УДК 004

Нич В.О.
Савицька Л.А.
Богомолов С.В.

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ DDoS АТАК РЕАЛІЗОВАНИХ З ВИКОРИСТАННЯМ ХМАРНИХ СЕРВІСІВ

Вінницькій національний технічний університет

Анотація
Робота присвячена технології виявлення і запобігання DDoS атак реалізованих з використанням хмарних сервісів. Проаналізовано існуючі типи та види мереж, їх класифікація та топології. Виконано аналіз вразливостей сучасних мереж до атак, визначено інструментарій для боротьби із атаками, а саме їх виявлення попередження та запобігання
Ключові слова: атака, DDoS, хмарний сервіс

Abstract
The thesis is devoted to the technology of detecting and preventing DDoS attacks implemented using cloud services. Existing types and kinds of networks, their classification and topologies are analyzed. The analysis of vulnerabilities of modern networks to attacks is performed, the tools for combating attacks are identified, namely their detection and prevention.
Keywords: attack, DDoS, cloud

Актуальність роботи. У сучасному світі використання комп'ютерів та комп'ютерних мереж зростає з кожним днем. Все частіше зустрічаються як мобільні пристрої - телефони і планшети, так і розумна побутова електроніка - телевізори, холодильники, сучасні ігрові приставки. Однією з найпоширеніших загроз є атаки відмови в обслуговуванні. Ця атака робить систему неможливою, частково або повністю блокує ресурси та послуги, необхідні користувачеві.

Атаки відмови в обслуговуванні можна розділити на дві основні групи - це атаки відмови в обслуговуванні та розподілені атаки відмови в обслуговуванні. Останні характеризується використанням декількох мережних вузлів для здійснення атаки, як правило, досить великої кількості, що дуже ускладнює виявлення такої атаки та захист від неї. Для полегшення виявлення та захисту від таких атак необхідно мати чітку класифікацію за різними критеріями. Наразі існує велика кількість класифікацій DoS-атак, але відсутня така, яка максимально характеризує всі сучасні особливості DoS-атак, з можливістю застосування в реальних системах.

Метою є дослідження та використаня методів для раннього виявлення DDoS атак, і подальшого блокування загрозливого трафіку із викориистанням хмарних сервісів.

Для досягнення зазначеної мети для дипломної роботи поставлено такі завдання: проаналізувати сучасний стан DDoS атак, та провести аналіз нинішнього стану технологій для вирішення проблем захисту інформації, дослідити математичні моделі атак з врахуванням опису сезонності мережного навантаження, визначити алгоритм ідентифікації точок початку атаки та алгоритм поділу змішаного трафіку на надійний та загрозливий, який враховує сезонну кількість мережного навантаження, вирішити завдання по використанню хмари для виявлення DDoS-атакам малої інтенсивності.

Об'єктом дослідження є розподілені атаки на інформаційну систему.

Предметом дослідження виступають моделі та методи виявлення DDoS атак, і виділення зловмисного трафіку.

Методи дослідження, котрі використовуватимуться для дослідження: апарат теорії алгоритмів, теорії захисту інформації, системного аналізу, теорії імовірності та математичної статистики, кластерного і системного аналізу.

Практичне значення полягає у дослідженні методу та алгоритмів захисту мережних ресурсів від DDoS-атак, що дозволяють проводити активну протидію безпосередньо на стороні атакованого ресурсу. Це підтверджується дослідженням та подальшою реалізацією хмарних сервісів для виявлення DDoS-атак, та подальше блокування нелегітимних звернень на різних рівнях інформаційної системи.

Використання шестифазної моделі пом'якшення DDoS від Cisco є гарним початком, і його також можна постійно переглядати при створенні обґрунтованої політики DDoS. Підготовка є ключовою частиною будь-якої стратегії DDoS.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Meyer, Bertrand (1997). Object-Oriented Software Construction. Prentice Hall. ISBN 0-13-629155-4.
2. Luzhetsky, V., Savitskaya, L.Development and research of adaptive data compression methods based on linear fibonacci form Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2015, 1(9), стр. 16–22

Нич Вадим Олегович- студент групи 2КІ-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: nychvadsm@gmail.com

Савицька Людмила Анатоліївна – доцент кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця, e-mail: **savytska.liudmyla@vntu.edu.ua**

Богомолов Сергій Віталійович – доцент кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця, e-mail: sergeyivanoff18@gmail.com

Nych Vadym - student of group 2KI-18b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nychvadsm@gmail.com

Savytska Liudmyla - Associate Professor of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: **savytska.liudmyla@vntu.edu.ua**

Bogomolov Sergii - Associate Professor of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: sergeyivanoff18@gmail.com