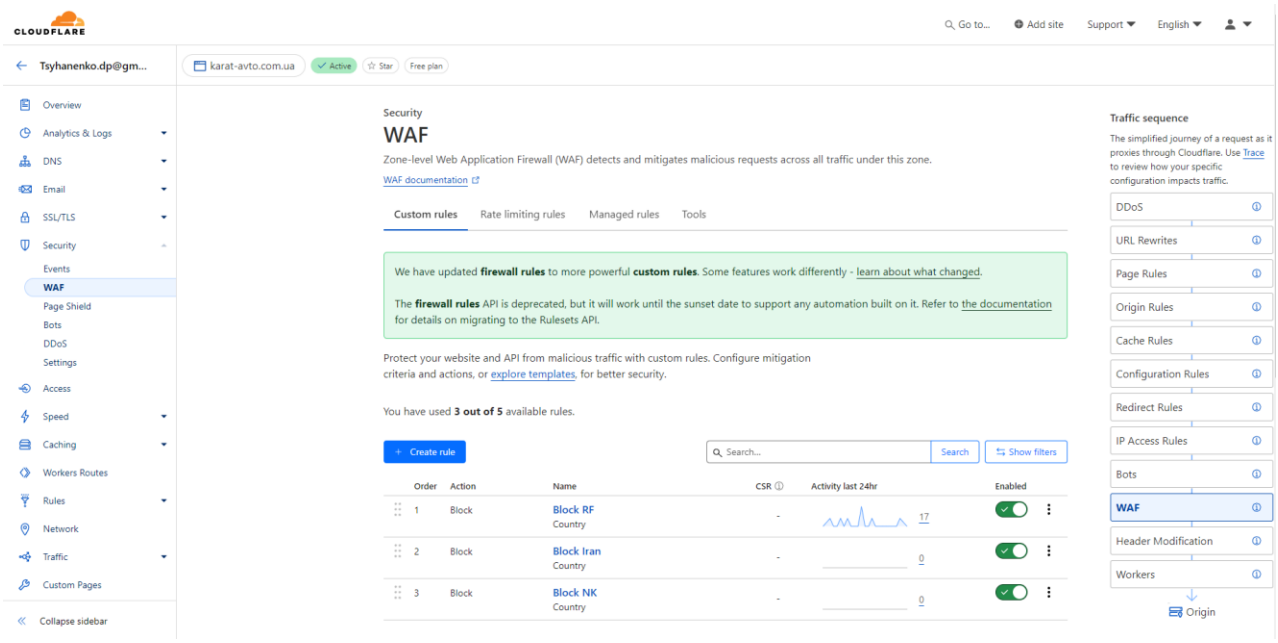


Рисунок 2.6 – Панель керування WAF Cloudflare

3. ПРАКТИЧНА РЕАЛІЗАЦІЯ DDOS АТАКИ ТА ЗАХИСТ

3.1 Аналіз вразливостей веб-додатку до DDoS атак

Для демонстрації моделювання налсідків DDoS атаки я створив тестове середовище для цієї задачі. Тествий веб-додаток створено за допомогою мови програмування Python та фреймворку Django[10]. Також до додатку підключив СУБД PostgresQL. Додаток розроблений в найпростішому вигляді для зрзумілої демонстрації вразливості та неоптимізованості системи до високих навантажень. З кодом додатку можна ознайомитись в моєму GitHub репозиторії [11].

Систему я розгорнув на VPS (Virtual Private Server) від Digital Ocean. Отже маю наступну систему:

1) Вебсервер Nginx приймає запити від користувачів. Конфігурацію Nginx наведено в Додатку А;

2) PostgresQL зберігає дані про користувачів та інші інформаційні активи додатку;

3) Django веб-додаток оброблює запити та надсилає відповідь по протоколу HTTPS кристувачу.

При відкритті сторінки автомобіля на якій є вразливість завантажується більше 9 секунд і дуже навантажує систему веб-сервера (рис.3.1). В панелі керування Digital Ocean відображається ця активність. Сервер досить слабкий, але це чітко показує наскільки одна людина може навантажити систему своїм запитом.

Один користувач зміг навантажити CPU аж на 2%. Отже, сервер може витримати не більше 50 таких запитів одночасно. Це досить вразливе місце веб-додатку.

Відбувається таке навантаження через те, що дані про автомобіль не кешуються і при кожному запиті система перебирає дані в СУБД і створює безліч однотипних запитів. В самому запиті повертається багато інформації про автомобіль такі як зображення, головна інформація, опис, характеристики, та декілька таблиць даних про комплектації та ціни.

Щоб отримати ці дані сервер задіє велику кількість ресурсів для фрмування правильної відповіді, що і призводить до навантаження.

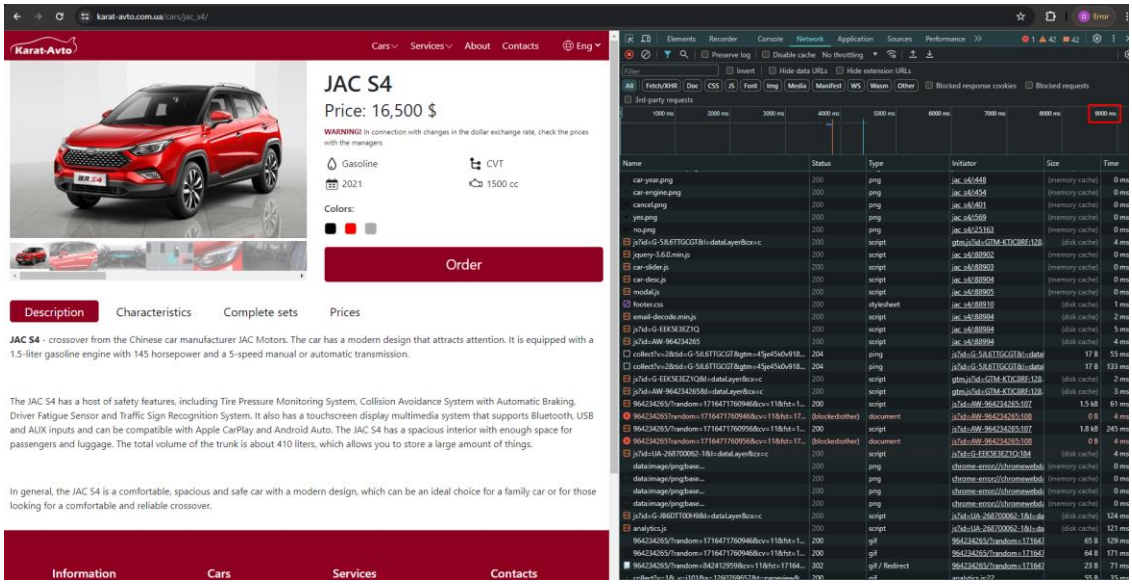


Рисунок 3.1 – Час завантаження сторінки автомобіля

Рисунок 3.2 – Навантаження сервера за аналітикою Digital Ocean

Я як розробник знаю вразливі місця мого додатку, але зазвичай для виявлення таких вразливостей слід проаналізувати історію запитів в логах та перевірити де саме виникають труднощі при атаках. Також слід увімкнути логування SQL запитів з додатку в тому випадку якщо використовується ORM система.

В даному випадку саме неоптимізованість запитів до бази даних навантажує сервер, змушуючи його задіяти більші потужності ніж потрібно для пошуку та обробки інформації.

Для демонстрації вразливості змодельовано найпростішу DDoS атаку за допомогою написаного власноруч скрипта на мові Python та бібліотеки Requests для імітації відкриття сторінки користувачем. Код скрипту знаходиться в Додатку Б.

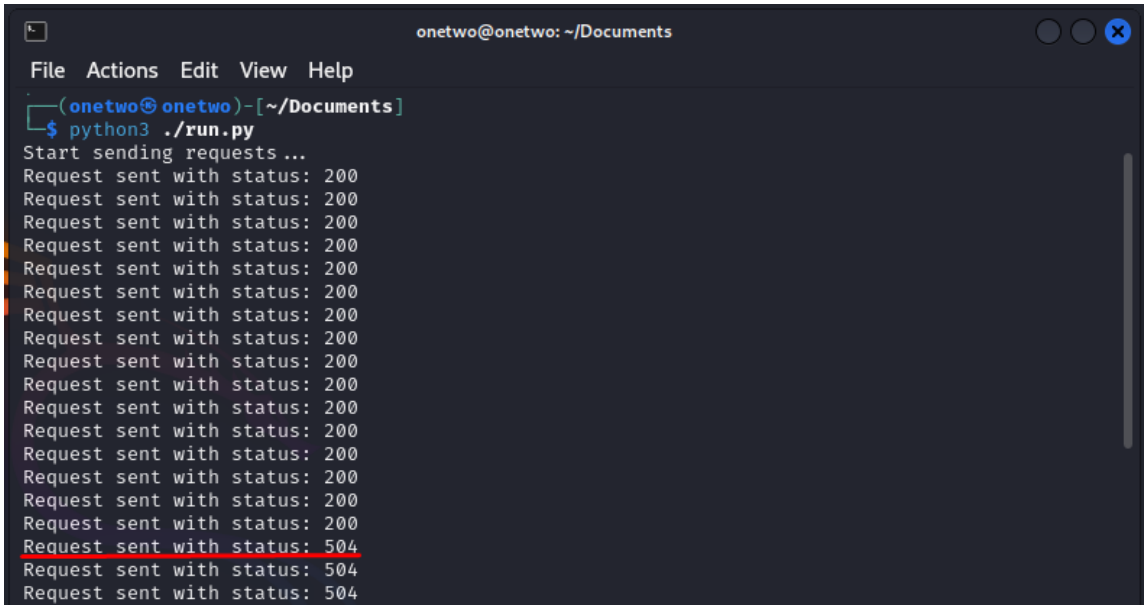
3.2 Впровадження захисних заходів та моніторинг їх ефективності

Після запуску тестової атаки на одну з сторінок додатку з усіх трьох віртуальних машин сервер намагається обробити запити, але цей процес зупиняється приблизно через 25-30 запитів. Йому не вистачає потужності.

Проаналізувавши відповіді які я отримав у результаті виконання атаки можна зрозуміти, що перші запити сервер все ж таки встигає обробити. Про це свідчить HTTP статус відповіді 200, але навантаження від наступних запитів система все ж таки не витримує і починає відповідати статусом HTTP 504.

Спробувавши відкрити сторінку веб-додатку з браузера можна побачити те, що він недоступний. Це показано на рисунку 3.3.

Мій сервер налаштовано так, щоб додаток сам перезапускався під час помилок, тому через деякий час він автоматично відновив роботу.



Риснок 3.3 – Запуск атаки на одній з віртуальних машин

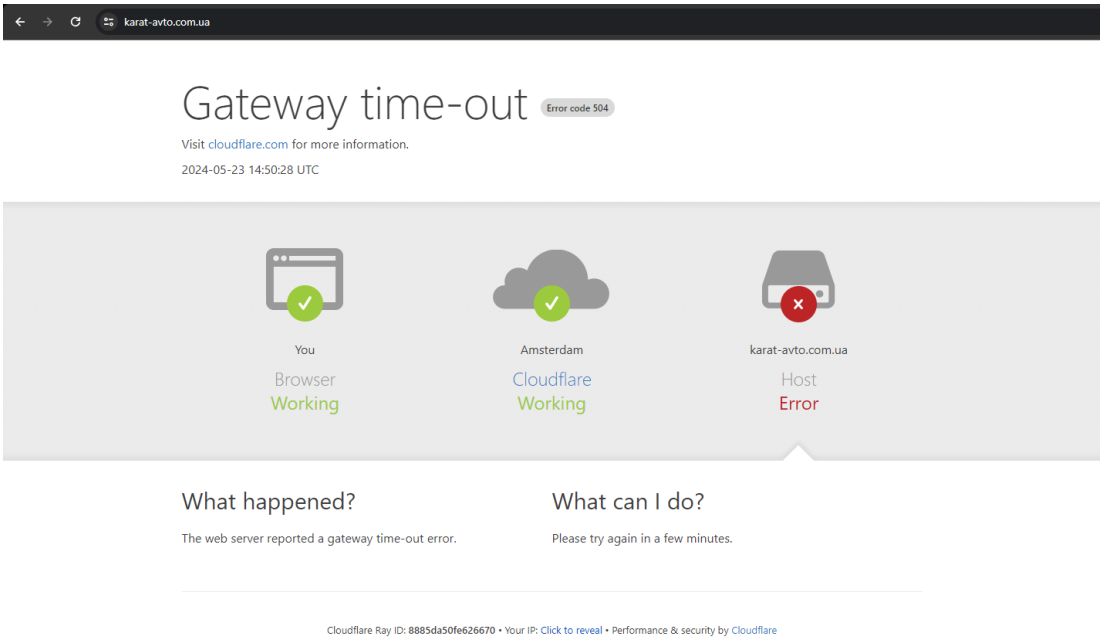


Рисунок 3.4 – Помилка доступу до веб-додатку з браузера

Перейшовши в панель керування Digital Ocean я проаналізував графік навантаження CPU сервера. За даними з графіку видно, що процессор був навантажений на 99,7%, що стало критичним показником і сервер відмовився приймати нові запити. Графік навантаження на CPU наведено на рисунку 3.5.

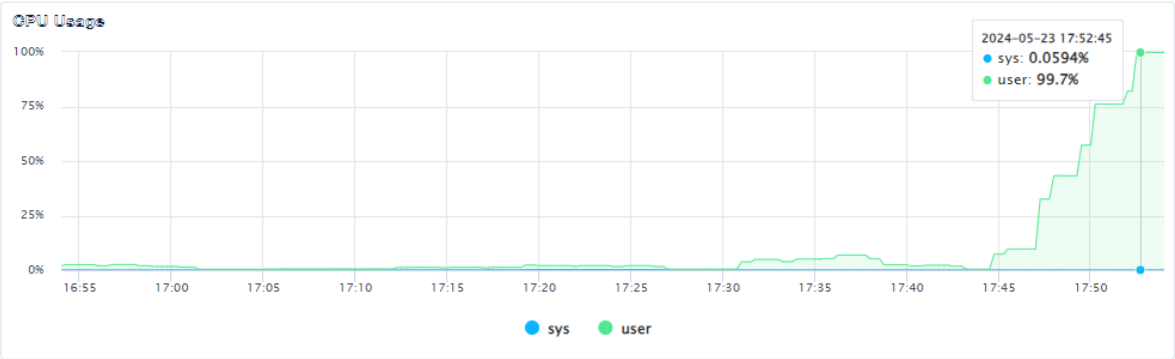


Рисунок 3.5 – Графік навантаження CPU в панелі керування Digital Ocean

Даний вид змодельованої атаки досить легкий, так як було використано лише 3 машини і ті віртуальні, отже обмежені в потужності. Але, як видно з результатів, і цього достатньо, щоб вплинути на працездатність невеликих веб-додатків.

Для захисту від подібних атак зазвичай використовують готові рішення, так як ручне налаштування потребує багато часу. Сервіси, такі як Clodflare, дають можливість підприємству отримати швидку і автоматизовану систему, в основі якої запрограмовані звичайні налаштування IPS/IDS, WAF, кешування, тощо. Таким чином, під час атаки система автоматично заблокує аномальний трафік, що не потребує моніторингу трафіку від системного адміністратора для спостереження за працездатністю серверу.

Отже, на основі мого досвіду з переддипломної практики було вирішено підлючити та продемонструвати можливості Cloudflare. Сервіс надає можливість ввімкнути режим «під атакою». В такому режимі Cloudflare буде автоматично моніторити всі запити, що надходять на веб-додаток і фільтрувати їх у разі сумнівної активності. Підключення такого режиму зображено на рисунку 3.6.

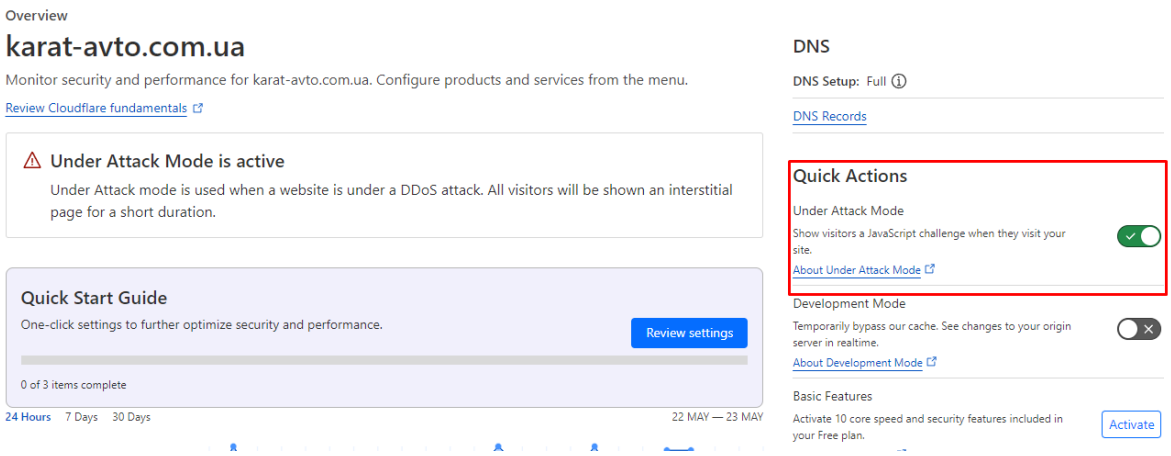


Рисунок 3.6 – Under attack mode

Я спробував провести повторне моделювання атаки в тих самих умовах і отримав HTTP статус 403 - помилку у відпові на запит, що означає Forbidden (Доступ заборонений) (рис. 3.7.).

Така відповідь свідчить про те, що скоріш за все, саме IP адреси з яких відправлялись запити були заблоковані IPS/IDS системою сервісу чи за допомогою WAF в автоматичному режимі.

Рисунок 3.7 – Повторна атака на веб-додаток

Як показано на рисунку 3.8, система Cloudflare помітила аномалію в трафіку і заблокувала IP з яких було відправлено велику кількість запитів.

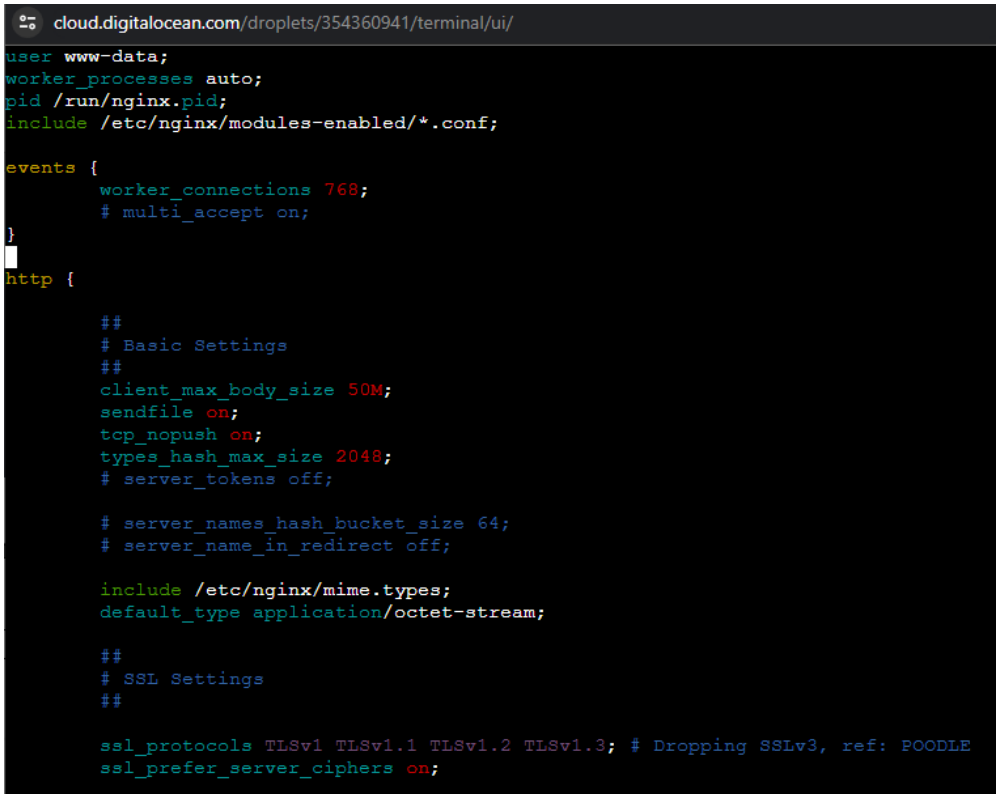
Рисунок 3.8 – Аномалія активності трафіку на графіку Cloudflare

Сервіс добре справляється з легкими атаками, але більш складні та децентралізовані DDoS атаки йому скоріш за все будуть не під силу, а для безкоштовної версії тим паче.

Для вирішення цього питання пропоную модифікувати Nginx конфігурацію на самому сервері, та збільшити кількість так званих воркерів. Це допоможе обробляти більшу кількість запитів одночасно, але буде потребувати більших ресурсів сервера.

Зробити це можна за допомогою параметра workers в файлі /etc/nginx/nginx.conf

За замовчуванням workers_processes має значення auto, але зазвичай більше 3-х воркерів воно не виділяє навіть при навантаженні (рис.3.9).



Рискунок 3.9 - Конфігурація nginx.conf за замовчуванням

Замінивше значення на 5, або більше, додаток буде самостійно розподіляти навантаження на 5 різних копій додатку, що значно покращить обробку більшої кількості запитів.

Це допоможе обробляти більшу кількість запитів, але не оптимізувати їх. Для зменшення навантаження на CPU в даному випадку слід звернути увагу саме на SQL запити та використати їх оптимізацію та індексацію. Ці дії значно зменшують час обробки запиту та навантаження на систему для його обробки. Також я б використав кешування за допомгою Redis, а також в парі з ним чергу задач за допомгою Celery. Таким чином повторні запити будуть братись з кешу Redis, а нові запити будуть ставати в чергу, що не буде навантажувати систему на 100% і вона зможе поступово обробити всі запити. Таке рішення потребує більшого обсягу оперативної пам’яті, так як кешування зберігає дані саме там.

ВИСНОВКИ

В роботі розглянуто та проаналізовано сутність DDoS атак, методи їх організації та захисту від них. Для цього створено тестовий полігон в якому задіяно VPS від Digital Ocean. Саме на ньому і знаходився розроблений мною веб-додаток. Також задіяно три віртуальні машини які виступали в ролі ботів для проведення атаки на яких було запущено скрипт для імітування HTTP GET запитів на веб-додаток.

Отримавши результат атаки, було проаналізовано навантаження на сервер та програмну частину веб-додатку. Виявлено вразливу сторінку зі складною структурою даних, що він отримує. Саме цей запит і навантажував систему.

Для демонстрації захисту я використав сервіс Cloudflare. Я обрав саме його через легкість налаштування та його авторитет серед великих підприємств. Було налаштовано автоматизацію моніторингу трафіку та реагування на DDoS атаки. Після чого я провів повторну атаку і отримав новий резульат, після аналізу якого можна сказати, що змодельована атака було стримана успішно.

На основі проведеного дослідження, можна зробити висновок, що ефективний захист від DDoS-атак потребує комплексного підходу. Оскільки DDoS-атаки можуть мати різні форми і методи реалізації, захист не може обмежуватися одним-двома засобами чи методами. Необхідно використовувати поєднання різних технологій, інструментів та стратегій, щоб забезпечити максимально ефективний захист. Саме тому надано рекомендації щодо оптимізації системи, а саме полегшення SQL запиту до бази даних, кешування запитів та даних за допомогою сервісу Redis в парі з сервісом Celery для створення черги запитів. Саме ці рішення вирішили проблему з доступністю веб-додатку під час та після атаки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Світличний В. А. Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем // Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. Одеса : ОДУВС, 2018. С. 88-89.

2. DDoS-атака: що це, так як працює // VPS.ua : сайт. 27.08.2018. URL: https://vps.ua/blog/ddos-attacks-and-their-types/ (дата звернення: 19.05.2024).

3. А.П. Кортко. Види ddos - атак та алгоритм виявлення ddos – атак типу flood – attack /Кортко. А// науковий журнал «Комп'ютерно – інтегровані технології: освіта, наука, виробництво». 2015. 18. С. 18-25.

4. Sansone, I. The Damaging Impacts of DDoS Attacks [Електронний ресурс] / Corero. — Режим доступу : https://www.corero.com/thedamaging-impacts-of-ddos-attacks/ — Дата доступу : січень 2023. — Назва з екрана.

5. Kumar, G. Denial of service attacks – an updated perspective [Text] / Systems science & control engineering. — 2016. — Vol. 4, № 1. — P. 285 – 294.

6. Johnson, A. Python Popularity: The Rise of a Global Programming Language [Електронний ресурс] / Flatiron School. — Режим доступу : https://flatironschool.com/blog/python-popularity-the-rise-of-a-globalprogramming-language/ — Дата доступу : березень 2023. — Назва з екрана

7. Richard R. Brooks Professor Holcombe Department of Electrical and Computer Engineering Clemson University ˙Ilker Oz¸celik ¨ Assistant Professor Department of Computer Engineering Recep Tayyip Erdogan University - Distributed Denial of Service Attacks Real-world Detection and Mitigation.

8. Kesavamoorthy, R., Alaguvathana, P., Suganya, R., & Vigneshwaran, P. (2020). Classification of DDoS attacks–A survey. Test Eng. Manag., 83, 12926- 12932.

9. Kirichenko, L. O., & Radivilova, T. A. (2019). Fractal analysis of selfsimilar and multifractal hour series. Kharkiv, Kh-NURE [in Ukrainian]

10. Ghimire, D. Comparative study on Python web frameworks: Flask and Django [Text] / D. Ghimire, K. Salo // Metropolia University of Applied Sciences. — 2020. — 40 p.

11. GitHub project URL: https://github.com/tsyhanenkod/Karat-Avto

ДОДАТОК А

ПОЧАТКОВА КОНФІГУРАЦІЯ NGINX

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name karat-avto.com.ua www.karat-avto.com.ua;

    # Перенаправление с HTTP на HTTPS
    return 301 https://$host$request_uri;
}

server {
    listen 443 ssl default_server;
    listen [::]:443 ssl default_server;
    server_name karat-avto.com.ua www.karat-avto.com.ua;

    ssl_certificate /etc/letsencrypt/live/karat-avto.com.ua/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/karat-avto.com.ua/privkey.pem;

    location /static/ {
        alias /home/www/karat-avto/static/;
    }

    location / {
        proxy_pass http://127.0.0.1:8000;
        proxy_set_header X-Forwarded-Host $server_name;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_redirect off;
        add_header P3P 'CP="ALL DSP COR PSAa OUR NOR ONL UNI COM NAV"';
        add_header Access-Control-Allow-Origin *;

        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host $http_host;
        proxy_set_header X-Script-Name /;
        proxy_set_header X-CSRFToken $cookie_csrftoken;

        expires 1h;
        add_header Cache-Control "max-age=86400";
    }
}
```

ДОДАТОК Б

КОД PYTHON СКРИПТУ ДЛЯ ВІДПРАВКИ ЗАПИТІВ

```python
import aiohttp
import asyncio

url = "https://karat-avto.com.ua/cars/jac_s4/"

async def send_request(session, url):
    try:
        async with session.get(url) as response:
            print(f"Request sent with status: {response.status}")
    except Exception as e:
        print(f"Request error: {e}")

async def main():
    async with aiohttp.ClientSession() as session:
        tasks = []
        for i in range(100):
            tasks.append(send_request(session, url))
        await asyncio.gather(*tasks)

print("Start sending requests...")
asyncio.run(main())
print("Attack finished.")
```