ДОСЛІДЖЕННЯ МЕТОДІВ КІБЕРЗАХИСТУ ВІД АТАКИ ТРАНСПОРТНОГО РІВНЯ TCP SYN FLOOD

Качан В.Є.

Кафедра «Інфокомунікаційної інженерії ім. В.В. Поповського»,
Харківський національний університет радіоелектроніки, Україна

E-mail: vadym.kachan@nure.ua

Abstract

One of the most pressing and critical issues is ensuring protection against the threat of denial of service (DoS) attacks. In this work, the importance of protection against a "denial of service" attack at the transport level, which is critical when establishing connections and data transmission, was indicated. The methods of protection against the SYN Flood attack, which is one of the most popular DoS-attacks of the transport layer, were considered, the disadvantages and advantages of specific solutions were analyzed, and they were implemented. According to the results, the decision about the best cyberprotection method was made.

Розвиток інформаційно-комунікаційних систем (ІКС) призвів до невпинного зростання кількості і якості кібератак на усіх рівнях моделі Open System Interconnection (OSI). Одними з таких є атаки типу «відмова в обслуговуванні» (Distributed Denial of Service, DDoS), що на сьогоднішній день постають як одна з найпріорітетніших проблем безпеки систем обробки та передачі інформації. Рівень за рівнем, DDoS-атаки викликають переповнення буферів пам'яті, обчислювальних ресурсів обладнання та завдають непоправних збитків, зважаючи на характер своєї масовості.

Повноцінними рішеннями забезпечення кіберзахисту ІКС від «відмов в обслуговуванні» вважаються комплексні системи, що здатні обмежити та запобігти наслідкам таких атак на функціонуюче обладнання. Не має сумнівів в тому, що усі сім рівнів моделі OSI є вразливими і жоден з них не має першочерговості в питаннях захисту, в тому числі і від DDoS-атак. Атаки на високо рівневі протоколи, такі як Hyper Text Transfer Protocol (HTTP) наразі є загрозою для найсучасніших інструментів, що використовуються для роботи з інформацією, таких як, наприклад, хмари [1]. Незважаючи на це, слід приділити особливу увагу саме транспортному рівню, адже він, згідно своєї ролі та функціоналу, являє собою так звану «пляшкову шийку», атака і переповнення якої призведе до неможливості роботи системи.

Кіберзахист на транспортному рівні, як і на усіх інших, потребує розуміння загальних тенденцій атак даного рівня і частоти їхнього використання. Так, згідно звіту компанії Cloudflare [2], 57,4% атак четвертого рівня припадають на атаку TCP Synchronize (SYN) Flood, яка є одним з різновидів DDoS-атак. Так як даний вид загрози передбачає заповнення буферу TCB (transmission control block) сегментами із встановленим флагом SYN, то рішення, шо доцільні для розгляду, повинні протидіяти такому переповненню, мінімізувати або виключити його наслідки. Статистичні методи можуть використовуватись для виявлення такої атаки [3], а серед методів протидії SYN Flood виділяються наступні:

- SYN Cookie;
- обробка пакетів в черзі «напіввідкритих» з'єднань»;
- SYN Proxy;
- SYN Authentication;
- фільтрація пакетів із прапором SYN;
- кешування запитів [4];
- алгоритм «три лічильники» [5].

Зважаючи на доступні для проведення лабораторного експерименту методи, в рамках дослідження використовуються три методи із вищенаведеного списку, а саме SYN Cookie, обробка чер-

ги пакетів та фільтрація. Як правило, найефективніша система кіберзахисту являє собою комплексне рішення, але проведення лабораторного експерименту, що включатиме в себе проведення атаки із можливістю зміни її параметрів і кількісну характеристику методів захисту на основі їх впровадження під час такої атаки є доцільним методом оцінки ефективності впровадження комплексної системи. Для прийняття рішення щодо раціональності використання трьох зазначених засобів, як результативних механізмів захисту, важливо впровадити ці механізми та проаналізувати їхні показники в усіх можливих варіаціях, тобто в незалежному використанні один від одного, комбіновано по парах та у комплексному вигляді. Показниками, що оцінюються, є використання ресурсів процесора у відсотках, втрата луно-пакетів запиту (echo request) та доступність ресурсу, яким є веб-сервер.

В ході досліду використовуваними операційними системами є Ubuntu (розгорнуто веб-сервер, що приймає запити) та Kali Linux (інструмент зловмисника) із вбудованими нею утилітами для реалізації SYN Flood.

Перш за все, у випадку відсутності механізмів захисту, система має 100% завантаженості ресурсів процесора і сервер повністю перестає відповідати.

За допомогою вбудованих у ядро Linux параметрів перевірено ефективність трьох методів захисту під час проведення атаки. Першим з них є SYN Cookie, що має такі результати:

- завантаженість ресурсів процесора – максимальне значення приблизно 60%, середнє – 52,7%;
- кількість втрачених луно-запитів – 25%;
- доступність сервера зберігається.

Для наступного метода, яким є обробка черги з'єднань, реалізація вимагає проведення досліду із різними значеннями заданих параметрів. Такими є значенням backlog (кількість збережених запитів) та retries (максимальна кількість можливих повторних запитів). Для використання ресурсів процесора отримано наступні результати:

- обробка черги з’єднань (backlog=1000, retries=3) – 48,7%;
- обробка черги з’єднань (backlog=3000, retries=2) – 48,8%;
- обробка черги з’єднань (backlog=5000, retries=1) – 47,2%.

Середні значення мають незначну розбіжність і усі вони є критично високими. Даний метод за середнім значенням використання процесорних ресурсів не суттєво відрізняється від такого ж значення у механізму SYN Cookie.

Втрати пакетів для даного методу є наступними:

- обробка черги з’єднань (backlog=1000, retries=3) – 46,1%;
- обробка черги з’єднань (backlog=3000, retries=2) – 44,4%;
- обробка черги з’єднань (backlog=5000, retries=1) – 41,6%.

Сервер став недоступним під час атак. Порівняно із SYN Cookie, обробка черги програє у ефективності. Її значення є незадовільними, адже майже не впливають на систему під час атаки, тобто не запроваджують той захист, що є необхідним. Для подальшого порівняння використовуватиметься значення результатів обробки з’єднань із параметрами backlog=5000 та retries = 1.

Останнім реалізованим методом є фільтрація пакетів запиту. Було отримано такі результати:

- завантаженість ресурсів процесора – максимальне значення приблизно 50%, середнє – 38,8%;
- кількість втрачених луно-запитів – 21,4%;
- доступність сервера зберігається.

Незважаючи на те, що даний метод надав найкращі показники у порівнянні із обробкою черги та SYN Cookie, було проведено додаткове дослідження для комплексних рішень, що являють собою попарне використання розглянутих механізмів і одночасне для усіх.

Результатом проведеного дослідження стало те, що за середнім значенням завантаженості ресурсів процесора комплексне рішення є меншим майже у 6 разів за найбільше значення, яке система має під час атаки без впровадження засобів захисту і у майже 1,5 рази менше за другий найменший показник комбінованого рішення із використанням SYN Cookie та фільтрації. Схожі результати можна спостерігати і за втратами пакетів ICMP, яких майже у 6 разів менше при використанні комплексного рішення порівняно із втратами за відсутності методів захисту та майже в 2 рази менше при другому найменшому показникові, який також має рішення із реалізацією фільтрації пакетів та SYN Cookie. За показником доступності веб-сайту, її було втрачено лише при відсутності методів захисту та при використанні рішення щодо обробки черги з’єднань.

Висновки

Безпека транспортного рівня займає важливе місце у забезпеченні захисту рівнів моделі OSI. Найбільш загрозливою атакою даного рівня є TCP SYN Flood [2], що була розглянута в даній роботі. За допомогою інструментів, вбудованих в Linux-дистрибутиви, було проведено цю атаку та реалізовано деякі з доступних методів захисту від неї. Виходячи з їхніх показників, а саме доступності веб-сайту під час атаки, відсотку використання процесорних ресурсів та втрат луно-пакетів, зроблено висновок щодо доцільності використання наведених механізмів кіберзахисту. За результатами лабораторного експерименту, найефективнішим механізмом стала комплексна система, що включала в собі усі реалізовані методи. Показник використання процесорних ресурсів у такої системи надав значення 17%, що майже у 6 разів менше за такий же показник при відсутності методів захисту та майже у 1,5 рази менше ніж у другого найнижчого показника. Аналогічно, за втратами пакетів запиту комплексна система надала значення 10% втрат, що майже у 6 разів нижче за втрати при відсутності захисту і майже у 2 рази нижче за кількість втрат порівняно із другим найнижчим значенням, при цьому доступність веб-сайту через браузер не постраждала, тобто було підтверджено ефективність такої системи.

Література

1. Shapovalova A., Yevdokymenko M. (2019), "Investigation of the Impact of HTTP DoS Attacks on the Cloud Web Server", International Conference On Natural Science And Technology, Kharkiv, Ukraine, 18-20 September, P. 25.

2. The Cloudflare Blog (2022), "DDoS Attack Trends for 2022 Q1", available at: https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/ (last accessed 10.10.2022).

3. Радівілова Т. А., Тавалбех М.Х., Глушаєв Д.Я., Заіка М.В (2019), «Виявлення DDoS атак статистичними методами», Третя міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології», Харків, Україна, 137 с.

4. Lemon J. (2002). Resisting SYN Flood DoS Attacks with a SYN Cache. BSDCon 2002, P. 1-9.

5. Gavaskar, S., Surendiran R., Ramaraj E. (2010), "Three counter defense mechanism for TCP SYN flooding attacks", International Journal of Computer Applications 6.6: 0975-8887, P. 12-15. DOI: https://doi.org/10.5120/1083-1399.