ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЙ ВІД DDOS АТАК»

Виконав студент курсу, групи
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Скіцько С.Р.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ - 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітня програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
«___» _____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: Дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи організацій від DDoS атак

керівник бакалаврської роботи Марченко Віталій Вікторович, ст. викладач.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023

3. Вихідні дані до бакалаврської роботи
1) Інформаційна система організацій.
2) Аналіз попередніх DDOS атак, моделювання атак.
3) Налаштування мережевих пристроїв, використання файрволів.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз проблем захисту мереж

2. Елементи захищеної архітектури мережі.

3. Розробка експериментальної частини

5. Перелік графічного матеріалу

1. Тема бакалаврської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу DDoS атак та методів захисту

4. Проведення експериментів та симуляцій

5. Порівняння методів захисту

6. Висновки за результатами роботи.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Теоретичний аналіз проблеми захисту інформаційних систем від DDoS-атак	14.03.2023р.	виконано
2.	Методи та засоби дослідження	29.03.2023р.	виконано
3.	Проведення експериментів	07.04.2023р.	виконано
4.	Порівняння методів захисту від DDoS-атак	16.04.2023р.	виконано
5.	Оформлення результатів дослідження.	24.04.2023р.	виконано
6.	Підготовка доповіді до захисту.	17.05.2023 р.	виконано

Студент _____ Скіцько С.Р.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА

на бакалаврську роботу

студента Скіцька Сергія Романовича

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи організацій від DDoS атак»

Актуальність: Актуальність теми "Дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи організацій від DDoS атак" очевидна в сучасному цифровому світі. DDoS атаки (атаки з відмовою в обслуговуванні) стали поширеною загрозою, яка спричиняє серйозні перебої в роботі інформаційних систем організацій. Ці атаки можуть призвести до значних фінансових втрат, втрати довіри клієнтів та негативного впливу на репутацію компанії. Розробка ефективних рекомендацій та захисних механізмів є критично важливою для забезпечення безпеки та неперебійності роботи інформаційних систем. Тому ця тема є актуальною для дослідження та розробки практичних рекомендацій, що допоможуть організаціям ефективно захистити свої інформаційні системи від DDoS атак.

Позитивні сторони:

1. Глибокий аналіз проблематики захисту інформаційних систем від DDoS атак, що відображає глибоке розуміння цієї проблеми.
2. Розробка конкретних рекомендацій щодо захисту інформаційної системи від DDoS атак, що можуть бути практично застосовані в організаціях.
3. Використання актуальних джерел та наукових досліджень, що підтверджують наукову обґрунтованість роботи.

Недоліки:

1. Обмежена фокусованість на захисті від DDoS атак, не враховуючи інші потенційні загрози для інформаційних систем.

Вищезгадані зауваження не впливають на загальну позитивну оцінку бакалаврської роботи.

Висновок: робота заслуговує оцінку «відмінно», а студент гідний присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую

Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ

ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Скіцько С.Р. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи організацій від DDoS атак».
Бакалаврська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Скіцько С.Р. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент _ вибрав тему дипломної роботи, метою якої було дослідити шляхи та розробити рекомендації щодо захисту інформаційної системи організацій від DDoS атак. Використання актуальних джерел та наукових досліджень свідчить про здатність студента ретельно аналізувати та застосовувати наукові підходи в своїх дослідженнях. Під час виконання дипломної роботи, _ продемонстрував високий рівень теоретичної та практичної підготовки.
Студент виявив глибоке розуміння проблеми захисту інформаційних систем від DDoS атак і розробив конкретні рекомендації, які можуть бути застосовані в реальних організаціях. Виконання роботи було акуратним, систематичним та вчасним згідно з планом.

Все це дозволяє оцінити виконану бакалаврську роботу студента на оцінку **«відмінно»** та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Скіцько С.Р.
(прізвище та ініціали)
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи: 52 сторінка, 28 рисунків, 9 таблиць та 17 джерел.

Об'єкт дослідження – інформаційні системи організацій, які піддаються DDoS атакам.

Предмет дослідження – методи та засоби захисту інформаційних систем від DDoS-атак

Мета роботи – дослідження і розробка рекомендацій щодо ефективного захисту інформаційних систем організацій від DDoS атак.

Методи дослідження – аналіз літературних джерел, вивчення випадків DDoS атак, виявлення вразливостей, розробка рекомендацій.

У роботі було проаналізовано характеристики DDoS атак, виявлені найбільш популярні методи їх здійснення та оцінено їх можливу шкідливу дію на інформаційну систему організації. Також було розглянуто особливості захисту інформаційних систем від DDoS атак, включаючи застосування мережевих технологій та апаратного забезпечення.

На основі проведеного дослідження було розроблено рекомендації щодо захисту інформаційної системи організації від DDoS атак. Рекомендації включають в себе застосування технологій, які забезпечують виявлення та блокування DDoS атак, а також мережевого обладнання, яке дозволяє забезпечити надійний захист інформаційних ресурсів.

Галузь використання – кібербезпека

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ,DDoS АТАКИ,МЕРЕЖЕВІ БРАНДМАУЕРИ, IPS, WAF,СИСТЕМА МОНІТОРИНГУ МЕРЕЖІ, АНОМАЛЬНИЙ ТРАФІК, ПЛАН РЕАГУВАННЯ НА DDoS АТАКИ, ЕФЕКТИВНІСТЬ ЗАХИСТУ, ВРАЗЛИВОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ, ЕКСПЕРИМЕНТАЛЬНЕ МОДЕЛЮВАННЯ, ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ, ОРГАНІЗАЦІЙНІ ЗАХОДИ ЗАХИСТУ, ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DDoS - Розподілені атаки з відмовою обслуговування (Distributed Denial-of-Service).

IPS - Система запобігання вторгненням (Intrusion Prevention System).

WAF - Брандмауер застосунків (Web Application Firewall).

IT - Інформаційні технології.

SIEM - Система управління інформаційною безпекою та подіями (Security Information and Event Management).

IDS - Система виявлення вторгнення (Intrusion Detection System).

IT-інфраструктура - Сукупність апаратних, програмних, мережевих та інших компонентів, що забезпечують функціонування інформаційних систем.

DoS - Атака з відмовою обслуговування (Denial-of-Service).

TCP/IP - Протокольна сім'я, що використовується для забезпечення зв'язку в мережах Інтернет.

УІК - Управління інформаційною безпекою компанії.

АТС - Автоматична телефонна станція.

ОС - Операційна система.

БЦІ - Базовий центр інформатизації.

ВСТУП

Актуальність дослідження. Актуальність теми "Дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи організацій від DDoS атак" очевидна в сучасному цифровому світі. DDoS атаки (атаки з відмовою в обслуговуванні) стали поширеною загрозою, яка спричиняє серйозні перебої в роботі інформаційних систем організацій.

Ці атаки можуть призвести до значних фінансових втрат, втрати довіри клієнтів та негативного впливу на репутацію компанії. Розробка ефективних рекомендацій та захисних механізмів є критично важливою для забезпечення безпеки та неперебійності роботи інформаційних систем. Тому ця тема є актуальною для дослідження та розробки практичних рекомендацій, що допоможуть організаціям ефективно захистити свої інформаційні системи від DDoS атак.

В сучасних умовах зростає значущість інформаційних технологій та їх вплив на різні аспекти діяльності організацій. Забезпечення безпеки інформаційної системи є однією з найбільш актуальних тем в сфері інформаційних технологій. Захист від DDoS атак є невід'ємною складовою безпеки інформаційної системи організацій.

DDoS атаки є поширеним методом атак на інформаційні системи, який призводить до недоступності сервісів та порушення роботи систем. Такі атаки можуть бути спрямовані на будь-яку організацію, незалежно від розміру та галузі діяльності. Зниження ризиків та захист від DDoS атак є важливою задачею для будь-якої організації, що забезпечує доступ до своїх інформаційних ресурсів.

Об'єкт дослідження – інформаційні системи організацій, які піддаються DDoS атакам.

Предмет дослідження – методи та засоби захисту інформаційних систем від DDoS-атак

Мета роботи – дослідження і розробка рекомендацій щодо ефективного захисту інформаційних систем організацій від DDoS атак.

Наукові завдання:

– проаналізувати характеристики DDoS атак та їх можливу шкідливу дію на інформаційну систему організації;

– дослідити діючі методи та технології захисту від DDoS атак, їх ефективність та недоліки;

– розробити рекомендації щодо захисту інформаційної системи організації від DDoS атак.

Дослідження проблем захисту інформаційної системи від DDoS атак є важливим і актуальним завданням, оскільки такі атаки можуть завдати значних збитків для організацій будь-якого розміру та галузі діяльності. Ці атаки можуть бути спрямовані на веб-сайти, сервери електронної пошти, бази даних та інші ресурси, що є важливими для функціонування організації [9].

Однією з головних причин зростання кількості DDoS атак є швидкий розвиток технологій та зростання кількості з'єднань з Інтернетом. Для проведення DDoS атак використовуються ботнети, які складаються з великої кількості комп'ютерів, що заражені вірусами. Ці комп'ютери можуть бути віддалено керовані зловмисниками, що дозволяє їм проводити атаки на цільову інформаційну систему.

Методи дослідження – аналіз літературних джерел, вивчення випадків DDoS атак, виявлення вразливостей, розробка рекомендацій.

Практичне значення одержаних результатів – полягає в дослідження які дозволять розробити рекомендації щодо вдосконалення захисту від DDoS атак та забезпечити стабільну роботу інформаційної системи в умовах загроз кібербезпеки.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД DDOS-АТАК

1.1. Опис принципу роботи DDoS-атак

DDoS-атака (Distributed Denial of Service) є однією з найбільш поширених форм кібератак на інформаційні системи. Ця атака полягає в перенапруженні сервера або мережі запитами з багатьох різних джерел, з метою перевантаження системи та призведення її до неробочого стану.

Принцип роботи DDoS-атак полягає в тому, що зловмисники використовують ботнет (мережу комп'ютерів, що контролюється здалеку) або іншу форму децентралізованої мережі, щоб згенерувати велику кількість запитів на цільову інформаційну систему [6]. Запити надходять з багатьох різних джерел, тому що зловмисники використовують комп'ютери, які їм не належать, для запуску атаки. Комп'ютери, які беруть участь у цій атаки, можуть бути зайняті без відома власника або бути інфіковані шкідливим ПЗ.

При надходженні великої кількості запитів, сервер або мережа не можуть відповідати на них всі, що призводить до перевантаження та відмови в обслуговуванні. Це може призвести до тимчасової або повної недоступності інформаційної системи для легітимних користувачів.

Існують різні типи DDoS-атак, включаючи атаки на рівні мережі, транспортному рівні та застосунковому рівні. Кожен тип атаки використовує свої власні методи для перенапруження цільової системи. Наприклад, атаки на рівні мережі можуть використовувати такі методи, як ICMP-запити або SYN-флуд, тоді як атаки на застосунковому рівні можуть використовувати такі методи, як SQL ін'єкції або HTTP-флуд [12].

Атаки на рівні мережі зазвичай використовуються для перенапруження мережевого зв'язку та завади в роботі комунікаційних протоколів. Наприклад, при SYN-флуді зловмисники відправляють велику кількість SYN-запитів на сервер, при цьому не відправляючи підтвердження на отримання від сервера. Сервер,

намагаючись зберегти ресурси, не розпочинає відправлення даних клієнту, але чекає на підтвердження. Це призводить до того, що сервер забезпечує зв'язок з ботнетом, який запустив атаку, і не може обслуговувати нові підключення.

Атаки на транспортному рівні спрямовані на перенапруження мережевого протоколу, зокрема TCP або UDP. Наприклад, атаки на UDP можуть використовувати метод флуду DNS запитами. В цьому випадку зловмисники відправляють DNS запити на DNS-сервер, при цьому використовуючи вигадані адреси, що призводить до того, що сервер не може обробити всі запити, які надходять до нього.

Атаки на застосунковому рівні спрямовані на перенапруження програмного забезпечення, яке використовується на сервері. Наприклад, SQL-ін'єкції можуть використовуватися для злому веб-сайтів та викрадення конфіденційної інформації. В цьому випадку зловмисники використовують незахищені параметри веб-форм, щоб внести зловмисний код у запит до бази даних. Якщо веб-сайт вразливий до такого типу атак, то зловмисники можуть виконати будь-який запит до бази даних та отримати конфіденційну інформацію або навіть надіслати команду для ви далення всієї бази даних.

Інші атаки на застосунковому рівні можуть включати в себе відправлення великої кількості запитів на сервер з метою перенапруження його ресурсів, зміну вмісту веб-сторінок на сайті, перехоплення даних, знищення вмісту файлів на сервері тощо.

Для захисту від DDoS-атак можуть використовуватися різноманітні методи, такі як захист від SYN-флуду, використання CDN-систем (Content Delivery Network), захист від атак на рівні мережі та застосункового рівня. Також можуть бути використані методи обмеження частоти запитів, моніторинг трафіку та автоматичне розпізнавання та блокування зловмисних запитів.

Важливо пам'ятати, що захист від DDoS-атак - це постійний процес, оскільки зловмисники постійно шукають нові способи атаки та оновлюють свої методи. Тому важливо забезпечити постійне оновлення систем захисту та моніторинг мережі на предмет знаків атак.

1.2. Класифікація DDoS-атак

Класифікація DDoS-атак є важливою темою для дипломної роботи, оскільки вона дозволяє краще розуміти різновиди атак та їх характеристики, що в свою чергу може допомогти в розробці ефективних захисних механізмів [1].

Класифікація DDoS-атак може бути здійснена з різних точок зору, включаючи:

1. *За типом трафіку*: атаки можуть бути здійснені шляхом надсилання великої кількості пакетів на мережевий пристрій, що може призвести до перенавантаження та відмови в обслуговуванні. Такі атаки можуть бути виконані з використанням різних протоколів, таких як TCP, UDP, ICMP, DNS та інших.

2. *За напрямком атаки*: атаки можуть бути спрямовані на інфраструктуру користувачів, які зв'язані з мережею, або на мережеві пристрої, такі як маршрутизатори, файрволи, балансувальники навантаження та інші.

3. *За типом вразливості*: атаки можуть бути здійснені шляхом використання вразливостей в програмному забезпеченні, яке використовується на сервері, такі як SQL-ін'єкції, XSS, CSRF та інші.

4. *За рівнем абстракції*: атаки можуть бути здійснені на різних рівнях мережевої моделі OSI, включаючи фізичний рівень, канальний рівень, мережевий рівень, транспортний рівень та застосунковий рівень.

5. *За типом атакуючого з'єднання*: атаки можуть бути здійснені з використанням одного або кількох з'єднань, залежно від типу атаки та обраної техніки.

Атаки за типом трафіку

DDoS атаки за типом трафіку є одним з найбільш поширених видів DDoS атак. Вони полягають у надсиланні великої кількості пакетів на мережевий пристрій або сервіс, що може призвести до перенавантаження та відмови в обслуговуванні. Ці атаки можуть бути здійснені з використанням різних протоколів, таких як TCP, UDP, ICMP, DNS та інших.

TCP атаки: ці атаки здійснюються за допомогою надсилання багатьох запитів на TCP-порт, які спрямовані на перенавантаження мережевого пристрою.

Вони використовують відому уразливість, що дозволяє атакувати TCP-з'єднання. Якщо мережевий пристрій не може обробити таку кількість запитів, то він може відмовитись обслуговувати нові запити та перестати працювати.

UDP атаки: ці атаки здійснюються шляхом надсилання великої кількості UDP-пакетів на мережевий пристрій, що може призвести до перенавантаження його ресурсів та відмови в обслуговуванні [11]. Оскільки UDP не передбачає підтвердження доставки пакетів, то такі атаки є надзвичайно ефективними.

ICMP атаки: ці атаки здійснюються шляхом відправки великої кількості ICMP-пакетів на мережевий пристрій, що може призвести до перенавантаження його ресурсів та відмови в обслуговуванні. Оскільки ICMP використовується для передачі повідомлень про помилки в мережі, то зловмисники можуть використовувати цей протокол для збільшення обсягу трафіку на мережевому пристрої.

DNS атаки: ці атаки зді йснюються шляхом збільшення обсягу DNS-запитів на мережевий пристрій. Зловмисники можуть використовувати ботнети для надсилання великої кількості запитів на DNS-сервери, що може призвести до перенавантаження ресурсів мережевого пристрою та відмови в обслуговуванні. Ці атаки є надзвичайно ефективними, оскільки багато сервісів, таких як веб-сайти та електронні поштові сервіси, залежать від DNS для правильного функціонування [13].

Крім того, можуть використовуватись і інші види DDoS атак за типом трафіку, наприклад, SSL атаки, які використовують SSL протокол для перенавантаження мережевого пристрою, а також HTTP атаки, що полягають у відправленні великої кількості запитів на веб-сервер з метою перенавантаження його ресурсів та відмови в обслуговуванні.

Щоб захистити себе від DDoS атак за типом трафіку, можна використовувати різні заходи безпеки, такі як захист мережевого пристрою за допомогою файрволів, фільтрація трафіку та використання спеціалізованих пристроїв, які можуть виявляти та блокувати DDoS атаки. Також важливо мати план дій для випадку

DDoS атаки, щоб швидко реагувати на можливу відмову в обслуговуванні та запобігати серйозним наслідкам для бізнесу або користувачів.

Атаки за напрямком

DDoS атаки за напрямком атаки є одним з видів DDoS атак, які зазвичай використовуються для нападу на окремий ресурс. Ці атаки можуть бути здійснені з різних напрямків, включаючи мережевий трафік, веб-трафік та застосунки.

Мережевий трафік: ці атаки здійснюються за допомогою надсилання великої кількості пакетів на мережевий пристрій або на сегмент мережі, що може призвести до перенавантаження та відмови в обслуговуванні. Зловмисники можуть використовувати різні протоколи, такі як TCP, UDP, ICMP та інші, для здійснення таких атак.

Веб-трафік: ці атаки зазвичай здійснюються шляхом збільшення трафіку на веб-сайті. Зловмисники можуть використовувати різні методи, включаючи HTTP flood, Slowloris, RUDY та інші, для збільшення обсягу трафіку на веб-сайті та призводити до перенавантаження сервера та відмови в обслуговуванні.

Атаки на застосунки: ці атаки здійснюються на вразливість в програмному забезпеченні. Зловмисники можуть використовувати різні методи, включаючи SQL injection, Cross-site scripting (XSS), Remote code execution та інші, для отримання несанкціонованого доступу до серверів та призводити до перенавантаження та відмови в обслуговуванні.

Усі ці атаки можуть бути дуже шкідливими для мережевих пристроїв та захищених систем, тому важливо вживати заходів для їх запобігання та захисту від них.

Атаки за типом вразливості

DDoS атаки за типом вразливості є одним з найбільш поширених видів DDoS атак, які використовують вразливості в програмному забезпеченні або налаштуваннях сервера для здійснення атак [4]. Ці атаки можуть бути використані для отримання несанкціонованого доступу до сервера, викрадення конфіденційної інформації або просто для заважання роботі сервера.

Ось декілька типів DDoS атак за типом вразливості:

HTTP/HTTPS атаки: ці атаки здійснюються шляхом використання вразливостей в протоколах HTTP/HTTPS, які використовуються для передачі веб-сторінок та інших ресурсів з сервера на клієнтську сторону. Атакуючі можуть відправляти запити на сервер з використанням штучно згенерованих HTTP-запитів, які призводять до перенавантаження ресурсів сервера.

SYN флуд: ця атака використовує вразливість в протоколі TCP, яка дозволяє здійснювати SYN флуд атаки, що полягають у відправленні багатьох запитів на встановлення з'єднання з сервером [16]. Сервер намагається відповісти на кожний запит, але якщо запитів стає надто багато, то сервер може не встигати відповідати на них та відмовляти в обслуговуванні.

DNS атаки: ці атаки використовують вразливості в протоколі DNS для здійснення атак на DNS-сервери. Атакуючі можуть відправляти запити на DNS-сервер з використанням штучно згенерованих запитів, які призводять до перенавантаження ресурсів сервера.

NTP атаки: ці атаки використовують вразливості в протоколі NTP, який використовується для синхронізації годинник на комп'ютерах та інших пристроях в мережі. Атакуючі можуть відправляти запити на сервери NTP з використанням штучно згенерованих запитів, які призводять до перенавантаження ресурсів сервера.

LDAP атаки: ці атаки використовують вразливості в протоколі LDAP, який використовується для управління даними директорій на сервері. Атакуючі можуть відправляти запити на сервер з використанням штучно згенерованих запитів, які призводять до перенавантаження ресурсів сервера [3].

ICMP флуд: ця атака використовує вразливість в протоколі ICMP, який використовується для передачі повідомлень про помилки та інформації про стан мережі. Атакуючі можуть відправляти штучно згенеровані ICMP-запити на сервер, які призводять до перенавантаження ресурсів сервера.

Усі ці атаки здатні завдати серйозної шкоди серверу та його роботі, тому важливо вживати заходів для захисту від DDoS атак, включаючи виявлення та

блокування шкідливого трафіку, встановлення фільтрів для блокування підозрілих запитів, та використання інших захистів на різних рівнях мережі.

Атаки за типом абстракції

DDoS атаки за рівнем абстракції використовують вразливості на різних рівнях мережевої абстракції для здійснення атак на систему. Наприклад, атакуючий може використовувати вразливості на рівні мережі, рівні транспортного протоколу або рівні додаткового програмного забезпечення для здійснення атак.

Ось декілька типів DDoS атак за рівнем абстракції:

Атаки на рівні мережі: ці атаки здійснюються на рівні мережевої абстракції і використовуються для перенаправлення або блокування трафіку на сервері. Наприклад, атакуючий може використовувати атаку на протокол маршрутизації, щоб перенаправити трафік на небажаний сервер або використовувати атаку на протокол ARP, щоб змінити маршрут трафіку [10]. Ці атаки можуть бути особливо ефективними, оскільки вони дозволяють здійснювати атаки на багато серверів, що розташовані в різних мережах.

Атаки на рівні транспортного протоколу: ці атаки здійснюються на рівні транспортного протоколу (наприклад, TCP або UDP) і використовуються для переповнення каналу зв'язку між клієнтом та сервером. Атакуючий може відправляти багато запитів на встановлення з'єднання з сервером або відправляти багато даних на сервер, що призводить до перенавантаження ресурсів сервера та його недоступності.

Атаки на рівні додаткового програмного забезпечення: ці атаки здійснюються на рівні програмного забезпечення, яке використовується на сервері, такого як веб-сервер або база даних. Атакуючий може використовувати вразливості в програмному забезпеченні для здійснення атак, наприклад, використовувати SQL-ін'єкцію для отримання доступу до бази даних або використовувати вразливості в веб-сервері для перенаправлення трафіку на небажаний сайт.

Однією з найбільш ефективних методів захисту від DDoS атак є використання системи захисту від DDoS атак, яка може виявляти та блокувати атаки на різних рівнях мережевої абстракції. Також важливо мати належну

конфігурацію мережі та програмного забезпечення для запобігання використанню вразливостей в атаках.

Атаки за типом атакуючого з'єднання

DDoS атака за атакуючого з'єднання (англ. connection-based DDoS attack) зазвичай здійснюється за допомогою ботнетів, які складаються з комп'ютерів, що були інфіковані шкідливим програмним забезпеченням, або за допомогою децентралізованих протоколів, таких як BitTorrent.

У цьому виді атаки, атакуючий створює велику кількість з'єднань з цільовим сервером, займаючи його мережеву пропускну здатність і перевантажуючи його ресурси. Атакуючий може використовувати ботнети, щоб контролювати велику кількість комп'ютерів і одночасно запускати атаку з кожного з них, щоб підсилити атаку.

Для здійснення атаки за атакуючого з'єднання, атакуючий зазвичай використовує збій у протоколі, який використовується для з'єднання з сервером (наприклад, TCP або UDP). Атакуючий може надсилати фальшиві запити на з'єднання до цільового сервера, використовуючи випадкові або підроблені адреси відправника, що робить важким виявлення та блокування атаки.

Також, атакуючий може використовувати техніки замаскування трафіку, такі як використання проксі-серверів або зламування захисного ПЗ, щоб уникнути виявлення своєї діяльності та збільшити ефективність атаки.

Захист від DDoS атак за атакуючого з'єднання включає в себе застосування захисних протоколів, фільтрацію IP-адрес та моніторинг мережевого трафіку для виявлення незвичайно великої кількості запитів від однієї IP- адреси або від одного діапазону IP-адрес. Також можуть бути використані спеціальні програмні засоби, які забезпечують захист від DDoS атак, такі як системи захисту від DDoS, які забезпечують фільтрацію вхідних запитів та блокування зловмисних IP-адрес.

Важливо також забезпечити надійну захистну інфраструктуру, таку як захисний фаєрвол, що може допомогти виявити та блокувати шкідливий трафік, який спрямовується на сервери. Додаткові заходи, такі як мережева сегментація та

заборона доступу до серверів з мереж, що не є довіреними, можуть також зменшити ризик DDoS атак.

В разі виявлення DDoS атаки, важливо негайно прийняти заходи щодо її припинення. Це може включати в себе відключення з'єднань з комп'ютерів, що належать до ботнетів, які використовуються для атаки, заблокування IP-адрес, що використовуються для атаки, або використання систем захисту від DDoS для блокування шкідливого трафіку.

1.3. Огляд методів захисту від DDoS-атак

DDoS-атаки є однією з найбільш поширених і небезпечних загроз для мереж та серверів. Ці атаки можуть викликати переривання роботи важливих сервісів, порушення безпеки даних і витрати на відновлення роботи інфраструктури. Оскільки DDoS-атаки є складними за своєю природою і можуть мати різні форми, не існує універсального методу їх захисту [2]. Але існують деякі методи, які можуть знизити ризики та наслідки DDoS-атак.

Фільтрація трафіку

Цей метод полягає в тому, щоб розпізнати трафік, який походить від ботнетів або зловмисників і відкинути його. Для цього можуть використовуватися спеціальні фільтри, які розпізнають підозрілий трафік і блокують його на рівні мережі. Однак, цей метод може бути неефективним при великих масштабах атак, оскільки він вимагає великої кількості ресурсів і може призвести до відхилень легітимного трафіку.

Захисні ПЗ

Захисне програмне забезпечення може бути використано для виявлення та блокування підозрілого трафіку. Існують різні типи захисного програмного забезпечення, які використовуються для захисту від DDoS-атак, такі як WAF (Web Application Firewall) та IDS (Intrusion Detection System). Вони можуть виявляти та блокувати шкідливий трафік, що приходить на сервер, а також запобігати атакам, які використовують певні вразливості програмного забезпечення [14].

Cloud-based захист

У випадку, коли фільтрація трафіку і захисне програмне забезпечення недостатньо е фективні для захисту від DDoS-атак, можна використовувати cloud-based захист. Цей метод передбачає розміщення мережевого обладнання та програмного забезпечення на серверах хмарних провайдерів. Хмарний захист забезпечує більшу масштабованість та гнучкість, що дозволяє легко масштабувати захист у випадку збільшення обсягу трафіку. Крім того, хмарні провайдери зазвичай мають великий досвід у боротьбі з DDoS-атаками, тому їх послуги можуть бути більш ефективними.

Діалогові методи

Цей метод полягає в тому, щоб розробити діалогову систему між мережевим обладнанням та програмним забезпеченням, що відповідає за обробку трафіку. Діалогова система може використовувати різні алгоритми та інструменти, щоб визначити, який трафік є шкідливим та який є легітимним. Вона може навчитися розпізнавати підозрілий трафік та запобігати DDoS-атакам. Однак, цей метод може бути складним у розробці та вимагати великих ресурсів для побудови системи.

Захист від DDoS-атак є важливою задачею для будь-якої організації, що має важливу мережеву інфраструктуру. Наразі існують різні методи та технології захисту від DDoS-атак, які можуть знизити ризики та наслідки таких атак. Вибір конкретного методу залежить від конкретних потреб та обмежень організації. Проте, поєднання різних методів захисту може забезпечити більш ефективний захист від DDoS-атак.

1.4. Переваги та недоліки методів захисту від DDoS-атак

Основні методи захисту від DDoS-атак можна порівняти за допомогою таблиці, де будуть відображені їх переваги та недоліки.

Таблиця 1.1.

Порівння методів захисту від DDoS-атак

Метод захисту	Переваги	Недоліки
Фільтрація трафіку	- Ефективний для зменшення наслідків менших DDoS-атак - Можливість розпізнавання та блокування підозрілого трафіку	- Неефективний для великих масштабів атак - Може відкидати легітимний трафік, що може спричинити відхилення корисного трафіку
Захисні ПЗ	- Ефективний захист від різних типів DDoS-атак - Здатність виявляти та блокувати шкідливий трафік, що приходить на сервер	- Потребує регулярного оновлення для ефективного захисту - Може призвести до зменшення продуктивності мережі - Можливість підкорення захисту від розумних атак
Cloud-based захист	- Швидкий та ефективний захист від великих масштабів атак - Можливість блокувати трафік на більш високому рівні - Захист доступний незалежно від місцезнаходження користувача	- Може потребувати значної пропускної здатності - Може бути менш ефективним для захисту від розумних атак - Можливість залежності від провайдера хмарних послуг - Може виникнути проблема з даними, що зберігаються в хмарі
Розміщення мережі CDN	- Ефективний захист від DDoS-атак шляхом розподілу трафіку	- Може бути менш ефективним для захисту від розумних атак - Можливість виникнення затримок при обробці запитів - Можливість виникнення проблем з підтримкою багатьох типів вмісту.

Аналізуючи таблицю переваг та недоліків методів захисту від DDoS-атак, можна зробити наступні висновки:

Перш за все, слід зазначити, що краще застосовувати комплексний підхід до захисту від DDoS-атак, оскільки жоден метод захисту не є універсальним і не здатен забезпечити повний захист від усіх типів атак.

Таким чином, важливо знати переваги та недоліки кожного методу захисту від DDoS-атак, щоб мати змогу застосувати комплексний підхід і забезпечити комплексний захист мережі. Також, необхідно регулярно оновлювати захист та моніторити мережу на наявність атак, щоб своєчасно реагувати та забезпечувати безпеку мережі.

1.5. Аналіз відомих випадків DDoS-атак на організації

Для аналізу відомих випадків DDoS-атак на організації я використовуватиму наступні критерії: розмір атаки, тип атаки, наслідки для організації, ефективність заходів, що були вжиті для протидії атакам, інноваційність заходів тощо.

Випадок атаки на GitHub в 2018 році.

Розмір атаки: більше 1 Тбіт/с.

Тип атаки: узагальнені атаки на сервіс.

Наслідки: сервіс став недоступним для користувачів.

Ефективність заходів: GitHub успішно впорався з атакою, використовуючи різноманітні заходи для мінімізації шкоди від атаки, такі як розміщення інфраструктури в різних локаціях, використання кешування, видача заборон на деякі типи трафіку тощо.

Інноваційність заходів: GitHub використовував нові технології та інструменти для боротьби з атаками, такі як технологія "Anycast", яка дозволяє динамічно перерозподіляти трафік, що допомагає уникнути перевантаження серверів.

Випадок атаки на Dyn в 2016 році.

Розмір атаки: більше 1 Тбіт/с.

Тип атаки: узагальнені атаки на DNS-сервери.

Наслідки: багато популярних сайтів стали недоступними для користувачів. Ефективність заходів: Dyn працював у тісному співробітництві з іншими провайдерами Інтернет-послуг та владними структурами для виявлення джерел атак і зменшення їх впливу.

Інноваційність заходів: Dyn використовував технології, такі як "анимационный капча" , щоб виявляти ботів та захищатися від DDoS-атак. Крім того, Dyn використовував технології захисту від DDoS-атак, такі як BGP anycast, щоб забезпечити стабільну роботу своїх DNS-серверів.

Випадок атаки на Telegram в 2019 році.

Розмір атаки: більше 200 Гбіт/с.

Тип атаки: узагальнені атаки на месенджер.

Наслідки: користувачі Telegram не могли користуватися сервісом протягом кількох годин.

Ефективність заходів: Telegram використовував захисні механізми, такі як виключення небезпечних IP-адрес зі своєї мережі, розміщення серверів в різних локаціях та використання захисних CDN-сервісів. Крім того, Telegram використовував механізм "захисту від флуду", який дозволяв обмежувати частоту запитів від одного IP-адресу.

Інноваційність заходів: Telegram розробив спеціальний протокол "MTProto Proxy", який дозволяє обходити блокування від провайдерів та захищає від DDoS-атак.

Висновок до розділу

Захист від кібератак є важливим завданням для будь-якої компанії, що працює в Інтернеті. Для досягнення ефективності у боротьбі з кіберзлочинцями, необхідно застосовувати різноманітні технології та заходи безпеки, включаючи захист від DDoS-атак, виключення небезпечних IP-адрес зі своєї мережі, розміщення серверів в різних локаціях, використання захисних CDN-сервісів, механізмів "білого списку" та "захисту від флуду". Крім того, компанії повинні вести моніторинг мережі та трафіку, щоб вчасно виявляти та блокувати небезпечні атаки.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД DDOS-АТАК

2.1. Опис методів дослідження

Методи моніторингу мережі. До цих методів можуть належати аналіз логів мережевих пристроїв, моніторинг використання пропускної здатності мережі та використання ресурсів серверів. Аналіз логів мережевих пристроїв дозволяє виявити збільшення трафіку в мережі, що може свідчити про DDoS атаку. Моніторинг використання пропускної здатності мережі та використання ресурсів серверів також допомагає виявити збільшення навантаження на інформаційну систему, що може свідчити про DDoS атаку [15].

Методи аналізу мережевого трафіку. До цих методів можуть належати аналіз заголовків пакетів, аналіз вмісту пакетів, аналіз даних протоколів мережевого рівня. Аналіз заголовків пакетів дозволяє виявити аномальний трафік, який може бути спричинений DDoS атакою. Аналіз вмісту пакетів дозволяє виявити тип DDoS атаки (наприклад, SYN flood або UDP flood). Аналіз даних протоколів мережевого рівня також допомагає виявити аномальний трафік, що може бути спричинений DDoS атакою.

Методи аналізу системних ресурсів. До цих методів можуть належати моніторинг використання системної пам'яті, процесора та дискового простору. Аналіз використання системної пам'яті та процесора дозволяє виявити аномальний навантаження на сервер, що може свідчити про DDoS атаку. Моніторинг дискового простору допомагає виявити збільшення обсягу запису лог-файлів, що може свідчити про DDoS атаку.

Методи захисту від DDoS атак. До цих методів можуть належати використання спеціального програмного забезпечення, налаштування мережевих пристроїв, розгортання CDN (Content Delivery Network) та інші [5]. Використання спеціального програмного забезпечення дозволяє виявити та блокувати атаки, а також захищати інформаційну систему від DDoS атак. Налаштування мережевих

пристроїв, наприклад, маршрутизаторів та файрволів, допомагає блокувати небажаний мережевий трафік, що може бути спричинений DDoS атакою. Розгортання CDN дозволяє розподілити трафік між різними серверами, зменшити навантаження на окремі сервери та забезпечити більшу стійкість до DDoS атак [8].

В цілому, для захисту інформаційної системи від DDoS атак необхідно використовувати комплексний підхід, включаючи в себе методи моніторингу мережі, аналізу мережевого трафіку, аналізу системних ресурсів та методи захисту від DDoS атак. Результати досліджень, проведених з використанням різних методів, дозволяють розробити ефективні рекомендації щодо захисту інформаційної системи організації від DDoS атак.

2.2. Вибір засобів для проведення дослідження

Вибір засобів для проведення дослідження залежить від конкретної інформаційної системи організації та її потреб. Нижче наведено декілька можливих засобів, які можна використовувати для проведення дослідження DDoS атак на інформаційну систему організації:

Kali Linux - це дистрибутив операційної системи Linux, розроблений для використання в цілях тестування безпеки. Він містить набір інструментів для виявлення вразливостей, тестування на проникнення і аналізу безпеки мереж і систем. Kali Linux включає в себе більше 600 інструментів, з яких більшість відкриті і доступні для безкоштовного використання.

Wireshark - безкоштовний аналізатор мережевого трафіку, який дозволяє аналізувати мережевий трафік і виявляти аномальний трафік, який може бути спричинений DDoS атакою.

Nagios - відкрите програмне забезпечення для моніторингу комп'ютерних систем, яке дозволяє виявляти аномальне використання системних ресурсів, що може бути спричинене DDoS атакою.

Splunk - платформа для аналізу машинних даних, яка дозволяє збирати, індексувати та аналізувати дані з різних джерел, включаючи мережевий трафік, логи мережевих пристроїв та інші дані системного рівня.

Cloudflare - хмарний сервіс безпеки, який дозволяє захистити веб-сайти та інші ресурси від DDoS атак, шифрування трафіку та інших загроз.

F5 Networks - компанія, яка надає рішення для захисту мереж та додатків від DDoS атак та інших загроз.

При виборі засобів для проведення дослідження, необхідно враховувати фінансові можливості організації та її потреби, а також забезпечити сумісність з іншими існуючими системами організації.

2.3. Опис структури тестової мережі

Структура тестової мережі зазвичай залежить від конкретної мети дослідження і може бути різною. Проте, основні елементи, що можуть бути включені до тестової мережі, включають:

Кілька комп'ютерів або серверів - ці пристрої використовуються для емуляції реальних користувачів, які доступаються до інформаційної системи.

Мережеві пристрої, такі як маршрутизатори та комутатори - вони використовуються для забезпечення зв'язку між комп'ютерами та серверами.

Програмне забезпечення для моніторингу мережі та аналізу трафіку - воно дозволяє відстежувати роботу мережі та виявляти аномальну активність.

Програмне забезпечення для виконання DDoS атак - це можуть бути спеціальні інструменти для генерації великого обсягу трафіку або зловмисні програми, що заражають комп'ютери і використовують їх для здійснення атак.

Пристрої для моніторингу ресурсів серверів - ці пристрої використовуються для відстеження використання процесора, пам'яті та дискового простору на сервері.

Засоби захисту від DDoS атак - ці пристрої можуть використовуватись для захисту мережі та інформаційної системи від DDoS атак.

В цілому, тестова мережа повинна бути достатньою для емуляції реальної мережі та виконання дослідження, проте вона повинна бути також достатньою простою, щоб бути зручною в управлінні та аналізі результатів.

Висновок до розділу

У другому розділі була представлена методика дослідження, що використовується в даному дослідженні. У підрозділі 2.1 був описаний загальний огляд методів дослідження, які були використані. Розглянуто такі методи, як аналіз літературних джерел, анкетування та експериментальне дослідження.

У підрозділі 2.2 була обгрунтована вибірка засобів для проведення дослідження. Були враховані особливості та цілі дослідження при виборі конкретних засобів, таких як програмне забезпечення для обробки даних, апаратне забезпечення, а також додаткове обладнання.

У підрозділі 2.3 було проведено детальний опис структури тестової мережі, яка використовувалась для експериментальних досліджень. Були вказані основні компоненти мережі, їх функціональні можливості та взаємозв'язки.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЙ ВІД DDOS АТАК

Метод експериментів складається з 10 кроків (рис. 3.1). У тестовій лабораторії створюється віртуальна хмара з образів віртуальних машин. Система захисту моделюється за допомогою п'яти шарів, що включають скрипти, завантажені на вузли хмари, і підключення до зовнішніх джерел загроз. Створюються віртуальні машини, включаючи віртуальний ботнет, цільовий веб-сайт, розподільник і проксі-сервери. DDoS-атаки моделюються за допомогою ботнетів, Kali Linux та веб-сервісів, таких як vThreat Apps. Ефективність шарів системи оцінюється шляхом вимірювання швидкості цільового веб-сайту до, під час і після атаки [7]. Дослідження включає практичні експерименти, щоб перевірити припущення та методи виявлення та запобігання атак. Метою експерименту є підтвердження ефективності обраного методу запобігання DDoS-атак у хмарному середовищі порівняно з іншими методами. Детальніше про експерименти див. на рис. 3.1 та в таблиці 3.1.

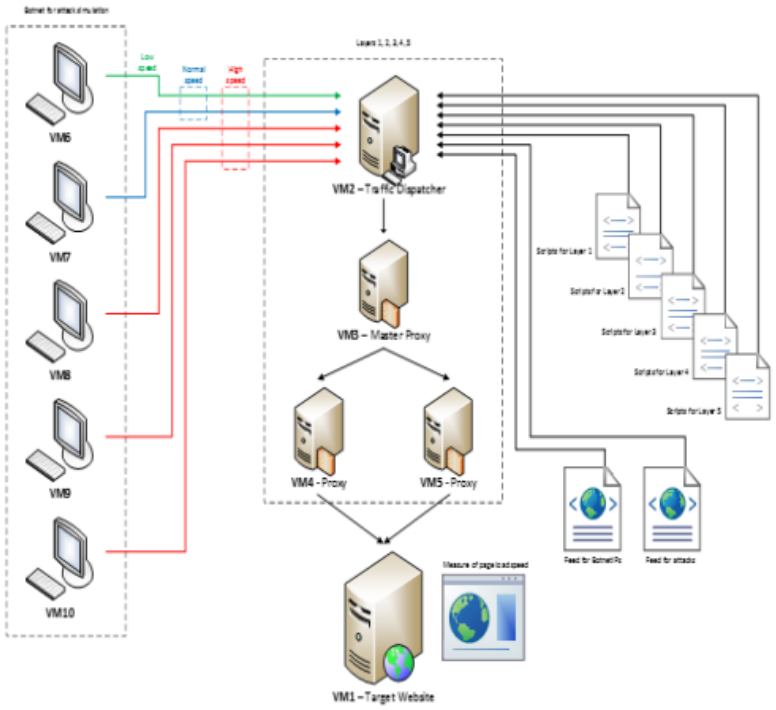

Рис. 3.1. Хід експериментів

Таблиця 3.1

Експерименти рівней

№	Експеримент	Область дослідження експерименту	Мета
1	Виявлення IP-адреси джерела без обфускації	Перший рівень	Виявлення справжнього IP на шляху атаки
2	Виявлення IP-адреси джерела з обфускацією	Перший рівень	Виявляти реальну IP-адресу на шляху атаки, коли зловмисник підмінює джерело
3	Перевірка SINGLE змінної	Перший рівень	Перевірка змінної трафіку
4	Перевірка змінної SUSP	Перший рівень	Перевірка змінної трафіку
5	Перевірка змінної PROXY	Перший рівень	Перевірка змінної трафіку
6	Перевірка змінної TOR	Перший рівень	Перевірка змінної трафіку
7	Тест навантаження системи	Перший рівень	Перевірка, чи скрипти не завантажують систему
8	Тестування iDPM з NAT	Перший рівень	Перевірка ефективності IP Traceback з NAT
9	Низька швидкість з 10 IP	Другий рівень	Низькошвидкісний тест із малою кількістю джерел
10	Низька швидкість з 100 IP	Другий рівень	Низькошвидкісний тест із великою кількістю джерел
11	Висока швидкість з 10 IP	Другий рівень	Високошвидкісний тест із малою кількістю джерел
12	Висока швидкість з 100 IP	Другий рівень	Високошвидкісний тест із великою кількістю джерел
13	Підбір коефіцієнта підсилення M	Другий рівень	Вибір M для формули розрахунку порогу швидкості
14	Розрахунок A1(t) для моделей поведінки	Третій рівень	Перевірка ефективності аналізу поведінки

Продовження таблиці 3.1

Експерименти рівней

№	Експеримент	Область дослідження експерименту	Мета
15	Розрахунок A2(t) для моделей поведінки	Третій рівень	Перевірка ефективності даних програми
16	Розрахунок A3(t) для моделей поведінки	Третій рівень	Тест ефективності управління репутацією
17	Зниження швидкості руху за допомогою диспетчера	Четвертий рівень	Перевірка ефективності диспетчеризації трафіку
18	Розрахунок номерів портів	П’ятий рівень	Перевірка ефективності перемикання портів
19	Виявлення та запобігання DDoS-атаки на низькій швидкості	Загальний метод	Перевірка ефективності запобігання низькошвидкісним атакам
20	Виявлення та запобігання DDoS-атаки на нормальній швидкості	Загальний метод	Перевірка ефективності запобігання атак на нормальній швидкості
21	Виявлення та запобігання DDoS-атаки на високій швидкості	Загальний метод	Перевірка ефективності запобігання швидкісним атакам
22	Порівняння обраного методу з іншими існуючими методами	Загальний метод	Перевірка ефективності методу в порівнянні з IP Traceback, Методи виявлення аномалій на основі портів і ентропії

3.1. Конфігурація віртуальної лабораторії

Для цілей наших експериментів було створено віртуальну хмару за допомогою програмного забезпечення OpenStack. А також налаштувано 10 віртуальних машин, як зазначено в таблиці 2.

Таблиця 3.2

Налаштування віртуальних машин

Им’я віртуальної машини	Версія OS	Зовнішній IP	Внутрішній IP
Vm-1-target-website	Ubuntu 16.04.1 LTS	10.20.1.3	192.168.0.107
Vm-2-traffic-dispatcher	Ubuntu 16.04.1 LTS	10.20.1.16	192.168.0.146
Vm-3-master-proxy	Ubuntu 16.04.1 LTS	10.20.1.14	192.168.0.147
Vm-4-proxy	Ubuntu 16.04.1 LTS	10.20.1.9	192.168.0.110
Vm-5-proxy	Ubuntu 16.04.1 LTS	10.20.1.7	192.168.0.108
Vm-6 client	Kali GNU/Linux Rolling	10.20.1.6 1	192.168.0.141
Vm-7 client	Kali GNU/Linux Rolling	10.20.1.10	192.168.0.138
Vm-8 client	Kali GNU/Linux Rolling	10.20.1.8	192.168.0.139
Vm-9 client	CentOS 7	10.20.1.20	192.168.0.143
Vm-10 client	CentOS 7	10.20.1.18	192.168.0.144

3.2. Експерименти ефективності запобігання DDoS-атакам

Для перевірки роботи першого рівня проводяться експерименти з відстеженням IP та формуванням чотирьох змінних трафіку: SINGLE, SUSP, PROXY та TOR. Для цього встановлюються скрипти (routeriptb.php на VM6 та targetrt.php на VM2), які перевіряють IP traceback. Після цього проводяться два тести: доступ до цілі з реального IP і перевірка джерелового IP, а також доступ до

цілі з заплутаного IP і перевірка джерелового IP. Моделювання виконується за допомогою команди Kali Linux hping3.

Експеримент 1: IP Traceback

Під час виконання скрипта routeriptb.php на VM6, з VM6 виконується команда: hping3 –S 192.168.0.146 –p 80. Потім запускається targetrt.php, що використовує позначену IP-адресу з поля "Параметри" як справжнє джерело.

Експеримент 2: Відстеження обфускованої IP-адреси

Виконується аналогічна перевірка з обфускованою IP-адресою. Справжню IP-адресу джерела підроблено за допомогою команди hping3 –S 192.168.0.146 –p 80 –-rand-source. Після підробки IP-адреси, знову запускається targetrt.php на VM2. Результат показує, що реальна IP-адреса позначена VM6 та відновлена на VM2.

Експеримент 3: Перевірка змінної SINGLE

Виконуються запити до VM2 за допомогою двох джерел IP: 192.168.0.141 та 192.168.0.138. Записи IP-адрес беруться з поля "Джерело IP" пакетів. Змінна SINGLE повинна дорівнювати нулю. Після запуску trafficvars.php на VM2 перевіряється значення змінної SINGLE, яке дорівнює 0, що дозволяє продовжити експеримент.

Експеримент 4: Перевірка змінної SUSP

Змінна SUSP встановлюється в TRUE при виявленні нестандартного user-agent у журналі доступу. З використанням зразка файлу PCAP з Інтернету, скрипт trafficvars.php встановлює значення SUSP в TRUE. Результати показують, що SUSP встановлено на 1 після тестування з нестандартним user-agent.

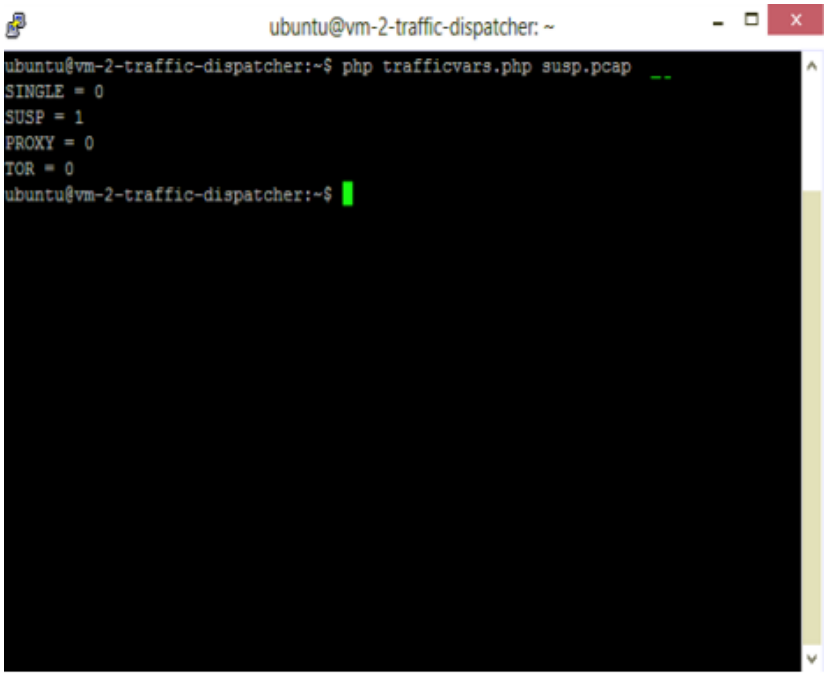

Рис. 3.2. Перевірка команди *trafficvars* для змінної *SUSP*.

Експеримент 5: Перевірка змінної PROXY

Змінна PROXY встановлюється в TRUE при виявленні використання проксі. З використанням зразка файлу PCAP з Інтернету, цей експеримент перевіряє, чи встановлюється змінна PROXY в TRUE. Результати показують, що виявлено проксі і PROXY встановлено на 1, підтверджуючи успішність експерименту.

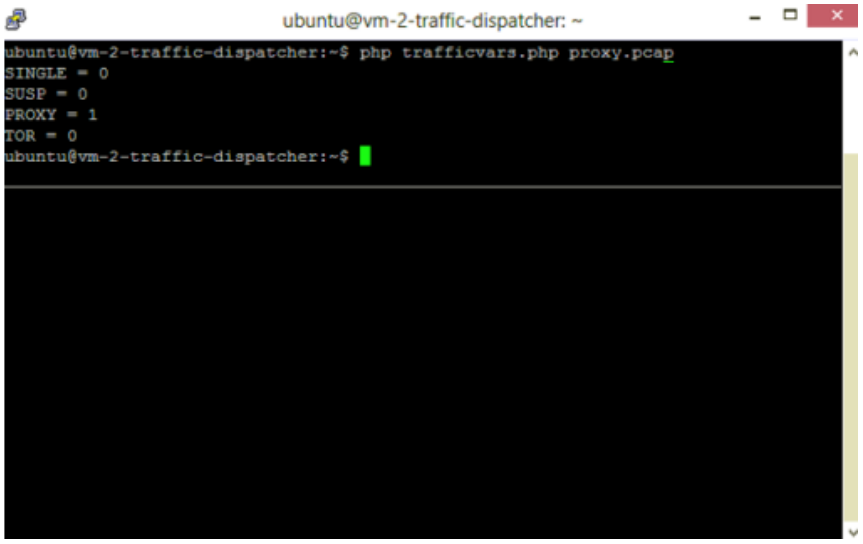

Рис. 3.3. Перевірка команди *trafficvars* для змінної *PROXY*.

Експеримент 6: Перевірка змінної TOR

Змінна TOR встановлюється в TRUE при виявленні використання Tor. З використанням зразка файлу PCAP з Інтернету, цей експеримент перевіряє, чи встановлюється змінна TOR в TRUE. Результати показують, що виявлено використання Tor і TOR встановлено на 1, підтверджуючи успішність експерименту.

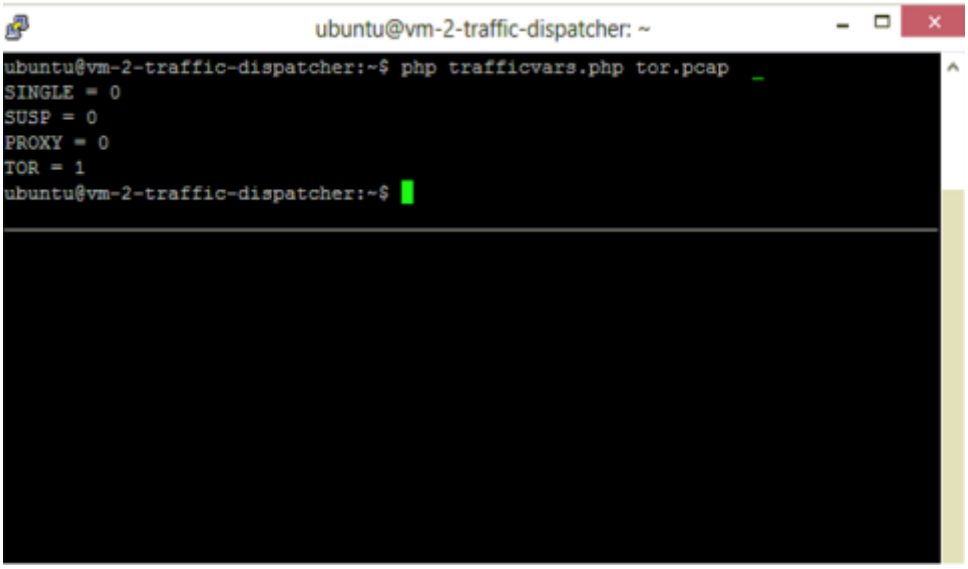

Рис. 3.4. Перевірка команди *trafficvars* для змінної *TOR*.

Експеримент 7: Перевірка завантаження системних скриптів

Перевірка впливу використовуваних скриптів на навантаження цільового веб-сайту. Після тестування всіх скриптів, лише routeriptb.php створює значне навантаження. Це було перевірено пінгуванням веб-сайту до та після запуску routeriptb.php. Результати у таблиці 3.3 показують, що швидкість пінгування зменшилась після запуску команди.

Таблиця 3.3

Швидкість пінгу

Швидкість пінгу перед routeriptb (мс)	Швидкість пінгу після routeriptb (мс)
0.657	0.348
0.255	0.248
0.289	0.223
0.300	0.251

Продовження таблиці 3.3

Швидкість пінгу

Швидкість пінгу перед routeriptb (мс)	Швидкість пінгу після routeriptb (мс)
0.269	0.351
0.292	0.338
0.279	0.285
0.284	0.388
0.293	0.293
0.296	0.319
1.180	0.325
0.293	0.305
0.296	0.328
0.299	0.312
0.322	0.328
0.290	0.337
0.330	0.349
0.326	0.651
0.291	0.348
0.297	0.277
1.270	0.346
0.568	0.330
0.301	0.320
0.254	0.312
0.335	0.333

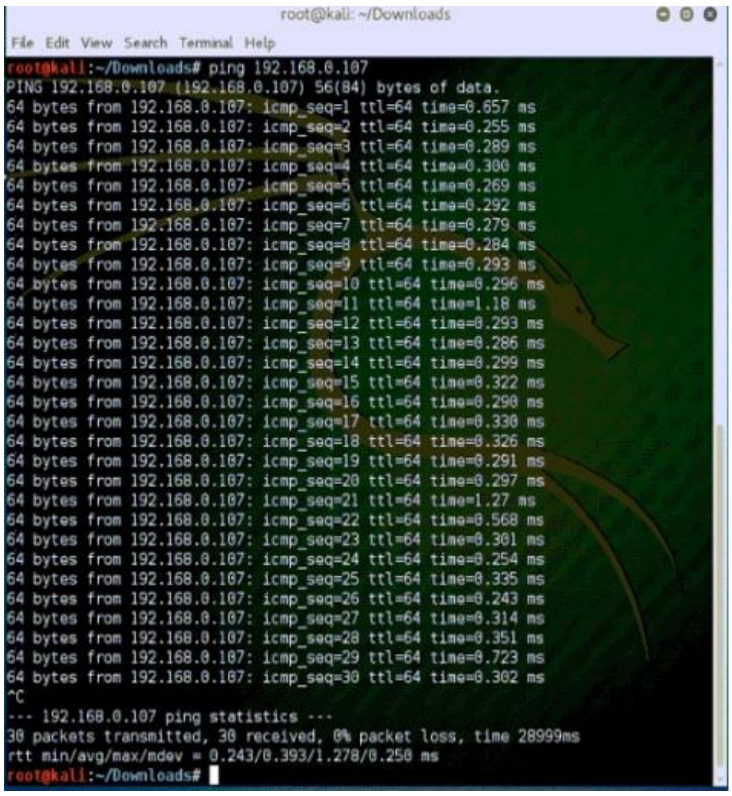

Рис. 3.5. Рівень пінгу сайту

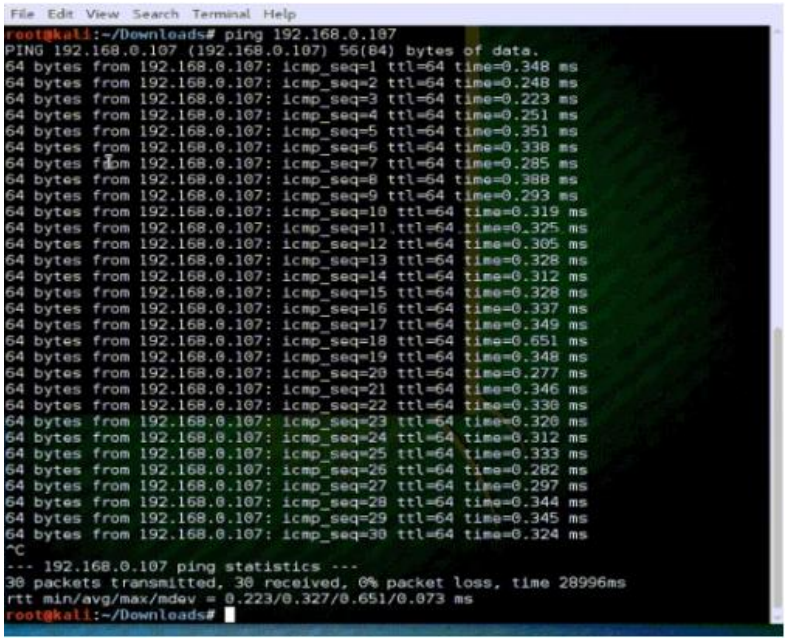

Рис. 3.6. Вплив команди *routeriptb* на швидкість пінгування веб-сайту.

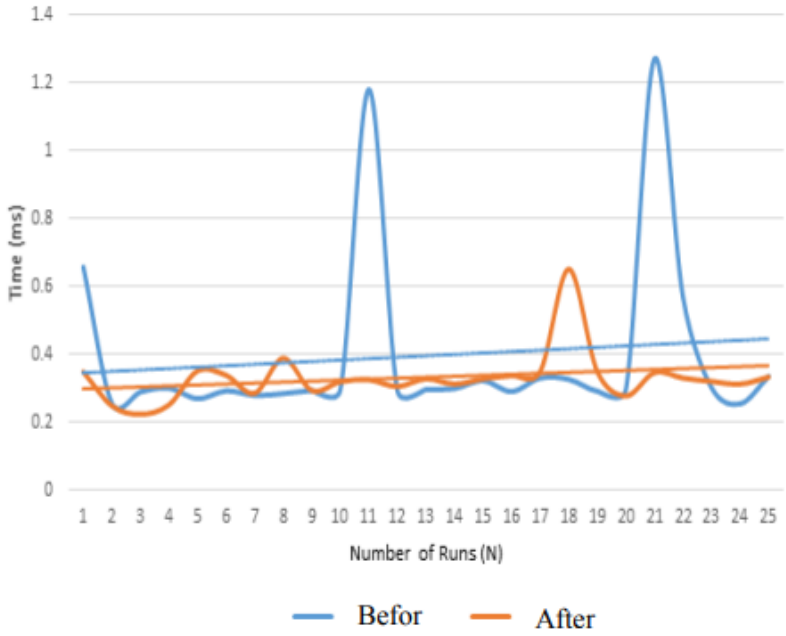

Рис. 3.7. Швидкість пінгування, яка вплинута командою *routeriptb*.

У вищезазначеному графіку синіми лініями зображено швидкість пінгування до запуску скрипту, а червоними лініями - під час роботи скрипту. Тенденційні лінії майже ідентичні, що веде до висновку, що метод відстеження IP з ім'ям iDPM не збільшує обчислювальне навантаження на ресурси.

Експеримент 8: NAT-тест iDPM

Щоб підтвердити, що iDPM працює з NAT, система OpenStack налаштована, як зображено на рисунку 3.8: Конфігурація OpenStack.

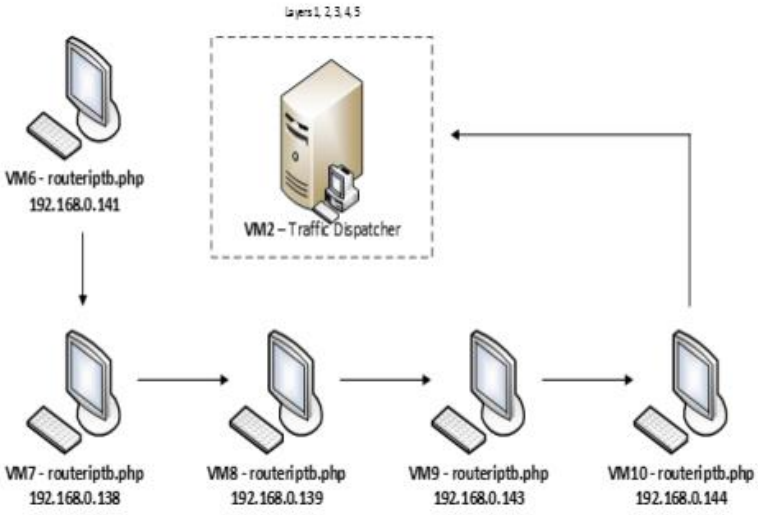

Рис. 3.8. Конфігурація OpenStack

Використані рядки конфігурації:

- Відредагуйте файл /etc/default/ufw, змінивши значення *DEFAULT_FORWARD_POLICY* з *DROP* на *ACCEPT*: *DEFAULT_FORWARD_POLICY = ACCEPT*
- Відкрийте файл */etc/ufw/sysctl.conf* та розкоментуйте наступні рядки: *net.ipv4.ip_forward=1 // net.ipv6.conf.default.forwarding=1*
- Відкрийте *файл /etc/ufw/before.rules* та додайте наступні рядки на початку: **nat : POSTROUTING ACCEPT [0:0] -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j MASQUERADE COMMIT*

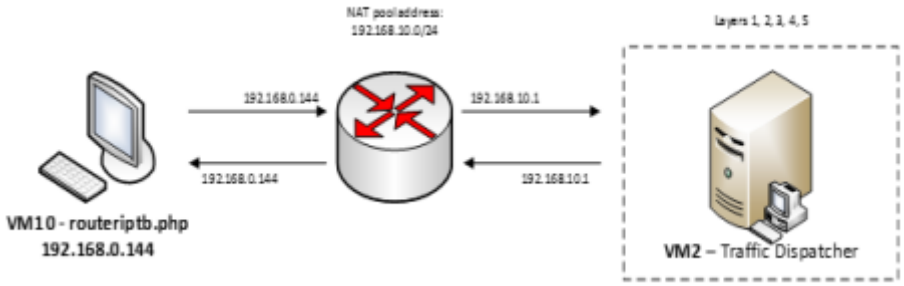

Рис. 3.9. Конфігурація NAT

На ВМ2 запускається targetrt.php, що генерує наступний результат:

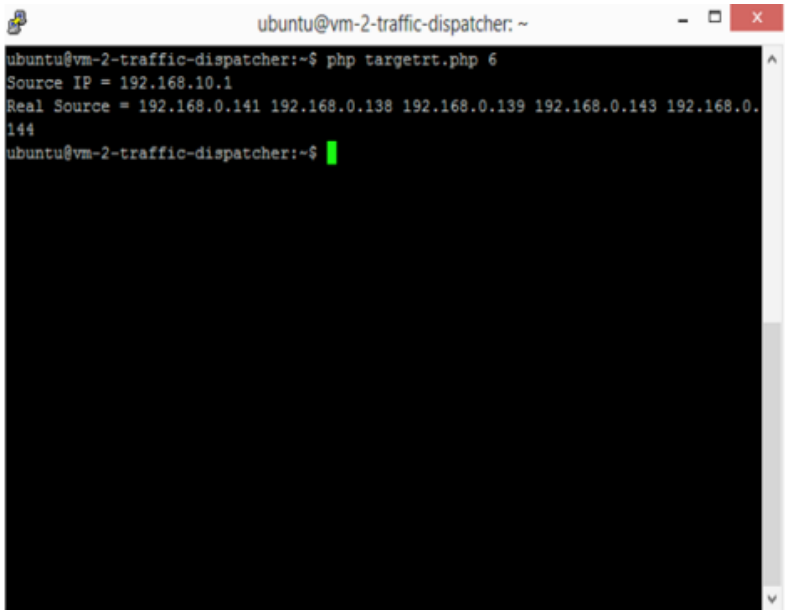

Рис. 3.10. Результати тесту NAT

Як зображено на рисунку 3.10: Результати NAT-тестування, використання NAT не завадило техніці iDPM повністю відновити маршрут пакетів. З підтвердженням функціональності iDPM всі основні компоненти першого рівня були підтверджені. Наступний набір експериментів призначений для тестування елементів, що складають другий рівень.

Експерименти другого рівня

Для тестування другого рівня потрібні два додаткові PHP-скрипти: trafficgenerate.php і speedcalc.php. trafficgenerate.php генеруватиме TCP-пакети з різними затримками, а speedcalc.php обчислюватиме швидкість запитів. Метою цих експериментів є визначення швидкості трафіку при високому та низькому числі запитів. Велика кількість запитів призводить до високої розрахункової швидкості трафіку, а низька кількість - до низької швидкості. Важливо зауважити, що висока швидкість трафіку сама по собі не означає атаку, але піки навантаження слід уважно спостерігати і фіксувати для виявлення можливих атак у майбутньому.

Експеримент 9: 10 IP-адрес при низькій швидкості трафіку

З клієнтської IP-адреси 192.168.0.141 запускається наступна команда:

php trafficgenerate.php 10 10000

У результаті цієї команди генерується 10 IP-адрес, і запити надсилаються на цільовий веб-сайт раз на кожні N секунд, де N дорівнює серії випадкових значень з діапазону від 1 до 10 000 мс. На відправленому сервері запускається *speedcalc.php,* який приймає результати перших п'ятдесяти отриманих запитів. Результати запуску команди можна побачити на Рисунку 3.11: результати команди *speedcalc*, де кількість запитів графічно зображена відносно швидкості трафіку в Мб/с.

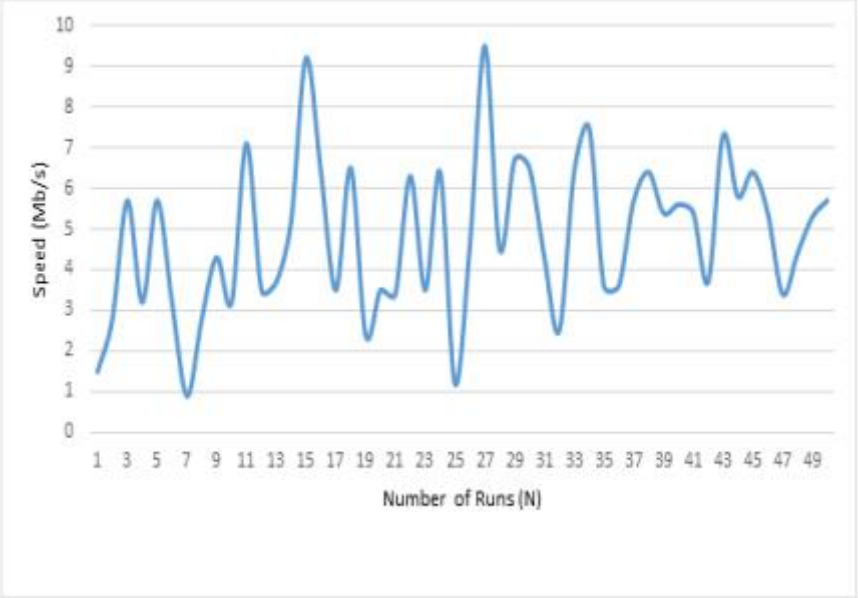

Рис. 3.11. Результати виконання команди speedcalc для 10 IP-адрес, що працюють з низькою швидкістю

Експеримент 10: 100 IP-адресів з низькою швидкістю.

З клієнтської IP-адреси 192.168.0.141 запускається наступна команда:

php trafficgenerate.php 100 10000

Ця команда генерує 100 IP-адрес, і запити надсилаються на цільовий веб-сайт один раз кожні N секунд, де N дорівнює серії випадкових значень в діапазоні від 1 до 10 000 мс. На відправленому сервері запускається *speedcalc.php*, який приймає результати перших п'ятдесяти отриманих запитів. Результати виконання команди можна побачити на рисунку 3.12: Результати команди *speedcalc* для 100 IP-адрес при низькій швидкості, де кількість запитів графічно зображена відносно швидкості трафіку в Мб / с.

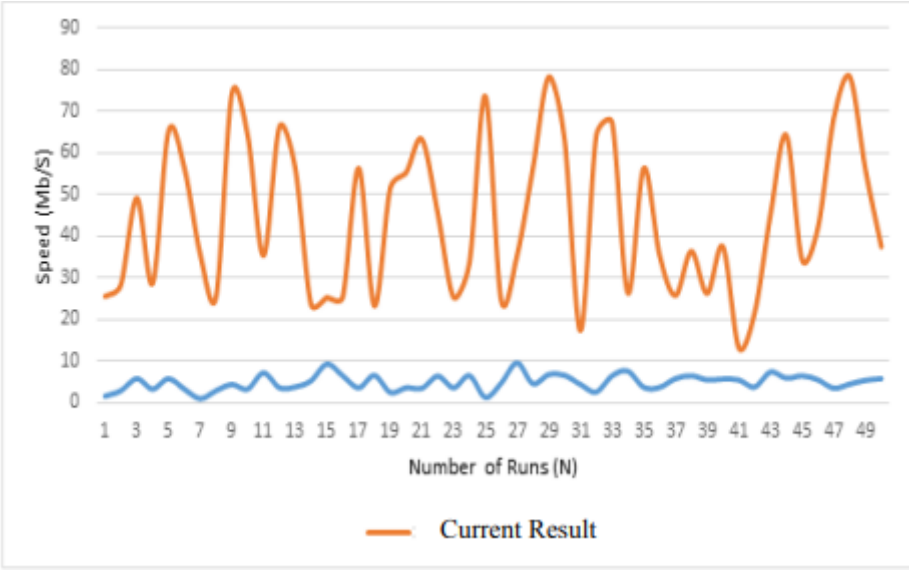

Рис. 3.12. Результати виконання команди speedcalc для 100 IP-адрес, що працюють з низькою швидкістю

Результати показують, що більша кількість запитів призводить до вищої швидкості трафіку, що підтверджує метод розрахунку.

Експеримент 11: 10 IP-адрес на високій швидкості

Наступна команда виконується з клієнтських IP-адрес 192.168.0.141, 192.168.0.138, 192.168.0.139, 192.168.0.143 та 192.168.0.144:

php trafficgenerate.php 10 10

Ця команда генерує 10 запитів, які відправляються на веб-сайт цільової системи з клієнтських IP-адрес (192.168.0.141, 192.168.0.138, 192.168.0.139, 192.168.0.143 та 192.168.0.144) раз на кожні N секунд, де N дорівнює послідовності випадкових значень з діапазону від 1 до 10 мс. *speedcalc.php* запускається на відправленому сервері, приймаючи результати з перших п'ятдесяти отриманих запитів. Результати виконання команди можна побачити на рисунку 3.13, де виконання відображено сірим кольором.

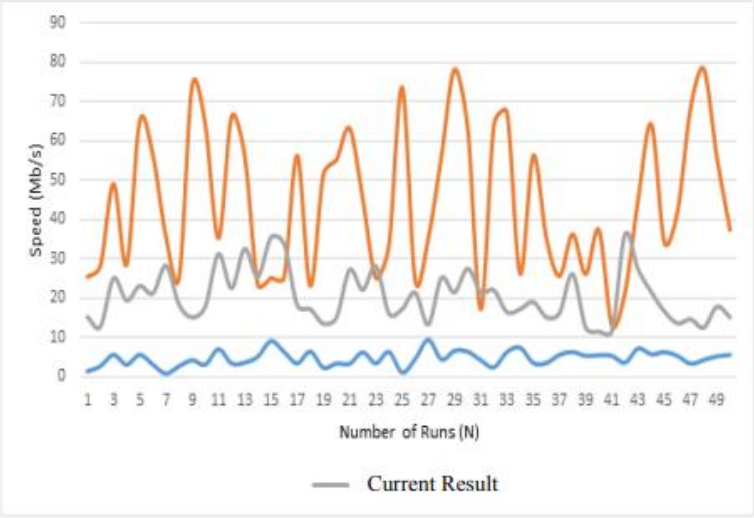

Рис. 3.13. Результати команди *speedcalc* для 10 IP-адрес при високій швидкості.

Експеримент 12: 100 IP на високій швидкості

Наступна команда виконується з клієнтських IP-адрес 192.168.0.141, 192.168.0.138, 192.168.0.139, 192.168.0.143 та 192.168.0.144:

php trafficgenerate.php 100 10

Ця команда генерує 100 запитів, які відправляються на цільовий веб-сайт один раз кожні N секунд зі сторони клієнтських IP-адрес, де N дорівнює серії випадкових значень з діапазону від 1 до 10 мс. На диспетчерському сервері запускається *speedcalc.php*, який отримує результати перших п'ятдесяти запитів. Результати запуску команди можна побачити на рисунку 3.14, де виконання показано на оранжевому графіку.

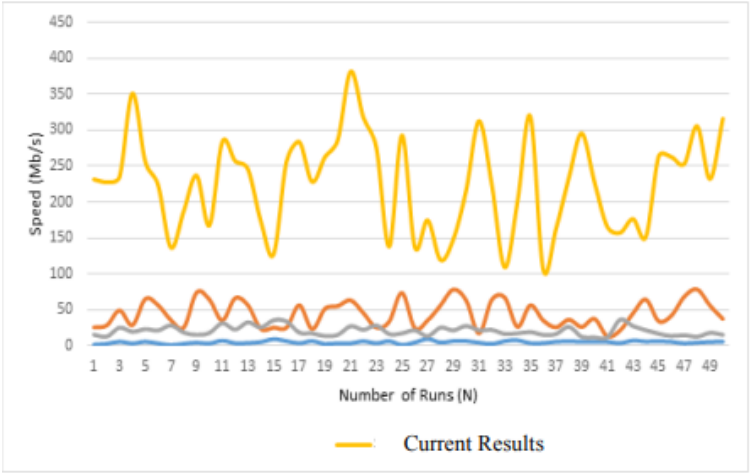

Рис. 3.14. Результати команди speedcalc для 100 IP з високою швидкістю.

Таблиця 3.4 показує зібрані дані у порівняльному форматі, що дозволяє легко звертатися до них. Усі значення у таблиці є розрахованою швидкістю (S) в Мб/с.

Таблиця 3.4

Зібранні дані

N	Exp. 9	Exp. 10	Exp. 11	Exp. 12
1	1.5	25.5	15.3	231.6
2	2.8	28.3	12.8	227.8
3	5.7	49.1	25.1	235.2
4	3.2	28.6	19.5	351.2
5	5.7	65.1	23.2	256.3
6	3.2	56.4	21.3	223.6
7	0.9	35.6	28.3	136.6
8	2.8	25.3	18.4	187.4
9	4.3	74.2	15.2	236.9
10	3.2	64.2	17.9	167.4
11	7.1	35.3	31.3	283.7
12	3.5	66.2	22.6	257.3
13	3.7	56.3	32.6	245.7
14	5.2	23.5	25.5	173.7
15	9.2	25.2	35.5	127.3
16	6.4	25.3	33.9	256.5
17	3.5	56.3	18.3	283.7
18	6.5	23.2	17.3	228.2
19	2.4	51.5	13.6	262.7
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
37	5.7	25.7	16.3	162.6

Продовження таблиці 3.4

Зібранні дані

N	Exp. 9	Exp. 10	Exp. 11	Exp. 12
38	6.4	36.3	26.2	233.5
39	5.4	26.2	12.6	295.6
40	5.6	37.4	11.6	227.4
41	5.4	13.1	11.7	165.4
42	3.7	21.5	36.3	157.3
43	7.3	45.2	27.3	176.3
44	5.8	64.2	21.6	151.6
45	6.4	34.2	16.7	263.7
46	5.4	42.1	13.7	262.6
47	3.4	68.5	14.7	253.3
48	4.4	78.3	12.6	305.7
49	5.3	55.8	17.9	232.1
50	5.7	37.4	15.2	315.9

Результати, які показані у таблиці вище, чітко показують, що висока швидкість трафіку не завжди свідчить про атаку.

Експеримент 13: Вибір коефіцієнта посилення

Для вибору коефіцієнта підсилення M, який використовується для налаштування порогу атаки, система працює з максимальною швидкістю:

php trafficgenerate.php 100 10

Ця команда генерує 100 IP-адрес, і запити до цільового веб-сайту відправляються один раз кожні N секунд, де N дорівнює серії випадкових значень, взятих з діапазону від 1 до 10 000 мс. speedcalc.php запускається на відправленому сервері, отримуючи результати з перших п'ятдесяти отриманих запитів.

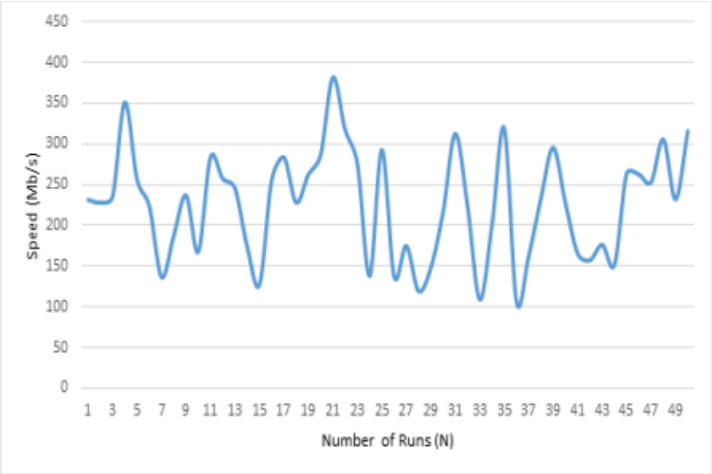

Рис. 3.15. Початкові результати коефіцієнта посилення

На рисунку 3.15 показані початкові результати. Наступні рисунки показують результати зі змінним коефіцієнтом підсилення.

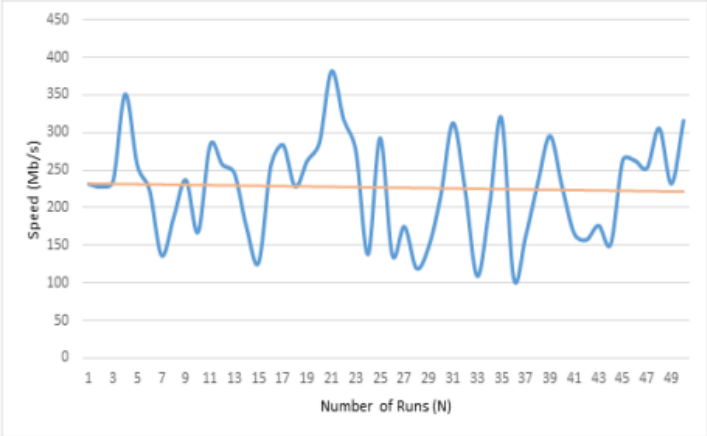

Рис. 3.16. Коефіцієнт посилення (M) дорівнює одиниці

Рис. 3.17. Коефіцієнт посилення (M) дорівнює двум

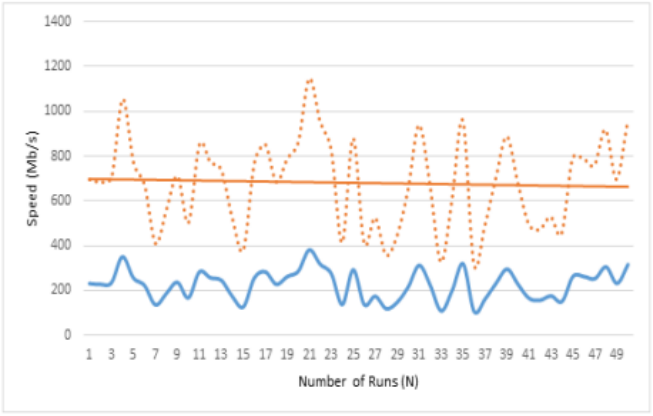

Рис. 3.18. Коефіцієнт посилення (M) дорівнює трьом

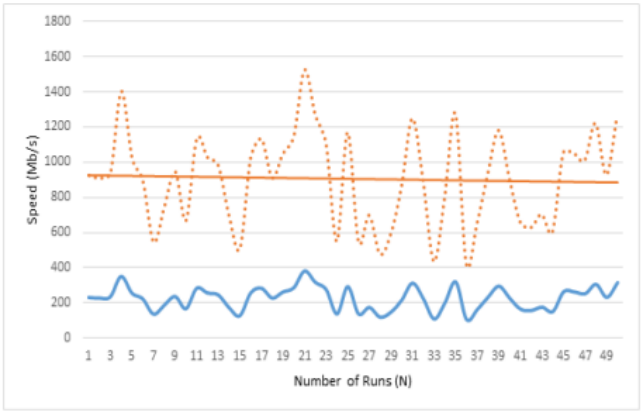

Рис. 3.19. Коефіцієнт посилення (M) дорівнює чотирьом

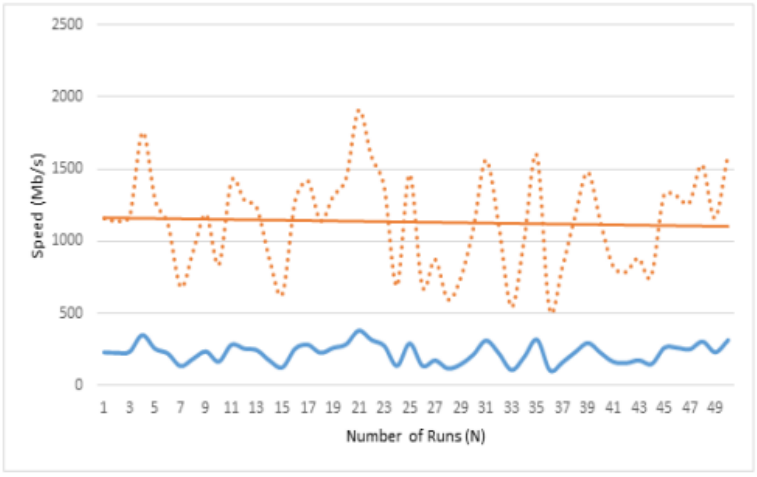

Рис. 3.20. Коефіцієнт посилення (M) дорівнює п’ять

Графіки вище показують наступні факти: при M = 2 максимальна швидкість майже доторкається лінії тренду порогу атаки, що може спричинити помилкові

спрацювання при різкому збільшенні законного трафіку. При M = 4 і M = 5 поріг є надмірно високим, що може призвести до невизнання законних атак. При M = 3 лінія тренду знаходиться в оптимальному положенні як поріг атаки, зменшуючи помилкові спрацювання і одночасно виявляючи багато атак.

Експерименти третього рівня

Експеримент 14: Обчислення моделі поведінки

Команда *php trafficgenerate.php* 100 10 на VM7 (192.168.0.138) генерує 100 запитів до цільового веб-сайту з інтервалом від 1 до 10 мс. Значення A1 для обчислення потребують P (сторінки на візит), T (час на сайт), V (нові відвідувачі) і B (коефіцієнт відскоку), які можна отримати з журналу доступу до веб-сайту за допомогою команди *php grepaccesslog.php.*

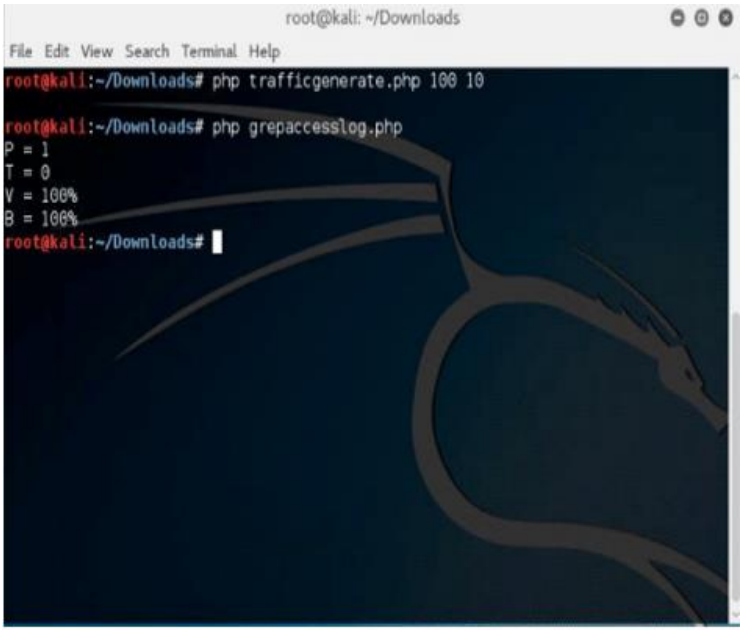

Рис. 3.21. Результати команди *grepaccesslog*

Використання цих значень у формулі показує, що всі умови для A1 виконуються, тому A1 = 1.

Експеримент 15: Обчислення даних програми

З використанням *javascript* скрипту, система може розрахувати час відповіді сторінок цільового веб-сайту. Скрипт запускається з браузера клієнта, повертаючи значення 0,1 мс (рисунок 3.22). Це стрімко зменшується до нуля, тому A2 = 0.

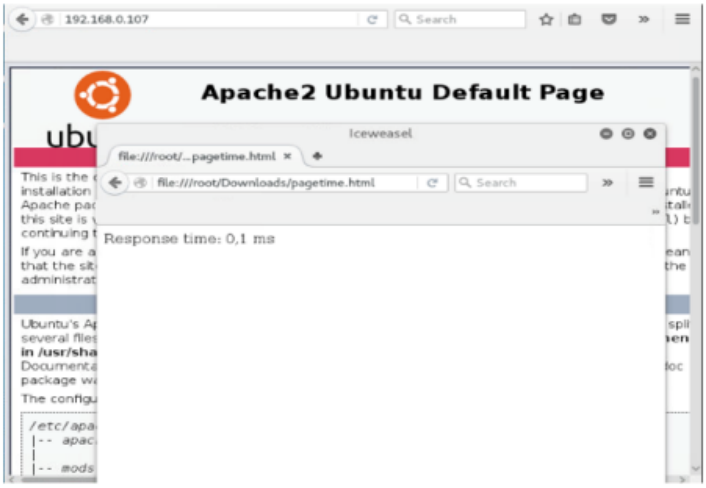

Рис. 3.22. Час відгуку цільових сторінок веб-сайту

Використання результатів експериментів 3, 4, 5, 6 для отримання значень змінних трафіку і знаходження всіх змінних, що мають значення TRUE, призводить до RT = 1.

Формула для RP використовується для знаходження значення, взявши значення S з експерименту 12 та встановивши його на рівень 231,6 Мб/с:

1 / (1 / (0.1 * 231.6)) * 100 = 2,316 %

A3 спрацьовує, коли RP >= 100%; у цьому випадку A3 = 1.

Отримана формула для A, яка вказує, чи є активна атака, складається з логічного оператора AND для A1, A2 та A3, відповідно встановлених як 1 AND 0 AND 1 = 0. Отриманий результат оператора AND дає A = 0, що означає, що атака не проводиться. Цей висновок є правильним, оскільки тест імітував високу швидкість, генеруючи IP-адреси, які викликали змінні трафіку TRUE, але не впливали на продуктивність цільового веб-сайту.

Експерименти четвертого рівня

Експеримент 17: Диспетчер зменшує швидкість руху

Результати третього рівня показують, що цільовий сайт зазнає високої швидкості, але атаки не відбувається. Четвертий рівень повинен бути здатний вирішити проблему високої швидкості. За допомогою програми на мові C на стороні Диспетчера система генерує наступні значення швидкості порівняно з найвищими значеннями з Експерименту 12: 100 IP з високою швидкістю.

Таблиця 3.5

Порівняння швидкості між експериментами 12 і 17

Exp. 12	Exp. 17	Exp. 12	Exp. 17
231.6	114	174.8	70
227.8	169	119.4	60
235.2	69	148.2	64
351.2	128	216.2	192
256.3	168	312.7	122
223.6	156	223.7	130
136.6	190	109.1	161
187.4	109	200.6	131
236.9	95	319.4	199
167.4	160	106.3	141
283.7	182	162.6	100
257.3	101	233.5	189
245.7	179	295.6	63
173.7	136	227.4	135
127.3	76	165.4	161
256.5	177	157.3	185
283.7	164	176.3	188
228.2	193	151.6	141
262.7	174	263.7	133
286.7	63	262.6	65
381.7	105	253.3	130
317.3	171	305.7	97
276.1	106	232.1	198
137.9	151	315.9	104
292.8	85	137.5	178

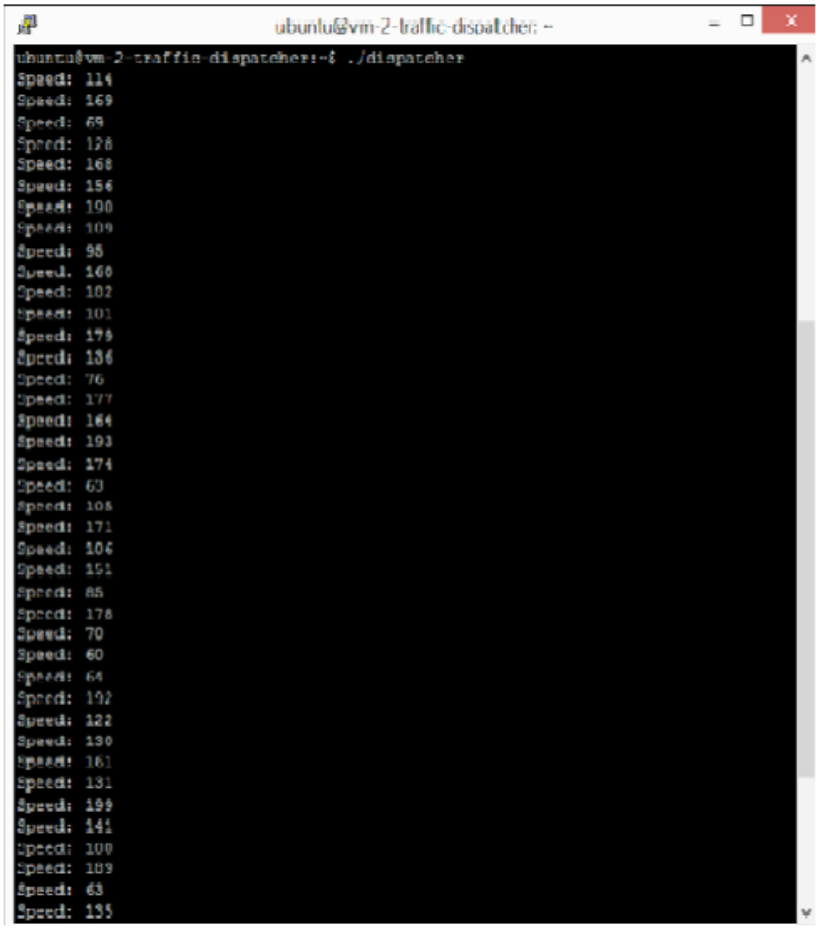

Рис. 3.23. Результати диспетчерської швидкості

Рис. 3.24. Порівняння швидкості між експериментами 12 і 17

Рисунок 3.24 графічно зображує результати обох експериментів: експеримент 12 позначений синьою, а експеримент 17 червоною кольорами.

Графічне зображення чітко показує, що швидкість знизилась, коли було активовано Диспетчера.

Експерименти п’ятого рівня

Експеримент 18: Розрахунок номера порту

З використанням програми на мові С на боці Диспетчера, система бере перші двадцять п'ять результатів і запускає скрипт протягом п'яти раундів, забезпечуючи, що значення не повторюються та не можуть бути легко відновлені зловмисним користувачем.

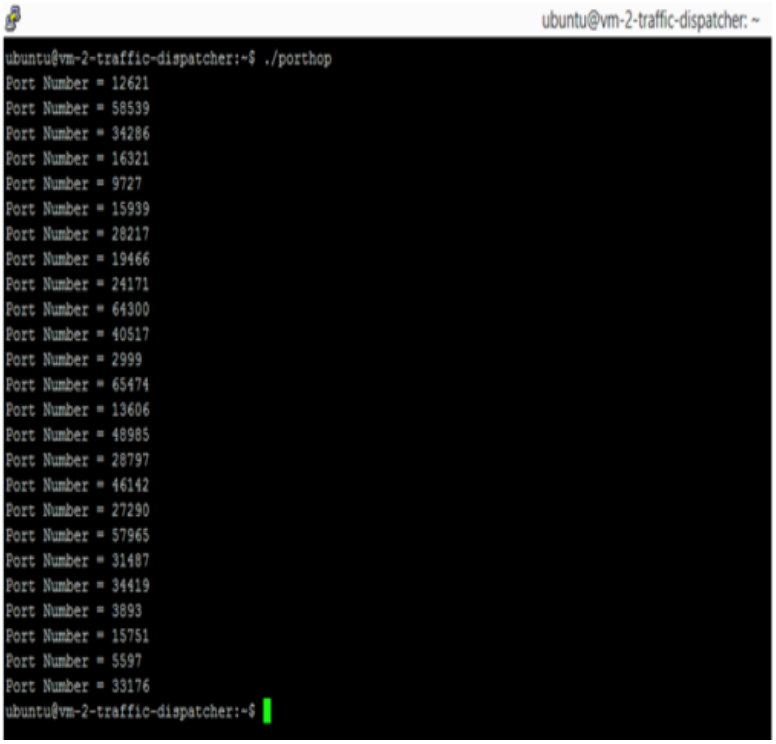

Рис. 3.25. Результати розрахунку стрибків портів

Рисунок 3.25 показує результати в командному рядку. Для більш детального аналізу дивіться таблицю .

Таблиця 3.6

Результати порт-хопінгу протягом п'яти раундів

Time /t (s)	P (1)	P (2)	P (3)	P (4)	P (5)
T	12621	14107	47958	62763	15057
1	58539	37518	40469	24220	4608
2	34286	34090	10488	37057	63686

Продовження таблиці 3.6

Результати порт-хопінгу протягом п'яти раундів

Time /t (s)	P (1)	P (2)	P (3)	P (4)	P (5)
3	16321	2744	10060	24956	29071
4	9727	37539	7897	63236	27461
5	15939	6700	7236	22802	57240
6	28217	21450	49327	41906	11600
7	19466	13322	6605	52758	17233
8	24171	56651	14982	7540	47162
9	64300	25530	48335	44576	55800
10	40517	23939	16152	54368	49607
11	2999	3712	25676	56480	41657
12	65474	29948	48927	48912	49
13	13606	63866	9533	31654	33922
14	48985	22039	40669	19382	55303
15	28797	49897	25294	47075	43959
16	46142	3947	58108	32356	11055
17	27290	12551	11060	64173	1956
18	57965	4298	27377	32600	12194
19	31487	42940	15465	12658	15732
20	34419	39770	40275	60113	7051
21	3893	49502	26684	54589	56165
22	15751	49609	39277	15192	33183
23	5597	47089	24037	4075	48499
24	33176	8107	34047	9460	39228

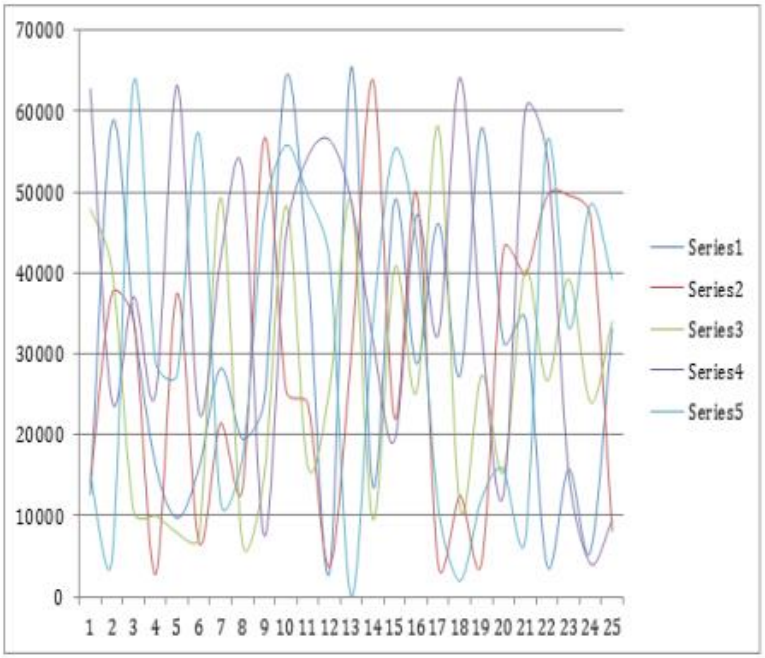

Рис. 3.25. Графічне зображення ефективності порт-хопінгу.

На рисунку 3.25 зображено п'ять серій з п'яти раундів завершення скрипту. Номери портів показані як повністю переплетені, що дає підстави стверджувати, що номер порту не може бути легко вгаданий зловмисним користувачем. Атакувальник може знати формулу, але не може знати синхронізаційні цикли між диспетчером та цільовим веб-сайтом.

Експерименти зі загальною роботою системи.

Експеримент 19: Виявлення та запобігання DDoS-атак - низька швидкість.

На VM6 запускаються два сценарії:

php routeriptb.php

php trafficgenerate.php 100 10

На VM 7 запускається один сценарій:

php trafficgenerate.php 100 10

Один сценарій виконується на VM8:

php trafficgenerate.php 100 10

Один сценарій виконується на VM9:

php trafficgenerate.php 100 10

Один сценарій виконується на VM10:

php trafficgenerate.php 100 10

На VM2 запускаються три сценарії:

./dispatcher

./porthop

php ti.php

Результатом запобігання та виявлення атак є створення правил брандмауера, які блокують вхідні атаки. Файл *ipfw.rules* повинен бути спочатку порожнім, як підтверджується.

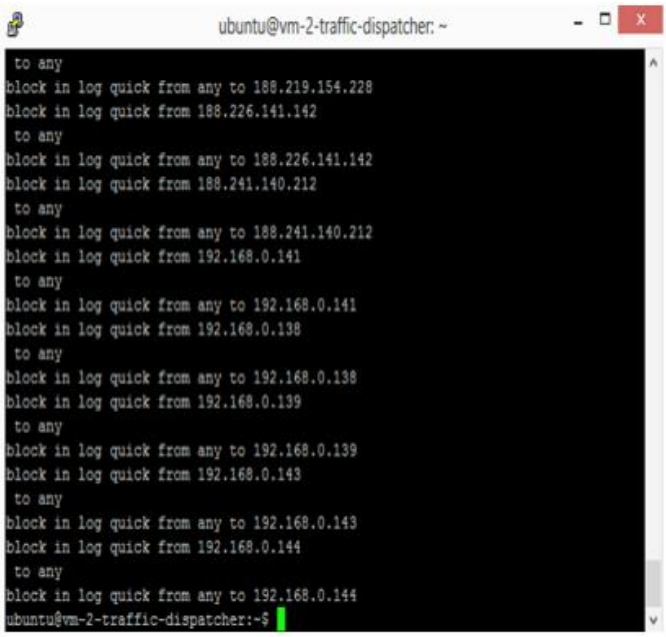

Рис. 3.26. Високошвидкісна перевірка правил брандмауера

Лишаються тільки останні результати, як показано на рисунку 3.26. Ми залишаємо тільки останні результати, які стосуються VM6 - VM10:

block in log quick from 192.168.0.141 to any

block in log quick from any to 192.168.0.141

block in log quick from 192.168.0.138 to any

block in log quick from any to 192.168.0.138

block in log quick from 192.168.0.139 to any

block in log quick from any to 192.168.0.139

block in log quick from 192.168.0.143 to any

block in log quick from any to 192.168.0.143

block in log quick from 192.168.0.144 to any

block in log quick from any to 192.168.0.144

Це підтверджує бажаний результат, і атака успішно виявлена і заблокована.

Порівняння методів

Запропонований метод використовує 6 технологій: IP-трасування, Threat Intelligence, аналіз поведінки, управління репутацією, розподіл трафіку і перехід по портах. Інші методи використовують лише 1 технологію.

Метод є повністю автоматизованим, не потребує дій користувача. IP-трасування, перехід по портах і виявлення аномалій можуть бути автоматизовані.

У експерименті були проведені 10 запусків з різними налаштуваннями. Запропонований метод не показав жодних хибнопозитивних результатів. Один із методів показав 0% хибнопозитивних результатів, але вимагає втручання оператора для визначення наявності атаки. Інший метод зменшує наслідки атаки, але не виявляє її наявність. Існує 20% ймовірність помилкового виявлення атаки для третього методу.

В цілому, запропонований метод є ефективним і повністю автоматизованим, забезпечуючи низький рівень хибнопозитивних результатів. Проте, інші методи мають свої обмеження, такі як необхідність втручання оператора або можливість помилкового виявлення атаки.

Виконання скриптів без навантаження не впливає на продуктивність сервера. У експерименті 7 було показано, що це не має впливу на час відповіді цільового веб-сайту 192.168.0.107, який був виміряний за допомогою пінгу. Середній час відгуку становить 0,328 мс.

Експеримент 19 проводився для дослідження низького навантаження. Було запущено скрипти на VM6 та VM2, а після цього виміряний час відповіді цільового веб-сайту. Запропонований метод мав середній час відгуку 0,346 мс, перший метод - 0,564 мс, другий метод - 0,287 мс, а третій метод - 0,334 мс.

Експеримент 20 був проведений для вивчення часу відгуку цільового сервера при нормальному навантаженні. Було запущено скрипти на VM6, VM7 та VM2, і було виміряні різні часи відгуку для запропонованого методу та інших трьох методів (метод 1, метод 2, метод 3), які були позначені відповідними кольорами на рисунку 3.28 та таблиці 7.

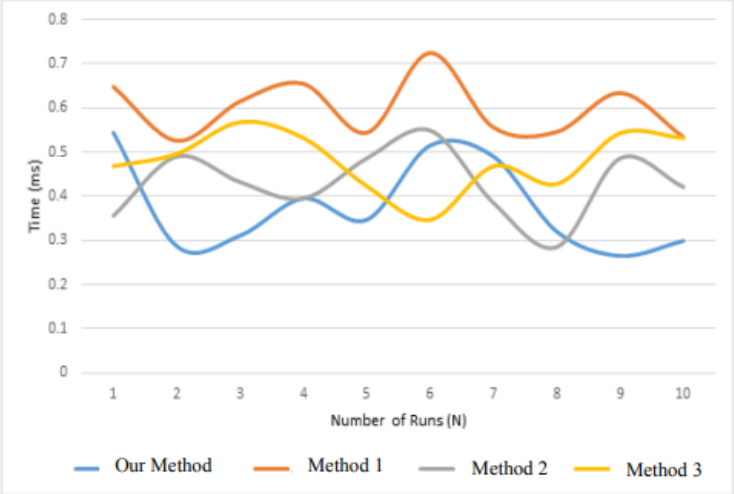

Рис. 3.27. Час відгуку цілі при нормальному навантаженні

Таблиця 3.7

Порівняння часу відгуку методу нормального навантаження

Завантаження	Обраний Метод	Метод 1	Метод 2	Метод 3
1	0.544	0.648	0.356	0.468
2	0.287	0.526	0.490	0.496
3	0.311	0.615	0.432	0.568
4	0.395	0.655	0.395	0.532
5	0.347	0.544	0.486	0.423
6	0.515	0.725	0.549	0.347
7	0.490	0.556	0.385	0.468
8	0.320	0.546	0.285	0.428

Продовження таблиці 3.7

Порівняння часу відгуку методу нормального навантаження

Завантаження	Обраний Метод	Метод 1	Метод 2	Метод 3
9	0.265	0.634	0.486	0.543
10	0.299	0.534	0.421	0.532
Середнє	0.377	0.598	0.429	0.481

В експерименті 21 досліджується час відповіді цільової системи на високому навантаженні.

Дані, зображені на Рисунку 3.28 та в Таблиці 3.8, представляють різні часи відповіді. Синій колір представляє запропонований метод, червоний - метод 1, сірий - метод 2, а помаранчевий - метод 3.

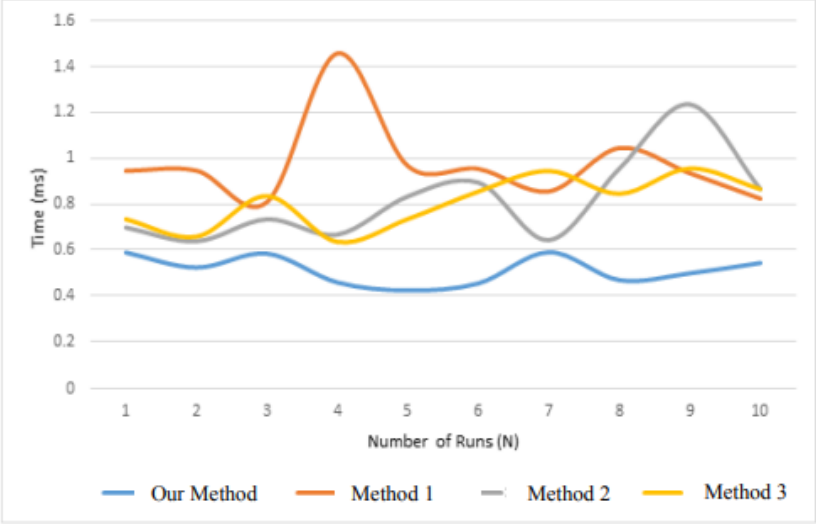

Рис. 3.28. Час відгуку цілі на високе навантаження

Таблиця 3.8

Порівняння часу відгуку методу високого навантаження

Завантаження	Обраний метод	Метод 1	Метод 2	Метод 3
1	0.589	0.945	0.698	0.734
2	0.523	0.946	0.638	0.658
3	0.584	0.809	0.734	0.835
4	0.458	1.458	0.667	0.635
5	0.423	0.966	0.834	0.735
6	0.454	0.954	0.894	0.855
7	0.590	0.856	0.643	0.945
8	0.468	1.045	0.955	0.845
9	0.498	0.935	1.235	0.956
10	0.543	0.824	0.866	0.865
Середнє	0.513	0.974	0.816	0.806

3.3. Розробка рекомендацій щодо захисту інформаційної системи організацій від DDoS атак

Рекомендації щодо захисту інформаційної системи організацій від DDoS атак базуються на наступних пунктах:

1. *Аналіз потенційних загроз*: Рекомендується провести детальний аналіз потенційних DDoS-загроз, які можуть вплинути на інформаційну систему організації. Це допоможе ідентифікувати можливі вразливості та слабкі місця, що можуть бути використані атакаторами.

2. *Встановлення системи моніторингу:* Рекомендується встановити систему моніторингу трафіку, яка буде виявляти аномальну активність та попереджати про потенційні DDoS-атаки. Це дозволить вчасно реагувати на загрози та приймати відповідні заходи.

3. *Використання розподіленого хостингу*: Рекомендується розглянути можливість використання розподіленого хостингу, який забезпечує розподілення навантаження між декількома серверами. Це допоможе уникнути перевантаження та забезпечити нормальну роботу системи під час DDoS-атаки.

4. *Встановлення спеціалізованих систем захисту*: Рекомендується встановити спеціалізовані системи захисту від DDoS, які здатні виявляти та мінімізувати наслідки атак. Ці системи можуть використовувати методи аналізу трафіку, фільтрації та розподіленої обробки запитів для забезпечення нормальної роботи системи.

5. *Забезпечення резервного копіювання та відновлення*: Рекомендується розробити процедури регулярного резервного копіювання інформації та відновлення системи в разі атаки. Це дозволить зменшити втрати даних та мінімізувати період простою системи після атаки.

6. *Планування і навчання персоналу*: Рекомендується розробити план дій у разі DDoS-атаки та провести навчання персоналу з використанням цього плану. Це допоможе забезпечити швидку реакцію та ефективність заходів при атаках.

7. *Оновлення програмного забезпечення*: Рекомендується регулярно оновлювати програмне забезпечення, включаючи операційну систему, серверне програмне забезпечення та застосунки. Це допоможе усунути вразливості, які можуть бути використані атакаторами.

8. *Співпраця з провайдерами послуг*: Рекомендується співпрацювати з провайдерами послуг IT-безпеки, які можуть надавати захист від DDoS-атак на рівні мережі. Це дозволить забезпечити додатковий рівень захисту та вчасну реакцію на атаки.

9. *Проведення планових аудитів безпеки*: Рекомендується регулярно проводити аудит безпеки системи з метою виявлення потенційних вразливостей та удосконалення системи захисту. Це дозволить підтримувати систему на актуальному рівні безпеки.

10. *Усвідомлення персоналом*: Рекомендується проводити навчання персоналу організації щодо DDoS-атак, їх потенційних наслідків та методів

захисту. Це допоможе залучити персонал до процесу безпеки та забезпечити колективний внесок у захист системи.

Враховуючи ці рекомендації, організації зможуть забезпечити ефективний рівень захисту їх інформаційних систем від DDoS-атак. Перед їх впровадженням рекомендується провести детальний аналіз потреб і можливостей організації та підібрати найбільш оптимальні рішення для їх виконання.

Висновок до розділу

Враховуючи усі наведені вище відомості, можна зробити наступні висновки щодо загальної продуктивності всіх розглянутих методів:

Запропонований метод: відмінний. Він не залежить від підписів і здатний ефективно виявляти невідомі загрози.

Метод 1: хороший. Він також не залежить від підписів і здатний виявляти невідомі загрози.

Метод 2: хороший. Він не залежить від підписів і може успішно виявляти невідомі загрози.

Метод 3: хороший. Він також не залежить від підписів і має здатність виявляти невідомі загрози.

Отже, всі розглянуті методи демонструють добру продуктивність і мають здатність ефективно протистояти різноманітним загрозам без потреби в підписах.

ВИСНОВКИ

В результаті дослідження було встановлено, що DDoS-атаки є серйозною загрозою для інформаційної безпеки організацій. У рамках роботи було проаналізовано та порівняно чотири методи захисту від таких атак: метод 1 - захист на основі відслідковування IP, метод 2 - захист на основі фільтрації портів, метод 3 - захист на основі виявлення аномалій, та запропонований метод, що використовує Threat Intelligence.

В результаті порівняння було встановлено, що запропонований метод є найбільш ефективним, оскільки він забезпечує захист від різних видів атак, включаючи невідомі атаки, та може здійснювати фільтрацію як в середині організації, так і на зовнішніх ресурсах. Метод 1 також виявився досить ефективним, але його практична реалізація може бути досить складною через потребу внесення змін до апаратного забезпечення. Методи 2 та 3 також є ефективними, але менш прогресивними порівняно з запропонованим методом.

Отже, дослідження показало, що для ефективного захисту інформаційної системи від DDoS-атак необхідно використовувати комплексний підхід, який включає в себе застосування різних методів захисту, забезпечення резервного копіювання даних та навчання співробітників. Запропонований метод на основі Threat Intelligence є найбільш ефективним та прогресивним серед розглянутих, тому рекомендується його використовувати в організаціях для захисту інформаційних ресурсів від DDoS-атак.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Bhattacharyya S., Kalita J. K., Kar S. A review of DDoS attack and its mitigation techniques. International Journal of Computer Science and Network Security : International Journal, 2016. URL: https://www.researchgate.net/publication/309640905_Field_dependence_of_polarization_in_polyvinylidene_fluoride_derived_from_quasi-stationary_poling_currents (дата звернення: 01.05.2023).

2. Shen X., Huang Y. A survey on DDoS attacks and defense mechanisms in cloud computing: навчальний посібник. Journal of Network and Computer Applications, 2016. URL: https://www.sciencedirect.com/science/article/pii/S108480451630022X (дата звернення: 01.05.2023).

3. Al-Fayoumi M. A., Ababneh O. I., Jararweh Y. A comprehensive survey on DDoS attacks and their mitigation techniques: підручник. Journal of Network and Computer Applications, 2017. 88 с. URL: https://www.sciencedirect.com/science/article/pii/S1084804517300433 (дата звернення: 01.05.2023).

4. Islam M. R., Khatun F., Bhuiyan M. Z. A. DDoS attack and its defense mechanism : навч. посіб. . In 2018 IEEE 4th International Conference on Computer and Communications (ICCC), 2018. 113 с. URL: https://ieeexplore.ieee.org/abstract/document/8478347(дата звернення: 01.05.2023).

5. Zhang S., Wang H., Wen Y. A novel DDoS attack detection method based on anomaly score and clustering analysis: навч. посіб. Security and Communication Networks, 2019. 25 с. URL: https://www.researchgate.net/publication/357899357_A_novel_LDoS_attack_detection_method_based_on_reconstruction_anomaly (дата звернення: 01.05.2023).

6. Singh M., Singh K., Kumar R. Detection and mitigation of ddos attack: a survey.: навч. посіб. In Proceedings of the 4th International Conference on Frontiers in

Intelligent Computing, 2017. 90 с. URL: https://www.sciencedirect.com/science/article/pii/S1877050916305014 (дата звернення: 01.05.2023).

7. Wang R., Duan Z. A DDoS attack detection method based on machine learning: навч. посіб. Journal of Ambient Intelligence and Humanized Computing, 2017. 620 с. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1237/3/032040 (дата звернення: 01.05.2023).

8. Chen J., Zhang W., Xie L. A hybrid model for ddos attack detection based on clustering and SVM.: навч. посіб. Future Generation Computer Systems, 2019. 962 с. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9142183 (дата звернення: 01.05.2023).

9. Xu B., Xu C., Yang J. A survey on DDoS attacks and defense mechanisms in software-defined networkin: підручник. IEEE Access, 5, 21017-21028., 2017. 520 с. URL: https://www.sciencedirect.com/science/article/pii/S0167739X21000911 (дата звернення: 01.05.2023).

10. Arshi M., Nasreen M. A survey of DDOS attacks using machine learning techniques. E3s-conference. 2020. Т. 1, № 1. С. 6. URL: https://www.e3s-conferences.org/articles/e3sconf/pdf/2020/44/e3sconf_icmed2020_01052.pdf (дата звернення: 01.05.2023).

11. Tariq E. A., Chong Y.-W., Manickam S. Machine learning techniques to detect a ddos attack in SDN: a systematic review : навч. посіб. National Advanced IPv6 Centre, Universiti Sains Malaysia, Gelugor 11800, Penang, Malaysia: Universiti Sains Malaysia, 2023. 3183 с. URL: https://www.mdpi.com/2076-3417/13/5/3183 (дата звернення: 01.05.2023).

12. Kamal A., Raju G. A study on ddos attacks, detection techniques and mitigation mechanisms.: курс лекцій. Journal of Network and Computer Applications, 2018. 113 p. URL: https://www.researchgate.net/publication/261020917_DDoS_Attack_detection_method_and_mitigation_using_pattern_of_the_flow (дата звернення: 01.05.2023).

13. Alazab M., Aslam B., Abawajy M. Detection and mitigation techniques for distributed denial of service attacks: a survey.: курс лекцій / ред. J. Hobbs. Security and Communication Networks, 2018. 20 с. URL: https://pdf.sciencedirectassets.com/280203/1-s2.0-S1877050916X00117/ (дата звернення: 01.05.2023).

14. Wang W., Sun Y., Huang X. An efficient deep learning approach for DDoS attack detection in edge computing: підручник. Future Generation Computer Systems, 2021. 116 с. URL: https://www.mdpi.com/1999-5903/15/2/76 (дата звернення: 01.05.2023).

15. Zhang W., Chen J. A new feature selection method based on enhanced genetic algorithm for DDoS attack detection: навч. посіб. IEEE Access, 8, 2020. 520 с. URL: https://www.sciencedirect.com/science/article/abs/pii/S0957417423009065 (дата звернення: 01.05.2023).

16. Huang X., Li K., Li X. A new detection method for DDoS attacks based on SVM optimized by artificial bee colony algorithm: навч. посіб. 3-тє вид. Peer-to-Peer Networking and Applications, 2021. 950 с. URL: https://www.diva-portal.org/smash/get/diva2:1735253/FULLTEXT01.pdf (дата звернення: 01.05.2023).

17. Bhattacharyya S., Kalita J. K., Kar S. A review of DDoS attack and its mitigation techniques: навч. посіб. International Journal of Computer Science and Network Security, 2016. 312 с.
URL: https://www.researchgate.net/publication/348120039_Denial-of-Service_and_Botnet_Analysis_Detection_and_Mitigation (дата звернення: 01.05.2023).

Демонстраційні матеріали(Презентація)