УДК 004.45 DOI: 10.31673/2412-4338.2023.031221

Гайдур Г.І., Гахов С.О., Сич М. В. Дмітрієв В.Є.
Державний університет інформаційно-комунікаційних технологій

АНАЛІЗ ЗАГРОЗ МЕРЕЖЕВОГО ТРАФІКУ РІВНІВ МОДЕЛІ OSI ДЛЯ ДИНАМІЧНОГО РОЗРАХУНКУ RTO В КОНТЕКСТІ БОРОТЬБИ З DDoS АТАКАМИ

Анотація. *В статті роведено огляд актуальних загроз мережевої безпеки, з точки зору аналізу мережевого трафіку на різних рівнях моделі OSI. Розглянуто різновиди атак розподіленої відмови в обслуговуванні (DDoS) та їх вплив на протокол керування передачею (TCP), зокрема, на важливий параметр - час очікування повторної передачі (RTO). Розкрито основні алгоритми та методи розрахунку RTO, включаючи адаптивні стратегії з залученням машинного навчання та штучного інтелекту для оптимізації стека TCP/IP.*

Зокрема, надано інформація щодо роботи алгоритму розрахунку RTO, який є важливим для надійності передачі даних через TCP. Описано, як цей алгоритм адаптивно змінює значення RTO в залежності від стану мережі та вимірюваних значень RTT (часу проходження всього шляху). Також наведено формули, які використовуються для розрахунку RTO з різними параметрами.

Додатково, розглянуто можливості використання методів машинного навчання та аналізу даних для виявлення та запобігання DDoS атак. Пояснено, як сучасні технології дозволяють використовувати ці методи для мінімізації хибно позитивних виявлень шкідливих пакетів трафіку та підвищення ефективності захисту інформаційних систем.

Приведено приклад програмних та апаратних засобів, що використовуються для практичної реалізації алгоритмів в пристроях передачі даних по Ethernt підключенню.

Дана робота дає уявлення про сучасні проблеми та виклики, які існують в сфері захисту мережевої безпеки в умовах зростаючого числа DDoS атак. Ця інформація корисна для студентів та фахівців, які вивчають мережеву безпеку та розробляють заходи для захисту мереж та систем.

Ключові слова: *загрози мережевої безпеки, RTO (час очікування повторної передачі), DDoS атаки, Протокол TCP, Машинне навчання, Оптимізація мережевого трафіку*

Haidur H., Gakhov S., Sych M., Dmitriiev V.
State University of Information and Communication Technologies

ANALYSIS OF NETWORK TRAFFIC THREATS ACROSS OSI MODEL LAYERS FOR DYNAMIC RTO CALCULATION IN THE CONTEXT OF COMBATING DDoS ATTACKS

Abstract. *This document provides an examination of current threats to network security, viewed through the lens of network traffic analysis at various OSI model layers. It delves into the different forms of Distributed Denial of Service (DDoS) attacks and their ramifications on the Transmission Control Protocol (TCP), with a specific focus on a critical parameter - the Retransmission Timeout (RTO). The text also divulges fundamental algorithms and techniques for calculating RTO, encompassing adaptive methodologies that harness machine learning and artificial intelligence for optimizing the TCP/IP stack.*

In particular, it offers insights into the functioning of the RTO calculation algorithm, a pivotal element ensuring the reliability of data transmission via TCP. The document elaborates on how this

algorithm dynamically adjusts the RTO value based on network conditions and measured Round Trip Time (RTT) values. Furthermore, it furnishes formulas for computing RTO with diverse parameters.

Moreover, the document explores the potential of employing machine learning and data analysis methodologies to detect and preempt DDoS attacks. It elucidates how contemporary technologies empower the use of these approaches to minimize false positives in identifying malicious traffic packets, thereby enhancing the effectiveness of safeguarding information systems.

Additionally, it provides an illustration of software and hardware tools employed for the practical implementation of these algorithms in devices facilitating data transmission via Ethernet connections.

In summary, this work offers insights into contemporary challenges and issues in the realm of network security, especially in the context of the escalating frequency of DDoS attacks. This information proves valuable for students and professionals engaged in the study of network security and the development of measures to fortify networks and systems.

Keywords: *network security threats, RTO (Retransmission TimeOut), DDoS attacks, TCP protocol, Machine Learning, Network Traffic Optimization*

1. Вступ

З розвитком технологій та поглибленням діджиталізації різних аспектів людської діяльності, збільшується кількість сервісів, якими люди користуються онлайн, а отже і кількість даних, що передаються в мережі.

Згідно порталу Statista сума збитків спричинених відомими випадками кіберзлочинів перевищила 10 мільярдів доларів в 2022 році, в цілому збільшившись в 7 разів за останні 5 років. Ця статистика має тенденцію до зростання.

Причиною цього є збільшення кількості векторів атак з розвитком таких технологій як штучний інтелект та популяризацією розумних пристроїв і збільшенням використання мобільних пристроїв.

Згідно статистики зібраної Unit 42 в Palo Alto Networks, серед нововиявлених вразливостей, які публікуються IT спільнотою на популярних інформаційних порталах, вразливість до атаки “Відмова в обслуговуванні” посідає друге місце (проаналізований період з Листопада 2021 по Січень 2022 р). Необхідно відмітити, що з проаналізованих вразливостей майже 70% можуть бути використані через підключення до мережі. Проаналізувавши 200 мільйонів унікальних сесій дослідники виявили 167.34 мільйонів унікальних шкідливих сесій (включаючи сканування).

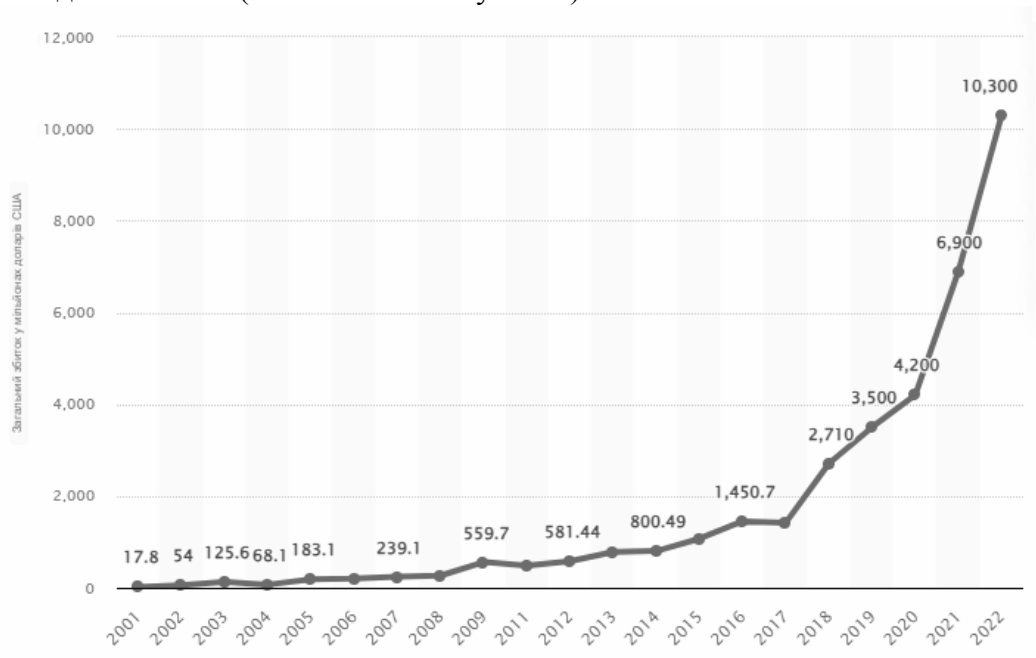

Рис.1. Збитки завдані зафіксованими кіберзлочинами в Сполучених Штатах за даними порталу Statista [5]

2. Анатомія та небезпеки DDoS атак

Атака “Відмова в обслуговуванні” еволюціонувала в новий вид “Розподілена відмова в обслуговуванні”. Використовуючи різні інструменти зловмисник ініціює одночасну відправку даних з великої кількості пристроїв в мережі у напрямку жертви. Кількість цих атак збільшується щороку, також збільшується трафік даних в мережі внаслідок такої активності.

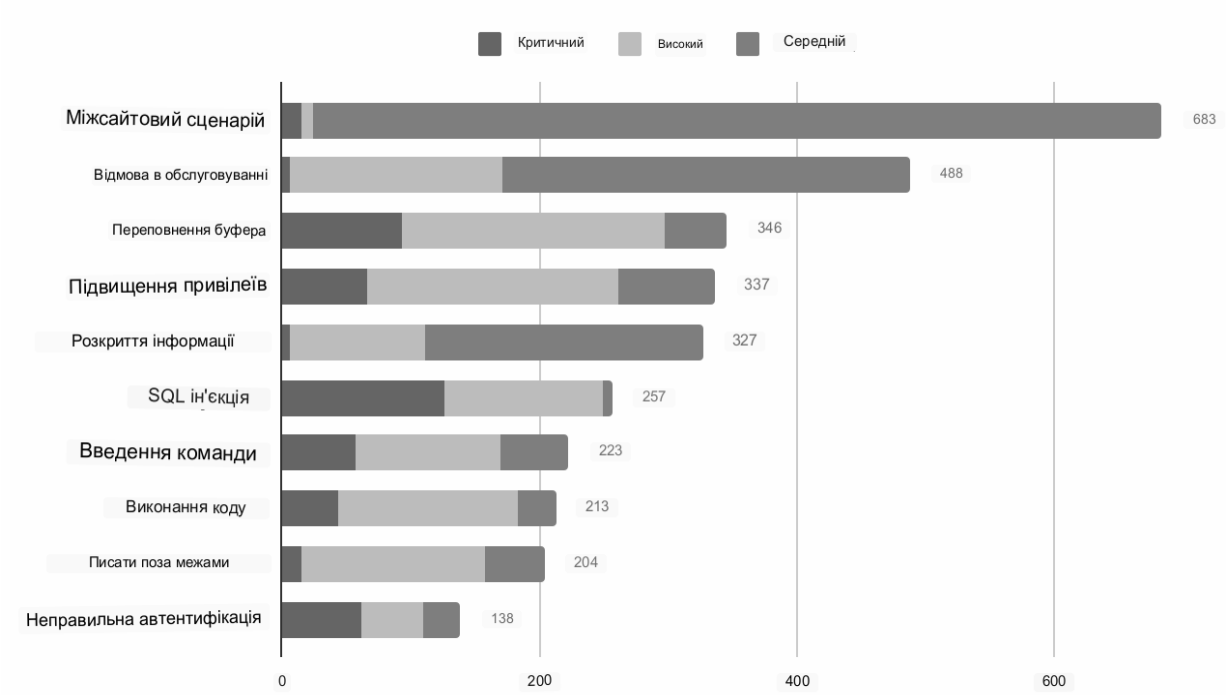

Рис. 2. Найпоширеніші типи вразливостей, що публікуються на загальнодоступних ресурсах згідно з Unit 42 [7]

DDoS атака може бути частиною більш складної атаки, а також цілком окремою атакою спрямованою на ресурс з ціллю порушення його коректного функціонування та втратою можливості приймати дані чи створювати нові підключення. Можна виділити кілька окремих підвидів цієї атаки:

- Атаки засновані на об’ємі (Volume Based Attacks): повені UDP, ICMP та інші. Ця атака має за мету перевантаження доступної пропускної здатності жертви за рахунок відправки великої кількості даних жертві;
- Атаки на рівні протоколів (Protocol Attacks): атака спрямована на вичерпання ресурсів сервера або проміжного мережевого обладнання.
- Атаки на рівні застосунків (Application Layer Attacks).

В наслідок успішно проведеної атаки, сервер відмовить клієнту в обслуговуванні. Магнітуда атак вимірюється в запитах за секунду (Rps), а під час атак на рівні протоколів також вимірюється кількість пакетів за секунду (Pps).

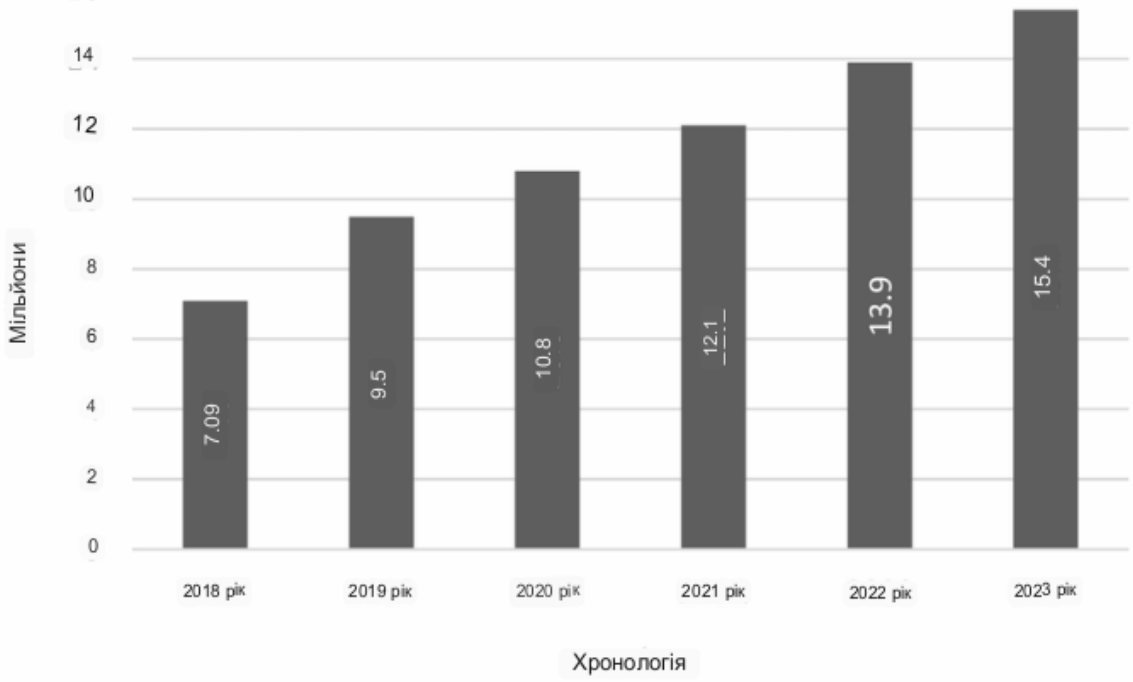

Рис. 3. Об’єм трафіку DDoS атак в мережі з 2018 по 2023 роки (дані на графіку в Тб) за даними порталу Researchgate [11]

DDoS атаки поширюються на 3 рівні в 7 рівневій мережевої OSI моделі.

Існує багато способів боротьби з цими типами DDoS атак, що використовують аналіз трафіку, чи потребують відповідного налаштування мережі і обладнання. Якщо розглядати DDoS атаки

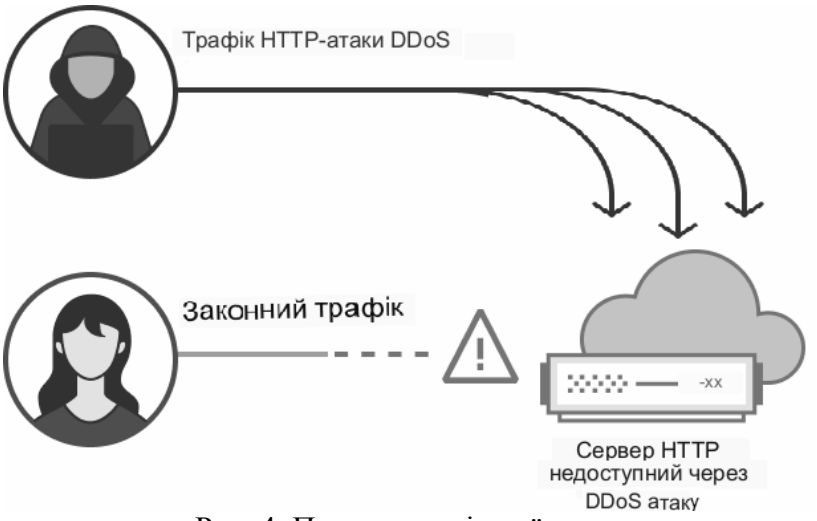

Рис. 4. Приклад успішної атаки

UDP DDoS атака має на меті вичерпати ресурси мережі чи серверу, цей протокол не потребує встановлення з’єднання для відправки пакетів, які ще й можуть бути фрагментовані. Найбільш ефективним вирішенням проблем з цим видом атаки є втручання інтернет провайдера, який переадресовує трафік на спеціально створені Black Hole сервери.

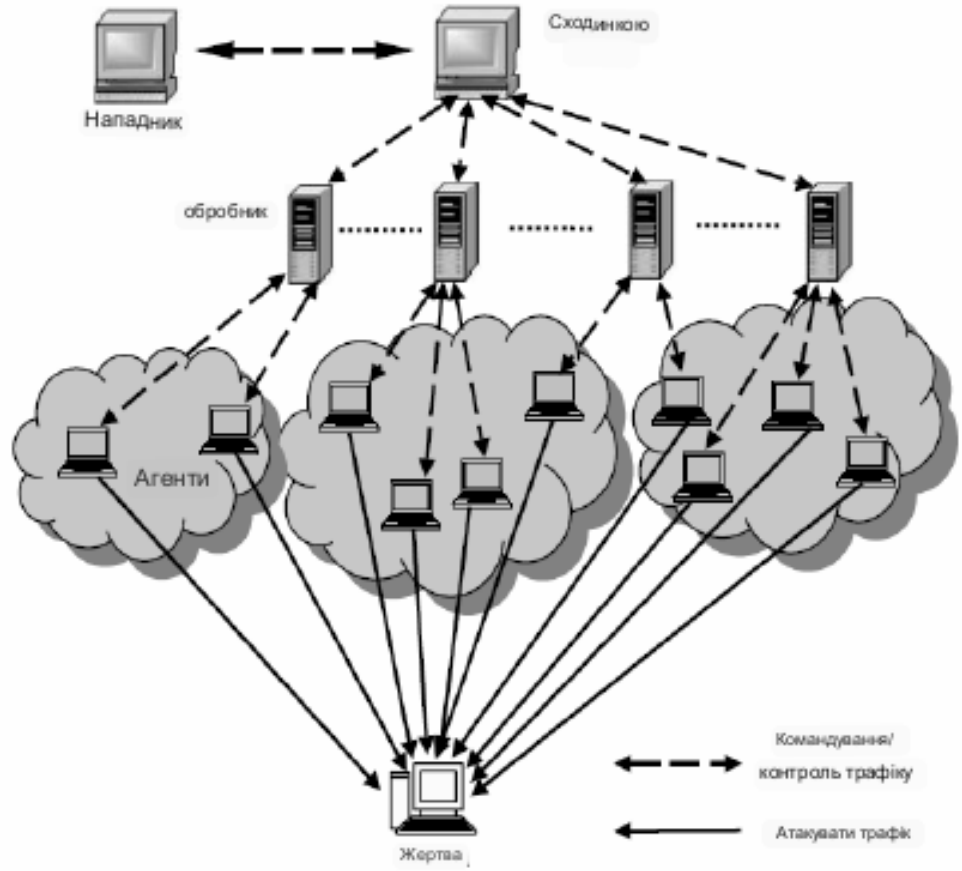

Рис. 5. Анатомія DDoS атаки

TCP DDoS атака має більш конкретне застосування, маючи за ціль визначений порт чи підключення. варто зауважити, що атаки можна розділити на 3 типи: атаки на рівні додатків (Application Layer), атаки на рівні мережі та об'ємні атаки. Використовуючи значно менше ресурсів та особливості встановлення TCP з'єднання, зловмисник може зробити сервіс недоступним для підключення.

3. Атаки з використанням TCP пакетів. Аналіз статистики

Вектори атак можуть бути різними та переслідувати різноманітні цілі, сконцентруємося на типах TCP DDoS атак, а конкретно на атаках рівнів 3/4 OSI моделі.

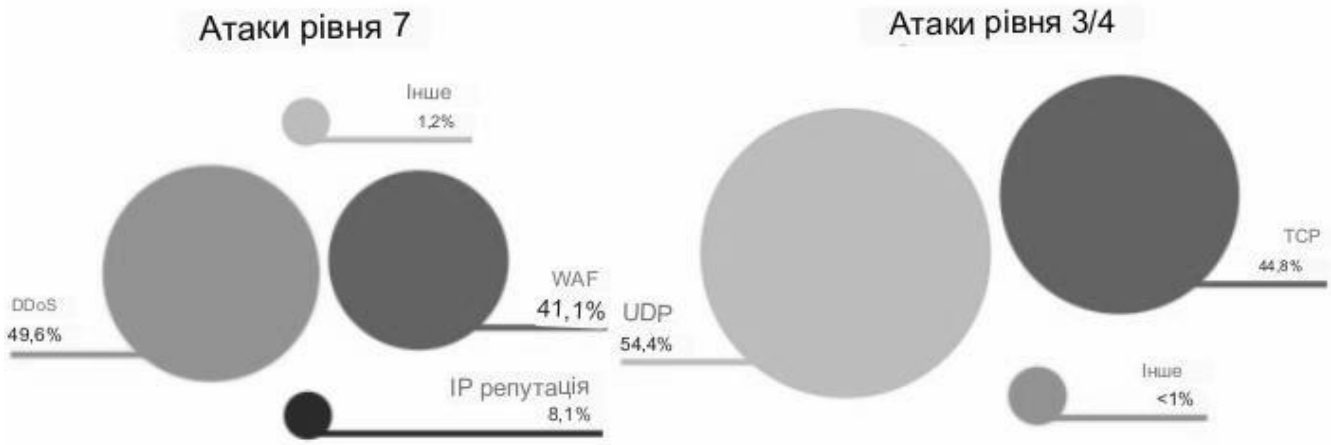

Рис. 6 .Розподіл шкідливого трафіку у першому кварталі 2023 року згідно Cloudfare Radar [12]

Протокол контролю передачі (TCP) - це стандарт, що працюючи з інтернет протоколом

(IP) визначає як комп'ютери відправляють пакети даних один одному. Протокол TCP відповідає за наступне:
визначає, як розділити дані на пакети, які може доставити мережа;

- відправляє та отримує пакети з мережевого рівня;
- керує потоком даних;
- веріфікує всі пакети, які отримує, забезпечуючи цілісність передачі даних;

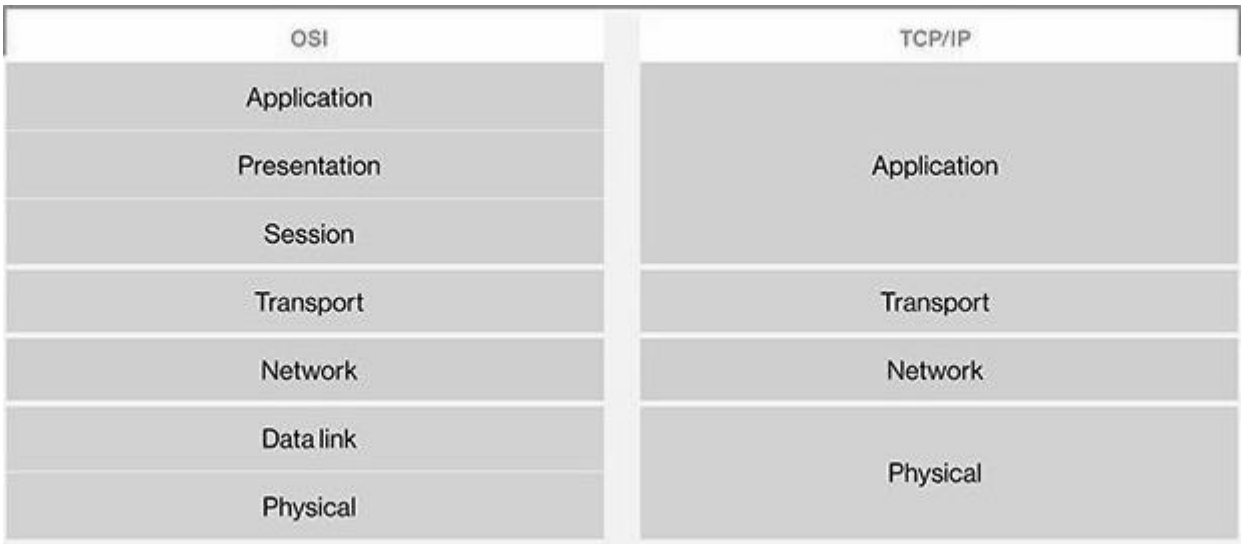

Рис. 7. Рівні в яких відбувається робота протоколу TCP

TCP відрізняється від UDP тим, що забезпечує цілісність даних, що передаються, тому перед початком передачі встановлюється з'єднання. Для встановлення з'єднання необхідно, щоб як сервер так і клієнт провели так зване трьохстороннє рукостискання:

- клієнт відправляє серверу SYN пакет - запит на з'єднання.
- сервер відповідає SYN/ACK пакетом, визнаючи отримання запиту на з'єднання;
- клієнт отримує SYN/ACK пакет та відповідає власним ACK пакетом.

Використовуючи особливості роботи TCP з'єднання, зловмисники можуть організовувати різноманітні атаки nbge Flood (повінь): SYN, SYN-ACK, ACK&PUSH, ACK Fragmentation, RST/FIN та ін. SYN пакети рідше за все відхиляються сервісом та являються найбільш легітимними, зловмисник відправляє велику кількість таких пакетів на різні порти сервера. Сервер відповідає пакетами SYN-ACK з відкритих портів. Опрацьовуючи велику кількість запитів на з'єднання, сервер тримає ці з'єднання "напів-підключеними". Як результат таблиця підключень сервера заповнюється і справжній запит на підключення від реального клієнта буде відхилено.

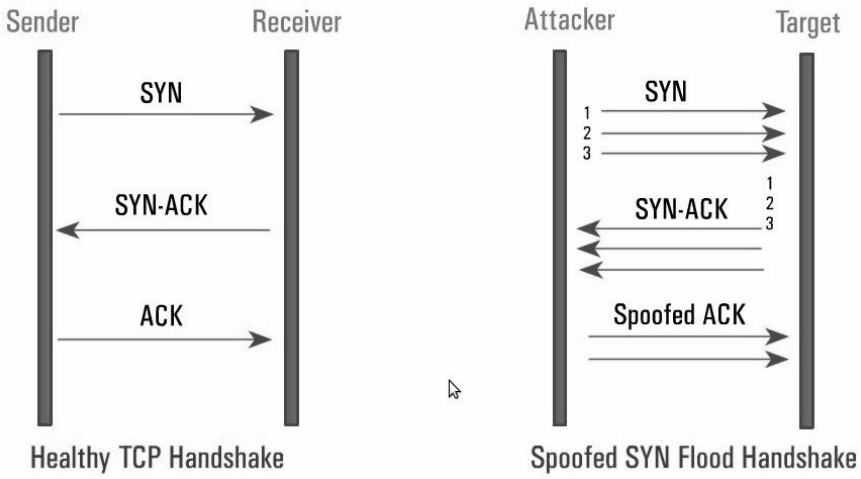

Рис. 8. Схематичне зображення TCP DoS атаки

Адміністратори використовують різні способи вирішити проблеми TCP Flood атак, наприклад мікро блокування, використання кукі чи налаштування стека. Налаштування стека - це серйозний інструмент, який дозволяє змінити: максимальний розмір сегмента, алгоритм контролю перевантаження, налаштування “keepalive”, вибіркове підтвердження, максимальну кількість підключень та ін.

RTO (час очікування повторної передачі) важливий параметр оптимізації стека TCP/IP. Значення RTO - це параметр TCP протоколу, що визначає час очікування відправником перед повторною передачею пакети, що міг бути втраченим у мережі. Атаки TCP DoS часто використовують пакети, що активують сеанс пакетом SYN і залишають без відповіді пакети SYN-ACK тримаючи підключення у напів-відкритому стані. Документ RFC 6298 містить вказівки щодо обробки таймеру повторної передачі RTO.

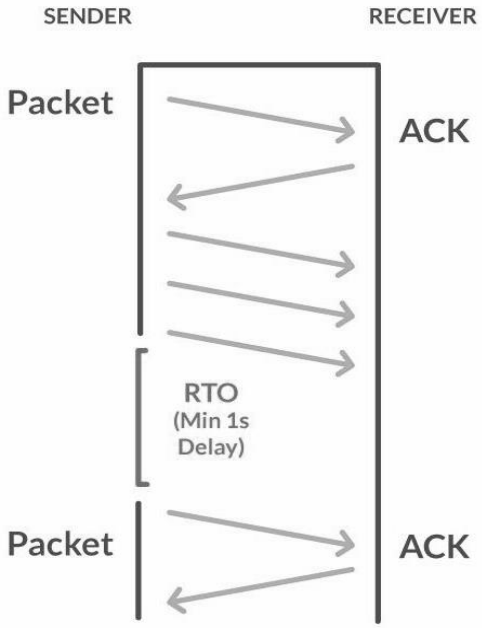

Рис. 9. Таймаут повторної передачі RTO

4. Алгоритм розрахунку RTO. Принцип роботи, практичне застосування.

Один із способів внести зміни в налаштування TCP - зміни ядра системи Linux. Команда “$ man tcp” виводить також і інформацію про кількість повторної відправки пакетів та посилається на RTO. Документ Request for Comments: 6298 визначає стандартний алгоритм, що використовується для розрахунку таймаута повторної відправки даних TCP. Через погане підключення, активність в мережі чи навіть налаштування драйвера та ядра лінукс, пакети втрачаються, RTO дозволяє визначити час повторної відправки та зробити передачу даних більш стабільною.

RTO вимірюється наступним чином, коли з’єднання встановлюється то алгоритм ініціалізує вимірювання RTT (час проходження всього шляху) та встановлює значення змінної RTTVAR (усереднений час проходження всього шляху), як половину виміряного RTT. Особливості розрахунку залежатимуть від налаштувань та версії TCP.

Протягом процесу передачі даних відправник продовжує вимірювати RTT для кожного відправленого пакету. SRTT оновлюється використовуючи середні значення RTT, які змінюються відповідно до стану мережі. Відправник також оновлює RTTVAR, щоб реагувати на зміни у виміряному RTT, та його різницею з SRTT. Тобто формула для розрахунку RTO:

$$RTO = SRTT + \max(G, K * RTTVAR)$$

де:

- `G` коефіцієнт, який зазвичай має мале значення (наприклад, 1 такт).
- `K` множник для масштабування RTTVAR.

Алгоритм RTO адаптивно обраховує значення затримки в залежності від поточного стану мережі та вимірюваних значеннях RTT. RTO також налаштовується відповідно до змін у RTT і RTTVAR.

Звичайно це не єдиний варіант розрахунку, в більш популярному варіанті RFC 793 - “Transmission Control Protocol”, формула виглядає так:

$$SRTT = (ALPHA * SRTT) + ((1-ALPHA) * RTT)$$
$$RTO = min[UBOUND,max[LBOUND,(BETA*SRTT)]]$$

Розрахунок RTO також впливає на ефективність роботи комп’ютеризованих систем в умовах здійснення DoS атаки. Зловмисники комбінують багато різних підходів та використовують особливості RTO для того, щоб час очікування повторної відправки пакетів збільшився, а ресурси мережевого обладнання чи сервера вичерпалися. У випадку виявлення DDoS атаки трафік перенаправляється або фільтрується в залежності від налаштувань фаєрволу та мережевого обладнання. Однією з проблем є можливість хибно позитивного визначення процесу DDoS атаки, в такому випадку трафік від легітимних джерел буде відхилено.

Сучасні технології дозволяють використовувати метод машинного навчання та аналізу даних для того, щоб мінімізувати кількість хибно позитивних виявлень шкідливих пакетів трафіку за рахунок передбачення процесу нормальної роботи в поточних умовах роботи мережі та очікуваного навантаження. Не існує єдиного алгоритму чи порядку дій, адже працювати доводить з різними рівнями передачі даних та з новими видами атак. Нові технології штучного інтелекту та машинного навчання дають багато можливостей для створення нових способів захисту інформаційних систем.

5. Засоби реалізації динамічного керування конфігурацією пакетами TCP/IP

Існує багато апаратних та програмних засобів для реалізації динамічної моделі розрахунку RTO. Одним з прикладів є програмний комплекс "Dynamic C," який використовується на контролерних платах, заснованих на мікропроцесорі "Rabbit 3000."

Пристрій "Rabbit 3000" є мікропроцесором із тактовою частотою 30 МГц, оснащеним флеш-пам'яттю обсягом до 512K і оперативною пам'яттю SRAM обсягом до 512K. Він має 52 цифрових входи/виходи та 6 послідовних портів (IrDA, HDLC, асинхронний, SPI) та працює з напругою 3,3 В, маючи режими низького споживання енергії в "сплячому" стані (< 2 мА).

Детальні характеристики цього пристрою доступні в документації продукту. Надійне управління цим пристроєм можливе завдяки інструменту "iDigi Manager Pro™," який забезпечує безпечне управління з будь-якої точки.

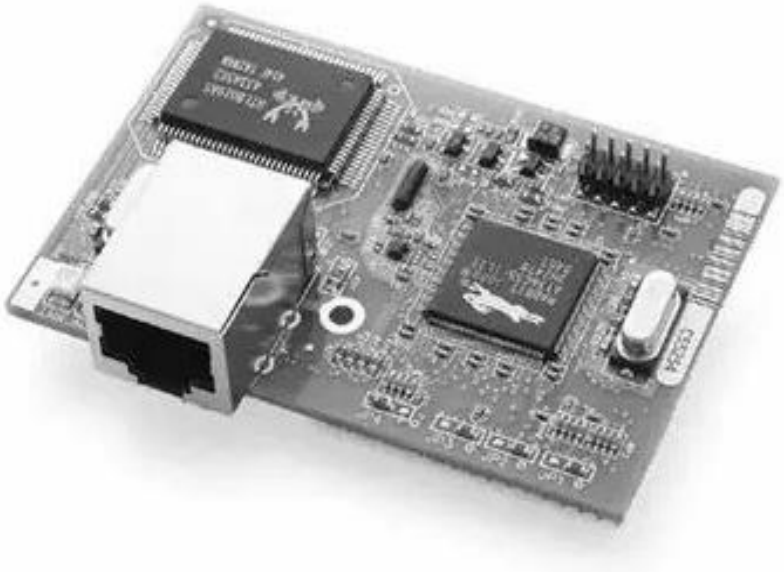

Рис. 10. Мережева плата RCM3000 series

Програмний комплекс "Dynamic C" представляє собою потужний інструмент для розробки вбудованих систем, спеціально призначений для використання на контролерних платах з можливістю підключення до мережі Ethernet.

Для успішного використання "Dynamic C" необхідні знання про мережі та протокол TCP/IP (Transmission Control Protocol/Internet Protocol). Реалізація TCP/IP в "Dynamic C" включає декілька бібліотек, основною з яких є DCRTCP.LIB. Починаючи з версії "Dynamic C" 7.05, ця бібліотека є містить DNS.LIB, IP.LIB, NET.LIB, TCP.LIB та UDP.LIB. Ці бібліотеки втілюють DNS (Domain Name Server), IP, TCP і UDP (User Datagram Protocol). Разом із бібліотеками ARP.LIB, ICMP.LIB, IGMP.LIB та PPP.LIB вони становлять транспортний та мережевий рівні стеку протоколів TCP/IP.

Таблиця 1

Бібліотеки Dynamic C, включені, коли значення макросу USE_* Macro Value > Zero

Configuration Macro	Realtek.lib*	Ppp.lib	Ppplink.lib	Pppoe.lib	WiFiG.lib
USE_ETHERNET	yes	no	no	no	no
USE_PPP_SERIAL	no	yes	yes	no	no
USE_PPPOE	yes	yes	no	yes	no
USE_WIFI	no	no	no	no	yes

Програмний комплекс "Dynamic C" взаємодіє з мікропроцесором "Rabbit 3000" та надає засоби для динамічного розрахунку RTO в контексті мережевої комунікації. Налаштування стеку TCP/IP починається з розуміння та визначення того, які інтерфейси будуть використовуватися і скільки їх потрібно. Крім того, потрібно визначитися з необхідними функціями програмного забезпечення. Наприклад, які будуть використовуватися протоколи DNS, TCP, UDP або DHCP. Зокрема, починаючи з Dynamic C 7.30, можна оптимізувати свій стек, видаливши непотрібні функції за допомогою умовної компіляції, підвищивши оптимізацію ресурсів.

6. Висновок

У цьому дослідженні ми глибоко дослідили критичну сферу загроз мережевій безпеці, зосереджуючись зокрема на атаках розподіленої відмови в обслуговуванні (DDoS) і їхньому

впливі на протокол керування передачею (TCP), зокрема на тайм-аут повторної передачі (RTO). Наше дослідження виявило передові алгоритми та методи для розрахунку RTO, а також адаптивні стратегії для оптимізації стеку TCP/IP у відповідь на ці загрози.

Список використаної літератури

1. Ferguson, P., Senie, D., & Huston, G. (2000). Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827. Retrieved from https://tools.ietf.org/html/rfc2827

2. Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

3. Stone, R. (2000). CenterTrack: An IP Overlay Network for Tracking DoS Floods. In Proceedings of the 9th USENIX Security Symposium.

4. Mirkovic, J., & Reiher, P. (2005). A Collaborative Defense Architecture for Mitigating DDoS Attacks. ACM Transactions on Computer Systems (TOCS), 23(3), 250-297.

5. Statista. (2023). Annual amount of financial damage caused by reported cybercrime in the U.S. (2001-2022). Retrieved from https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/

6. RFC 6298 - Computing TCP's Retransmission Timer (RTO). Retrieved from https://tools.ietf.org/html/rfc6298

7. Unit24. Network Security Trends: November 2021 to January 2022. May 31, 2022 Retrieved from https://unit42.paloaltonetworks.com/network-security-trends-cross-site-scripting/

8. Wang, Z., & Xu, D. (2017). A Survey of Advanced Persistent Threats in Cloud Computing. Journal of Computer and Communications, 5(14), 27-40.

9. Sivanathan, A., & Alazab, M. (2019). Machine Learning for Anomaly Detection and Threat Hunting in Cybersecurity: An Empirical Review. IEEE Access, 7, 159841-159855.

10. Bishop, M. (2003). Computer Security: Art and Science. Addison-Wesley.

11. Researchgate. Global Trend of DDoS Attacks 2018-2023. Retrieved from https://www.researchgate.net/figure/Global-Trend-of-DDoS-Attacks-2018-2023-7_fig1_348639527

12. Cloudflare Radar. Insight into network and application layer attack traffic. Retreived from https://radar.cloudflare.com/security-and-attacks