МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ЗАХИСТУ ВІД АТАК ТИПУ "ВІДМОВА В ОБСЛУГОВУВАННІ" (DOS/DDOS) У КОРПОРАТИВНИХ МЕРЕЖАХ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Марк КАНЕВЕЦЬКИЙ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Марк КАНЕВЕЦЬКИЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Віталій САВЧЕНКО
д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент: _____
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Каневецькому Марку Олександровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи захисту від атак типу "відмова в обслуговуванні" (DOS/DDOS) у корпоративних мережах”,
керівник кваліфікаційної роботи САВЧЕНКО Віталій, д.т.н., професор,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *програмний комплекс для віртуалізації, інструменти проведення DDoS атак, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Аналіз поняття безпеки мережі
4.2. Дослідження поширених атак в відмові обслуговування та способи їх виявлення.
4.3. Розроблення рекомендацій щодо реалізації захисту від атак на відмову в обслуговуванні в корпоративних мережах.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	05.03.2025	
2.	Збір та аналіз літератури.	10.03.2025	
3.	Аналіз впливу атак на відмову в обслуговуванні на корпоративні мережі	05.04.2025	
4.	Аналіз алгоритму роботи інструментів для проведення атак на відмову в обслуговуванні.	08.04.2025	
5.	Дослідження методів для захисту корпоративної мережі від DDoS-атак	15.04.2025	
6.	Реалізація DDoS-атак в тестовому середовищі	25.04.2025	
7.	Оформлення роботи.	05.05.2025	
8.	Оформлення презентації.	08.05.2025	
9.	Отримання рецензії на роботу.	10.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ Марк КАНЕВЕЦЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Каневецький М.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Методи захисту від атак типу "відмова в обслуговуванні" (DOS/DDOS) у корпоративних мережах”

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КАНЕВЕЦЬКИЙ Марк у кваліфікаційній роботі проаналізував методи захисту від атак типу “Відмова в обслуговуванні“ (DoS/DDoS) у корпоративних мережах, дослідив основні характеристики таких атак, їхні механізми реалізації та наслідки. Він вивчив сучасні підходи до виявлення та нейтралізації DoS/DDoS-атак, проаналізував ефективність різних технологій захисту, а також розробив практичні рекомендації для підвищення рівня кібербезпеки корпоративних мереж.

КАНЕВЕЦЬКИЙ Марк продемонстрував глибоке розуміння проблеми дослідження, володіння теоретичними та практичними методами її вирішення, застосував науковий підхід у своїй роботі, а також проявив себе як організований і відповідальний виконавець. Результати його дослідження були апробовані на двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КАНЕВЕЦЬКОГО Марка на оцінку “відмінно“ та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою “Управління інформаційною та кібернетичною безпекою“.

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Каневецький М.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КАНЕВЕЦЬКОГО Марка
на тему “Методи захисту від атак типу "відмова в обслуговуванні" (DOS/DDOS) у корпоративних мережах”

Актуальність. У сучасному світі, де компанії, державні установи та інші організації активно використовують корпоративні мережі, атаки типу "Відмова в обслуговуванні" (DoS/DDoS) стають серйозною загрозою. Такі атаки можуть спричинити значні фінансові втрати, зниження продуктивності та порушення критично важливих бізнес-процесів. З постійним розвитком технологій кіберзахисту, а також удосконалення методів атак зловмисників, важливо досліджувати та впроваджувати ефективні стратегії протидії DoS/DDoS-атакам.

З огляду на зазначене, дослідження проблеми захисту від атак типу DoS/DDoS у корпоративних мережах є актуальним науковим завданням..

Позитивні сторони.

1. У роботі досліджено особливості сучасних методів захисту від атак типу "Відмова в обслуговуванні" (DoS/DDoS) у корпоративних мережах, розглянуто ефективність різних технологій виявлення та запобігання таким атакам.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено згідно з планом, зроблено логічні висновки. Ключові положення роботи представлені у вигляді рисунків та схем.
3. Автор опрацював значну джерельну базу: близько 26 публікацій, зокрема англомовних, що дозволило здійснити глибокий аналіз сучасних підходів до кіберзахисту.
4. За результатами дослідження запропоновано рекомендації щодо підвищення ефективності методів захисту корпоративних мереж від DoS/DDoS-атак.

Недоліки.

Доцільно було б приділити більше уваги детальному аналізу та класифікації програмних і апаратних засобів захисту від атак типу "Відмова в обслуговуванні" (DoS/DDoS), а також оцінці їхньої ефективності у різних сценаріях кібератак.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач КАНЕВЕЦЬКИЙ Марк заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технік виявлення та пом’якшення впливу DDoS-атак у корпоративних мережах. Робота складається зі вступу, чотирьох розділів, що містять 26 рисунків, 4 таблиці, висновків і списку використаних джерел із 42 найменувань. Загальний обсяг роботи становить 81 аркуш, з яких 5 аркушів займає список використаних джерел.

Метою роботи є розробка рекомендацій щодо підвищення ефективності виявлення та протидії DDoS-атакам у корпоративному середовищі.

Об’єктом дослідження є атаки на відмову в обслуговуванні.

Предметом дослідження є техніки виявлення та способи пом’якшення впливу DDoS-атак на корпоративні мережі.

Методи дослідження. Опрацьовано технічну літературу за темою, проведено аналіз експлуатаційної документації, тестування інструментів та порівняльний аналіз сервісів.

Короткий зміст роботи. У роботі проаналізовано поняття DDoS-атак та їх вплив на безпеку корпоративних мереж. Наведено класифікацію типів атак: на мережеві ресурси, серверні ресурси та програмні системи. Виділено два основні підходи до виявлення атак: сигнатурний та поведінковий. Досліджено можливості сучасних інструментів для здійснення та протидії атакам типу «відмова в обслуговуванні». На основі результатів дослідження розроблено рекомендації щодо захисту корпоративної мережі із застосуванням відповідних сервісів.

Галузь застосування. Отримані результати можуть бути використані для побудови або вдосконалення систем виявлення DDoS-атак у сфері корпоративної кібербезпеки.

Ключові слова: КІБЕРБЕЗПЕКА, МЕРЕЖА, БЕЗПЕКА МЕРЕЖІ, BOTNET, DDOS, НЕСАНКЦІОНОВАНЕ ВТРУЧАННЯ, ВІДМОВА В ОБСЛУГОВУВАННІ, КІБЕРАТАКА.

ABSTRACT

The bachelor's qualification paper is devoted to the study of techniques for detecting and mitigating the impact of DDoS attacks on corporate networks. The paper consists of an introduction, four chapters containing 26 figures and 4 tables, conclusions, and a list of 42 references. The total volume of the work is 81 pages, including 5 pages of references.

***The aim of the rese*arch** is to develop recommendations to improve the efficiency of DDoS detection and mitigation in corporate environments.

The object of the study is denial-of-service (DoS) attacks.

The subject of the study is the techniques for detecting and mitigating DDoS attacks in corporate networks.

Research methods. The research includes literature review, analysis of technical documentation, tool testing, and comparative analysis of protection services.

Summary of the work. The paper examines the concept of DDoS attacks and their impact on corporate network security. It outlines the classification of DDoS attack types, including network-level, server-targeted, and application-level attacks. Two main detection approaches are highlighted: signature-based and behavior-based. The capabilities of tools used for launching and countering denial-of-service attacks are explored. Based on the research findings, recommendations are developed for implementing protection measures against DDoS attacks in corporate networks.

Field of application. The results can be applied to build or improve DDoS detection systems in corporate cybersecurity infrastructures.

Keywords: CYBERSECURITY, NETWORK, NETWORK SECURITY, BOTNET, DDOS, UNAUTHORIZED ACCESS, DENIAL OF SERVICE, CYBERATTACK.

ЗМІСТ

ВСТУП

На сьогоднішній день Інтернет є невід'ємною частиною життя понад мільярда людей, забезпечуючи доступ до інформації, виконання фінансових операцій, онлайн-покупок та інших важливих функцій. Соціальні мережі стали важливим інструментом для бізнесу та організацій у просуванні бренду, побудові взаємин із клієнтами та забезпеченні стабільного доходу. Однак разом із перевагами цифрових технологій виникають і ризики, серед яких особливу загрозу становлять технічні збої.

Атаки на доступність, зокрема DDoS (розподілені атаки відмови в обслуговуванні), є одними з найбільших викликів у сфері кібербезпеки. Такі атаки здійснюються через різні вектори, включаючи TCP, HTTP/S, низькошвидкісні методи, а також уразливості SSL, і спрямовані на порушення нормальної роботи веб-сайтів. Наслідки DDoS-атак можуть бути руйнівними: простої сервісів, витоки даних, фінансові втрати та зниження репутації компаній.

Згідно з дослідженнями компанії Corero Network Security, у третьому кварталі 2021 року кількість DDoS-атак на організації у світі сягала 237 спроб щомісяця, що в середньому становить 8 атак щодня. Цей показник зріс на 35% у порівнянні з попереднім кварталом та майже на 91% порівняно з початком року. Інша аналітика, проведена Incapsula, вказує, що середня вартість простою через DDoS-атаку може сягати $40 000 за годину. Короткочасні перебої здатні спричинити значні фінансові втрати, зниження довіри клієнтів та репутаційні ризики.

Об’єкт дослідження – атаки на відмову в обслуговуванні.

Предмет дослідження – техніки виявлення та пом’якшення впливу DDoS атак на корпоративні мережі.

Мета роботи – розробка рекомендацій щодо підвищення ефективності виявлення та протидії DDoS-атак в корпоративній мережі.

Методи дослідження – опрацювання технічної літератури за темою, аналіз експлуатаційної документації, проведення тестування інструментів, порівняльний аналіз сервісів.

В роботі проаналізовано поняття DDoS та розкрито питання актуальності і важливості безпеки мережі. Досліджено класифікація типів DDoS-атак.

Проаналізовано основні типи атак націлених на мережеві ресурси, на ресурси сервера та атаки, які спрямовані на ресурси програм. Виокремлено два основних метода для ефективного для своєчасного виявлення атак на відмову в обслуговуванні.

Досліджено основні можливості інструментів для проведення атак на відмову в обслуговуванні.

На основні досліджень проведених в роботі, розроблено рекомендації щодо застосування сервісів для захисту від атак на відмову в обслуговуванні.

Завдання бакалавської роботи:

1. Проаналізувати поняття DDoS-атак та обґрунтувати їхню актуальність у сучасному інформаційному просторі.
2. Вивчити та класифікувати основні типи атак на відмову в обслуговуванні (на мережеві ресурси, серверні ресурси та програмні ресурси).
3. Провести огляд сучасних методів та інструментів для виявлення та пом'якшення впливу DDoS-атак.
4. Визначити два основних методи, які забезпечують своєчасне виявлення атак на відмову в обслуговуванні.
5. Дослідити функціональні можливості існуючих інструментів для імітації та аналізу DDoS-атак.
6. Розробити рекомендації для підвищення ефективності виявлення та захисту від атак на відмову в обслуговуванні в корпоративних мережах.

Методи дослідження:

– Аналіз наукової та технічної літератури з питань кібербезпеки та протидії DDoS-атакам.

– Вивчення експлуатаційної документації сучасних сервісів та інструментів кіберзахисту.

– Проведення практичного тестування програмних рішень для виявлення та пом'якшення атак.

– Порівняльний аналіз функціональних можливостей різних інструментів захисту.

Практичне значення одержаних результатів:

- Результати роботи мають прикладний характер і можуть бути використані для:
- Розробки стратегії захисту корпоративних мереж від DDoS-атак.
- Впровадження ефективних інструментів виявлення атак на відмову в обслуговуванні в інформаційних системах підприємств.
- Підвищення рівня кібербезпеки організацій за рахунок застосування запропонованих рекомендацій.
- Навчання фахівців із кібербезпеки основним методам протидії DDoS-атакам.

Нещодавно такі популярні веб-сайти, як Spotify, Twitter, Netflix і PayPal, стали об'єктами атак типу «відмова в обслуговуванні» (DDoS). Протягом кількох днів вони зазнавали масованих атак, під час яких хакери створювали величезний потік хибного трафіку, паралізуючи доступ користувачів до ресурсів. Унаслідок цього сайти залишалися недоступними годинами, що завдало значних фінансових і репутаційних втрат. Ці випадки демонструють, наскільки серйозною стала загроза з боку зовнішніх зловмисників.

Паралельно з цим організації стикаються із внутрішніми загрозами. Співробітники або колишні працівники можуть навмисно чи ненавмисно створювати загрози, прагнучи отримати доступ до конфіденційної інформації, як-от зарплати колег або корпоративні дані. Таким чином, сучасні організації змушені одночасно боротися із зовнішніми та внутрішніми ризиками.

Щорічно корпорації, уряди та інші установи витрачають мільярди доларів на забезпечення безпеки мереж, і ці витрати постійно зростають.

Мережева безпека передбачає усунення загроз для комп’ютерної інфраструктури шляхом розробки та впровадження політик і процедур, що захищають цілісність, конфіденційність і доступність даних. Ефективна безпека мереж забезпечує не тільки технічний захист, але й довіру з боку користувачів та клієнтів.

Основні цілі мережевої безпеки:

1. Захист активів компанії.

Основним завданням безпеки є захист інформаційних активів, які є критично важливими для діяльності організації. Інформація повинна бути захищена від несанкціонованого доступу, змін і витоків.

2. Отримання конкурентної переваги.

Компанії, які забезпечують високий рівень безпеки, отримують довіру клієнтів, особливо в сфері фінансових послуг та електронної комерції. Наприклад, платформи з високим рівнем безпеки отримують більшу лояльність клієнтів у порівнянні з конкурентами.

3. Дотримання нормативних вимог.

РОЗДІЛ 1. АНАЛІЗ ВПЛИВУ DDoS-АТАК НА ЗАХИЩЕНІСТЬ МЕРЕЖ

1.1 Загальні аспекти мережевої безпеки

Корпоративні посадові особи зобов’язані розробляти політики, що відповідають вимогам кібербезпеки, забезпечуючи стабільну роботу організації та захист інвестицій акціонерів.

Збереження безперервності бізнесу.

Організація, що забезпечує надійний захист своїх активів, знижує ризик виникнення критичних збоїв, які можуть призвести до втрат прибутків або репутації.

Виклики забезпечення мережевої безпеки.

Ідеальним способом захисту є ізоляція комп’ютерів від зовнішніх мереж, але це практично неможливо в умовах сучасного світу, де обмін даними є необхідністю. Тому організації повинні впроваджувати технічні, організаційні та адміністративні заходи для мінімізації ризиків [1].

Основною метою мережевої безпеки є досягнення так званої тріади КЦД (конфіденційність, цілісність, доступність (рис. 1.1)):

– ***Конфіденційність.*** Інформація повинна бути доступною тільки авторизованим особам.

– ***Цілісність.*** Захист даних від несанкціонованих змін або видалення.

– ***Доступність.*** Гарантія доступу до даних та ресурсів тоді, коли це необхідно.

Практичні заходи захисту.

Для зменшення ризиків організації впроваджують такі рішення:

1. Використання міжмережевих екранів (файрволів) для контролю трафіку.
2. Системи виявлення та запобігання вторгненням (IDS/IPS).
3. Регулярне оновлення програмного забезпечення для усунення вразливостей.

4. Навчання персоналу основам кібербезпеки.

5. Використання багатофакторної аутентифікації для доступу до корпоративних ресурсів.

Рис. 1.1. Тріада (Цілісність, Конфіденційність, Доступність) [1].

1.2 Ключові вимоги до забезпечення захисту корпоративних мереж

Основою для забезпечення мережевої безпеки є розуміння моделі OSI, яка представляє собою еталонну модель взаємодії відкритих систем. Ця модель є міжнародним стандартом, що визначає структуру мережі через сім рівнів. Вона допомагає розділити складну мережеву систему на прості компоненти, кожен із яких можна захистити окремо.

Передача інформації в моделі OSI здійснюється через послідовний рух даних від верхнього рівня (рівень додатків) до найнижчого (фізичний рівень) (рис1.2). На кожному рівні реалізуються певні протоколи, що забезпечують цей процес. Коли дані доходять до кінцевого пристрою, вони знову "піднімаються" з фізичного рівня до рівня додатків, доставляючи користувачеві потрібну інформацію [2].

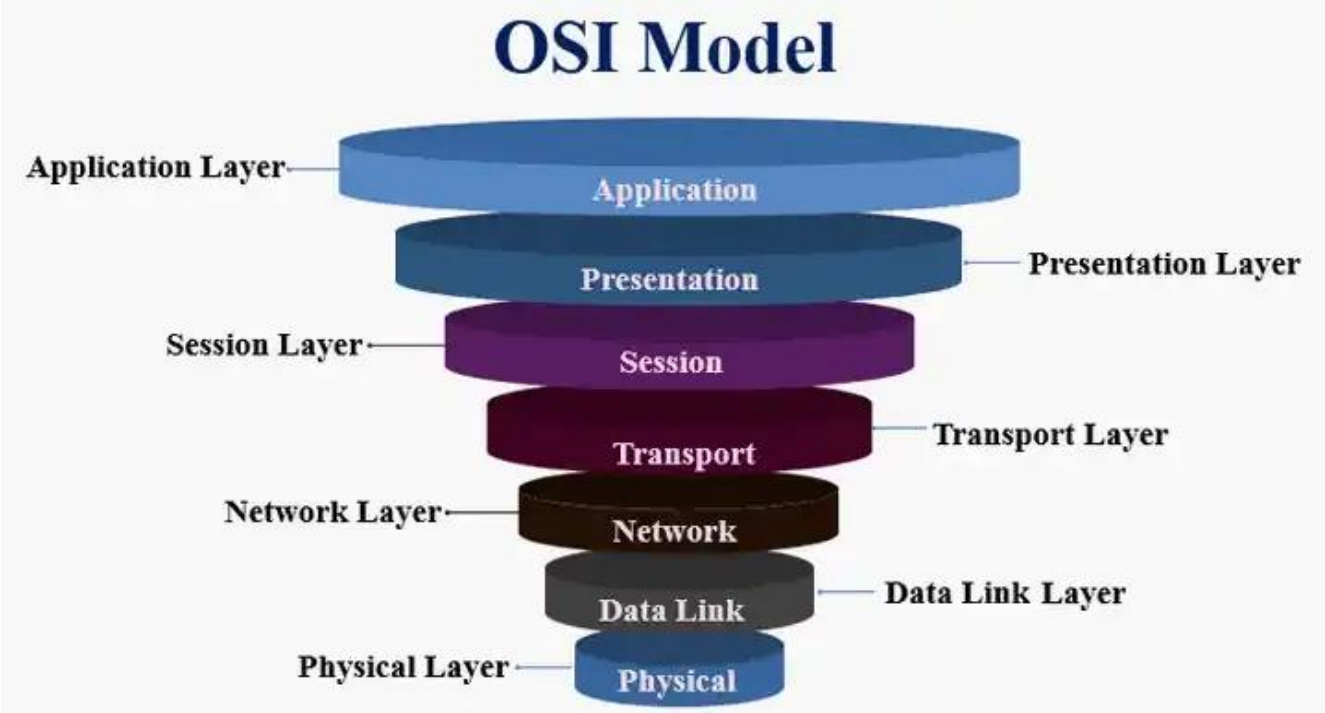


Рис. 1.2. Модель OSI [2].

1. Основні етапи забезпечення безпеки мережі.

Ідентифікація активів мережі. До активів мережі належать операційні системи, програми, маршрутизатори, комутатори, а також дані, які передаються через мережу. Кожен із цих активів необхідно виявити, оцінити їхню важливість і визначити потенційні ризики, пов'язані з несанкціонованим доступом чи саботажем.

2. Аналіз ризиків безпеки.

Ризики варіюються від дій зловмисників до необачних дій користувачів, наприклад, завантаження програм, які можуть містити шкідливий код. Наслідками таких дій можуть бути викрадення або зміна даних, а також порушення доступу до мережевих ресурсів.

3. Оцінка вимог безпеки.

Вимоги до безпеки передбачають реалізацію тріади КЦД (конфіденційність, цілісність, доступність). Забезпечення цих аспектів може вимагати компромісів між продуктивністю мережі, резервуванням та використанням обчислювальних ресурсів.

4. Розробка плану забезпечення безпеки.

План забезпечення безпеки – це стратегічний документ, що визначає дії організації для виконання вимог безпеки. Він базується на аналізі активів і ризиків і включає опис мережевої топології, список послуг (наприклад, електронна пошта, FTP, веб-доступ) і їхніх адміністраторів, а також механізми доступу.

5. Створення політики безпеки.

Політика безпеки – це офіційний набір правил, яких повинні дотримуватися всі користувачі, які мають доступ до ресурсів організації. Вона включає загальні вимоги, а також специфічні правила, адаптовані під потреби конкретної організації.

6. Розробка процедур безпеки.

Процедури безпеки – це практичні інструкції, які реалізують політику безпеки. Вони включають налаштування систем, процеси аудиту, управління доступом, реагування на інциденти та обслуговування мережі. Ці процедури мають бути зрозумілими як для технічних фахівців, так і для кінцевих користувачів.

7. Підтримка безпеки.

Для забезпечення довготривалої безпеки необхідно регулярно проводити аудити, аналізувати журнали, реагувати на інциденти, оновлювати політики та плани, а також навчати персонал і впроваджувати нові технології. Також важливо стежити за рекомендаціями та попередженнями відповідних агентств.

1.3 Еволюція методів та тактик DDoS-атак

Розподілені атаки типу «відмова в обслуговуванні» (DDoS) стали повсякденною або, як дехто може стверджувати, щогодинною проблемою. Використовуючи різні методи, DDoS-атаки здійснюють і використовують різні суб'єкти загроз - від хакерів-одинаків, злочинних угруповань і хактивістів до державних суб'єктів.

Ці атаки здійснюються з метою зниження продуктивності та відключення мережевого зв'язку. Ці цілі можуть бути малі або великі підприємства, постачальники послуг Інтернету, виробники, роздрібні торговці, постачальники медичних послуг, школи та університети або інші організації. Особливою метою зловмисників є державні установи, силові структури, організації оборонного сектора. По суті будь-яка організація з Інтернет-присутністю може стати метою DDoS [3].

Є три основні причини, чому люди створюють ботнет: для отримання фінансової вигоди шляхом вимагання (заплатіть, або ми продовжимо атаку); для того, щоб вплинути на діяльність (зробіть те, що ми вимагаємо, і атака зупиниться); або, якщо йдеться про державні суб'єкти, для шпигунства або як тактика кібервійни.

З цієї статті ви дізнаєтеся, як виникають ботнети та DDoS-атаки - як виникають ботнет-атаки та DDoS-атаки - найпоширеніший механізм здійснення атак з використанням сукупності віддалено керованих, зламаних сервісів або пристроїв.

Ботнети можуть включати комп'ютери, смартфони, віртуалізовані машини та/або широкий спектр пристроїв IoT, таких як IP-камери, смарттелевізори, маршрутизатори, будь-що, що має підключення до Інтернету і може бути скомпрометовано. Зокрема, вразливість і неправильна конфігурація IoT дуже поширені на споживчому ринку, тому хакерам дуже легко створити IoT-ботнет. До того ж, ботнети, особливо коли вони стають частиною ботнету IoT, можуть бути величезними; один ботнет може складатися з сотень тисяч або навіть мільйонів скомпрометованих пристроїв.

Захоплення пристроїв для ботнет-мережі має на увазі пошук пристроїв, що мають уразливість у системі безпеки, що дозволяють заразити їх «botware» - шкідливим програмним забезпеченням, яке буде встановлено на пристрої. Але пристрої, заражені «ботпрограмою», - не єдине, що потрібно бот-мережі.

Багато джерел, включно з Вікіпедією, зовсім точно визначають, що таке ботнет. Хоча найочевиднішим елементом ботнету є велика кількість пристроїв,

визначальним компонентом виступає Command and Control система (C&C), що регулює дії мережі ботів.

На кожному зламаному пристрої бот-програма зв'язується з C&C системою ботнету і стає частиною мережі ботів. За командами «ботмейстера» або «ботхантера» - людини або групи, що керує ботами, - деякі або всі пристрої в бот-мережі виконують усе, що від них вимагається (рис. 1.3).

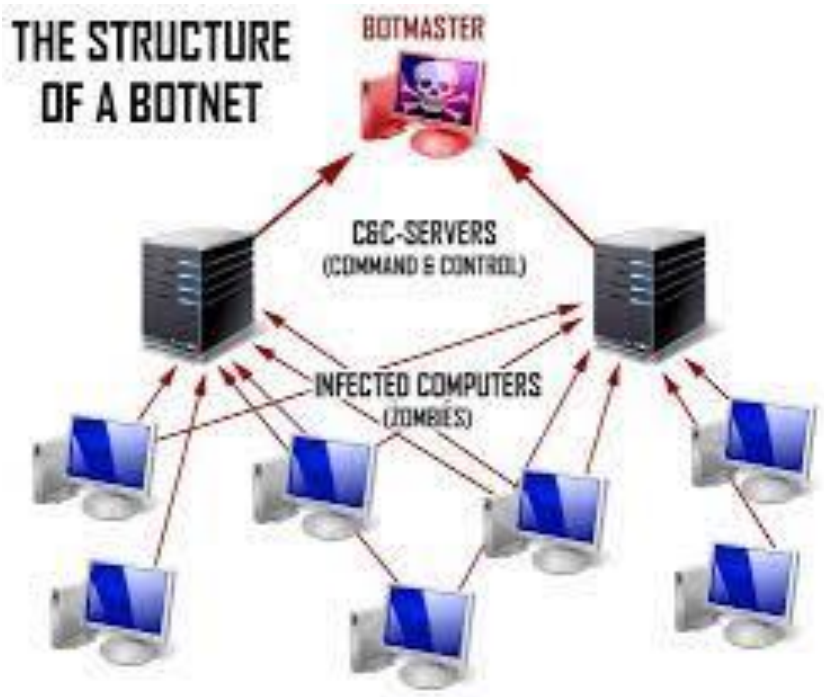


Рис. 1.3. Релізація «Ботнет» [4].

Command and Control ботнету

Перший зв'язок між C&C і бот-програмами на зламаних пристроях був заснований на моделі клієнт-сервер з використанням, наприклад Internet Relay Chat (IRC). Бот-програма підключалася до IRC-каналу і чекала команд. Кожен бот може також відповідати на тому ж каналі з оновленням статусу або віддаленими даними. Як альтернативу IRC можна використовувати з'єднання Telnet і HTTP-запити до веб-сторінок або сервісів користувача. Слід зазначити, що деякі ботмережі використовують ієрархічну систему C&C, де рівні ботів

спілкуються за принципом клієнт-сервер із ботами на рівні вище і передають команди на рівень нижче [4].

Новітні засоби Command and Control комунікації ботнетів базуються на зв'язках peer-to-peer (P2P). У цій моделі скомпрометовані пристрої виявляють один одного, скануючи діапазони IP-адрес, щоб знайти певні порти і служби протоколу, а коли ідентифіковано іншого учасника ботнету, обмінюються списками відомих однорангових пристроїв і команд. Цей тип розподіленої сітчастої мережі, очевидно, складніше створити, але також набагато важче розірвати (рис. 1.4).

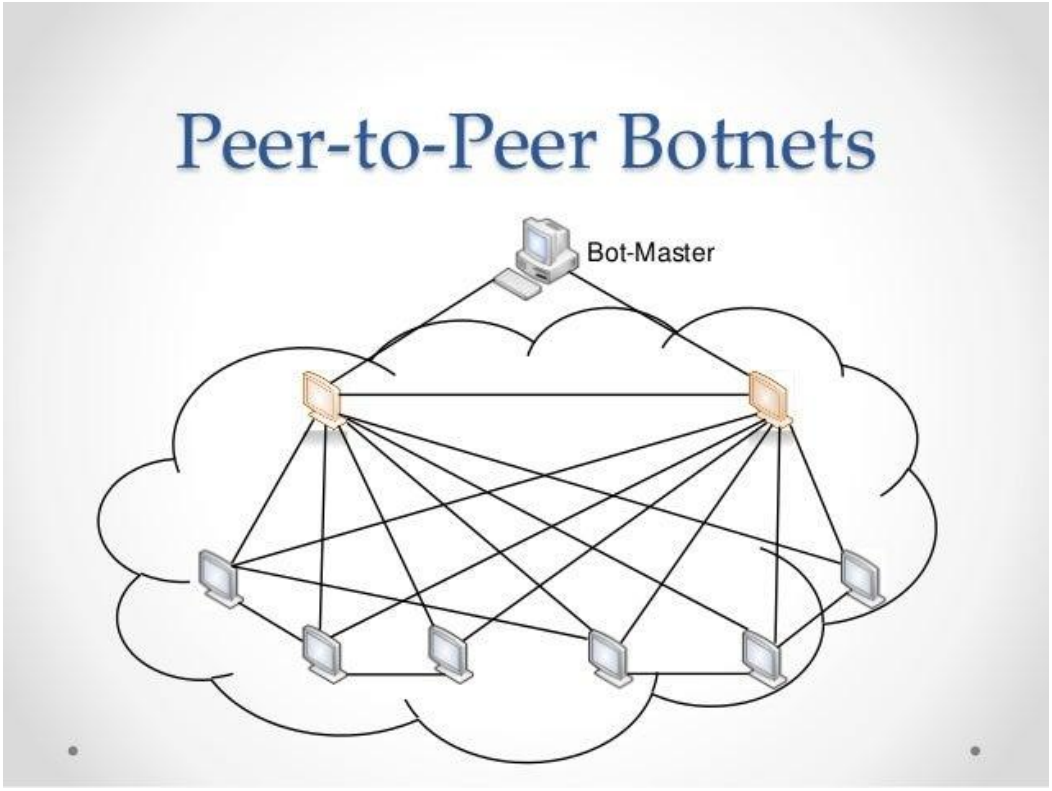


Рис. 1.4. Peer-to-Peer Botnets [5].

Розвиток ботнету IoT

Пристрої IoT охоплюють величезну кількість комерційних і споживчих пристроїв, як-от системи вимірювання температури, смарт-телевізори, IP-камери, розумні дверні дзвінки, системи безпеки, мережеві маршрутизатори та комутатори і навіть дитячі іграшки. Незважаючи на величезну кількість попереджень про вразливість IoT і добре зрозумілих рекомендацій щодо

поліпшення їхньої безпеки, основні засоби захисту, як-от вимога ефективних паролів і заборона на використання стандартних логінів і облікових записів користувачів, як і раніше, ігноруються. Ще одне джерело вразливостей IoT пов'язане з тим, що постачальники не надають оновлення для вирішення проблем безпеки та/або власники пристроїв не встановлюють оновлення [5].

Ботнети використовуються для чотирьох основних завдань, і, як правило, ботнет може бути повністю або частинами переключений для виконання будь-якого з цих завдань.

Спам і фішинг

Одним із перших способів використання ботнетів було створення спаму, небажаної комерційної або шахрайської електронної пошти. Використовуючи для цієї мети ботів, спамери уникають проблеми потрапляння своїх IP-адрес масової розсилки до чорного списку, а також якщо деякі боти потраплять до чорного списку, завжди можна знайти більше ботів.

Більш цілеспрямоване використання ботнет-спаму для фішингу з метою крадіжки особистих даних. Створюючи величезну кількість спам-повідомлень електронною поштою, які запрошують одержувачів відвідати рекламні вебсайти, вебсайти, що виглядають як банки або інші фінансові установи, взяти участь у конкурсах тощо, шахраї намагаються отримати особисту інформацію, як-от реквізити банківського рахунку, дані кредитної картки та логіни вебсайтів.

Pay-per-Click махінації

Щоб збільшити доходи від реклами на веб-сайті (рекламні мережі, як-от Google, платять за клік реклами, що розміщується вебсайтами), використовуються ботнети для підробки взаємодії користувачів. Через розподілену природу джерел кліків рекламним мережам важко розпізнати помилкові кліки.

Криптомайнінг

Ботнет IoT є ідеальною платформою для майнінгу криптовалют, таких як Bitcoin і Ether завдяки запуску алгоритмів майнінгу на десятках тисяч ботів. Таким чином, викрадена комп'ютерна потужність власника пристрою дає змогу

отримати значний дохід без звичайних витрат на майнінг, головним чином, витрат на електроенергію.

DDoS-атаки як послуга

Розподілені атаки на відмову в обслуговуванні легко запускаються за допомогою ботнетів, і, як і у випадку зі спамом, створеним ботнетом, розподілена природа ботів ускладнює фільтрацію трафіку DDoS. Ботнети можуть виконувати будь-які види DDoS-атак і навіть запускати кілька типів атак одночасно.

Відносно новим видом хакерського бізнесу є DDoS-as-a-Service. У Dark Web і тепер, навіть у звичайному Інтернеті, ви можете купити DDoS-атаки всього за 5 доларів США за годину; ціна залежить від необхідного масштабу і тривалості атаки [6].

1.4 Дослідження специфіки проведення DDoS-атак

Розподілена атака типу «відмова в обслуговуванні» (DDoS) – це цілеспрямоване перевантаження ресурсу величезною кількістю запитів, які надходять із численних джерел одночасно. Таке навантаження значно перевищує можливості системи обробляти запити, що призводить до її збоїв і недоступності для звичайних користувачів. Атака організовується з різних пристроїв, об'єднаних у ботнет, і завдяки цьому досягає високої ефективності. В Інтернеті DDoS часто порівнюють із "зброєю масового ураження" через її руйнівну потужність.

Однією з найпростіших форм такої атаки є Smurf-атака. У її межах один комп'ютер генерує велику кількість ICMP-ехо-запитів до інших хостів у мережі, що змушує ці хости відповідати на запити. У результаті масові відповіді спрямовуються на цільову систему, створюючи перевантаження. Значна за обсягом атака такого типу здатна вивести з ладу навіть великі мережі. DDoS-атаки є надзвичайно складними для запобігання, адже їхній трафік часто схожий на звичайний користувацький трафік.

Крім того, кількість запитів під час таких атак може зростати в геометричній прогресії, що ускладнює їхнє виявлення. Важливо зазначити, що організувати DDoS-атаку нині стало досить просто навіть для людей без технічних навичок. У темному сегменті Інтернету існують платні сервіси, які дозволяють орендувати ботнет для виконання атак. Вартість таких послуг коливається від 5 до 200 доларів за годину, залежно від масштабу та складності атаки. Зловмисникам залишається лише обрати ціль – це може бути окремий сайт, сервер чи навіть ціла мережа, що має вразливості [7].

Етапи DDoS-атаки ("Ланцюжок кіберубивств").

1. Розвідка На цьому етапі зловмисник визначає вразливі точки цільової системи. Це може бути як великий центр обробки даних, так і окремий комп'ютер. Метою є збір інформації про мережу, пристрої, методи безпеки (брандмауери, IPS тощо). Зловмисник шукає шляхи обходу цих систем.

2. Використання зброї.

Використовуються інструменти для експлуатації вразливостей: віруси, черв’яки або спеціальні експлойти. Вони створюються або купуються на чорному ринку.

3. Доставка Кіберзброя впроваджується в систему жертви через:

фішингові електронні листи;

завантаження з шкідливих сайтів;

заражені USB-накопичувачі.

Методи доставки шкідливого коду:

– Розповсюдження з центрального джерела: скомпрометована система підключається до центрального сховища зловмисника, звідки отримує код.

– Розповсюдження зі зворотним ланцюгом: інструменти зловмисника надсилаються безпосередньо на заражений хост.

– Автономне поширення: зловмисник переносить інструменти безпосередньо на хост без залучення зовнішніх джерел.

4. Експлуатація.

Шкідливе програмне забезпечення починає використовувати вразливості в програмному забезпеченні, слабкі механізми безпеки та недоліки у поведінці користувачів. Експлойти збільшують ризик, навіть якщо вразливість незначна.

5. Встановлення.

На цьому етапі шкідливе ПЗ інсталюється у систему жертви. Інсталяція може відбуватися: У просторі користувача: легше виявити. У просторі ядра: важче виявити антивірусними рішеннями.

6. Керування та контроль.

Скомпрометована система входить до ботнету – мережі пристроїв, контрольованих зловмисником. Через віддалений доступ зловмисник активує ботнет для проведення DDoS-атаки.

Методи захисту від DDoS-атак

Превентивні заходи

– Використання систем раннього виявлення атак.

– Оптимізація мережевої інфраструктури.

– Використання CDN для зменшення навантаження.

– Встановлення брандмауерів веб-додатків.

Реактивні заходи

– Аналіз та фільтрація трафіку під час атаки.

– Використання сервісів для перенаправлення трафіку до центрів очищення.

Відстеження джерела атаки

– Виявлення джерел за допомогою аналізу пакетів.

– Використання трасувальних механізмів для ідентифікації атакуючих систем.

Таблиця 1.1.

Глобальна таблиця: Етапи DDoS-атаки та їх опис

Етап	**Опис дій зловмисника**
Розвідка	Вивчення вразливостей цільової системи, аналіз мережі та методів захисту.
Використання зброї	Підготовка шкідливих інструментів (вірусів, черв'яків, експлойтів).
Доставка	Впровадження кіберзброї через фішинг, заражені пристрої або мережеві завантаження.
Експлуатація	Активація шкідливого коду для використання вразливостей у програмному забезпеченні або мережі.
Встановлення	Інсталяція шкідливого ПЗ у систему жертви (простір користувача чи ядра).
Керування та контроль	Створення ботнету та запуск атаки.

Висновки до розділу 1

У даному розділі проаналізовано вплив DDoS-атак на захищеність мереж, зокрема досліджено загальні аспекти мережевої безпеки та ключові вимоги до захисту корпоративних мереж. Розглянуто еволюцію методів та тактик DDoS-атак, що дозволяє краще зрозуміти, як ці атаки змінюються та адаптуються до нових умов. Визначено, що атаки стали значно складнішими і можуть бути спрямовані не лише на мережеву інфраструктуру, але й на сервіси та додатки.

Також проведено дослідження специфіки проведення DDoS-атак, що включає різноманітні методи і стратегії, що застосовуються зловмисниками. Показано, що для ефективного захисту необхідно враховувати постійні зміни у тактиках атак та впроваджувати інтегровані підходи до їх запобігання та виявлення на всіх рівнях мережі.

РОЗДІЛ 2. ВИДИ АТАК НА ВІДМОВУ В ОБСЛУГОВУВАННІ ТА ПІДХОДИ ДО ЇХ ВИЯВЛЕННЯ

2.1 Атаки на інфраструктуру мережі

Атаки на інфраструктуру мережі є одним із найпоширеніших видів загроз, що спрямовані на порушення роботи базових компонентів мережевої інфраструктури. Ці атаки здатні вивести з ладу ключові елементи системи, такі як маршрутизатори, комутатори, сервери та інші пристрої, які забезпечують функціонування мережі. Основна мета таких атак – перешкодити нормальному функціонуванню мережі, знизити її продуктивність або повністю зупинити роботу. Нижче детально описані основні типи атак на мережеву інфраструктуру, їхні механізми дії та можливі наслідки [8].

1. Атаки типу SYN-флуд (SYN Flood)

Цей тип атак є класичним прикладом використання вразливостей протоколу TCP (Transmission Control Protocol). Зловмисник експлуатує механізм триетапного хендшейка, що використовується для встановлення з’єднання між клієнтом і сервером. Під час атаки зловмисник надсилає велику кількість SYN-запитів до цільового сервера, але не завершує процес встановлення з’єднання. Це призводить до того, що сервер витрачає свої ресурси на утримання напіввідкритих з'єднань.

Наслідки:

– Перевантаження пам’яті та ресурсів сервера.

– Нездатність обробляти нові підключення.

– Відмова у доступі до сервісів для легітимних користувачів.

Методи захисту:

– Використання механізмів SYN-куки для обробки підозрілих з'єднань.

– Обмеження кількості одночасних напіввідкритих з'єднань.

– Налаштування тайм-аутів для скидання неактивних з'єднань.

2. UDP-флуд (UDP Flood)

UDP-флуд є одним із найпростіших і водночас ефективних способів перевантаження мережі. У цій атаці зловмисник надсилає величезну кількість UDP-пакетів до випадкових портів цільового сервера. Сервер витрачає ресурси на перевірку цих пакетів або створення ICMP-відповідей типу "Destination Unreachable".

Наслідки:

– Виснаження мережевих ресурсів і пропускної здатності.

– Порушення доступу до послуг, які надає сервер.

– Можливе "зависання" пристроїв через перенавантаження.

Методи захисту:

– Фільтрація UDP-трафіку на рівні брандмауера.

– Використання обмеження швидкості трафіку (Rate Limiting).

– Налаштування блокування ICMP-пакетів, які не є критично необхідними.

3. ICMP-флуд (ICMP Flood)

Цей тип атак експлуатує протокол ICMP (Internet Control Message Protocol), що використовується для обміну службовими повідомленнями між пристроями в мережі. У разі ICMP-флуду зловмисник надсилає велику кількість ICMP Echo-запитів (так званих ping-запитів) до цільового пристрою, перевантажуючи його [9].

Наслідки:

– Підвищення затримок у мережі.

– Зниження продуктивності мережевого обладнання.

– Повна відмова мережевого пристрою обробляти нові запити.

Методи захисту:

– Обмеження кількості ICMP-запитів за одиницю часу.

– Використання налаштувань брандмауера для блокування ICMP-трафіку з підозрілих джерел.

– Вимкнення ICMP Echo-запитів на зовнішніх інтерфейсах мережевого обладнання.

4. Атаки на маршрутизатори

Маршрутизатори є основою будь-якої мережі, тому вони часто стають мішенню для атак. Зловмисники можуть використовувати протоколи маршрутизації (BGP, OSPF) для маніпуляцій трафіком або просто перенавантажувати маршрутизатор великою кількістю запитів [10].

Методи атак:

– **BGP Hijacking**: маніпулювання протоколом BGP для перехоплення трафіку.

– **Flooding**: генерація надмірного трафіку для перевантаження маршрутизатора.

Наслідки:

– Порушення роботи маршрутизації.

– Затримки та збої у передачі даних.

– Втрата доступності мережевих послуг.

Методи захисту:

– Аутентифікація маршрутизаторів у протоколах маршрутизації.

– Обмеження доступу до адміністративних інтерфейсів маршрутизаторів.

– Використання резервних маршрутів.

5. Атаки на комутатори

Комутатори відповідають за передачу даних між пристроями у межах локальної мережі. Вони також піддаються атакам, спрямованим на порушення їхньої роботи.

Типи атак:

– **MAC-флудинг**: переповнення таблиці MAC-адрес, через що комутатор починає пересилати весь трафік у режимі broadcast.

– **VLAN Hopping**: зловмисник обходить ізоляцію між VLAN, отримуючи доступ до інших сегментів мережі.

Наслідки:

– Збільшення навантаження на комутатор.

– Порушення конфіденційності даних.

– Можливість перехоплення мережевого трафіку.

Методи захисту:

– Використання функції Port Security для обмеження кількості MAC-адрес на порт.

– Впровадження правил VLAN ACL для посилення ізоляції між сегментами мережі.

6. Атаки на брандмауери

Брандмауери є важливими компонентами захисту мережі, однак і вони можуть стати об'єктами атак. Зловмисники можуть перенавантажити брандмауер великою кількістю запитів або спробувати обійти його налаштування.

Методи атак:

– **Flooding**: велика кількість запитів для перевантаження правил брандмауера.

– **Obfuscation**: зміна пакунків, щоб уникнути виявлення.

Наслідки:

– Зниження ефективності фільтрації трафіку.

– Прорив у захищену мережу.

Методи захисту:

– Регулярне оновлення прошивки.

– Налаштування автоматичних правил блокування при перевантаженні.

– Моніторинг аномалій у трафіку.

Мережевий рівень є важливим компонентом у функціонуванні будь-якої мережі, оскільки він забезпечує передачу даних між пристроями. Протоколи цього рівня, такі як IP, TCP і UDP, а також механізми маршрутизації, надають базові функції для комунікації, але водночас містять вразливості, які можуть

бути використані зловмисниками для атак. Ці вразливості, часто обумовлені відкритою архітектурою та широкою доступністю протоколів, залишають значний простір для різноманітних загроз [11].

Протокол IP забезпечує передачу даних між вузлами в мережі, але його дизайн, створений ще в часи, коли безпека не була пріоритетом, має ряд недоліків. Однією з головних вразливостей є можливість підробки IP-адреси (IP Spoofing). Зловмисники використовують цю техніку для маскування своїх дій або перенаправлення трафіку. Інша критична проблема – відсутність механізмів аутентифікації в протоколі. IP-пакети можуть бути змінені під час передачі, і мережеві пристрої не мають вбудованих засобів для перевірки їхньої достовірності. Крім того, протокол IP схильний до атак на фрагментацію, коли зловмисник надсилає некоректно фрагментовані пакети, що можуть викликати збої в обробці даних або навіть зламати систему. Особливо небезпечні такі атаки для систем із застарілим обладнанням або неправильними налаштуваннями.

Протокол TCP відповідає за встановлення надійного з'єднання між пристроями, але саме його механізм хендшейку (триетапного встановлення з'єднання) стає мішенню для атак. Найвідоміша з таких атак – SYN-флуд, де зловмисник перевантажує сервер великою кількістю напіввідкритих з'єднань, виснажуючи його ресурси. TCP також схильний до атак перехоплення сеансу (TCP Session Hijacking), коли зловмисник втручається в активне з'єднання, захоплюючи контроль над передачею даних. Окрему загрозу становить відсутність вбудованих механізмів шифрування в TCP, через що дані можуть бути легко перехоплені, якщо не застосовуються додаткові засоби захисту, наприклад, TLS. Крім того, TCP не може забезпечити захист від атак на цілісність даних, таких як маніпулювання порядком пакетів або їх дублювання.

Протокол UDP, який використовується для передачі даних у режимі без з'єднання, має свої особливості та недоліки. Оскільки UDP не забезпечує перевірку доставки даних і не потребує встановлення з'єднання, він стає привабливим для атак на перевантаження (наприклад, UDP-флуд). Зловмисники можуть надсилати величезну кількість пакетів UDP до випадкових портів на

сервері, змушуючи його витрачати ресурси на обробку цих запитів. Інша вразливість – це відкритість протоколу до атак на підробку джерела (Source Spoofing), коли зловмисник змінює IP-адресу джерела, ускладнюючи виявлення справжнього джерела атаки. UDP також часто використовується у підсилювальних атаках (Amplification Attacks), таких як DNS Amplification, де невеликий обсяг запитів може генерувати велику кількість відповідей, спрямованих на цільову систему.

Механізми маршрутизації також є вразливим місцем мережевої інфраструктури. Протоколи маршрутизації, такі як BGP (Border Gateway Protocol) та OSPF (Open Shortest Path First), зазвичай не мають вбудованих механізмів аутентифікації та шифрування. Це створює можливості для атак, наприклад, BGP Hijacking, коли зловмисник змінює маршрути, перенаправляючи трафік через свої вузли. Інша серйозна загроза – це атаки на конфігурацію маршрутизаторів. Недостатній захист адміністративного доступу або використання стандартних паролів може дати зловмисникам контроль над маршрутизаторами. Також варто згадати про атаки на відмову в обслуговуванні, спрямовані на перевантаження маршрутизаторів шляхом надсилання надмірної кількості запитів.

Атаки на мережеву інфраструктуру демонструють значну еволюцію у методах, масштабах та цілях. Вони спрямовані на порушення роботи мережевих систем, виснаження їхніх ресурсів і, у підсумку, зупинку обслуговування користувачів. Такі атаки використовують як технічні вразливості протоколів і налаштувань обладнання, так і координацію великої кількості пристроїв у ботнетах. Це робить їх однією з найсерйозніших загроз у сучасному кіберпросторі.

Окремі приклади, наведені в таблиці 2.1, демонструють, наскільки складними і руйнівними можуть бути такі атаки. Наприклад, атака Mirai Botnet стала знаковим випадком, коли зловмисники використали слабкі паролі IoT-пристроїв для створення ботнету, що паралізував роботу популярних сервісів, таких як Twitter і Netflix. Інший яскравий приклад – атака на GitHub, яка

використала техніку Memcached Amplification, що підвищує обсяг трафіку до критичного рівня за рахунок неправильного налаштування серверів.

Ці атаки вказують на необхідність постійного вдосконалення методів кіберзахисту. Великі корпорації, такі як Google і Amazon, також не застраховані від подібних загроз.

Таблиця 2.1.

Відомі атаки на мережеву інфраструктуру

Атака	**Рік**	**Ціль атаки**	**Метод атаки**	**Масштаб атаки**	**Наслідки**
Mirai Botnet	2016	IoT-пристрої, DNS-сервіси	Інфікування IoT-пристроїв, DDoS через ботнет	Сотні тисяч IoT-пристроїв	Недоступність популярних сервісів, наприклад, Twitter і Netflix, та вразливість IoT.
GitHub Attack	2018	GitHub платформа для зберігання коду	Memcached Amplification (підсилення через неправильно налаштовані сервери)	1.35 Тбіт/с	Швидке реагування Akamai мінімізувало вплив, атака тривала кілька хвилин.
Attack on Google	2017	Мережі та сервери Google	Багаторазовий ботнет трафік із різних джерел	2.54 Тбіт/с	Демонстрація нових масштабів DDoS-атак, уникнуто зупинки завдяки потужним системам захисту.
AWS Attack	2020	Хмарні сервіси AWS	Підсилення через вразливості протоколів	2.3 Тбіт/с	Декілька днів атак, успішне стримання завдяки AWS Shield, збереження сервісів.
Estonian Infrastructure Attack	2007	Урядові, фінансові та медіа ресурси Естонії	Масове перевантаження через ботнет і координація атак	Національна інфраструктура Естонії	Державні сервіси й банківські системи були недоступні протягом декількох днів.
Cloudflare Attack	2021	Сервіси Cloudflare	HTTP Flood через ботнет із мільйонів пристроїв	17.2 млн запитів на секунду	Сервіси Cloudflare залишилися функціональними завдяки адаптивному захисту.

2.2 Атаки, спрямовані на серверні системи

Серверні системи є ядром будь-якої інформаційної інфраструктури, оскільки вони забезпечують зберігання, обробку і передачу даних, а також підтримують функціонування різноманітних сервісів, таких як веб-додатки, бази даних, електронна пошта та інші корпоративні системи. Вони відіграють ключову роль у сучасних бізнес-процесах, забезпечуючи зв'язок між користувачами та додатками, управління даними, а також надання критично важливих послуг в режимі реального часу.

Через їхню стратегічну важливість серверні системи стають привабливою мішенню для зловмисників. Атаки на сервери можуть мати руйнівні наслідки для організацій, спричиняючи збої в роботі сервісів, втрату конфіденційної інформації, фінансові збитки та пошкодження репутації. Зловмисники застосовують різноманітні методи атак, використовуючи слабкі місця серверного програмного забезпечення, конфігурацій, а також помилки адміністрування [12].

Однією з причин вразливості серверних систем є їх відкритість до мережі. Сервери повинні бути доступними для клієнтів і користувачів, але цей доступ часто надає зловмисникам можливість скористатися слабкими місцями системи. Наприклад, невчасне оновлення програмного забезпечення може залишити сервер відкритим для експлуатації відомих уразливостей, а неправильна конфігурація безпекових механізмів може полегшити доступ до критичних ресурсів.

Зловмисники використовують сервери не тільки як ціль, а й як засіб для подальших атак. Наприклад, після отримання контролю над сервером, вони можуть використовувати його для запуску атак на інші системи, зберігання шкідливого програмного забезпечення або організації ботнетів.

Види атак на серверні системи можуть значно варіюватися залежно від цілі та методів. Це можуть бути атаки на виснаження ресурсів, які перевантажують сервери запитами, атаки на бази даних, спрямовані на викрадення або знищення

інформації, а також складні експлуатації вразливостей у серверному програмному забезпеченні. Особливий акцент робиться на використанні автоматизованих інструментів, які дозволяють здійснювати атаки великого масштабу та з мінімальними витратами для зловмисників.

З огляду на критичну роль серверних систем у сучасному цифровому світі, їхній захист є першочерговим завданням. Це вимагає комплексного підходу, який включає використання сучасних засобів кібербезпеки, таких як системи виявлення вторгнень (IDS), міжмережеві екрани (WAF), шифрування даних, а також регулярний моніторинг і аудит систем. Забезпечення належного рівня захисту серверних систем дозволяє організаціям знизити ризики і зберегти стабільність своєї інформаційної інфраструктури [13].

HTTP-флуд є одним із найпоширеніших методів DDoS-атак, спрямованих на сервери. Зловмисники надсилають велику кількість HTTP-запитів до веб-сервера з метою виснаження його ресурсів.

Механізм атаки:

– Зловмисники генерують значну кількість запитів, які виглядають як легітимні HTTP-запити до серверів.

– Запити можуть бути спрямовані на завантаження сторінок, виконання скриптів чи звернення до API.

– Більшість атак реалізується через ботнети, які імітують дії реальних користувачів.

Результати:

– Виснаження ресурсів сервера (CPU, RAM).

– Підвищення затримок у відповіді на запити.

– Недоступність веб-сайту для легітимних користувачів.

Приклад:

– Атака на GitHub у 2018 році, яка використовувала техніку Memcached Amplification, мала схожі наслідки.

Атаки з виснаженням ресурсів - цей тип атак націлений на перевантаження серверів шляхом створення великої кількості з'єднань або виконання ресурсомістких операцій.

Механізм атаки:

– Зловмисники використовують різні техніки, зокрема:

1. Створення великої кількості TCP-з'єднань (SYN-флуд).
2. Надсилання складних запитів до серверних скриптів або баз даних.
3. Виконання операцій із високими вимогами до обчислювальних ресурсів.

Результати:

– Виснаження доступної пам’яті та процесорного часу.

– Виникнення затримок у відповіді або повна недоступність сервера.

– Можливе пошкодження критичних систем через перевантаження.

Приклад:

– Атака Slowloris, яка повільно надсилає запити, змушуючи сервер зберігати їх у стані очікування.

Атаки на бази даних – бази даних є важливим елементом будь-якої інформаційної системи, оскільки вони зберігають критично важливі дані, такі як фінансова інформація, персональні дані користувачів, конфіденційні документи компаній та інше. Саме через це вони часто стають однією з головних цілей зловмисників. Атаки на бази даних можуть мати різні форми, залежно від методів, які використовуються.

Одним із найпоширеніших методів атак на бази даних є SQL-ін'єкція. Зловмисники використовують форми введення даних або URL-запити для впровадження шкідливих SQL-запитів. Це дозволяє отримати доступ до бази даних без авторизації, змінювати або видаляти дані, а також викрадати конфіденційну інформацію. Іншим популярним методом є перевантаження бази даних численними запитами, що призводить до виснаження ресурсів сервера і уповільнення його роботи або навіть до повної недоступності. Окрім цього, зловмисники можуть отримати доступ до бази даних і зашифрувати її вміст,

вимагаючи викуп за розшифрування. Такі атаки відомі як Ransomware і є одними з найнебезпечніших для компаній [14].

Наслідки атак на бази даних можуть бути катастрофічними. Викрадення конфіденційної інформації завдає серйозної шкоди репутації компанії та може спричинити юридичні й фінансові наслідки. Крім того, перевантаження або шифрування бази даних значно знижує продуктивність сервера, а в деяких випадках може призвести до втрати важливої інформації. Одним із найгучніших прикладів таких атак є інцидент з Equifax у 2017 році, коли через SQL-ін'єкцію було викрадено дані понад 140 мільйонів осіб.

Серверні додатки також є вразливою частиною інфраструктури, оскільки вони виконують основну логіку бізнес-процесів і обробку даних. Зловмисники часто використовують вразливості в програмному забезпеченні, яке працює на серверах, для виконання атак, спрямованих на отримання несанкціонованого доступу, порушення роботи додатків або використання серверів для інших шкідливих цілей.

Такі атаки можуть включати використання відомих вразливостей у веб-серверах, наприклад, Apache чи Nginx, або у фреймворках, які забезпечують роботу додатків. Зловмисники можуть здійснювати віддалене виконання коду (Remote Code Execution, RCE), що дозволяє їм впроваджувати і виконувати власний код на сервері. Окрім цього, атаки можуть бути спрямовані на недостатньо захищені API, через які здійснюється взаємодія додатків з іншими системами.

Результати таких атак можуть включати несанкціонований доступ до серверів, що створює загрозу для безпеки даних і сервісів. Порушення роботи серверних додатків може зупинити бізнес-процеси компанії, а використання серверів для подальшого поширення атак, наприклад, через ботнети, посилює загальну загрозу для кібербезпеки. Одним із найяскравіших прикладів таких атак є інцидент Log4Shell у 2021 році, коли вразливість у популярній бібліотеці Log4j дозволила зловмисникам виконувати довільний код на сервері. Це спричинило серйозні наслідки для багатьох організацій по всьому світу.

Атаки на сервери мають руйнівний вплив на їхні апаратні та програмні ресурси, що може призводити до значного зниження продуктивності або повного відключення серверних систем. Основними ресурсами, які стають ціллю атак, є центральний процесор (CPU), оперативна пам'ять (RAM) і мережева пропускна здатність. Нижче детально розглянуто, як кожен із цих компонентів страждає від атак.

Центральний процесор є "мозком" серверної системи, оскільки саме він обробляє всі запити, виконує розрахунки та керує роботою інших компонентів. Під час атак, особливо таких, як DDoS або атаки типу HTTP Flood, сервер може отримувати величезну кількість запитів одночасно. CPU витрачає ресурси на обробку цих запитів, включаючи розпізнавання, сортування, передачу даних і виконання відповідей [15].

Результати перевантаження CPU:

– Затримки у відповіді на запити, що може зробити сервіси повільними або недоступними.

– Зростання навантаження до критичного рівня, що може призвести до збоїв у роботі або перезапуску серверів.

– Неможливість виконання легітимних запитів через те, що CPU витрачає всі ресурси на обробку атакувального трафіку.

Атаки, спрямовані на виснаження CPU, можуть також включати складні обчислювальні операції, такі як шифрування, дешифрування або виконання скриптів, що створює додаткове навантаження на процесор.

Оперативна пам'ять забезпечує швидкодію серверів. Вона використовується для зберігання даних, необхідних для виконання запитів і роботи програмного забезпечення. Атаки, спрямовані на сервери, можуть використовувати методи, які переповнюють оперативну пам'ять.

Механізм впливу на RAM:

– Надсилання великої кількості одночасних запитів, кожен із яких резервує частину оперативної пам’яті.

– Використання запитів, що генерують великі об'єми проміжних даних (наприклад, при обробці складних SQL-запитів або скриптів).

– Зловмисники можуть створювати умови для витоку пам’яті (Memory Leak), коли програми не вивільняють зайняту пам’ять після завершення запиту.

Результати перевантаження RAM:

– Уповільнення роботи серверних додатків через брак доступної пам’яті.

– Система може почати використовувати файли підкачки (swap), що суттєво знижує швидкість роботи серверів.

– Втрата стабільності програмного забезпечення, що може призвести до збоїв або зупинки роботи сервера.

Мережева пропускна здатність визначає обсяг даних, який сервер може передавати або отримувати за одиницю часу. Вона є критичним ресурсом для будь-якої серверної системи, особливо для веб-додатків і сервісів, що працюють у режимі реального часу. Атаки, спрямовані на мережеву пропускну здатність, зазвичай мають форму DDoS-атак, де величезний обсяг трафіку спрямовується на цільовий сервер.

Механізм впливу на пропускну здатність:

– Генерація великого обсягу фальшивого трафіку, який перевищує можливості мережі.

– Використання підсилювальних атак (Amplification), таких як DNS Amplification або Memcached Amplification, де невеликий запит генерує масивну відповідь.

– Високий обсяг з'єднань, які блокують канали для легітимного трафіку.

Результати перевантаження мережі:

– Уповільнення швидкості передачі даних.

– Повна недоступність сервісів через блокування легітимного трафіку.

– Порушення роботи серверів, які залежать від зовнішніх API або інших ресурсів.

Протидія атакам, спрямованим на серверні ресурси, є критично важливою для забезпечення стабільної роботи серверів та захисту даних. Впровадження ефективних заходів захисту вимагає багаторівневого підходу, що включає комбінацію технічних засобів, налаштувань мережі та організаційних заходів. Нижче описані основні методи протидії таким атакам.

1. Моніторинг і виявлення аномалій

Моніторинг серверних систем у режимі реального часу є одним із ключових способів виявлення атак на ранніх етапах. За допомогою спеціалізованих інструментів можна виявляти аномальні навантаження на CPU, RAM або мережеву пропускну здатність.

Технології моніторингу:

– Використання систем виявлення вторгнень (IDS/IPS), які аналізують мережевий трафік і визначають підозрілу активність.

– Моніторинг системних метрик за допомогою таких інструментів, як Zabbix, Nagios або Prometheus.

– Впровадження рішень на основі машинного навчання, які автоматично визначають аномалії в поведінці серверів.

Реакція:

– Надсилання сповіщень адміністраторам при перевищенні порогів навантаження.

– Автоматичне блокування підозрілих IP-адрес чи трафіку.

2. Захист CPU та RAM

Для захисту обчислювальних ресурсів необхідно забезпечити обмеження доступу до серверів і ефективно керувати запитами.

Методи захисту:

– Встановлення обмежень на кількість з'єднань від одного клієнта.

– Використання механізму Rate Limiting, який дозволяє контролювати частоту запитів від конкретних IP-адрес.

– Використання технологій балансування навантаження (Load Balancing), які розподіляють запити між кількома серверами, запобігаючи перевантаженню одного з них.

– Оптимізація серверного програмного забезпечення для зниження ресурсомісткості обробки запитів.

3. Захист мережевої пропускної здатності

Захист мережі від атак, таких як DDoS, потребує впровадження спеціалізованих засобів, які фільтрують шкідливий трафік і забезпечують доступність сервісів.

Методи захисту:

– Використання хмарних сервісів захисту від DDoS, таких як Cloudflare, Akamai або Imperva, які відфільтровують шкідливий трафік на рівні глобальних центрів обробки даних.

– Встановлення міжмережевих екранів (WAF), які захищають веб-додатки від специфічних атак, таких як HTTP Flood.

– Впровадження політики доступу, наприклад, блокування підозрілих IP-адрес або регіонів, звідки надходить шкідливий трафік.

Резервування каналів:

– Забезпечення резервних інтернет-з'єднань із високою пропускною здатністю для мінімізації впливу атак.

4. Захист від атак на бази даних

Бази даних є критичним компонентом серверних систем, тому їхній захист потребує особливого підходу.

Методи захисту:

– Використання параметризованих запитів для захисту від SQL-ін'єкцій.

– Впровадження механізмів аутентифікації та шифрування даних у базах даних.

– Регулярний аудит безпеки баз даних для виявлення вразливостей.

– Обмеження доступу до бази даних лише для авторизованих користувачів і додатків.

Резервне копіювання:

– Регулярне створення резервних копій баз даних дозволяє швидко відновити їх у разі шифрування або видалення даних.

5. Підготовка до атак і реагування

Важливим аспектом захисту серверів є готовність до можливих атак та оперативне реагування на інциденти.

Планування:

– Розробка плану дій у разі атак, який включає кроки з ізоляції атакуваних ресурсів, відновлення роботи та повідомлення користувачів.

– Проведення регулярних тестувань, наприклад, імітацій DDoS-атак, щоб перевірити готовність систем до реальних загроз.

Реагування:

– Миттєве виявлення атак і перемикання на резервні ресурси.

– Використання механізмів автоматичного масштабування, які забезпечують тимчасове збільшення ресурсів у разі високого навантаження.

2.3 Загрози для прикладного рівня

Прикладний рівень є найвищим рівнем у моделі взаємодії мережевих протоколів, що забезпечує роботу таких сервісів, як веб-додатки, API, DNS-сервери та інші сервіси, які взаємодіють із користувачами та системами. Через важливість цього рівня в забезпеченні функціональності багатьох систем і додатків, він стає однією з головних цілей для зловмисників. Загрози для прикладного рівня можуть мати широкий спектр форм, кожна з яких спрямована на порушення роботи або викрадення даних.

Прикладний рівень інформаційних систем є однією з ключових складових сучасних мережевих технологій, оскільки саме на цьому рівні реалізуються сервіси, які взаємодіють із кінцевими користувачами. До таких сервісів належать

веб-додатки, API, DNS-сервери, електронна пошта та інші ресурси, які забезпечують обмін даними, обробку запитів і надання послуг. Через критичну роль прикладного рівня він є основною ціллю для атак зловмисників, які намагаються порушити його роботу, викрасти конфіденційні дані або скомпрометувати сервіси [16].

Однією з найпоширеніших загроз для прикладного рівня є атаки на веб-додатки, які мають безпосередній зв’язок із користувачами. Зловмисники часто використовують SQL-ін’єкції для доступу до баз даних, впровадження шкідливого коду через XSS (Cross-Site Scripting) або перебору паролів для отримання несанкціонованого доступу до облікових записів. Веб-додатки також можуть ставати мішенню для перехоплення сеансів, що дозволяє зловмисникам викрадати активні сесії користувачів і отримувати доступ до їхніх даних. Такі атаки можуть мати серйозні наслідки, включаючи втрату конфіденційної інформації, компрометацію даних і значне зниження репутації організації.

API, які забезпечують взаємодію між різними компонентами системи, також знаходяться під постійною загрозою. Зловмисники використовують уразливості в API для впровадження шкідливих даних, обходу обмежень на кількість запитів або використання зламаних облікових даних для отримання доступу до системи. Така активність може порушити роботу критичних сервісів або призвести до викрадення конфіденційної інформації.

DNS-сервери, які є основою роботи Інтернету, часто стають мішенню для атак через їх важливість у забезпеченні доступу до ресурсів. Зловмисники використовують методи DNS Spoofing для підробки відповідей або Cache Poisoning для компрометації кешу DNS-серверів. Такі атаки можуть перенаправляти користувачів на шкідливі сайти, порушувати роботу легітимних ресурсів і навіть сприяти реалізації потужних DDoS-атак.

Інші сервіси прикладного рівня, такі як електронна пошта, FTP або системи обміну повідомленнями, також часто стають мішенню для атак. Фішинг, підробка повідомлень (Spoofing) і використання вразливостей у протоколах є найпоширенішими методами атак на ці сервіси. Це може призводити до втрати

конфіденційності, поширення шкідливого програмного забезпечення та порушення роботи сервісів.

Загрози для прикладного рівня є надзвичайно різноманітними, що вимагає впровадження комплексного підходу до захисту. Використання міжмережевих екранів (WAF), систем виявлення вторгнень (IDS/IPS), регулярне тестування на проникнення та моніторинг безпеки допомагають ефективно знижувати ризики атак. У таблиці 2.2, узагальнені основні типи атак, їх цілі та наслідки, що дозволяє краще зрозуміти природу цих загроз та ефективно з ними боротися.

Таблиця 2.2.

Розповсюджені атаки прикладного рівня

Цільовий рівень	**Тип атаки**	**Мета атаки**
Веб-додатки	SQL-ін'єкції	Доступ до баз даних, викрадення або видалення даних.
Веб-додатки	XSS (Cross-Site Scripting)	Впровадження шкідливого коду для виконання на стороні користувача.
Веб-додатки	Brute Force	Отримання несанкціонованого доступу шляхом підбору паролів.
Веб-додатки	Session Hijacking	Перехоплення сеансів для доступу до облікових записів.
API	API Injection	Впровадження шкідливих даних через API-запити.
API	Rate Limiting Bypass	Обхід обмежень на кількість запитів до API.
API	Credential Stuffing	Використання зламаних облікових даних для доступу до API.
DNS-сервери	DNS Spoofing	Підробка DNS-відповідей для перенаправлення користувачів.
DNS-сервери	DNS Amplification	Використання DNS для підсилення DDoS-атак.
DNS-сервери	Cache Poisoning	Компрометація кешу DNS-сервера для надання фальшивих відповідей.
Інші сервіси	Phishing	Обман користувачів через електронну пошту для викрадення даних.
Інші сервіси	Exploit Attacks	Використання вразливостей у протоколах, таких як SMTP, IMAP, FTP.
Інші сервіси	Spoofing	Підробка адреси відправника або змісту повідомлень.

Прикладний рівень є найвразливішим через свою безпосередню взаємодію з користувачами, обробку даних і надання сервісів. Зловмисники використовують різні методи атак, спрямованих на порушення роботи систем,

викрадення конфіденційних даних або отримання несанкціонованого доступу. Нижче описані найбільш поширені методи атак на прикладному рівні, їх механізми дії та наслідки.

SQL-ін’єкції є одним із найпоширеніших методів атак, спрямованих на взаємодію веб-додатків із базами даних. Атака полягає у впровадженні шкідливого SQL-коду через поля введення або URL-запити, які сервер обробляє без належної перевірки.

Механізм атаки:

– Зловмисник вводить SQL-команди, які змінюють структуру запиту до бази даних.

– Наприклад, команда може додати запит на отримання всіх даних із бази або видалення певної інформації.

Наслідки:

– Викрадення конфіденційних даних.

– Порушення цілісності даних у базі.

– Можливість отримання доступу до адміністративних функцій.

XXE-атаки спрямовані на вразливості у процесі обробки XML-документів сервером. Вони дозволяють зловмисникам отримати доступ до внутрішніх ресурсів серверів або виконати шкідливий код.

Механізм атаки:

– Зловмисник додає шкідливі зовнішні сутності (entities) до XML-документів, які сервер обробляє.

– Це може призвести до отримання доступу до конфіденційних файлів на сервері, таких як паролі, або виконання команд системи.

Наслідки:

– Розкриття конфіденційної інформації.

– Порушення конфіденційності серверних систем.

– Виконання довільного коду на сервері.

Cross-Site Scripting (XSS)

Атаки типу XSS дозволяють зловмисникам впроваджувати шкідливий код у веб-додатки, який виконується на стороні клієнта.

Механізм атаки:

– Зловмисник додає шкідливий JavaScript-код до веб-додатка через форми введення, які не перевіряють дані.

– Цей код виконується в браузері користувача, коли він переглядає сторінку.

Наслідки:

– Викрадення кукі-файлів, які можуть містити сесійні токени.

– Поширення шкідливого програмного забезпечення.

– Маніпуляції з відображенням веб-сторінок.

Command Injection – це метод атаки, коли зловмисник додає команди для виконання на сервері до запитів додатка, який обробляє ці дані.

Механізм атаки:

– Зловмисник вводить команди через параметри URL або форми введення.

– Сервер виконує ці команди як частину системного процесу.

Наслідки:

– Виконання шкідливого коду.

– Отримання контролю над серверною системою.

– Видалення або модифікація критичних файлів.

Credential Stuffing – цей метод атаки полягає у використанні зламаних облікових даних, отриманих із компрометованих баз даних, для доступу до інших систем.

Механізм атаки:

– Зловмисники автоматизують перевірку комбінацій логінів і паролів у різних сервісах.

– Атака ефективна через те, що багато користувачів використовують однакові паролі для різних платформ.

Наслідки:

– Несанкціонований доступ до систем.

– Викрадення персональної інформації.

– Компрометація корпоративних або особистих облікових записів.

Distributed Denial of Service (DDoS) на прикладному рівні – атаки спрямовані на виснаження ресурсів веб-додатків або сервісів шляхом генерації великої кількості запитів.

Механізм атаки:

– Зловмисники використовують ботнети або автоматизовані скрипти для створення великого навантаження на веб-сервери.

– Мета – перевантажити сервер так, щоб він не міг обробляти легітимні запити.

Наслідки:

– Недоступність веб-сайтів або сервісів.

– Втрати продуктивності та збитки для бізнесу.

– Репутаційні ризики для компанії.

2.4 Огляд технологій для протидії DDoS-атакам

DDoS-атаки (Distributed Denial of Service) є одними з найскладніших і найбільш руйнівних типів кібератак, які можуть паралізувати роботу інтернет-ресурсів, веб-додатків та серверних систем. Ефективна протидія таким атакам потребує використання сучасних технологій захисту, які здатні виявляти та нейтралізувати шкідливий трафік, забезпечуючи при цьому доступність легітимних сервісів. Серед найбільш популярних і дієвих рішень для протидії DDoS-атакам можна виділити Web Application Firewall (WAF), Content Delivery Network (CDN) і системи виявлення та запобігання вторгнень (IDS/IPS). Кожна з цих технологій відіграє унікальну роль у забезпеченні кібербезпеки [17].

Web Application Firewall (WAF) – це захисна технологія, яка аналізує трафік на рівні веб-додатків та блокує підозрілі запити ще до того, як вони

досягнуть сервера. WAF працює як бар'єр між користувачем і сервером, захищаючи додатки від цілого спектру атак, зокрема SQL-ін'єкцій, XSS (Cross-Site Scripting), і HTTP Flood.

WAF здатен розпізнавати характерні патерни DDoS-атак на прикладному рівні, такі як надмірна кількість однотипних запитів або спроби перевантаження ресурсів додатків. Завдяки фільтруванню шкідливого трафіку WAF допомагає зберігати ресурси серверів для обробки легітимних запитів. Крім того, багато сучасних WAF-систем використовують машинне навчання для адаптації до нових загроз і автоматичного оновлення правил фільтрації. Одним із популярних прикладів таких рішень є Cloudflare WAF, який здатен захищати веб-додатки навіть під час масштабних DDoS-атак.

Content Delivery Network (CDN) є потужним інструментом для мінімізації впливу DDoS-атак за рахунок використання глобально розподіленої мережі серверів. Основна ідея CDN полягає в тому, щоб перенаправляти трафік через численні вузли, зменшуючи навантаження на основний сервер і розподіляючи запити між кількома географічно розташованими датацентрами.

CDN-сервіси, такі як Akamai, Cloudflare або AWS CloudFront, здатні виявляти та блокувати аномальний трафік ще на рівні мережі, не допускаючи його до основного серверного обладнання. Завдяки використанню кешування CDN також значно зменшує потребу в ресурсах для обробки повторюваних запитів. У випадку DDoS-атаки CDN може автоматично перенаправляти трафік на резервні вузли або використовувати механізми обмеження швидкості, забезпечуючи безперервну роботу сервісів.

Системи виявлення та запобігання вторгнень (IDS/IPS) є критично важливим елементом сучасної кібербезпеки, спрямованим на моніторинг, аналіз і реагування на аномалії в мережевому трафіку. IDS-функціонал забезпечує пасивне виявлення підозрілої активності, наприклад, спроби перевантаження мережі або надмірну кількість запитів із одного джерела. IPS-системи працюють у режимі реального часу, автоматично блокуючи виявлені загрози.

Завдяки використанню сигнатурного та поведінкового аналізу IDS/IPS-системи, такі як Snort або Suricata, можуть виявляти характерні ознаки DDoS-атак, наприклад, раптове зростання обсягу трафіку або нехарактерні дії користувачів. IPS, у свою чергу, дозволяє автоматично блокувати шкідливий трафік, налаштовувати правила доступу та фільтрувати запити. Комбінуючи ці функції, IDS/IPS забезпечує комплексний захист мережі та серверів від атак будь-якого масштабу.

Ефективне виявлення DDoS-атак є ключовим завданням для забезпечення кібербезпеки. З огляду на різноманітність і масштаби сучасних атак, традиційні методи виявлення можуть виявитися недостатніми. Тому сучасні механізми виявлення все більше орієнтовані на використання технологій аналізу трафіку в реальному часі та машинного навчання, що дозволяють ідентифікувати аномалії, класифікувати атаки та оперативно реагувати на загрози.

Аналіз мережевого трафіку в реальному часі є базовим компонентом сучасних систем виявлення DDoS-атак. Цей підхід передбачає безперервний моніторинг мережевого трафіку для виявлення аномалій, які можуть свідчити про атаку.

Основні функції:

– **Аналіз поведінкових патернів**: Виявлення відхилень у поведінці трафіку, наприклад, раптове зростання обсягу запитів, велика кількість з'єднань від одного джерела або нерівномірний розподіл трафіку.

– **Порівняння з базовими показниками**: Системи використовують історичні дані про звичайний трафік, щоб виявити аномалії.

– **Географічний аналіз**: Виявлення незвичних джерел трафіку з підозрілих регіонів.

Інструменти:

– Системи на основі NetFlow (наприклад, Cisco NetFlow) дозволяють збирати й аналізувати дані про мережевий трафік.

– Інструменти моніторингу, такі як SolarWinds або Wireshark, надають детальний аналіз трафіку.

Переваги:

– Швидке виявлення атак.

– Можливість миттєвого реагування, наприклад, блокування підозрілих IP-адрес або фільтрація трафіку.

– Підтримка інтеграції з іншими системами кібербезпеки, такими як IDS/IPS.

Машинне навчання (**ML**) стає важливим інструментом для виявлення та класифікації DDoS-атак завдяки його здатності аналізувати великі обсяги даних і автоматично виявляти складні закономірності, які можуть бути невидимими для традиційних систем.

Методи машинного навчання:

– **Наглядове навчання**: Використання попередньо класифікованих даних для тренування моделей, які можуть розрізняти легітимний і шкідливий трафік.

– **Безнаглядове навчання**: Виявлення аномалій у трафіку без попереднього маркування даних, що дозволяє ідентифікувати нові види атак.

– **Глибоке навчання (Deep Learning)**: Використання нейронних мереж для складного аналізу трафіку, включаючи виявлення аномальних патернів і передбачення майбутніх атак.

Процес роботи ML-систем:

– Збір даних про трафік, зокрема обсяг, джерела, протоколи та поведінкові характеристики.

– Аналіз даних для створення моделей нормального трафіку.

– Виявлення відхилень, які відповідають ознакам DDoS-атаки.

– Постійне навчання моделі на основі нових даних для адаптації до змін у поведінці атак.

Приклади рішень:

– Використання ML у хмарних платформах, таких як AWS Shield Advanced або Azure DDoS Protection, для автоматичного визначення атак.

– Локальні рішення, такі як використання TensorFlow або PyTorch для розробки індивідуальних моделей виявлення.

Переваги ML:

– Висока точність у виявленні складних атак, які важко ідентифікувати за допомогою простих правил.

– Адаптація до нових типів атак завдяки динамічному навчанню.

– Зменшення кількості помилкових спрацьовувань.

2.5 Аналіз підходів до ідентифікації DDoS-атак

У сучасному кіберсередовищі ідентифікація DDoS-атак є одним із ключових завдань забезпечення інформаційної безпеки. Основними техніками виявлення таких атак є аномалійний аналіз, сигнатурний аналіз та порівняння базових показників. Кожен із цих методів має свої переваги, недоліки та області застосування, що вимагають ретельного аналізу для забезпечення їх ефективного використання.

Аномалійний аналіз базується на виявленні відхилень від нормальної поведінки мережі. Цей підхід передбачає створення базового профілю мережевого трафіку за нормальних умов. У разі виникнення аномалій, які можуть бути викликані DDoS-атаками, система сигналізує про потенційну загрозу. Основними інструментами для реалізації цього підходу є методи машинного навчання, статистичний аналіз і моделювання.

Переваги аномалійного аналізу включають здатність виявляти невідомі або нові типи атак, які не можуть бути ідентифіковані за допомогою сигнатурного аналізу. Водночас, цей підхід схильний до високого рівня хибнопозитивних спрацьовувань, оскільки нормальна поведінка мережі може варіюватися в залежності від часу доби, типу користувачів або інших факторів [18].

Сигнатурний аналіз використовує базу даних відомих сигнатур атак для їх ідентифікації. Сигнатура являє собою унікальний шаблон або характеристику

атаки, що дозволяє швидко ідентифікувати загрозу, якщо її сигнатура вже відома системі.

Перевагою цього підходу є його висока точність і низький рівень хибнопозитивних спрацьовувань для відомих атак. Проте основним недоліком є неспроможність виявляти нові або модифіковані атаки, які не мають відповідних сигнатур у базі даних. Таким чином, для ефективного функціонування цього методу необхідне регулярне оновлення бази сигнатур.

Порівняння базових показників – цей підхід полягає у постійному моніторингу та порівнянні поточних характеристик мережевого трафіку із заздалегідь визначеними базовими показниками. До базових показників можуть належати такі параметри, як швидкість передачі даних, кількість з'єднань на одиницю часу, розмір пакетів тощо. У разі виявлення значних відхилень система може визначити, що це є ознакою DDoS-атаки.

Перевага цього методу полягає у його простоті реалізації та можливості швидкого налаштування. Недоліком є обмежена ефективність у разі складних або малопотужних атак, які можуть незначно змінювати поведінку мережевого трафіку, залишаючись непомітними для системи. Таблиця 2.3 допоможе оцінити переваги Wireshark, NetFlow та Zabbix, недоліки та області застосування

Таблиця 2.3.

Порівняння інструментів моніторингу трафіку

Інструмент	**Основні функції**	**Переваги**	**Недоліки**
Wireshark	Аналіз пакетів, глибоке вивчення мережевого трафіку	Інтуїтивний інтерфейс, потужні функції фільтрації	Не підходить для масштабного моніторингу
NetFlow	Збір та аналіз потоків даних, підтримка виявлення DDoS	Масштабованість, інтеграція з іншими системами	Менша деталізація в порівнянні з аналізом пакетів

Продовження таблиці 2.3.

Zabbix	Моніторинг мережевого обладнання, серверів, трафіку	Гнучкість, можливість налаштування автоматизації	Високі вимоги до ресурсів для великих мереж

Кожен з розглянутих підходів має свої особливості та оптимальні сфери застосування. Аномалійний аналіз забезпечує можливість виявлення нових атак, але вимагає ретельного налаштування і підвищеної обробки даних. Сигнатурний аналіз є ефективним для боротьби з відомими загрозами, але потребує постійного оновлення бази даних. Порівняння базових показників є простим і швидким у реалізації, але менш ефективним для складних атак. Оптимальним рішенням є комбінування цих підходів для досягнення максимальної ефективності захисту від DDoS-атак [19].

Висновки до розділу 2

Проаналізовано основні види атак на відмову в обслуговуванні, які націлені на інфраструктуру мережі, серверні системи та прикладний рівень. Виявлено, що кожен з цих рівнів має специфічні вразливості, які можуть бути використані для порушення нормальної роботи системи. Огляд технологій протидії DDoS-атакам показав, що ефективні методи захисту включають комбінацію фільтрації трафіку, аналізу аномалій та адаптивного реагування.

Проведено детальний аналіз підходів до ідентифікації DDoS-атак, що включає використання передових методів виявлення, таких як машинне навчання та поведінковий аналіз. Показано, що для своєчасного виявлення атак важливо застосовувати комплексний підхід, який дозволяє оперативно реагувати на загрози та забезпечити безпеку мережі.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ПРОТИДІЇ ТА ДОСЛІДЖЕННЯ АТАК

3.1 Розробка тестового середовища для моделювання DDoS-атаки

Для дослідження методів атак на відмову в обслуговуванні необхідно створити власний тестовий сервер. Використання безкоштовного та відкритого програмного забезпечення дозволяє зменшити витрати та забезпечує мінімальне споживання ресурсів.

Етапи налаштування веб-сервера на Windows

Підготовка

Перший крок – завантаження необхідного програмного забезпечення, яке забезпечує роботу сервера. Нижче наведено ключові компоненти для створення веб-сервера:

– Apache – основний веб-сервер. Це програмне забезпечення відповідає за обробку запитів від клієнтів (користувачів або браузерів) і передачу їм відповідної інформації.

– PHP – середовище для запуску скриптів, написаних на мові PHP, що використовується для динамічних веб-додатків.

– MySQL – система управління базами даних. Вона дозволяє зберігати дані в структурованому вигляді та забезпечує швидкий доступ до них.

– phpMyAdmin – зручний інтерфейс для роботи з базами даних, який спрощує управління MySQL.

Створення структури сервера.

Основною метою є впорядкування файлів для зручного обслуговування та резервного копіювання. Для цього у кореневій директорії (наприклад, на диску C:) створюється папка Server, яка буде містити всі необхідні файли та дані (рис. 3.1).

Далі у папці Server створюються підкаталоги:

- bin – для розміщення виконуваних файлів сервера та пов’язаних компонентів.
- data – для зберігання даних, включаючи:
- DB – папку для баз даних;
- htdocs – папку для файлів сайтів.

У підкаталозі DB створюється ще одна порожня папка data, яка слугуватиме для зберігання внутрішніх даних бази.

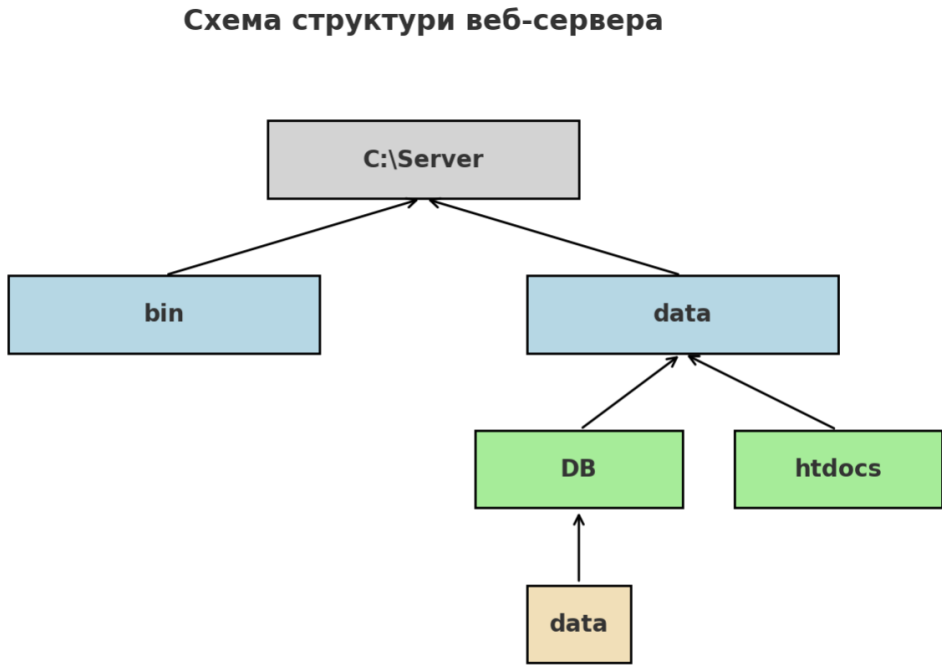


Рис. 3.1. Структурна реалізація Web-server.

Встановлення та запуск Apache 2.4 на Windows

1. Підготовка архіву з Apache Перед початком встановлення необхідно завантажити дистрибутив Apache 2.4 (наприклад, із офіційного сайту Apache Lounge) та розпакувати його. Архів рекомендується розпакувати в каталог C:\Server\bin\. У результаті структура папок повинна виглядати наступним чином:

C:\Server\bin\Apache24

2. Встановлення Apache як служби Windows (рис. 3.2). Для того щоб веб-сервер Apache працював як системна служба Windows, необхідно виконати наступні дії:

– Відкрити PowerShell або Командний рядок від імені адміністратора. (Для цього знайдіть відповідну програму через меню «Пуск», натисніть правою кнопкою миші та виберіть «Запустити від імені адміністратора»).

– Ввести команду для інсталяції служби Apache:

C:\Server\bin\Apache24\bin\httpd.exe -k install

3. Запуск веб-сервера Apache Після інсталяції служби необхідно запустити сервер. Для цього введіть у тому ж вікні PowerShell або командному рядку наступну команду:

C:\Server\bin\Apache24\bin\httpd.exe -k start

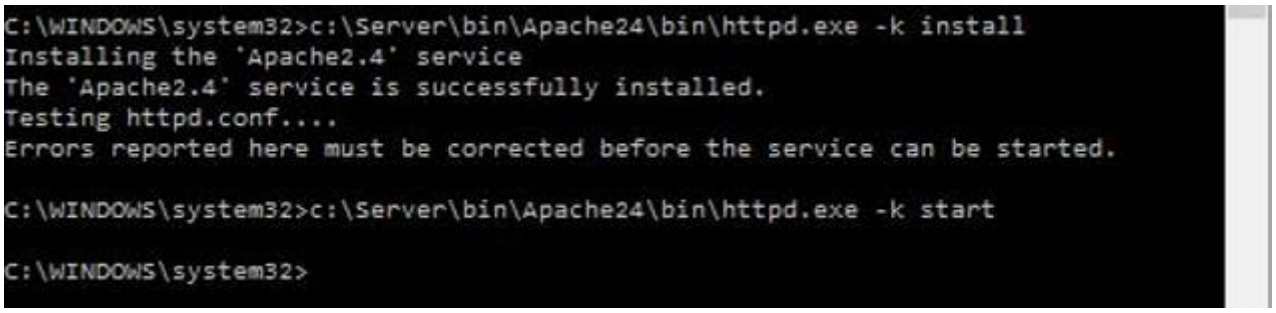


Рис. 3.2. Інсталяція Apache server.

4. Перевірка стану служби

Для переконання, що Apache працює, можна скористатися командою:

C:\Server\bin\Apache24\bin\httpd.exe -k status

1. Підготовка архіву з MySQL. Спочатку необхідно завантажити дистрибутив MySQL (наприклад, із офіційного сайту MySQL Community Downloads) та розпакувати його. Файли сервера MySQL рекомендується розмістити в каталозі:

C:\Server\bin\mysql-8.0

2. Ініціалізація бази даних. Щоб створити початкову структуру бази даних та виконати налаштування MySQL, необхідно виконати наступну команду в Командному рядку або PowerShell від імені адміністратора:

C:\Server\bin\mysql-8.0\bin\mysqld --initialize-insecure --user=root

3. Реєстрація MySQL як системної служби. Для забезпечення зручного запуску сервера MySQL необхідно зареєструвати його як службу в системі (рис. 3.3). Це робиться за допомогою наступної команди:

C:\Server\bin\mysql-8.0\bin\mysqld –install

4. Запуск сервера MySQL. Щоб запустити сервер, виконайте команду:

net start mysql

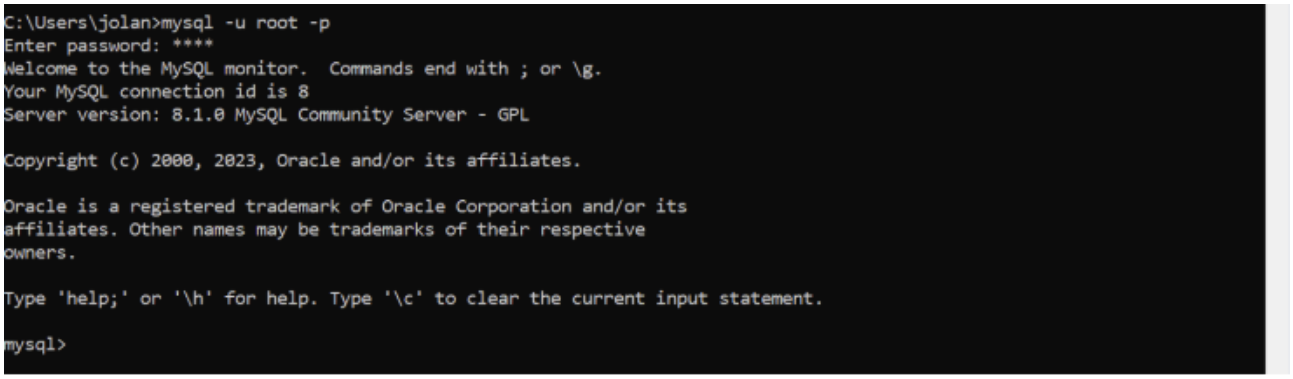


Рис. 3.3. Інсталяція MySQL.

Після завершення процесу встановлення та ініціалізації бази даних MySQL у каталозі (рис. 3.4), який використовується для зберігання даних, автоматично створюються необхідні файли та директорії на шляху C:\Server\data\DB\data\.

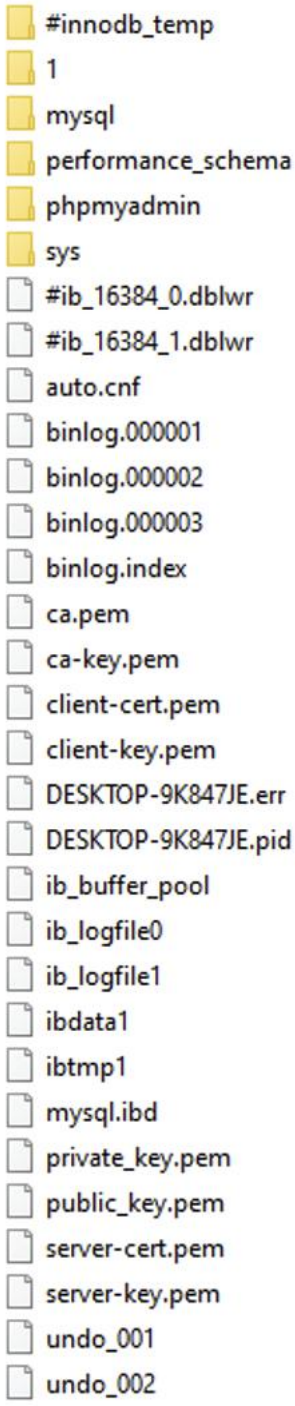


Рис. 3.4. Корнева директорія БД MySQL.

Інсталяція Frontend-PHP. У каталозі C:\Server\bin\ створюємо папку з назвою PHP. Потім розпаковуємо та переносимо в неї файли з архіву, завантаженого заздалегідь із дистрибутивом PHP.

Для встановлення phpMyAdmin необхідно скопіювати вміст завантаженого архіву в каталог c:\Server\data\htdocs\. Щоб локальний сайт став

доступним в Інтернеті, потрібно налаштувати переадресацію портів на роутері. Наприклад, на роутері TP-LINK Archer C80 потрібно налаштувати переадресацію порту 80. Після цього, щоб відкрити веб-сторінку, слід ввести зовнішню IP-адресу комп'ютера в адресний рядок браузера, використовуючи протокол HTTP (рис. 3.5).

	ID	Тип сервіса	Зовнішній порт	Внутрішній IP-адрес	Внутрішній порт	Протокол	Стан	Змінити
☐	1	HTTP	80	192.168.0.104	80	TCP		

Рис. 3.5. Мапінг зовнішнього порту для серверу на 80.

На наступному рисунку 3.6 зображений наш сервер у вигляді веб сторінки.

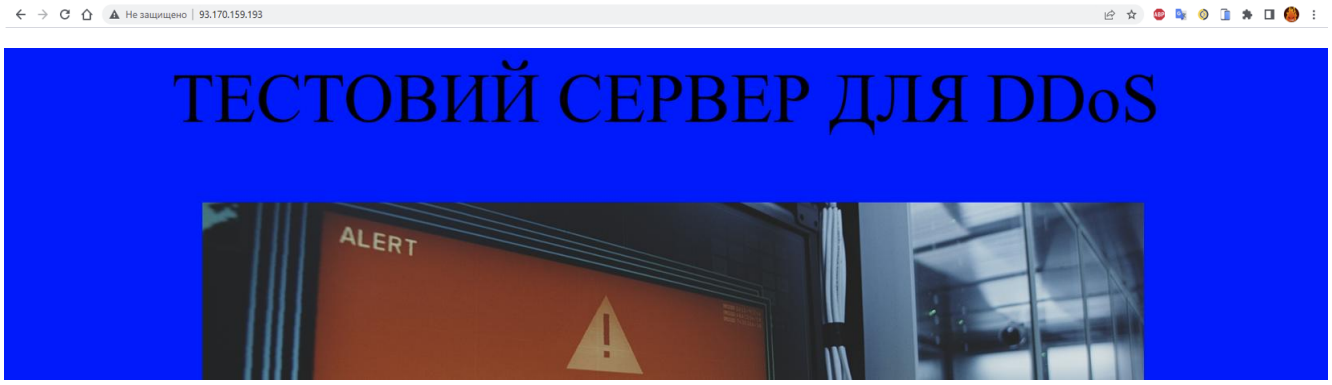


Рис. 3.6. Завантажений веб-сервер.

3.2 Інструменти для імітації атак типу відмова в обслуговування

В якості інструменту для атак можна розглянути LOIC (Low Orbit Ion Cannon) – програму з відкритим вихідним кодом, призначену для здійснення мережевих атак. Вона написана мовою програмування C# і спочатку була створена компанією Praetox Technologies, але згодом стала загальнодоступною [20]. Основне призначення LOIC – здійснення атак типу DoS (Denial of Service)

або DDoS (Distributed Denial of Service) шляхом надсилання великої кількості запитів до цільового сервера.

Програма працює за наступним принципом: вона генерує і відправляє величезний потік TCP, UDP або HTTP-запитів, що може призвести до перевантаження обчислювальних ресурсів сервера та, відповідно, до його відмови в обслуговуванні.

Налаштування та використання LOIC:

1. Запуск програми – завантаження та встановлення LOIC.

2. Вибір типу атаки:

DoS-атака – здійснюється з одного комп’ютера.

DDoS-атака – використовується велика кількість пристроїв, що одночасно надсилають запити на сервер.

3. Введення цілі:

Можна вказати IP-адресу або URL вебсайту, на який буде спрямована атака.

4. Налаштування параметрів:

Визначення кількості потоків та типу запитів (TCP, UDP, HTTP).

Встановлення режиму роботи – постійна або періодична атака.

5. Запуск атаки – після натискання кнопки "IMMA CHARGIN MAH LAZER", LOIC починає надсилати пакети на вказану ціль.

LOIC відомий тим, що не приховує IP-адресу атакуючого, що робить його небезпечним для користувача, оскільки правоохоронні органи легко можуть відстежити джерело атаки. У зв’язку з цим, у DDoS-атаках часто використовується ботнет або проксі-сервери для анонімності (рис. 3.7).

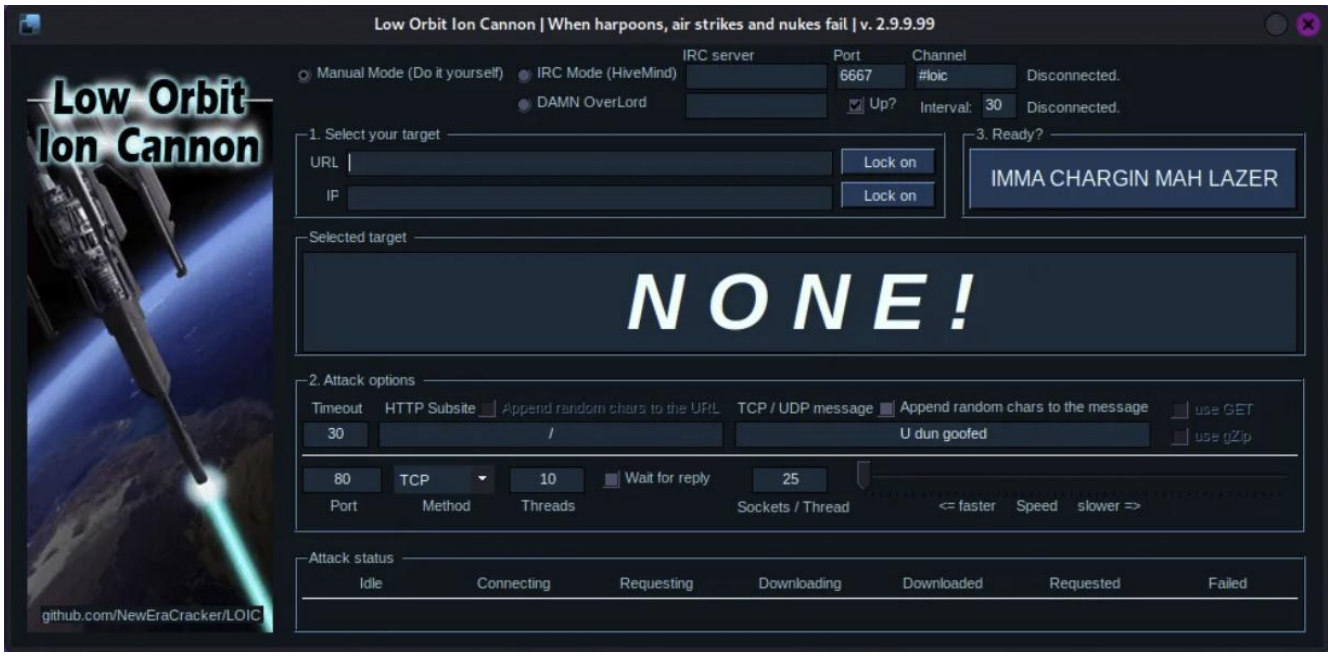


Рис. 3.7. Типовий інтерфейс LOIC.

Вибір цілі. У головному вікні LOIC користувач вводить IP-адресу або URL-адресу цільового сервера у поле "Select your target". Після цього вказана інформація відображається в секції "Selected Target", підтверджуючи правильність введених даних (рис. 3.8).

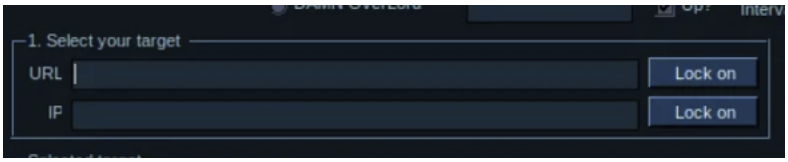


Рис. 3.8. Блок (Основна інформація про ціль).

Типи атак. Програма підтримує три основні методи атаки: TCP, UDP і HTTP-запити. TCP і UDP використовуються для прямого навантаження на сервер, а HTTP-запити імітують звернення до вебсторінок, що може викликати значне уповільнення роботи сайту (рис. 3.9).

Рис. 3.9. Блок (Вибір атаки).

Налаштування потужності атаки. LOIC дозволяє встановлювати кількість потоків, які будуть одночасно надсилати пакети, а також швидкість їх відправки. Чим більше потоків і вища частота запитів, тим потужніший трафік надходить на сервер. Режим "Hivemind". Дана функція дозволяє дистанційно керувати LOIC через IRC-канал, що особливо актуально для DDoS-атак [21]. При активації цього режиму комп’ютер користувача може бути використаний у ботнеті без його прямого контролю. Випадковий вибір портів. Опція "Random Port" змінює порти відправки пакетів, що ускладнює блокування атаки з боку цільового сервера (рис. 3.10). Це може допомогти обійти деякі прості системи захисту.

Рис. 3.10. Блок (Налаштування потужності).

Запуск атаки. Після налаштування всіх параметрів натискання кнопки "IMMA CHARGIN MAH LAZER" запускає атаку. LOIC починає генерувати запити на вказану адресу, створюючи значне навантаження на сервер. Безпека та анонімність. LOIC не приховує IP-адресу атакуючого, тому використання програми без VPN, проксі-серверів або ботнету робить користувача легко відстежуваним правоохоронними органами (рис. 3.11).

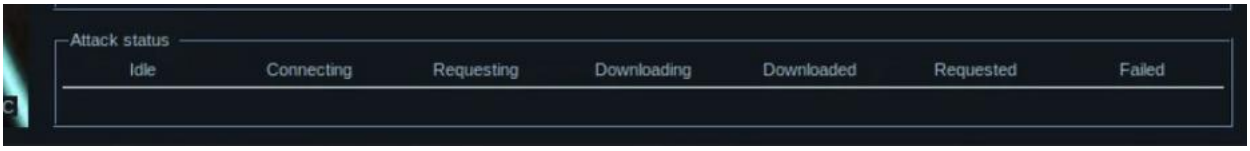


Рис. 3.11. Блок (Статус атаки).

Юридичні наслідки. Використання LOIC для атак на чужі сервери є незаконним у більшості країн. Несанкціоновані DDoS-атаки можуть призвести до кримінальної відповідальності, штрафів або навіть позбавлення волі.

Почнемо тестування. Для початку потрібно налаштувати її. Обрати тип атаки звичайну або розподілену атаку (рис. 3.12). Далі потрібно ввести посилання або IP адресу цілі

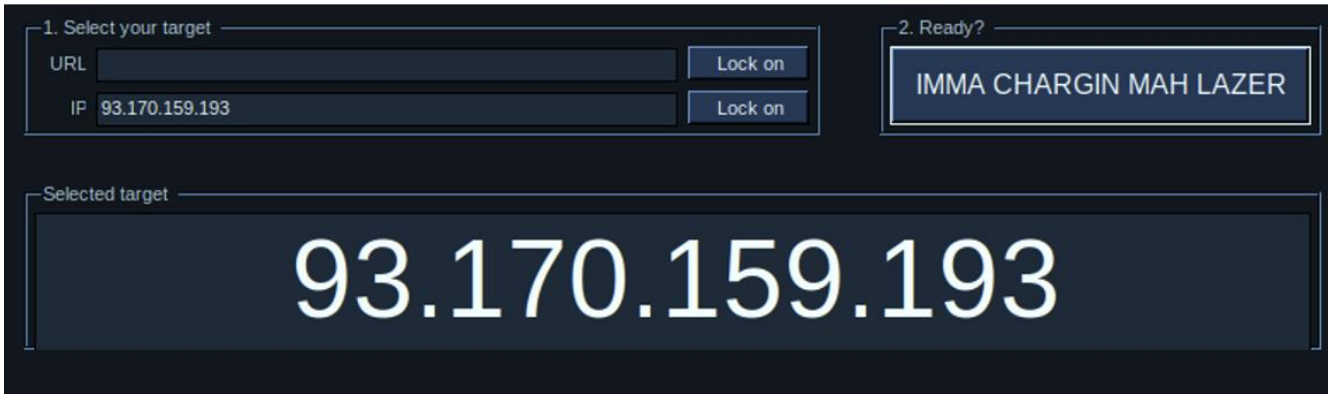


Рис. 3.12. Налаштування поточного значення цілі.

Атаку будемо виконувати методом tcp, тому обираємо його в наступному блоці налаштувань, а також порт та кількість пакетів (рис. 3.13).

Рис. 3.13. Налаштування опцій атаки.

Після запуску атаки в LOIC користувач може відстежувати її ефективність у режимі реального часу. У вікні програми відображається «кількість відправлених запитів», число отриманих відповідей від сервера, а також «пакети з помилками», що можуть свідчити про перевантаження цілі або блокування

трафіку. Це дозволяє аналізувати, наскільки ефективно працює атака, і при необхідності коригувати її параметри (рис. 3.14).

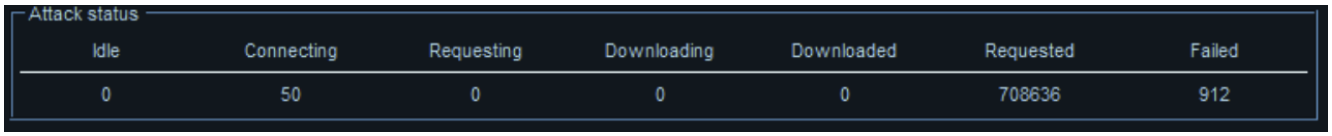


Рис. 3.14. Результати тестування системи атакою.

На рисунку 3.15. показано як програма WireShark пропускає капети з фіксуванням інструменту LOIC.

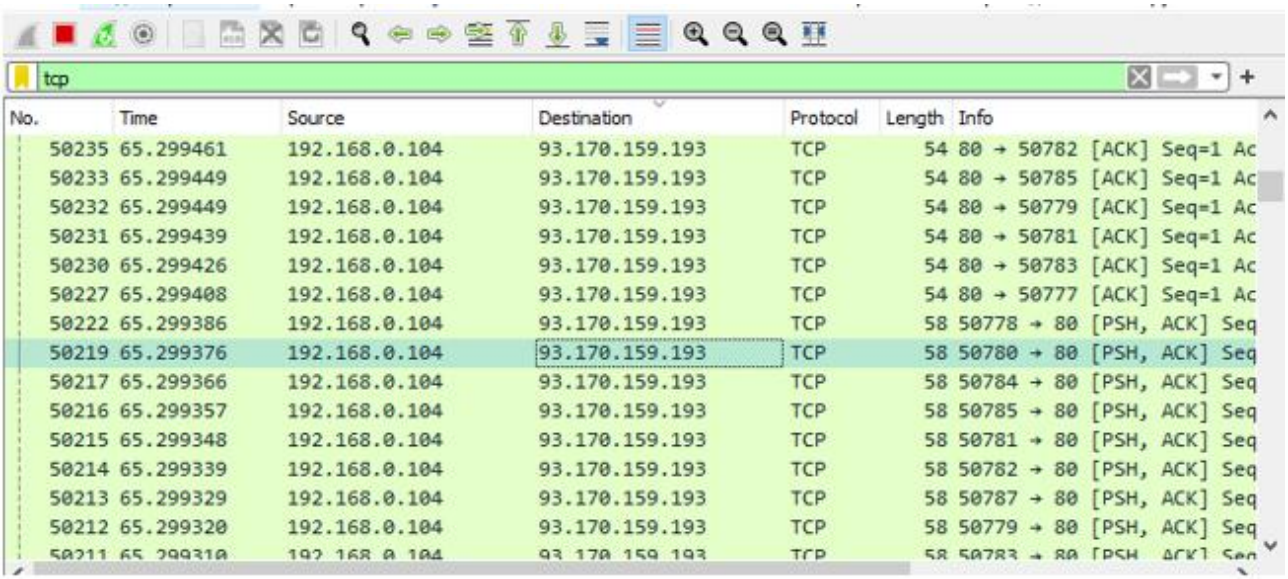


Рис. 3.15. Перегляд пакетів програмою WireShark.

Під час атаки LOIC разом із пакетами надсилає TCP/UDP-повідомлення, вміст яких можна налаштувати вручну. У цьому випадку було задано текстове повідомлення "Тестова атака". Для перевірки його доставки використовувалася програма Wireshark, яка дозволяє аналізувати мережевий трафік. Досліджуючи перехоплені пакети, вдалося підтвердити, що сервер успішно отримав надіслане повідомлення, що підтверджується відповідними записами в захоплених даних [22].

У мережі з’явився новий інструмент для здійснення атак на відмову в обслуговуванні – «DRipper» (рис. 3.16). Цей скрипт був розроблений для

створення потужного мережевого навантаження і підтримує кілька видів атак, зокрема «HTTP, TCP та UDP flood». Завдяки своїй простоті у використанні та ефективності, DRipper швидко привернув увагу користувачів, які шукають спосіб тестування стійкості серверів до DDoS-атак. Основна його особливість – можливість одночасно генерувати великий потік запитів, що може значно перевантажити цільову систему та порушити її роботу.

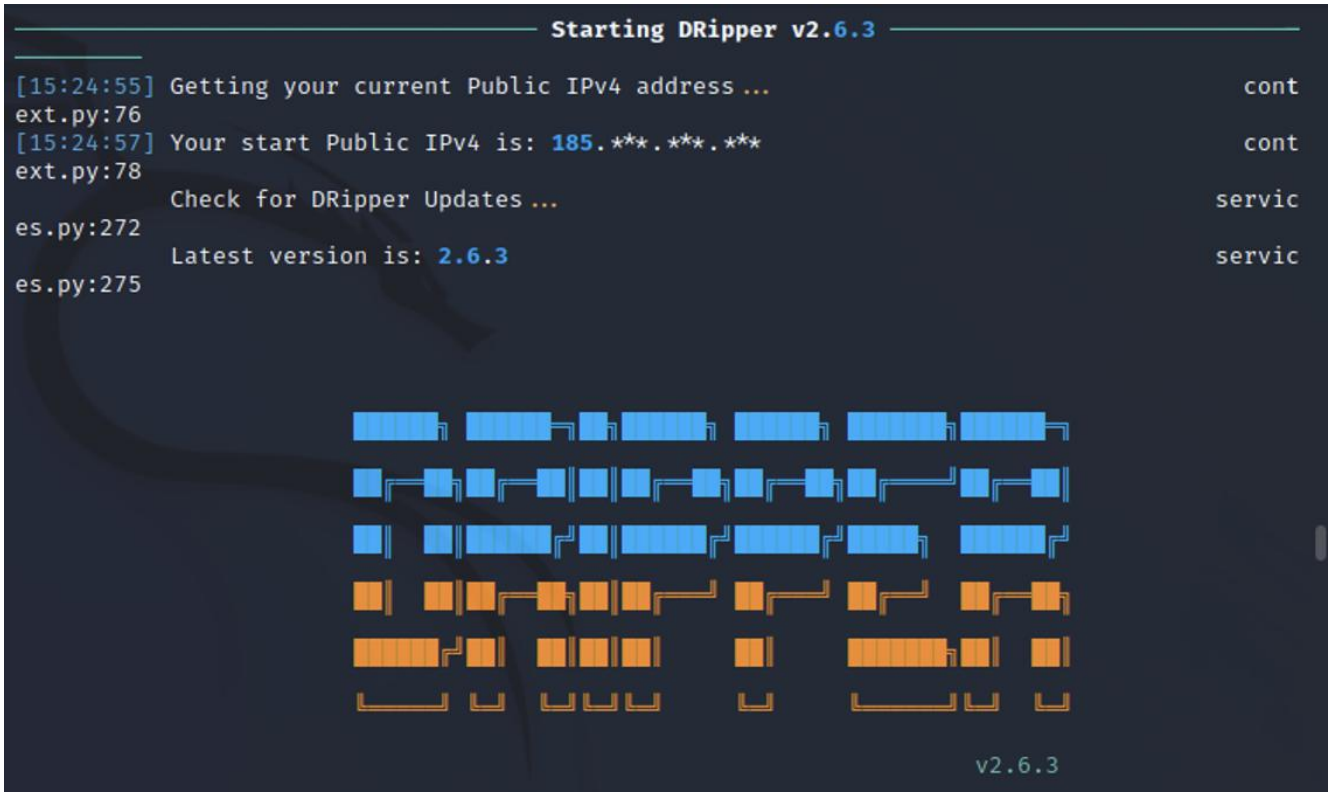


Рис. 3.16. Інтерфейс інструменту.

DRipper можна використовувати двома способами – як окремий «Python-скрипт» або в середовищі «Docker». Запуск безпосередньо через Python є більш продуктивним, оскільки Docker додає певні накладні витрати на ресурси системи.

Підтримувані методи атак у DRipper:

– HTTP Flood – атака на Прикладному рівні», що надсилає велику кількість HTTP-запитів, перевантажуючи вебсервер.

– HTTP Bypass – спеціалізований варіант HTTP Flood, що дозволяє обходити «антибот-захист Cloudflare» (зокрема, режим IUAM – "I'm Under Attack Mode").

– TCP Flood – атака на Транспортному рівні, що створює велику кількість одночасних TCP-з’єднань, виснажуючи ресурси сервера.

– UDP Flood – атака на Транспортному рівні, що генерує величезну кількість UDP-пакетів для створення навантаження на серверну інфраструктуру.

Основні можливості скрипта:

– Одночасне навантаження на кілька цілей – DRipper може атакувати декілька серверів одночасно.

– Журнал активності – ведеться детальний лог атак, що дозволяє відстежувати результати в реальному часі.

– Відображення швидкості атак – можна побачити середню кількість запитів на секунду та загальний обсяг трафіку.

– Контроль IP-адреси – регулярна перевірка публічного IP допомагає оцінити стабільність VPN або проксі-з'єднання.

– Моніторинг доступності цілі – перевірка працездатності серверів, що атакуються, у режимі реального часу.

– Статистика відповідей сервера – аналіз кодів відповіді, що дозволяє оцінити ефективність атаки.

– Виявлення обмежень швидкості та перенаправлень – скрипт повідомляє про зміни в поведінці цільового сервера.

Запуск DRipper у терміналі:

bash

python3 DRipper.py -t -m -s

де:

«-t» – визначає кількість потоків (стандартне значення – 100).

«-m» – задає метод атаки: udp-flood, tcp-flood, http-flood, http-bypass.

«-s» – встановлює цільовий сервер, формат: {scheme}://{hostname}[:{port}][{path}] (рис. 3.17).

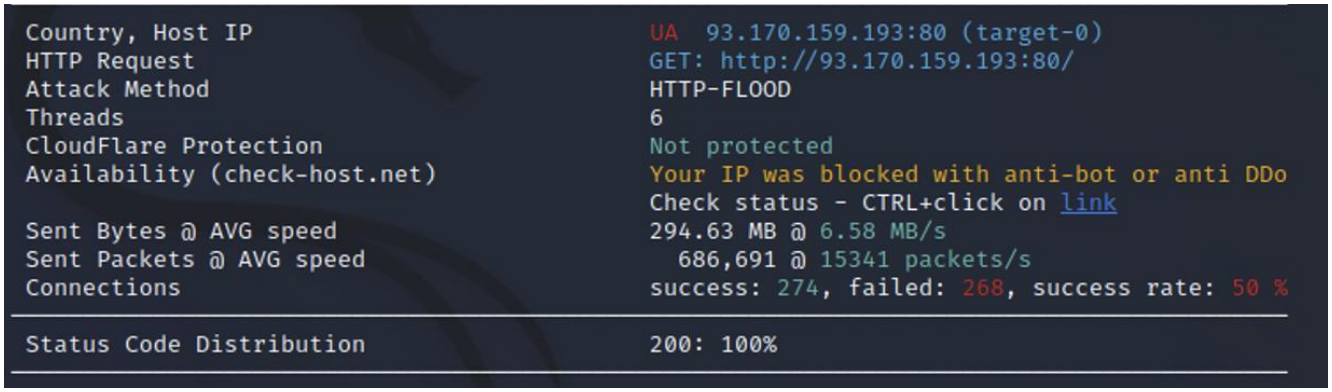


Рис. 3.17. Результат реалізації.

Преглянемо результат програмою WireShark щоб побачити фіксацію (рис. 3.18).

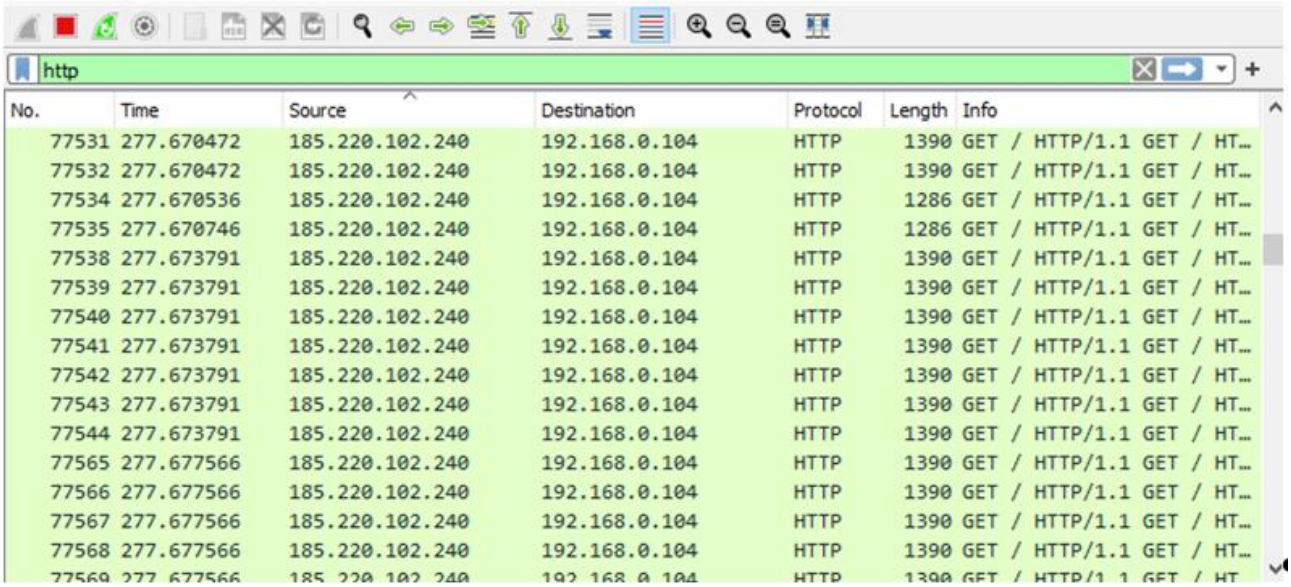


Рис. 3.18. Перегляд пакетів програмою WireShark.

HOIC (High Orbit Ion Cannon) – це потужніший наступник LOIC, розроблений для проведення атак DDoS (Distributed Denial of Service). На відміну від свого попередника, HOIC здатний генерувати значно більший трафік завдяки використанню множинних потоків та можливості одночасного атакування кількох цілей. Програма написана мовою Python і працює з HTTP-запитами, що робить її ефективною для перевантаження вебсерверів.

Основні можливості HOIC:

– Атака на кілька цілей одночасно – підтримка до 256 одночасних атак на різні сервери.

– Режим "Booster Scripts" – спеціальні скрипти, які дозволяють змінювати запити, уникаючи простих систем захисту.

– Масова HTTP-атака – інструмент генерує величезний потік HTTP-запитів, що спрямовані на вебсервери, змушуючи їх витрачати ресурси на обробку фальшивого трафіку.

– Параметри гнучкого налаштування – можливість змінювати швидкість атаки, кількість потоків та варіації заголовків HTTP.

– Відсутність маскування IP – як і LOIC, цей інструмент не має вбудованої функції анонімності, тому може бути легко відстежений.

HOIC використовує метод HTTP Flood, створюючи велику кількість запитів до вебсайтів. Це може призвести до значного споживання ресурсів сервера, через що сайт стає повільним або повністю виходить з ладу.

Налаштування та запуск HOIC:

1. Завантаження та встановлення

– Програму можна знайти в мережі та завантажити у вигляді виконуваного файлу або Python-скрипта.

– Вона не потребує складної установки і може бути запущена одразу після розпакування.

2. Введення цілі

– У головному вікні вводиться URL-адреса або IP сервера, на який буде спрямована атака.

3. Налаштування параметрів

– Визначається інтенсивність атаки (низька, середня, висока).

– Можна додати Booster Scripts, що змінюють HTTP-запити, роблячи атаку більш ефективною.

– Встановлюється кількість потоків, які використовуватимуться для атаки.

4. Запуск атаки

– Після натискання кнопки "FIRE TEH LAZER", HOIC починає надсилати запити на сервер, поступово збільшуючи навантаження.

Основні ризики та обмеження

- Легко відстежується – програма не приховує IP-адресу атакуючого, тому може бути виявлена системами безпеки.
- Не працює через проксі – HOIC не підтримує вбудовану анонімізацію, що робить його небезпечним для користувача.
- Юридична відповідальність – використання HOIC для атак на сторонні сервери є незаконним і може мати серйозні правові наслідки (рис. 3.19).

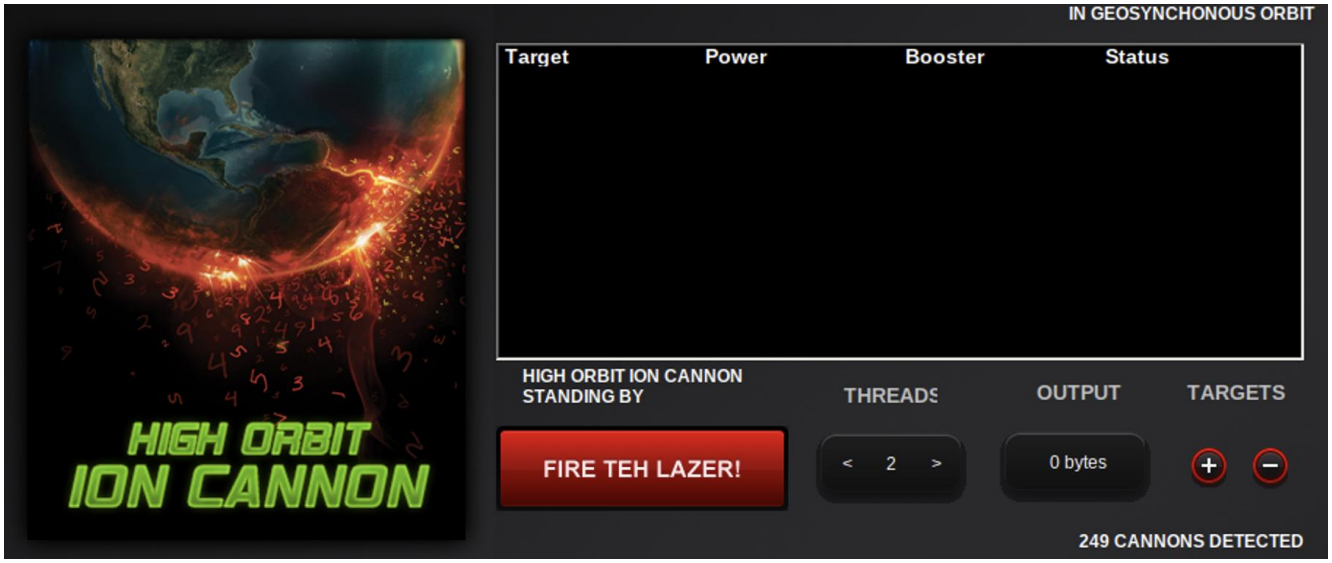


Рис. 3.19. Головний інтерфейс HOIC.

Для запуску атаки в HOIC необхідно спочатку додати ціль у вкладці "Targets". У цьому розділі користувач вводить URL або IP-адресу сервера, на який буде спрямовано атаку. Після додавання цілі можна налаштувати рівень потужності атаки, вибираючи один із доступних режимів – низький, середній або максимальний [23]. На рисунку 3.20 показаний приклад налаштування HOIC з доданою ціллю та встановленою максимальною потужністю атаки, що дозволяє створити максимальне навантаження на вебсервер.

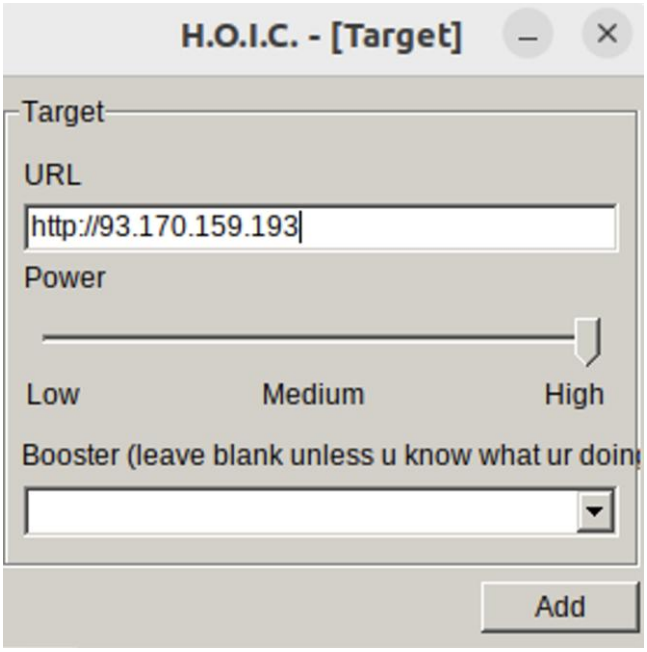


Рис. 3.20. Блок «Target».

Після того як ціль успішно додана та всі параметри атаки налаштовані, вона з’явиться на головному екрані програми. Для початку атаки необхідно натиснути кнопку "Fire Teh Lazer!", яка активує масову генерацію HTTP-запитів. Після запуску можна спостерігати за процесом атаки в реальному часі, відстежуючи кількість відправлених запитів і загальне навантаження на сервер. На рисунку 3.20 – 3.21 представлений приклад запуску атаки на власний сервер для тестування його стійкості до навантажень.

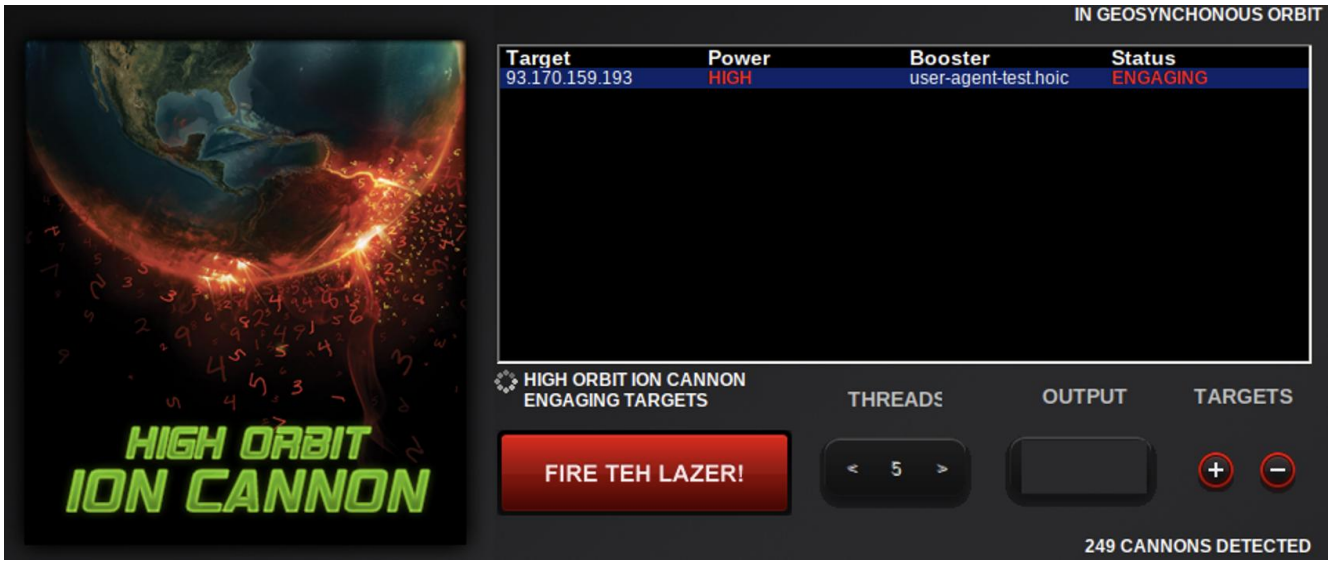
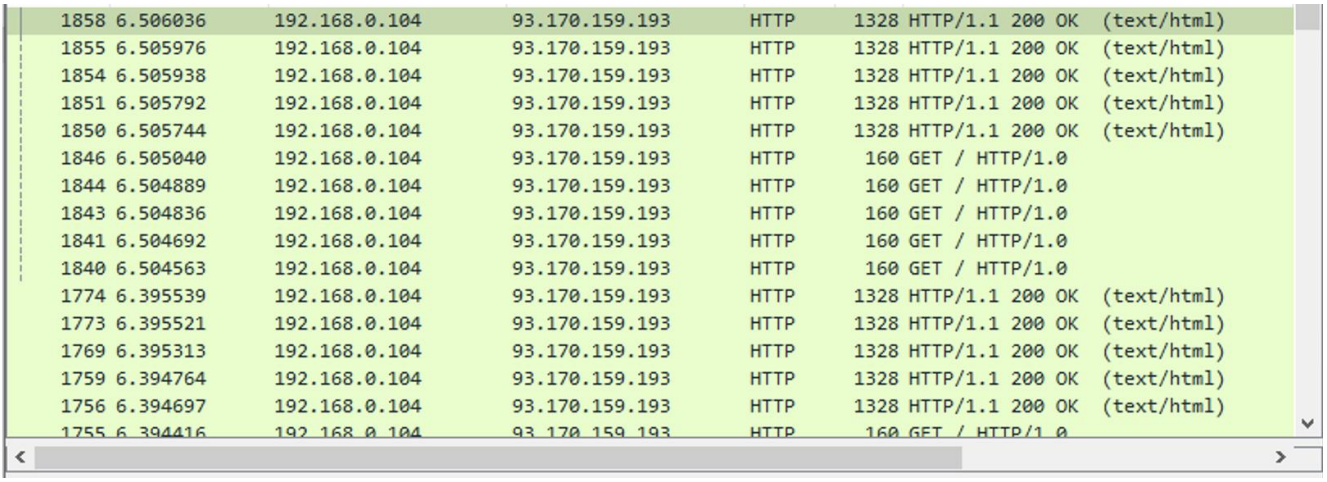


Рис. 3.21. Виявлення атаки.



1858	6.506036	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1855	6.505976	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1854	6.505938	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1851	6.505792	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1850	6.505744	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1846	6.505040	192.168.0.104	93.170.159.193	HTTP	160	GET / HTTP/1.0
1844	6.504889	192.168.0.104	93.170.159.193	HTTP	160	GET / HTTP/1.0
1843	6.504836	192.168.0.104	93.170.159.193	HTTP	160	GET / HTTP/1.0
1841	6.504692	192.168.0.104	93.170.159.193	HTTP	160	GET / HTTP/1.0
1840	6.504563	192.168.0.104	93.170.159.193	HTTP	160	GET / HTTP/1.0
1774	6.395539	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1773	6.395521	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1769	6.395313	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1759	6.394764	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1756	6.394697	192.168.0.104	93.170.159.193	HTTP	1328	HTTP/1.1 200 OK (text/html)
1755	6.394416	192.168.0.104	93.170.159.193	HTTP	160	GET / HTTP/1.0

Рис. 3.21. Процес атаки на вказану ціль та фіксування пакетів.

3.3 Дослідження та аналіз систем для захисту від атак типу DoS/DDoS слуговуванні

DDoS-атаки можуть серйозно впливати на функціонування бізнесу, зокрема на доступність веб-сайтів і додатків, не впливаючи на безпеку даних. Вони спричиняють великі затримки або повне відключення систем через перевантаження ресурсів. Захист від DDoS-атак стає важливим аспектом забезпечення стабільної роботи підприємства, особливо в таких критичних сферах, як фінансові послуги, e-commerce, телекомунікації та інші [24]. Функції, які мають бути вбудовані в рішення для захисту від DDoS-атак:

1. Угода про рівень обслуговування (SLA) із гарантованим часом усунення наслідків.

Наявність чітких угод про рівень обслуговування є важливим критерієм для вибору DDoS-защити. Вона гарантує, що захисне рішення оперативно реагуватиме на атаку і буде мати чіткі терміни усунення наслідків, з мінімальним часом відновлення після атаки [25].

2. Постійний час безвідмовної роботи та доступність додатків.

Доступність додатків та веб-сайтів навіть під час атаки є критично важливою. Високоякісні системи захисту здатні працювати безперебійно, що

дозволяє мінімізувати час простою. Це особливо важливо для онлайн-магазинів, фінансових інститутів, медичних установ, які повинні забезпечувати постійний доступ до своїх онлайн-ресурсів.

3. Якість та точність пом'якшення наслідків.

Точність фільтрації є ключовим моментом. Вибір рішення для DDoS-захисту з високим рівнем точності дозволяє правильно відрізняти законний трафік від атаки, не блокує або не уповільнює доступ до сайту для користувачів. Це дозволяє ефективно протидіяти атакам без шкоди для функціонування бізнесу.

4. Швидка та проста реєстрація.

Для компаній важливо, щоб процес підключення до сервісу захисту від DDoS був простим і швидким, щоб якнайшвидше впровадити рішення у разі потреби. Простота інтеграції з іншими сервісами та інструментами, такими як Terraform і API, робить рішення більш гнучким і зручним для використання.

5. Інтеграція з Terraform та іншими API.

Інтеграція з автоматизованими інструментами, такими як Terraform або іншими API, дозволяє забезпечити швидке налаштування та оновлення конфігурацій без участі розробників, що знижує час на відреагування на змінення загроз.

6. Захист для VoIP та телекомунікаційних додатків.

У сучасному світі голосова комунікація через IP (VoIP) є важливою частиною бізнесу, тому захист від DDoS-атак повинен охоплювати не лише традиційні веб-додатки, а й захист голосових та телекомунікаційних додатків. Це може включати запобігання атакам, спрямованим на телекомунікаційні мережі, сервери VoIP, а також безпеку та доступність систем управління дзвінками.

7. Хмарні, мобільні та IoT функції.

Інтеграція з хмарними платформами, мобільними пристроями та IoT-системами дозволяє масштабувати захист на різні рівні мережі і пристроїв. Оскільки IoT-устройства можуть стати вектором для DDoS-атак, наявність таких

функцій забезпечує ефективний захист від нових загроз, що з'являються через безпеку пристроїв IoT.

1. Cloudflare. Cloudflare є одним із найбільших і найефективніших постачальників послуг захисту від DDoS-атак, пропонуючи потужні хмарні рішення для забезпечення безпеки інтернет-сервісів. Вони надають декілька рівнів захисту, включаючи мережевий, додатний та рівень API, що дозволяє ефективно відбивати атаки будь-якого масштабу.

Глобальна інфраструктура: cloudflare використовує глобальну мережу дата-центрів для розподілу трафіку та мінімізації ризиків від атак. Це дозволяє їм забезпечити високу доступність і відновлення навіть під час масових атак, таких як DDoS-атаки на рівні 100+ Гбіт/с.

Захист від всіх типів атак: платформа автоматично виявляє та запобігає широкому спектру атак: від класичних DoS до складних DDoS атак, спрямованих на виснаження ресурсів серверів, а також атаки, орієнтовані на додатки та API.

Рішення для додатків та API: cloudflare надає спеціалізовані інструменти для захисту веб-додатків, включаючи фільтрацію API, обмеження доступу, автентифікацію запитів та інші заходи для забезпечення безпеки програмного рівня.

Безперервна аналітика: всі події та атаки моніторяться в реальному часі, з автоматичним оновленням політик безпеки для протидії новим типам атак. Прогнозування та попередження про можливі загрози дозволяють користувачам вчасно реагувати на небезпеки.

Цінова політика: плани варіюються залежно від рівня захисту та розміру бізнесу. План Business коштує від 200 $ на місяць, а Enterprise надається за індивідуальними умовами.

2. AWS Shield. Amazon Web Services (AWS) надає два рівні захисту від DDoS-атак через AWS Shield: AWS Shield Standard та AWS Shield Advanced. Ці послуги дозволяють захистити інфраструктуру AWS від різних типів атак, зокрема на рівні мережі, додатків і API.

Автоматичне виявлення атак: AWS Shield Standard захищає всі ресурси AWS без додаткових налаштувань. Всі DDoS-атаки на мережевому рівні виявляються і блокуються автоматично, не впливаючи на роботу користувачів.

Розширений захист з AWS Shield Advanced: цей рівень надає більш глибоке вивчення атак, можливість вручну налаштовувати захист і отримувати сповіщення про загрози. Підтримка у разі критичних атак через AWS DDoS Response Team (DRT) дозволяє ефективно координувати реагування.

Інтеграція з іншими службами AWS: AWS Shield інтегрується з іншими інструментами безпеки AWS, такими як AWS WAF, для блокування конкретних загроз на рівні додатків, та AWS CloudFront для розподілу трафіку та мінімізації навантаження на сервери.

Гарантія SLA: для клієнтів AWS Shield Advanced надається SLA (Service Level Agreement) з гарантією відшкодування за час простою або пошкодження, спричинене DDoS-атакою.

Цінова політика: AWS Shield Standard є безкоштовним для всіх користувачів AWS. AWS Shield Advanced має ціну від 3 000 $ на місяць, залежно від обраних сервісів і масштабів.

3. Radware DefensePro Radware DefensePro – це потужна система для захисту від DDoS-атак, яка надає миттєвий захист від атак, що використовують як традиційні, так і новітні методи для виснаження ресурсів або саботажу роботи додатків [26].

Миттєве виявлення та реагування: Radware DefensePro використовує передові алгоритми для виявлення аномалій у трафіку в реальному часі, що дозволяє швидко реагувати на атаки та зупиняти їх ще до того, як вони досягнуть кінцевої точки.

Глибокий аналіз трафіку: система забезпечує постійний моніторинг всього трафіку, визначаючи невластиві або підозрілі патерни і миттєво застосовуючи фільтрацію для блокування зловмисних запитів.

Підтримка багаторівневого захисту: DefensePro надає захист на мережевому рівні, рівні додатків і API, дозволяючи відбивати як прості атаки, так і складні спроби маніпулювання з API.

Інтелектуальне фільтрування: використання машинного навчання для вдосконалення фільтрації атак і підвищення точності захисту в умовах динамічних змін.

Цінова політика: ціна залежить від обраного рівня захисту і конкретних вимог клієнта. Зазвичай вартість рішення починається від кількох тисяч доларів на рік.

4. Imperva Incapsula Imperva Incapsula – це комплексне хмарне рішення для захисту від DDoS-атак, яке поєднує в собі безпеку веб-додатків, CDN та інші механізми для забезпечення безперебійної роботи інтернет-ресурсів.

Багатошаровий захист: incapsula забезпечує багаторівневий захист, починаючи з фільтрації на рівні мережі та додаючи рівень захисту на додатках і API для зупинки атак, що використовують вразливості на різних етапах.

Динамічна адаптація: платформа автоматично адаптується до змін у трафіку, мінімізуючи вплив атак на інфраструктуру і забезпечуючи швидке відновлення після атак.

Аналітика в реальному часі: використовує передові методи аналітики для виявлення і блокування атак, забезпечуючи наявність детальних звітів та історії подій для подальшого аналізу.

Рішення для API: imperva спеціалізується на захисті API, запобігаючи несанкціонованому доступу та маніпуляціям, що можуть порушити нормальну роботу додатків.

Цінова політика: ціни варіюються в залежності від масштабу організації та потреб захисту. Початкові ціни для бізнес-рішень становлять від 100 $ на місяць.

5. Arbor Networks Arbor Networks надає спеціалізовані рішення для захисту від DDoS-атак як для великих підприємств, так і для хмарних інфраструктур.

Вони пропонують як локальні, так і хмарні рішення для захисту мереж та додатків.

Потужні аналітичні можливості: arbor networks використовує спеціалізовані інструменти для глибокого аналізу трафіку і виявлення аномалій, що дозволяє швидко визначати джерела атак і мінімізувати їх вплив.

Виявлення і захист в реальному часі: технології Arbor забезпечують миттєве виявлення атак та зупинку атак, які можуть привести до великих втрат трафіку і ресурсів.

Інтеграція з іншими рішеннями: arbor дозволяє інтегрувати свої рішення з іншими засобами безпеки, включаючи платформи для моніторингу та реагування на інциденти, що дозволяє мати єдину точку управління для всіх аспектів безпеки.

Гнучкість та масштабованість: пропонуються рішення як для малих компаній, так і для великих підприємств, з можливістю масштабування в залежності від необхідних обсягів трафіку.

Цінова політика: ціна залежить від вимог клієнта та рівня послуг. Ціни можуть починатися від 1 000 $ на місяць для базових конфігурацій.

Висновки до розділу 3

У рамках проведеного дослідження та практичної реалізації методів протидії DDoS-атакам було розроблено тестове середовище для моделювання таких атак, що дозволило виявити критичні вразливості в системах та перевірити ефективність запропонованих засобів захисту. За допомогою спеціалізованих інструментів для імітації атак типу відмова в обслуговуванні (Dos/DDoS) було проведено серію тестів, що імітують реальні сценарії атак, зокрема як на рівні мережі, так і на рівні додатків.

Реалізовані механізми захисту були ефективно протестовані в умовах реальних атак, що дозволило визначити їх здатність до масштабування, а також точність фільтрації та швидкість реагування на загрози. В результаті дослідження було отримано цінні дані щодо оптимальних налаштувань для протидії атакам та забезпечення безперервної роботи веб-систем. Аналіз систем для захисту від DDoS-атак продемонстрував важливість комплексного підходу до безпеки, який включає як традиційні, та і новітні методи захисту.

ВИСНОВКИ

Проаналізовано вплив DDoS-атак на мережеву безпеку та досліджено їхні основні аспекти в контексті сучасних загроз. Особливу увагу приділено методам і тактикам, що використовуються при проведенні таких атак, а також їхній еволюції та розвитку в умовах зростаючої складності атак.

Розглянуто основні види атак на різні рівні інфраструктури – від мережі до серверних систем і прикладних сервісів. Це дозволило визначити основні вразливості та фактори, що підвищують ймовірність успішного здійснення DDoS-атак.

Розроблено тестове середовище для моделювання DDoS-атак, яке дало змогу провести низку експериментів з перевірки ефективності систем захисту. Імітація атак типу відмова в обслуговуванні продемонструвала реальні наслідки таких атак для різних типів систем, включаючи мережеву інфраструктуру та сервери. Це дозволило зібрати дані, необхідні для оцінки стійкості захищених мереж до великих обсягів трафіку та їх здатності до пом'якшення атак.

Проведено дослідження та аналіз існуючих систем для захисту від DDoS-атак, що включають як традиційні рішення на рівні мережі, так і новітні інструменти для захисту від атак на прикладному рівні.

Показано, що найефективніші системи базуються на комплексному підході, що включає використання хмарних рішень, автоматичних методів виявлення атак і масштабування ресурсів.

Зокрема, розглянуті механізми інтеграції таких систем з інфраструктурами компаній для забезпечення безперервної роботи.

В результаті роботи продемонстровано важливість поєднання теоретичних знань і практичних навичок для ефективної протидії DDoS-атакам.

Робота показала необхідність впровадження засобів захисту на всіх етапах роботи мережі, від ідентифікації загроз до моменту їх нейтралізації. Зібрані результати сприяють поглибленому розумінню сучасних загроз і можливостей для захисту від DDoS-атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Блоха А.О., Войтович О.П. Всеукраїнська науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії 2025. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki2023/paper/view/18298 (дата звернення: 26.02.2025).

2. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. – Київ: КПІ, 2020. 312 с.

3. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури: навч. посіб. Київ: КУБГ, 2019. 285 с.

4. Зінченко В.В., Зінченко М.В. Виявлення DDoS-атак прикладного рівня Радіотехнічні поля, сигнали, апарати та системи: матеріали міжнар. наук.-техн. Конф. Київ. 2015 С. 262–264.

5. Бурмака І.А. Захист інформації в комп’ютерних системах: конспект лекцій. Чернігів: ЧНТУ, 2018. 198 с.

6. Ковальчук О.В., Коваленко О.В. Оцінка засобів захисту інформаційних ресурсів. Наукові праці Львівської політехніки. 2017. № 6630. С. 99–105.

7. Хошаба О.М. Захист інформації в системах електронного урядування: навч. посіб. Одеса: ПНПУ, 2019. 240 с.

8. Жилін А.В. Методи аналізу та протидії DDoS-атакам у корпоративних мережах. Системи захисту інформації. 2022. № 5(47). С. 72–79.

9. Бурячок В.Л. Захист корпоративних мереж від DDoS-атак. Збірник наукових праць Національного авіаційного університету. 2021. № 18. С. 88–95.

10. Гаврилюк В.О. Методи забезпечення безпеки мережевої інфраструктури. Інформаційна безпека та криптографія. 2020. № 4. С. 50–57.

11. Корнієнко Д.А. DDoS-атаки та методи їх виявлення. Сучасні тенденції кібербезпеки. 2019. № 7. С. 30–37.

12. Verizon. 2023 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 26.02.2025).

13. CyberEdge Group’s 2021 Cyberthreat Defense Report. URL: https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDRReport-v1.1-1.pdf (дата звернення: 28.02.2025).

14. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. URL: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full (дата звернення: 20.03.2025).

15. DDoS Report for 2021. Link11. URL: https://www.link11.com/en/blog/press/new-link11-ddos-report-for-2021/ (дата звернення: 28.02.2025).

16. Dhanapal A. The Slow HTTP Distributed Denial of Service Attack Detection in Cloud. URL: https://www.researchgate.net/publication/332829479_The_Slow_HTTP_Distributed_Denial_of_Service_Attack_Detection_in_Cloud (дата звернення: 28.02.2025).

17. The 14 Most Common Cyber Attacks. URL: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-commoncyberattacks/ (дата звернення: 02.03.2025).

18. Collection and Analysis of Slow Denial of Service Attacks Using Machine Learning Algorithms. ProQuest. URL: https://www.proquest.com/openview/c5edb8073f8b9e10eb12c9c6e588d92e/1?pq-origsite=gscholar&cbl=18750&diss=y (дата звернення: 02.03.2025).

19. The Invicti AppSec Indicator Spring 2021 Edition: Acunetix Web Vulnerability Report. URL: https://www.acunetix.com/whitepapers/acunetix-web-application-vulnerability-report-2021/ (дата звернення: 02.03.2025).

20. Sikora M. Slow DoS Attacks Detection and Mitigation. URL: https://dspace.vutbr.cz/bitstream/handle/11012/186725/510_eeict2019.pdf?sequence=1 (дата звернення: 03.03.2025).

21. Outsmarting the Super-Hackers By Securing Smart Autonomous Systems. URL: https://partners.wsj.com/tii/catalyzing-change/outsmartingthe-superhackers/ (дата звернення: 03.03.2025).

22. PHP Manual / Mehdi Achour, Friedhelm Betz, Antony Dovgal, Nuno Lopes, Hannes Magnusson, Georg Richter, Damien Seguy, Jakub Vrana. URL: https://www.php.net/manual/en/ (дата звернення: 03.03.2025).

23. Jung J., Krishnamurthy B., Rabinovich M. Flash Crowds and Denial of Service Attacks: Characterization and Implication for CDNs and Web Sites // Proc. of World Wide Web (WWW) Conference. May 2002.

24. Дядін І.П. Дослідження та оптимізація методів захисту від DDoS-атак: дипломна робота. Донецьк: Донецький національний технічний університет, 2012. URL: https://masters.donntu.ru/2012/fkita/dyadin/diss/indexu.htm (дата звернення: 03.03.2025).

25. Джулій В.М., Чорненький В.І., Савіцька О.О. Метод виявлення та протидії розподіленим атакам, спрямованим на відмову в обслуговуванні. Вісник Хмельницького національного університету. 2019. № 1. С. 127–134.

26. Ковальчук О.В., Коваленко О.В. Оцінка засобів захисту інформаційних ресурсів. Наукові праці Львівської політехніки. 2017. № 6630. С. 99–105. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6630/17-99-105.pdf (дата звернення: 03.03.2025).

27. OWASP Foundation. OWASP Top Ten Project. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 15.05.2025).

28. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (дата звернення: 15.05.2025).

29. CERT Coordination Center. Understanding Denial of Service Attacks. URL: https://resources.sei.cmu.edu/library/subject-areas/denial-of-service/ (дата звернення: 15.05.2025).

30. Cisco Systems, Inc. Cisco IOS Security Configuration Guide. URL: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14131-3.html (дата звернення: 15.05.2025).

31. Mirkovic J., Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review. 2004. Vol. 34, Issue 2. P. 39–53.

32. Zargar S. T., Joshi J., Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials. 2013. Vol. 15, Issue 4. P. 2046–2069.

33. Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks. 2004. Vol. 44, Issues 5–6. P. 643–666.

34. Stallings W. Network Security Essentials: Applications and Standards. W. Stallings. 7th ed. Pearson, 2016. 400 p.

35. Easttom C. Network Defense and Countermeasures: Principles and Practice. C. Easttom. 5th ed. Pearson, 2018. 450 p.

36. Xie Y., Yu F., Ke Y. A novel hybrid detection method for DDoS attacks. Proceedings of the 3rd ACM Workshop on Network and System Support for Games. 2004. P. 17–22.

37. Mirkovic J., Lenk G., Reiher P. Source-end defense against distributed denial-of-service attacks. IEEE Network. 2002. Vol. 16, Issue 6. P. 28–37.

38. Yu S., Guan Y., Zhao M., Luo M. Detection and mitigation of low-rate DDoS attacks in software defined networks. Security and Communication Networks. 2017. Vol. 2017. Article ID 1505906.

39. Ross R., McEvilley M., Oren J. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. Gaithersburg, MD: NIST, 2012. 100 p.

40. Chen H., Li S., Liu Y. Anomaly detection for DDoS attacks based on data mining techniques. Computers & Security. 2014. Vol. 48. P. 50–59.

41. Liu H., Yu M., Zhang Y. DDoS attack detection and mitigation in software defined networking: a survey. Journal of Network and Computer Applications. 2019. Vol. 139. P. 56–73.

42. Alsmadi I., Xu D. Cyber Security and IT Infrastructure Protection. I. Alsmadi, D. Xu. Boca Raton : CRC Press, 2017. 400 p.