Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри управління
інформаційною безпекою, д.т.н., доцент
полковник служби цивільного захисту

_____ Ростислав ТКАЧУК
“____” _____2021 року

ДИПЛОМНА РОБОТА
БАКАЛАВРА

на тему **Аналіз засобів реалізації та методів атаки “Відмова в обслуговуванні”**

Виконав:
здобувач 4 курсу, групи КБ-41
спеціальності (освітньої програми)
125 «Кібербезпека»
(Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої програми))
Тарас СТЕФАНІВ
(ім’я та прізвище)
Керівник Ростислав ТКАЧУК
(ім’я та прізвище)

Рецензент Наталя ЛИСА
(ім’я та прізвище)

Львів-2021

АНОТАЦІЯ

Стефанів Т.І. - "«Аналіз засобів реалізації та методів атаки Відмова в обслуговуванні». Дипломна робота за спеціальністю 125 "Кібербезпека" складається з текстової частини, що містить 3 розділи, 50 сторінок, 1 таблиці, 16 рис., 27 літературних джерел.

Об'єкт дослідження - реалізація та методи атаки "відмова в обслуговуванні".

Мета роботи - дослідити та розробити методи захисту від різних видів атак типу "відмова в обслуговуванні".

Практичне значення роботи полягає зниженні вразливостей веб-сервісів та у виборі правильного методу захисту від атак виду "відмова в обслуговуванні"

Результати здійснених у дипломній роботі досліджень можуть бути використанні при проведенні атаки на веб-сервіс.

Наукови новизка дослідження полягає у розробленні нових методів захисту від атаки типу "Відмова в обслуговуванні" та підбору до кожного з виду правильний метод захисту.

Ключові слова: DoS атака, DDoS атака, OSI, ботнет, SDN, API, TCP, HTTP.

ABSTRACT

Stefaniv TI - "Analysis of the means of implementation and methods of attack Denial of service. Thesis in the specialty 125 "Cybersecurity" consists of a text containing 3 sections, 50 pp., 1 Tables, 16 figures, 27 sources.

The object of study - the implementation and methods of attack "denial of service".

The purpose of the work is to research and develop methods of protection against various types of "denial of service" attacks.

The practical significance of the work is to reduce the vulnerabilities of web services and to choose the right method of protection against attacks such as "denial of service".

The results of research conducted in the thesis can be used in an attack on a web service.

The scientific novelty of the study is to develop new methods of protection against attack type "denial of service" and the selection of each type of the correct method of protection.

Keywords: DoS atack, DDoS attack, OSI, ботнет, SDN, API, TCP, HTTP.

ЗМІСТ

ВИСНОВКИ

За темою дипломної роботи «Аналіз засобів реалізації та методів атаки «Відмова в обслуговуванні»» був проведений аналіз існуючих типів DDoS атак та методів їх впливу на мережі передачі даних, аналіз методів захисту від DDoS атак, аналіз існуючих рішень для захисту від DDoS атак.

Результатом даної роботи є моделювання атаки виду Syn-flood та використання програми-аналізатора для ідентифікації атаки цього ж самого виду. Моделювання показало як працює саме реалізація атаки, та методи, які потрібно застосовувати для того, щоб ідентифікувати цю атаку.

Результатом даної роботи також є аналіз і створення власних методів боротьби з атакою типу «відмова в обслуговуванні» таких видів, як:

- DoS-атака (відмова в обслуговуванні)
- DDoS-атака (розподілена атака типу «відмова в обслуговуванні»)
- SYN-flood атака.

Власні методи боротьби з атакою типу «відмова в обслуговуванні»:

- добавляння підозрілих айпі-адрес в чорний список хостингу;
- блокування найактивніших айпі-адрес;
- обмеження кількості запитів на сервер від одної айпі-адреси.

Також в результаті проведених досліджень нами було виявлено низку неможливостей вручну та програмними способами боротись із деякими видами атаки «відмова в обслуговуванні», оскільки часто атака проводиться не на веб-сайт, а на хостинг-провайдер, до якого доступу у власників веб-сервісів немає.

Основною проблемою є Syn-Flood атака, яка проводиться на сам хостинг веб-сайту, що унеможливлює власника цього сайту боротись із атакою.

Як результат проведених досліджень ми нами сформульовані найважливіші рекомендацій щодо запобігання DoS/DDoS атак:

1. Найбільше ефективним буде шлях нарощування потужності системи, яка дозволить витримувати сильну загрузку мережі;

2. Налаштування маршрутизатора має відбуватися таким чином, щоб весь непотрібний трафік не виходив далі маршрутизатора;

3. Альтернативою потужної системи буде розподілення навантаження між декількома серверами.

Список використаної літератури

1. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124).

2. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи розвитку системи безпеки життєдіяльності” (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.

3. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція “Інформаційна безпека в сучасному суспільстві” (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.

4. Полотай О, Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи. Захист інформації в інформаційно-комунікаційних системах : зб. тез. III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів. Львів, ЛДУ БЖД. – 2019. С. 76-78.

5. Полотай О, Рожко Д. Організаційно-технічні методи захисту інформації від несанкціонованого доступу. "Інформаційна безпека в сучасному суспільстві": збірник тез доповідей III Міжнародної науково-технічної конференції. – Львів: ЛДУ БЖД, 2018. – С. 52-53.

6. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

7. "DDoS, Machine Learning, Measures". // "Understanding Denial-of-Service Attacks". / , 2016. – (Taylor & Francis Group).

8. “Sdn architecture,” june 2014, accessed: 2014-09-12. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdnresources/technialreports/TR SDN ARCH 1.0 06062014.pdf

9. «Хакінг і Фрікінг» - книга Максима Левіна. Описання DDoS-атаки за допомогою катастрофи «Збірка» - А.К. Гуц, Д.Н. Лавров. Режим доступу до ресурсу: https://cyberleninka.ru/article/n/opisanie-ddos-ataki-s-pomoschyu-katastrofy-sborka/viewer

10. D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. // Journal of Network and Computer Applications. – 2018.

11. Distributed Denial of Service Attack and Defense, Shui Yu, 2018.

12. Famous DDoS Attacks | The Largest DDoS Attacks Of All Time [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

13. Hacking: Denial of Service Attacks Paperback – December 17, 2019 by Alex Wagner.

14. https://infocom.ua/- що таке DDoS атаки, та яку мету вони переслідують

15. Ilker Ozchelik, R.R.Brooks, «Distributed Denial of Service Attacks: Real-world Detection», 2020.

16. Internet Printing Protocol/1.0: Encoding and Transport [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc2565.

17. Jugal Kalita, Dhruba Kumar Bhattacharya «DDoS Attacks: Evolution, Detection, Prevention, Reaction», 2018.

18. M. Sachdeva, G. Singh, K. Kumar, and K. Singh, “Measuring impact of ddos attacks on web services,”2010.

19. M. Sachdeva, G. Singh, K. Kumar, and K. Singh, “Measuring impact of ddos attacks on web services,”2010.

20. O.Polotai, O. Belej, N. Nestor. Developing a local positioning algorithm based on the identification of objects in a wireless Wi-Fi network of the mall. IEEE

16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

21. O.Polotai, O. Belej., N. Nestor, S. Panchak Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

22. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115.

23. R. Braga, E. Mota, and A. Passito, “Lightweight DDoS flooding attack detection using nox/openflow,” in Proc. 35th IEEE Conf. Local Computer Networks (LCN), 2010.

24. S. Farahmandian, M. Zamani, A. Akbarabadi, J. M. Zadeh, S. M. Mirhosseini, and S. Farahmandian, “A survey on methods to defend against DDoS attack in cloud computing,” in Proc. Recent Advances in Knowledge Engineering and System Science, Feb. 2013.

25. S. Shin, V. Yegneswaran, P. Porras, and G. Gu, “Avant- Guard: Scalable and Vigilant Switch Flow Management in Software-Defined Networks,” Proc. ACM SIGSAC Conf. Computer & Commun. Security, 2013, pp. 413–24.

26. The Coremelt Attack [Електронний ресурс] – Режим доступу до ресурсу: https://netsec.ethz.ch/publications/papers/studer_esorics09.pdf.

27. Wang, H., Xu, L., & Gu, G. (2015, June). FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks. In Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP International Conference on(pp. 239-250). IEEE