MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Electronică şi Telecomunicaţii
Departamentul Telecomunicaţii şi Sisteme Electronice

Admis la susţinere
Şefă departament:
Tîrşu Valentina, conf. univ., dr.

_____
„____”_____ 2024

Analiza eficacității metodelor de prevenire și protecție împotriva atacurilor DDoS în rețelele avansate de comunicații

Анализ эффективности методов предотвращения и защиты от DDoS-атак в современных сетях связи

Teză de master

Student: **Stinga Serghei,**
gr. MMRT-221

Conducător: **Șestacova Tatiana,**
conf. univ., dr.

Chişinău, 2024

ADNOTARE

Autorul: Stinga Serghei, gr. MMRT-221

Titlul tezei de master: Analiza Eficienței Metodelor de Prevenire a Atacurilor DDoS în Rețelele de Comunicare Moderne

Structura lucrării: Include pagina de titlu, aprobare, rezumat, introducere, 3 capitole, concluzii și bibliografie.

Cuvinte cheie: DDoS, metode de prevenire, securitate cibernetică, rețele de comunicații, Docker.

Problematica studiului: Analiza și evaluarea metodelor actuale și emergente de combatere a atacurilor DDoS.

Scopul lucrării: Analizarea și evaluarea metodelor de detectare și protecție împotriva atacurilor DDoS utilizate în infrastructurile de rețea moderne.

Obiectivele:

1. Revizuirea conceptelor fundamentale și a strategiilor existente pentru protecția împotriva atacurilor DDoS;
2. Analiza metodelor tehnologice și a instrumentelor pentru atenuarea atacurilor DDoS;
3. Conducerea unei analize a eficacității metodelor de prevenire și protecție împotriva atacurilor DDoS;
4. Implementarea și testarea soluțiilor bazate pe Docker pentru simularea și evaluarea scenariilor de atac DDoS;
5. Compararea eficacității diferitelor metode de prevenire și protecție împotriva atacurilor DDoS.

Metode aplicate: Analiză comparativă, platforma software Docker, funcția de dezirabilitate a lui Harrington.

Rezultatele obținute: A fost efectuată o analiză și evaluare a celor mai eficiente practici, metode și instrumente pentru detectarea rapidă, prevenirea și protecția împotriva atacurilor DDoS în infrastructurile de rețea moderne. Este propusă o clasificare a tipurilor de atac, conform căreia sunt date recomandări pentru aplicarea celor mai eficiente metode de creștere a securității în rețelele de comunicații, cu potențial de implementare în Republica Moldova.

ANNOTATION

Author: Stinga Serghei, Group MMRT-221

Title: Analysis of the Efficiency of DDoS Attack Prevention Methods in Modern Communication Networks

Thesis structure: title page, abstract, introduction, 3 chapters, conclusions, and bibliography.

Keywords: DDoS, prevention methods, cybersecurity, communication networks, Docker.

Research problem: Analysis and evaluation of current and emerging methods for combating DDoS attacks.

Thesis purpose: To analyze and evaluate methods for detecting and protecting against DDoS attacks used in modern network infrastructures.

Objectives:

1. Review fundamental concepts and existing strategies for DDoS attack protection;
2. Analyze technological methods and tools for mitigating DDoS attacks;
3. Carry out an analysis of the effectiveness of prevention and protection methods against DDoS attacks;
4. Implement and test Docker-based solutions for simulating and evaluating DDoS attack scenarios;
5. Compare the effectiveness of various methods of preventing and protecting against DDoS attacks.

Applied Methods: Comparative analysis, Docker software platform, Harrington's desirability function.

The obtained results: An analysis and evaluation of the most effective practices, methods, and tools for quick detection, prevention, and protection against DDoS attacks in modern network infrastructures have been conducted. A classification of attack types is proposed, according to which recommendations are given for the application of the most effective methods to increase security in communication networks, with potential implementation in the Republic of Moldova.

АННОТАЦИЯ

Автор: Стинга Сергей, Группа ММРТ-221

Тема: Анализ эффективности методов предотвращения DDoS-атак в современных сетях связи

Структура работы: Включает титульный лист, утверждение, аннотацию, введение, 3 главы, заключение и библиографию.

Ключевые слова: DDoS, методы предотвращения, кибербезопасность, сети связи, Docker.

Область исследований: Анализ и оценка существующих и новых методов борьбы с DDoS-атаками.

Цель работы: Провести анализ и дать оценку методам обнаружения и защиты от DDoS-атак, используемых в современных сетевых инфраструктурах.

Задачи:

1. Рассмотреть основные концепции и существующие стратегии защиты от DDoS-атак;
2. Проанализировать технологические методы и инструменты для смягчения DDoS-атак;
3. Провести анализ эффективности методов предотвращения и защиты от DDoS-атак;
4. Реализовать и протестировать решения на базе Docker для симуляции и оценки сценариев DDoS-атак;
5. Сравнить эффективность различных методов предотвращения и защиты от DDoS-атак.

Применяемые методы: Сравнительный анализ, программная платформа Docker, функция желательности Харрингтона.

Полученные результаты: Проведён анализ и оценка наиболее эффективных практик, методов и инструментов для быстрого обнаружения, предотвращения и защиты от DDoS-атаки в современных сетевых инфраструктурах. Предложена классификация видов атак, согласно которой даны рекомендации по применению наиболее эффективных методов для повышения безопасности в сетях связи с потенциальной реализацией в Республике Молдова.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ ... 8
1. КЛАССИФИКАЦИЯ И АНАЛИЗ ОСНОВНЫХ ВИДОВ DDOS-АТАК ... 9
1.1 Основные характеристики и классификация DDoS-атак ... 9
1.2 Виды DDoS-атак ... 10
1.2.1 Виды атак по механизму действия. ... 10
1.2.2 Виды атак по цели нападения ... 12
1.2.3 Виды атак по объему трафика ... 13
1.3 Выводы ... 17
2. АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДОВ ПРЕДОТВРАЩЕНИЯ И ЗАЩИТЫ ОТ DDOS-АТАК ... 18
2.1 Анализ современных методов и техник предотвращения и защиты DDoS-атак ... 18
2.1.1 Блокировка IP-адресов ... 18
2.1.2 Ограничение трафика ... 19
2.1.3 Web Application Firewall (WAF) ... 21
2.1.4 Обнаружение и митигация атак ... 22
2.1.5 Облачные решения ... 24
2.2 Критерии эффективности методов ... 26
2.3 Расчёт комплексного показателя эффективности методов на базе функции желательности Харрингтона ... 29
2.4 Преимущества и недостатки методов ... 41
2.5 Рекомендации по выбору метода в зависимости от вида атак ... 42
3. ПРАКТИЧЕСКОЕ ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ ЗАЩИТЫ ОТ DDoS-АТАК ... 45
3.1 Выбор и подготовка тестовой среды ... 45
3.2 Методика и инструменты симуляции сценариев атак и защиты от них ... 52
3.3 Реализация экспериментальных исследований эффективности методов защиты от DDoS-атак ... 54
3.4 Анализ результатов и рекомендации ... 56
ЗАКЛЮЧЕНИЕ ... 58
БИБЛИОГРАФИЯ ... 61

ВВЕДЕНИЕ

В современном мире информационных технологий безопасность является одним из ключевых аспектов успешного функционирования любой организации или индивидуального пользователя. С ростом числа устройств, подключенных к Интернету, и увеличением объема передаваемой информации, угрозы безопасности становятся все более актуальными. Одной из наиболее разрушительных и сложных для предотвращения угроз является DDoS-атака (распределенная атака типа "отказ в обслуживании").

DDoS-атака представляет собой попытку злоумышленников заблокировать доступ к определенному ресурсу или сервису путем создания искусственного потока запросов, превышающего его возможности обработки. Это может привести к сбоям в работе сервиса, потере данных и другим негативным последствиям.

За последние годы число DDoS-атак значительно возросло, и они стали более сложными и масштабными. Это обусловлено рядом факторов, включая доступность инструментов для осуществления таких атак, увеличение числа уязвимых устройств и недостаточное внимание к вопросам безопасности со стороны разработчиков и администраторов.

В связи с этим анализ эффективности методов предотвращения DDoS-атак становится крайне актуальным. Понимание принципов работы различных методов и их преимуществ и недостатков позволит выбрать наиболее подходящий способ защиты для конкретной ситуации.

Целью работы является исследование и анализ современных методов предотвращения и защиты от DDoS-атак в сетях связи для определения наиболее эффективных методов и выработки рекомендаций по их применению.

Для достижения поставленной цели необходимо решение следующих ***задач*:**

1. Составить классификацию и провести анализ основных видов DDoS-атак.
2. Проанализировать существующие методы предотвращения DDoS-атак и их применение в современных сетях связи.
3. Оценить эффективность различных методов защиты на базе комплексных показателей качества.
4. Провести экспериментальные исследования эффективности методов защиты на основе симуляции сценариев DDoS атак и защиты от них.
5. Разработать рекомендации по выбору эффективных методов защиты для различных типов сетей и организаций.

БИБЛИОГРАФИЯ

1. DDoS-атаки в 2022 и методы защиты от них [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/slurm/articles/674218/

2. ȚURCANU, D., SPINU, N., POPOVICI, S., ȚURCANU, T. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.

3. Классификация DDoS: полное руководство по типам атак [Электронный ресурс]. Режим доступа: https://ddos-guard.net/ru/blog/classification-of-ddos-attacks

4. Коллинз, М. К60 Защита сетей. Подход на основе анализа данных / М. Коллинз; пер. с англ. А.В. Добровольская. – М.: ДМК Пресс, 2020. – 308 с.: ил. – ISBN 978-5-97060-649-0.

5. DDoS-атаки: типы атак и уровни модели OSI [Электронный ресурс]. Режим доступа: https://firstvds.ru/technology/ddos-ataki-tipy-atak-i-urovni-modeli-osi

6. "DDoS-атаки и механизмы защиты: классификация", Сингх К., Сингх П. и Кумар К. (Журнал сетевых и компьютерных приложений, 2017).

7. PECA, L., ȚURCANU, D. Network security: Practical examples solved to be introduced in network security. Chișinău, Publisher „Tehnica-UTM”, 2023, pp. 7-232.

8. "Обзор сетевых защитных механизмов, противодействующих проблемам DoS и DDoS-атак", Заргар С. Т., Джоши Дж. и Типпер Д. (ACM Computing Surveys, 2013).

9. "Всесторонний обзор DDoS-атак и механизмов защиты в IoT", Колиас С., Камбуракис Г., Ставру А. и Воас Дж. (IEEE Communications Surveys & Tutorials, 2017).

10. "Машинное обучение в смягчении последствий DDoS-атак", Бучак А. Л. и Гувен Э. (IEEE Communications Surveys & Tutorials, 2016).

11. "DDoS в IoT: Mirai и другие ботнеты", автор Антонакакис М. и др. (Компьютер, 2017).

12. "Оценка эффективности текущих мер защиты от DDoS-атак", Сенгар Х., Ванг Х. и Виджесекера Д. (В материалах Международной конференции по надежным системам и сетям, 2006).

13. "Тенденции в методах DDoS-атак и их предотвращение: всесторонний анализ", исследовательский отчет TechSci (2023).

14. Harrington, Jr. E. C. (1965). “The Desirability Function.” Industrial Quality Control, Volume 21, No. 10, pp. 494-498.

15. ȘESTACOVA, T. Metode științifice de optimizare experimentală a obiectelor electronice și de telecomunicații. Chișinău: Editura „Tehnica – UTM”, 2023, 40 p.