УДК 621.391:004.4

М. А. Шепітко
О. П. Войтович

ДОСЛІДЖЕННЯ МОДЕЛЮВАННЯ АТАК НА ВІДМОВУ В ОБСЛУГОВУВАННІ

Вінницький національний технічний університет

Анотація. *Розглянуто засоби моделювання атак на відмову в обслуговуванні та їх використання для дослідження стійкості інформаційних систем.*

Ключові слова: *DDoS, моделювання атак, інформаційна безпека, мережеві загрози, стійкість систем.*

Abstract. *The means of modeling denial-of-service attacks and their use for studying the stability of information systems are considered.*

Keywords: *DDoS, attack modeling, information security, network threats, system stability.*

Вступ

У сучасних умовах стрімкого розвитку інформаційно-телекомунікаційних технологій особливої актуальності набуває проблема забезпечення доступності мережевих ресурсів. Однією з найпоширеніших загроз залишаються атаки на відмову в обслуговуванні, які можуть призводити до порушення стабільної роботи інформаційних систем [1]. У зв'язку з цим важливим завданням є використання ефективних засобів моделювання таких атак для дослідження стійкості систем та розроблення методів їх захисту.

Атаки на відмову в обслуговуванні залишаються однією з найбільш поширених і небезпечних загроз для сучасних інформаційно-телекомунікаційних систем, оскільки вони безпосередньо впливають на доступність інформаційних ресурсів та стабільність функціонування мережевих сервісів. У зв'язку з цим використання засобів моделювання DoS/DDoS-атак набуває важливого значення у процесі дослідження стійкості інформаційних систем до мережевих загроз.

Результати дослідження

Атаки на відмову в обслуговуванні належать до класу мережевих загроз, спрямованих на порушення доступності інформаційних ресурсів шляхом перевантаження серверів, каналів передачі даних або мережевих пристроїв. В умовах сучасного розвитку інформаційно-телекомунікаційних систем моделювання таких атак є необхідним для оцінки стійкості систем та розробки ефективних методів захисту.

Моделювання DoS/DDoS-атак здійснюється за допомогою спеціалізованих програмних засобів, що дозволяють відтворювати різні типи мережевого навантаження [2]. Основними інструментами є генератори мережевого трафіку, такі як: LOIC (Low Orbit Ion Cannon), HOIC (High Orbit Ion Cannon), Hping3, Slowloris та Apache JMeter, які дозволяють моделювати різні типи перевантаження мережевих ресурсів. Програмні засоби тестування на проникнення, мережеві симулятори, а також системи віртуалізації та контейнеризації. Використання цих засобів дає можливість моделювати атаки різної інтенсивності та структури, включаючи SYN Flood, UDP Flood, HTTP Flood та інші типи перевантаження мережевих ресурсів.

Особливе значення у процесі моделювання відіграють віртуальні середовища. Вони дозволяють створювати ізольовані тестові мережі без ризику впливу на реальну інфраструктуру [3]. Завдяки цьому можна експериментально досліджувати поведінку серверів, мережевих пристроїв та веб-сервісів у разі перевантаження, оцінювати граничні значення пропускної здатності та визначати критичні точки мережевої інфраструктури.

Використання генераторів мережевого трафіку забезпечує можливість моделювання різноманітних сценаріїв атак з контролем інтенсивності та тривалості навантаження, що дозволяє аналізувати реакцію інформаційних систем у реальному часі [4]. Мережеві симулятори забезпечують дослідження поведінки систем у різних умовах функціонування, включаючи комбінації атак і навантажень, що дозволяє прогнозувати ефекти від складних сценаріїв DDoS.

Застосування віртуалізації та контейнеризації підвищує ефективність моделювання, забезпечуючи масштабованість тестових середовищ та можливість одночасного відтворення декількох типів атак. На рисунку 1 зображено схему контейнеризації.

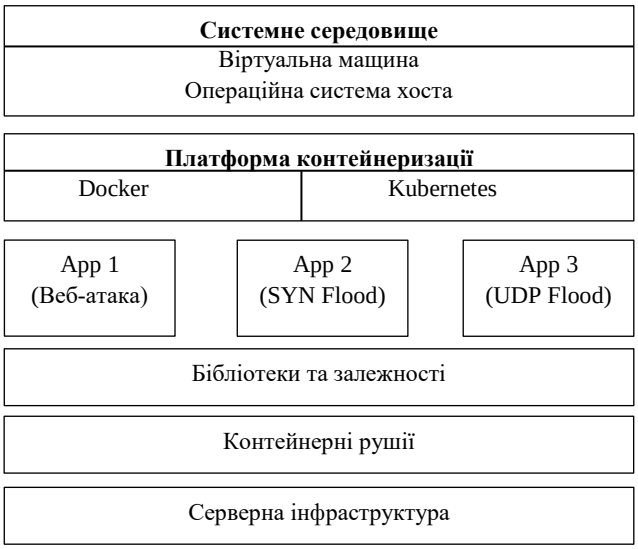

Рисунок 1 – Схема контейнеризації

Також це дозволяє оцінювати ефективність різних механізмів захисту, зокрема систем виявлення вторгнень, засобів фільтрації мережевого трафіку та методів обмеження швидкості запитів, без ризику для продуктивних систем.

Висновки

Застосування сучасних програмних засобів моделювання дозволяє відтворювати різні типи атак на відмову в обслуговуванні, аналізувати поведінку інформаційних систем за умов перевантаження та визначати критичні елементи мережевої інфраструктури. Використання віртуальних середовищ забезпечує можливість проведення експериментальних досліджень без ризику для реальних інформаційних систем та сприяє підвищенню ефективності дослідження мережевих загроз.

Засоби моделювання атак на відмову в обслуговуванні є важливим інструментом дослідження інформаційної безпеки та забезпечення стабільного функціонування інформаційно-телекомунікаційних систем у сучасних умовах розвитку мережевих технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Voitovych O. P., Baryshev Y.V., Kupershtein L.M., Kolibabchuk E.I.. Investigation of Simple Denial-of-Service Attacks. // Third International IEEE Conference “Problems of Infocommunications. Science and Technology” PICS&T`2016, Kharkiv, Ukraine, pp. 1-4. URL: https://ir.lib.vntu.edu.ua//handle/123456789/10094?utm_source=chatgpt.com
2. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks // Engineering Science and Technology, an International Journal. — Elsevier, 2021. — Vol. 24, P. 123–140. URL: https://www.sciencedirect.com/science/article/pii/S2215098621001944
3. Ahmad, A., AbuHour, Y., Alghanim, F. A Novel Model for Distributed Denial of Service Attack Analysis and Interactivity / A. Ahmad, Y. AbuHour, F. Alghanim // Symmetry. — 2021. — Vol. 13, No 12. — P. 2443. — URL: https://www.mdpi.com/2073-8994/13/12/2443
4. Ovcharuk, M., Ilin, M. Models of Denial of Service Attacks on Cyber-Physical Systems / M. Ovcharuk, M. Ilin // Theoretical and Applied Cybersecurity. — 2023. — Vol. 5, No 2. — P. 62–67. — URL URL:https://tacs.ipt.kpi.ua/article/view/289459

Шепітко Марина Анатоліївна - студентка групи 1БКС-22б, факультету інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sepitkomarina39@gmail.com

Науковий керівник – **Войтович Олеся Петрівна** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: voytovych.vk.vntu.edu.ua

Shepitko Maryna Anatoliivna - student of group 1BKS-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: sepitkomarina39@gmail.com

Supervisor – **Voytovych Olesya P**. — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: voytovych.vk.vntu.edu.ua