УДК 621.391

ДОСЛІДЖЕННЯ МЕТОДІВ ПРОТИДІЇ АТАКАМ ТРАНСПОРТНОГО РІВНЯ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

В.С. Момот, В.Ю. Порохняк
Харківський національний університет радіоелектроніки

Abstract *– The work analyzes the most common threats and defines network security objectives, as well as describes quantitative and qualitative indicators of network security, classified into five categories. The work contains an analysis of attacks targeting all seven layers of the Open Systems Interconnection (OSI) model and provides their common features and mechanisms, attack examples, and tools used to carry them out. A review and comparative characteristic of methods for countering transport layer attacks is performed, as well as an experimental study of the effectiveness of the selected methods for countering attacks using the example of the TCP PUSH ACK Flood attack. Particular attention is paid to the transport layer due to its popularity among cybercriminals who carry out distributed denial-of-service attacks using the shortcomings of the TCP and UDP protocols. After studying the theoretical information about the transport layer of the OSI model, special attention is paid to the mechanisms of the TCP protocol, in particular, the selected methods of countering attacks at the transport layer are studied, and their advantages and disadvantages are described. A conclusion is made regarding the effectiveness of the implemented methods of countering the TCP PUSH ACK Flood attack based on the average and maximum values of CPU usage, the percentage of lost packets (Packet Loss), the average and maximum response time, as well as the availability of access to the deployed web page on the victim's server. The final part of the work provides recommendations for improving server software and transport layer protocols, in particular TCP, in order to increase the effectiveness of countering distributed denial-of-service attacks, which are based on the abuse of prohibited flag combinations, IP address spoofing, and sending "Martian packets».*

Анотація *– У роботі проведено аналіз найпоширеніших загроз, визначенні завдання мережної безпеки, а також здійснено опис кількісних та якісних показників мережної безпеки, класифікованих за п'ятьма категоріями. Робота містить аналіз атак, націлених на всі сім рівнів моделі Open Systems Interconnection (OSI), наводяться їхні спільні риси, поширені механізми, приклади та засоби, що використовуються для їхнього проведення. Виконані огляд і порівняльна характеристика методів протидії атакам транспортного рівня, а також експериментальне дослідження ефективності використання обраних методів протидії атакам на прикладі атаки TCP PUSH ACK Flood. Особливу увагу в роботі приділено транспортному рівню, оскільки він часто використовується кіберзловмисниками, які проводять розподілені атаки на відмову в обслуговуванні, використовуючи недоліки функціонування протоколів TCP та UDP. Після опрацювання теоретичних відомостей про транспортний рівень моделі OSI велика увага приділена механізмам протоколу TCP, зокрема досліджено методи протидії атакам на транспортному рівні з описом їхніх переваг і недоліків. Зроблено висновок щодо ефективності реалізованих методів протидії атаці TCP PUSH ACK Flood на основі середнього та максимального значень використання ресурсів центральним процесором сервера, відсотка втрачених пакетів (Packet Loss), середнього та максимального часу відповіді ресурсу, а також наявності доступу до розгорнутої вебсторінки на сервері жертви. У заключній частині роботи надано рекомендації щодо вдосконалення програмного забезпечення серверів і протоколів транспортного рівня, зокрема TCP, з метою підвищення ефективності протидії розподіленим атакам типу «відмова в обслуговуванні», які базуються на зловживанні використання заборонених комбінацій прапорів, підміни (спуфінгу) IP-адрес та надсилання «марсіянських пакетів».*

Вступ

Надання сучасних інформаційних сервісів напряму забезпечується наявністю інфокомунікаційних мереж (ІКМ), що виконують передавання, пересилання та приймання сигналів, зображень, текстових або звукових повідомлень за допомогою проводових і безпроводових каналів зв'язку [1]. Ризик виведення з ладу ІКМ через спрямовані атаки, однією з яких є розподілена атака з відмови в обслуговуванні (Distributed Denial of Service, DDoS), залишається актуальним викликом. Відповідно до звіту компанії Cloudflare, що спеціалізується на захисті від атак цього типу, кількість DDoS-атак

у першому кварталі 2024 року виросла на 50% порівняно з першим кварталом 2023 року, збільшившись з 3 млн до 4,5 млн [2].

Повномасштабне вторгнення росії в Україну збільшило кількість спрямованих атак російськими хакерськими формуваннями. Близько 80% усіх кібератак у другому кварталі 2022 року було спрямовано на такі галузі, як телерадіомовлення, Інтернет, онлайн-ЗМІ та видавництва [3]. Згідно зі звітом CERT-UA, кількість атак на енергетичний сектор у другому півріччі 2023 року у порівнянні з першим півріччям збільшилась на 92% (52 атаки проти 27), проте водночас кількість критичних інцидентів зменшилась на 50% [4].

Таким чином, необхідність ефективного застосування методів захисту від атак, спрямованих на порушення доступності мережних ресурсів, та інших типів атак залишається нагальним питанням. Актуальність роботи полягає у необхідності дослідження та вдосконалення методів захисту від атак транспортного рівня в інфокомунікаційних мережах та успішного впровадження цих методів на прикладі атаки TCP PUSH ACK Flood. Важливість дослідження ефективності методів протидії саме цій атаці полягає у тому, що багато досліджень зосереджуються на інших атаках, не приділяючи достатньо уваги TCP PUSH ACK Flood.

I. Аналіз загроз, задач і показників мережної безпеки в інфокомунікаційних мережах

При аналізі загроз в інфокомунікаційних мережах використовуються три основні методи аналізу: статистичний, експертний та факторний [5]. Статистичний аналіз полягає в аналізі відкритих джерел і звітів організацій з мережної, інформаційної та кібербезпеки про виявлені інциденти та атаки. Цей тип аналізу надає змогу компаніям пріоритезувати захист від загроз відповідно до їхньої розповсюдженості. Факторний аналіз має на меті роботу з чинниками, що можуть бути передумовою до експлуатації вразливостей. Ці чинники можуть включати відсутність захисту серверного приміщення або відсутність антивірусного програмного забезпечення (ПЗ). Експертний аналіз проводиться безпосередньо експертом, який визначає чинники, що описують загрози безпеці інформації, а потім робить висновок стосовно рівня захищеності системи [5].

Відповідно до звіту Агентства Європейського Союзу з питань мережної та інформаційної безпеки (European Union Agency for Network and Information Security, ENISA) за 12 місяців (з липня 2022 року до червня 2023 року) програми-вимагачі та DDoS-атаки були найбільш розповсюдженими загрозами. Кругова діаграма загроз, що були причиною інцидентів безпеки, представлена на рис. 1 [6].

Як показано на рис. 1, понад 31% загроз становили програми-вимагачі, понад 21% – DDoS-атаки, ще понад 20 % – загрози, пов'язані з даними (порушення цілісності, конфіденційності та доступності даних, зокрема їхній витік). На рис. 1 у легенді до діаграми зазначено не тільки категорії загроз, але й категорії атак.

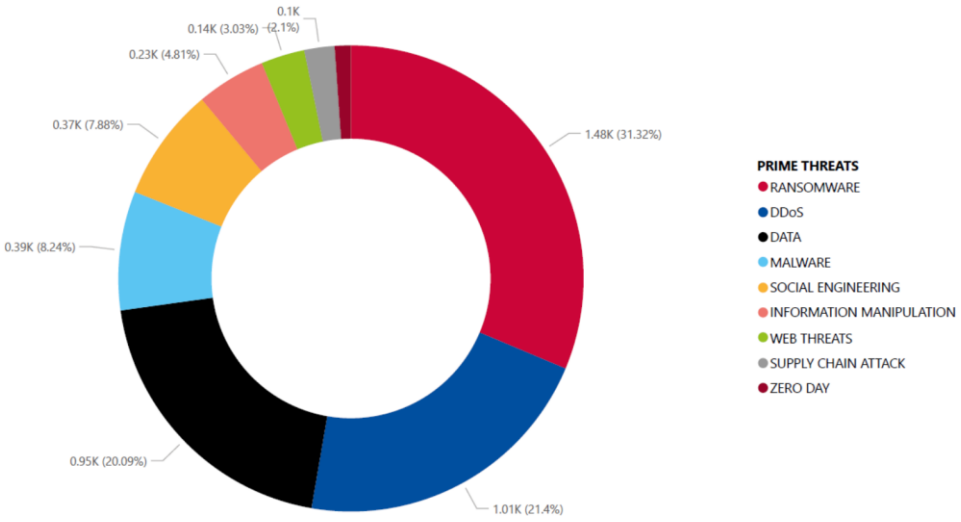

Рис. 1. Основні загрози безпеці [6]

Аналіз перших трьох категорій (програми-вимагачі, DDoS-атаки, дані) дозволив зробити висновок, що більш ніж 70% атак було пов'язано з такими загрозами безпеці:

– навмисне або ненавмисне зараження шкідливим ПЗ;
– порушення доступності (шифрування або блокування доступу);
– навмисне або ненавмисне ушкодження каналів зв'язку або пристроїв;
– порушення доступності інфокомунікаційної мережі шляхом відмови її елементів (споживання великого обсягу ресурсів, зниження пропускної здатності тощо);
– порушення конфіденційності інформації шляхом витоку даних.

Основними цілями мережної безпеки є забезпечення конфіденційності, цілісності, доступності, автентичності та надійності. Забезпечення цих властивостей, що стосуються інформації та користувачів, проводиться шляхом виконання таких завдань:

– організація безпечного та швидкого з'єднання між абонентами, стійкого до відмов;
– ідентифікація та автентифікація користувачів;
– надання доступу до мережних ресурсів лише авторизованим користувачам у визначений час;
– захист від шкідливого ПЗ, інцидентів і спрямованих атак;
– використання резервних пристроїв задля підвищення надлишковості;
– перевірка автентичності зовнішніх джерел, з яких надходять повідомлення, та однозначна ідентифікація внутрішніх;
– ведення журналу подій на кінцевих і транзитних пристроях.

Показники мережної безпеки – це стандартизовані показники, за якими вимірюється рівень мережної безпеки, проводиться оцінювання її надійності та захищеності [7]. Вони описують властивості мережі або її компонентів та надають можливість виявити потенційні слабкі місця в безпеці, а у подальшому скоригувати засоби захисту. Показники мережної безпеки поділяються на якісні та кількісні.

Якісні показники ефективності описують характеристику об'єкта у словесному вигляді та виражають:

– ступінь (низький, високий, середній);

– наявність або відсутність об'єкта або його властивості (наприклад, наявність резервного маршрутизатора).

Недоліками якісних показників є низька точність градації та велика ймовірність суб'єктивної оцінки, що залежить від окремої особи або групи осіб [8].

Кількісні показники ефективності – це ті показники, що можуть бути виражені в кількісних одиницях. Зазвичай їх зручніше використовувати в процесі оцінювання певного явища. Кількісні показники описують:

– безпосередньо кількість (наприклад, кількість вузлових пристроїв з налаштованим брандмауером);

– відсоткове значення від загальної кількості;

– оцінку або бал (наприклад, 97 із 100);

– рівень збитків у грошових одиницях.

Вибір та використання показників залежать від цілей організації. У деяких випадках зручним може виявитись оцінювання за комбінованими показниками. Наприклад, кількісний показник визначатиме відсоток маршрутизаторів, захищених паролем, а якісний – чи перевищує довжина паролю 8 символів.

Показники мережної безпеки можна класифікувати за п'ятьма категоріями:

1) Показники, що описують стійкість ІКМ до атак та вразливостей (метрики CVSS (Common Vulnerability Scoring System), середній час виправлення вразливості, середній час компрометації мережі, кількість відкритих портів тощо);

2) Показники, що описують надійність, доступність та безвідмовність системи (середній час роботи системи до повної відмови, середній час роботи системи між тимчасовими збоями, середній час недоступності мережного ресурсу тощо);

3) Показники, пов'язані з розпізнаванням та протидією атакам (середній час повного відновлення після інциденту безпеки, кількість спрямованих атак за певний період часу, кількість спроб несанкціонованого доступу тощо);

4) Показники, пов'язані з відповідністю ІКМ до прийнятих стандартів та нормативних документів (кількість впроваджених механізмів контролю безпеки, відсоток співробітників, ознайомлених з нормативно-правовими документами, наявність відповідності виробників програмного та апаратного забезпечення міжнародним стандартам тощо);

5) Показники, пов'язані з продуктивністю та доцільністю впроваджених механізмів безпеки в організації (рівень збитків, вартість інциденту безпеки, показник рентабельності інвестицій тощо).

Інфокомунікаційна мережа зберігає ймовірність бути атакованою на всіх рівнях мережної моделі OSI (Open Systems Interconnection). На транспортному рівні атаки пов'язані із використанням вразливостей протоколів TCP (Transmission Control Protocol) та UDP (User Datagram Protocol).

До розподілених атак на відмову в обслуговуванні, що спрямовані на перевантаження ресурсів сервера або мережного пристрою, відносять такі:

– атаки типу Flood, що містять за мету надсилання великої кількості запитів для перевантаження ресурсів пристрою, в тому числі і з нестандартними комбінаціями прапорів (SYN Flood, ACK Flood, Fragmented ACK Flood, Xmas Flood, UDP Flood, Fragmented UDP Flood тощо) [10];

– Fraggle Attack, що полягає у надсиланні широкомовних UDP-запитів, у яких адресою джерела вказана адреса жертви [11];

– LAND Attack, яка полягає у створенні пакета TCP SYN з ідентичними адресами джерела та призначення, таким чином пакет буде безкінечно оброблятись [12];

– Fake Session Attack, що полягає у створенні та надсиланні зловмисником послідовності пакетів з прапорами SYN, ACK та FIN, створюючи видимість справжнього сеансу [13].

Атаки, спрямовані на перехоплення та надсилання підроблених повідомлень, використовують особливість механізму номера послідовності у протоколі TCP (TCP Sequence Number). Початкове значення послідовності ISN (Initial Sequence Number) надсилається як клієнтом, так і сервером під час процесу тристороннього рукостискання та має розмір 32 біти [14]. Під час передачі даних воно збільшується на кількість даних, переданих у сегменті. Для того, щоб вгадати це значення, зловмисник повинен створити 2^{32} пакетів (більш ніж 4 мільярди), проте існує особливість функціонування протоколу TCP, що значно скорочує зловмисникам витрачений час та ресурси.

Існує так зване «вікно», у якому сервер має можливість приймати пакети, доставлені у хаотичній послідовності, та обробляти їх по черзі, збираючи їх у правильному порядку [15]. Цей механізм «вікна» значно скорочує кількість значень, необхідних для перебору значення номера послідовності. Формула для перебору має такий вигляд:

$$\mathrm{SEQ} = \frac{2^{32}}{\mathrm{ws}}, \tag{1}$$

де ws – розмір «вікна» (window size).

З формули (1) можна зробити висновок, що для ускладнення процесу вгадування значення номера послідовності повинна виконуватись одна з двох умов: або номер повинен бути достатньо великим, або значення розміру вікна мусить бути достатньо малим. В операційній системі Windows значення «вікна» дорівнює 64 Кбайт [16], але його можна змінити шляхом редагування реєстру.

До атак типу «людина посередині», що спрямовані на перехоплення на надсилання підроблених повідомлень, відносять такі дії:

– перехоплення сесії TCP (TCP Session Hijacking);

– передбачення номеру послідовності TCP (TCP Sequence Number Prediction Attack);

– TCP Reset Attack, що спрямована на припинення TCP-з'єднання.

Атаки, спрямовані на сканування портів та виявлення працюючих сервісів, мають на меті надсилання UDP-запиту (UDP Scan) або TCP-запиту з певним встановленим прапором для аналізу відповіді сервера на нього. До таких атак з використанням протоколу TCP відносяться Null Attack (прапори відсутні), Connect Scan (прапори SYN

та ACK), SYN Scan (прапор SYN), FIN Scan (прапор FIN), Xmas Scan (прапори PSH, URG та FIN) [17].

Класифікація атак за їхньою спрямованістю на усіх рівнях моделі OSI представлена у табл. 1.

Таблиця 1. Класифікація атак за рівнями OSI

Рівень OSI	Спільні риси та поширені механізми	Приклади атак	Засоби та ресурси
Прикладний	Втручання в роботу вебсерверів, поштового зв'язку, вебзастосунків; використання шкідливого ПЗ; використання вразливостей операційних систем та ПЗ, відмова в обслуговуванні, прослуховування трафіку	Slowloris, Permanent DoS, DHCP Flood, DHCP starvation, NTP Flood, DNS Flood, фішинг, міжсайтовий скриптинг, перехоплення cookie-файлу сеансу	Утиліти та ПЗ (LOIC, MHDDoS, Wireshark), в тому числі шкідливе ПЗ
Представницький	Злам шифрування, відмова в обслуговуванні	Підроблені запити SSL, SSL flood, Heartbeat, SSL renegotiation, SSL stripping	thc-ssl-dos, Cutwail botnet, Wireshark
Сеансовий	Перехоплення сеансу користувача, переривання віддаленого підключення, відмова в обслуговуванні; прослуховування трафіку	telnet sniffing, telnet DoS [9], злам паролів telnet та ssh	Wireshark
Транспортний	Сканування мережі, перехоплення сеансу, відмова в обслуговуванні, прослуховування трафіку	TCP SYN Flood, TCP ACK Flood, Fraggle, UDP Flood, TCP RST Attack, TCP SYN Scan, UDP Scan	Утиліти та ПЗ (hping3, nmap, db1000n, LOIC, MHDDoS, Wireshark)
Мережний	Підміна адреси, атаки типу «людина посередині», втручання в процес маршрутизації, відмова в обслуговуванні, прослуховування трафіку	Ping of Death, IP spoofing, ICMP Flood, Evil Twin, Smurf Attack, IP Fragmentation, Wormhole, Blackhole	Утиліти та ПЗ (LOIC, hping3, Wireshark)
Канальний	Підміна адреси, втручання в процес комутації, відмова в обслуговуванні, прослуховування трафіку	MAC spoofing, ARP spoofing, MAC flooding, крадіжка порту, VLAN hopping, пошкоджені кадри	Утиліти (iproute2, macchanger), Wireshark
Фізичний	Фізичне пошкодження пристроїв, відмова в обслуговуванні	Підміна пристроїв, глушіння (jamming), руйнування	Постановник завад, USB Killer

У табл. 1 можна побачити, що атака на відмову в обслуговуванні присутня на всіх рівнях моделі OSI. З підвищенням рівня підвищується частота використання програмного забезпечення та утиліт для проведення атак. Якщо атаки нижніх рівнів спрямовані на підміну характеристик мережних об'єктів (адрес, пристроїв), то атаки на верхніх рівнях спрямовані переважно на експлуатацію вразливостей протоколів.

II. Огляд та порівняльна характеристика методів протидії атакам транспортного рівня в інфокомунікаційних мережах

З метою коригування впроваджених методів захисту від атак транспортного рівня та для подальшого оцінювання захищеності мережі проведено аналіз методів протидії атакам, використовуючи якісні та кількісні показники. Обидва типи показників важливі для комплексного розуміння якості впроваджених заходів.

До якісних показників ефективності впроваджених методів відносяться:

– наявність доступу до вебсторінки;
– наявність очікування при запиті до вебсервера;
– наявність виявлення відкритих портів;
– наявність виявлення працюючих сервісів.

До кількісних показників ефективності протидії атакам можна віднести:

– середній час доступу (відповіді), мс;
– відсоток втрачених пакетів (Packet Loss), %;
– завантаження центрального процесора, %;
– використання оперативної пам'яті, %;
– максимальне значення потоку трафіку (Peak Traffic Flow), Мбіт/с;
– кількість знайдених відкритих портів, од.

Порівняльна характеристика методів протидії атакам транспортного рівня надана у табл. 2.

Як показано у табл. 2, при виборі методів протидії атакам транспортного рівня слід зберігати баланс між швидкістю мережі та ефективністю захисту. Вибір методу протидії залежить насамперед від типу атаки. Також можна зробити висновок, що найбільше методів застосовано саме до протидії атаці TCP SYN Flood, у той час як для інших атак кількість застосованих засобів значно менша. Це можна пояснити значною поширеністю та високою шкідливістю атаки TCP SYN Flood.

Налаштування мережного екрана є універсальним засобом протидії для всіх атак, спрямованих на відмову в обслуговуванні.

III. Експериментальне дослідження ефективності використання обраних методів протидії атакам транспортного рівня в інфокомунікаційних мережах

Атака TCP PUSH ACK Flood полягає у надсиланні з великою швидкістю сегментів з прапорами PSH (вимагає негайного надсилання даних на рівень застосунку) [15] та ACK (визначає номер послідовності, який отримувач очікує отримати). Використання пакету з цими прапорами без попередньої процедури тристороннього рукостискання робить його «пакетом поза станом» (out-of-state packet). Сервер, отримавши такий пакет без попередньої процедури тристороннього рукостискання, повинен надіслати у відповідь сегмент з прапором RST, обриваючи з'єднання [15].

Таблиця 2. Порівняльна характеристика методів протидії атакам

Метод протидії	Переваги	Недоліки
Сувора зворотна фільтрація адрес	Ефективність проти атак з підміни IP-адреси [18]	Низька ефективність проти атак з використанням ботнету
Збільшення кількості можливих одночасних з'єднань (записів TCB)	Дозволяє зберігати більшу кількість з'єднань до заповнення та відмови системи	Виділення додаткових ресурсів на управління з'єднаннями; процесор повинен бути швидким для вчасної обробки запитів
Збільшення черги SYN-запитів (backlog) [21]	Черга перевантажується не так швидко	Збільшений розмір черги впливає на використання ресурсів для обробки з'єднань
Зменшення кількості пересилань запитів SYN-ACK	Ефективність при атаці SYN Flood з підмінених адрес, які не відповідають на запит SYN-ACK	Ймовірність того, що легітимні клієнти не встигнуть відповісти на запит
Зменшення таймеру стану SYN-RECEIVED	Напіввідкриті з'єднання швидше знищуються, використовуючи менше системних ресурсів	З'єднання з легітимними клієнтами не буде встановлено, якщо клієнт довго не відповідатиме [18]
Знищення старих напіввідкритих з'єднань TCB	Метод ефективний при тривалому процесі встановлення з'єднання з клієнтом	Не є ефективним при швидкому заповненні таблиці TCB внаслідок атаки
SYN Cache	Секретні біти захищають «відра» від витіснення легітимних адрес	Повний запис TCB не зберігається та повинен доповнюватись додатковою інформацією [18]
SYN Cookie	Cookie не займає місця для зберігання та підвищує стійкість до атак з угадування номера послідовності	Для повторного підключення клієнта використовується новий Cookie
Автентифікація TCP SYN	Сервер не витрачає ресурси на обробку напіввідкритих з'єднань	Час встановлення з'єднання збільшується, спочатку проводиться з'єднання між клієнтом та проміжним пристроєм, а потім між клієнтом та сервером
Алгоритм «три лічильники»	Ефективність при відкиданні запитів з однаковими IP-адресами та портами	Збільшене навантаження через початкове надсилання пакетів двічі
Закінчення випадкового з'єднання	При DDoS-атаці існує велика ймовірність завершення з'єднання зі зловмисником	Існує ризик припинення з'єднання з легітимним користувачем
SYN Agent	Сервер отримує тільки автентифіковані з'єднання від перевірених клієнтів	Напіввідкриті з'єднання навантажують агент
SYN Proxy	Ефективність у відбитті атак TCP SYN-ACK Flood та TCP ACK Flood [22]	Зниження швидкості встановлення з'єднання через додаткове підключення між проксі та сервером
TCP Intercept	Ефективність проти атак TCP SYN Flood	Не рекомендується використовувати разом з мережним екраном зональної політики (zone-based firewall) Cisco IOS [19]

Продовження табл. 2

1	2	3
Обмеження швидкості вхідних TCP- та UDP-запитів	Пом'якшення наслідків розподіленої атаки на відмову в обслуговуванні	Необхідний досвід у налаштуванні правил мережного екрану
Відкидання TCP-запитів з комбінаціями прапорів	Ефективність проти атак, що базуються на нетипових комбінаціях прапорів	Необхідний досвід у налаштуванні правил мережного екрану
Вимкнення серверів	Крайня міра задля припинення поширення атаки та запобігання більшій шкоді	Через неактивність системи клієнти не отримуватимуть послуги
Резервні сервери	Балансування навантаження у разі виведення з ладу основного серверу	Потреба у додаткових ресурсах для адміністрування
Cloudflare Spectrum	Ефективність проти TCP та UDP-атак, швидке надсилання трафіку, балансування навантаження [20]	Доступна лише у плані Enterprise, вартість відповідає впровадженим методам захисту
Складний для передбачення ISN	Метод ефективний проти атак з перехоплення сеансу	–
Масштабування вікна	Ефективність при великій кількості запитів	Вразливість до атаки з вгадування номера послідовності
Зменшення вікна	Ефективність проти атак з вгадування номера послідовності	При хаотичній передачі частина сегментів опиниться поза вікном
Закриття портів	Зменшення області дії атаки та обмеження інформації про сервіси	–
Системи протидії вторгненням	Активна протидія атакам	Впливають на пропускну здатність мережі через аналіз трафіку, що проходить через них
Системи виявлення вторгнень	Реєструють потенційні події для подальшого аналізу	Не протидіють атакам

Перелічимо утиліти та програми, що використовуються при моделюванні атак та дослідженні ефективності впроваджених методів:

1) hping3 – утиліта для проведення DDoS-атак, що має широкий функціонал, зокрема реалізує надсилання пакетів UDP, TCP, ICMP; налаштування розміру пакетів, підміни IP-адреси тощо;

2) sar – утиліта для збору та запису статистики активності системи, зокрема використання ресурсів центрального процесора, трафіку мережних інтерфейсів та використання пам'яті за певний проміжок часу;

3) Утиліта ping необхідна для вимірювання відсотку втрат пакетів та часу відповіді вебсервера;

4) Аналізатор мережних пакетів Wireshark використовується для демонстрації процесу атаки;

5) Веббраузер Mozilla Web Browser використовується для перевірки доступу до вебсторінки;

6) Програмне середовище GNU Octave необхідне для побудови графіків за отриманими відсотками використання центрального процесора впродовж однієї хвилини.

У межах проведеного експерименту в ролі зловмисника використовувалась віртуальна машина на операційній системі Kali Linux 2024.1 (один процесор, 2048 Мбайт оперативної пам'яті), а як жертва – віртуальна машина на операційній системі Xubuntu 24.04 (два процесори, 4096 Мбайт оперативної пам'яті). Обидві віртуальні машини знаходяться у одній локальній мережі та під'єднані за допомогою мостового адаптера. IP-адреса жертви – 192.168.0.107, IP-адреса зловмисника – 192.168.0.108. Об'єктом атаки виступає вебсторінка, розгорнута на вебсервері nginx на порті 80 (HTTP). Схема мережі представлена на рис. 2.

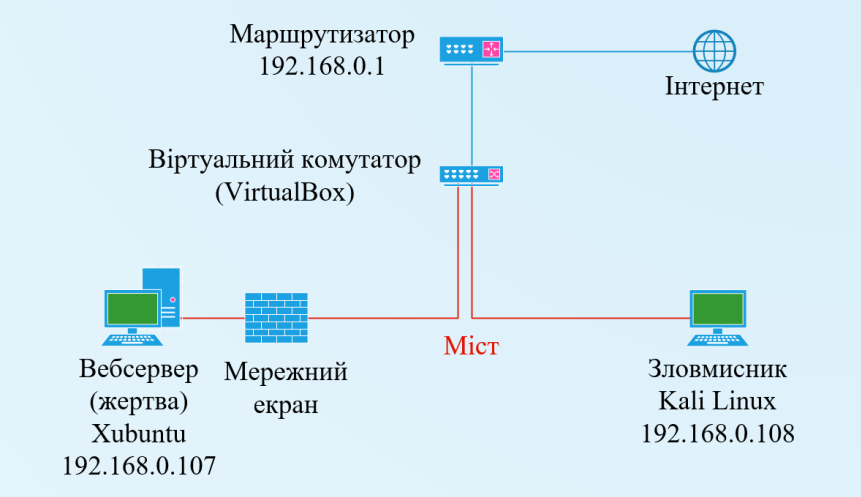

Рис. 2. Знімок екрану після моделювання атаки TCP PUSH ACK Flood з впровадженими параметрами захисту за замовчуванням

На рис. 2 можна побачити, що схема мережі складається з двох віртуальних машин (Xubuntu та Kali Linux), з'єднаних мостовим адаптером. Програмне забезпечення VirtualBox виступає в ролі віртуального комутатора.

За замовчуванням використані такі параметри конфігурації ядра:

– динамічна зміна розміру вікна (net.ipv4.tcp_window_scaling=1);

– вільна зворотна фільтрація адрес (net.ipv4.conf.default.rp_filter=1, net.ipv4.conf.all.rp_filter=1) [21].

Команда ping 192.168.0.107 -c 50 виконується впродовж атаки (50 секунд) для визначення показників середнього часу відповіді та відсотку втрат пакетів. Знімок екрану після проведеної атаки зображено на рис. 3.

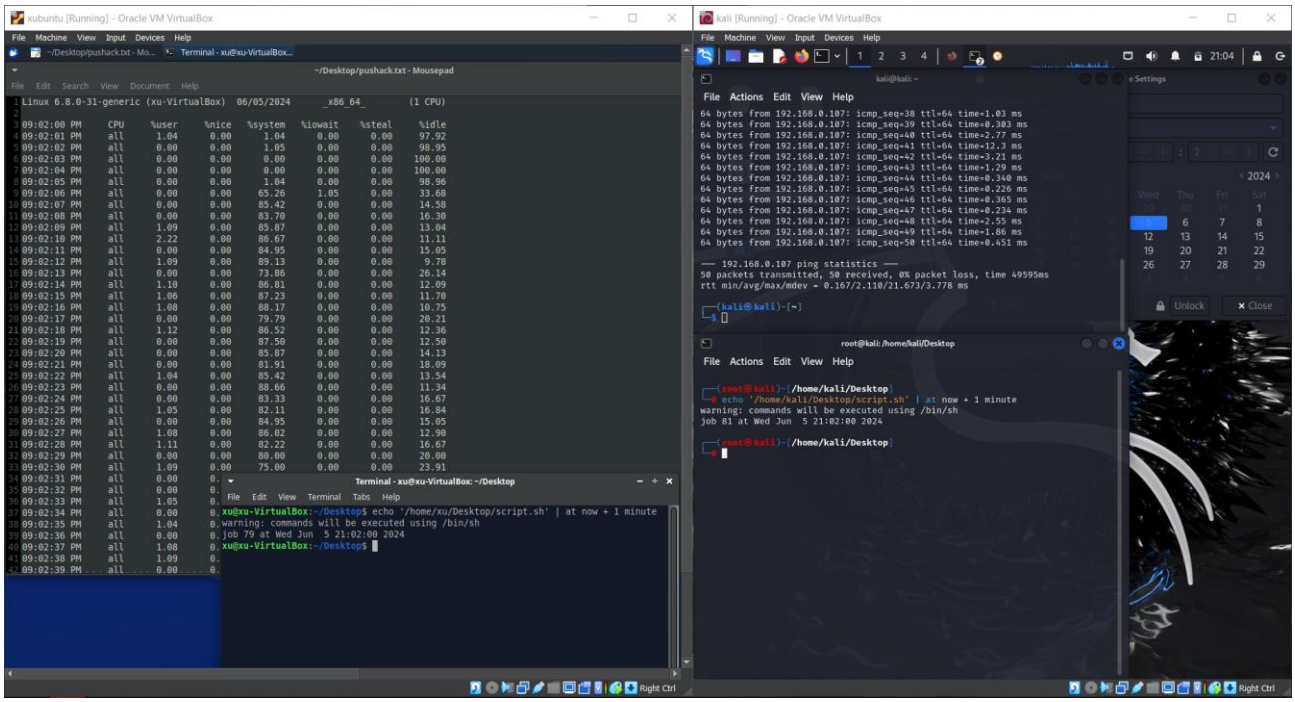

Рис. 3. Результати моделювання атаки TCP PUSH ACK Flood з впровадженими параметрами захисту за замовчуванням

На рис. 3 можна побачити інтерфейс обох операційних систем, Xubuntu (ліворуч) та Kali Linux (праворуч). Запуск обох скриптів не виводився динамічно у вікні терміналу, натомість скрипт запису показників навантаження процесора успішно зберіг інформацію у текстовому файлі. Для побудови графіка використовувалися значення з двох колонок файлу pushack.txt – з першої (час вимірювання характеристики) та п'ятої (використання центрального процесора під час виконання команд на системному рівні).

Графік використання центрального процесора під час виконання команд на системному рівні (ядра) зображено на рис. 4.

З рис. 4 можна зробити висновок, що після початку атаки відсоток використання ресурсів процесора коливався від 66 % до 94,95 %. Незважаючи на те, що атака не вивела з ладу вебсервер, вона збільшила споживання ресурсів процесора до критичного рівня. У середньому відсоток використання ресурсів під час атаки становив 84,47 %. Враховуючи те, що у даному експерименті атака проводилась з одного пристрою та одного вікна термінала, можна передбачити, що при використанні ботнету наслідками атаки було б тимчасове виведення вебсервера з ладу. Поза вікном атаки використання ресурсів центрального процесора знаходилось у межах 2%.

При використанні суворої зворотної фільтрації виконується перевірка кожного вхідного пакета у таблиці MAC-адрес, і якщо інтерфейс, на який надійшов пакет, не є кращим зворотним шляхом до джерела, то такий пакет відкидається [21]. Сувора зворотна фільтрація визначається в утиліті управління параметрами ядра операційної

системи (sysctl). Вона конфігурується параметрами net.ipv4.conf.all.rp_filter=1 (застосовує це налаштування для усіх інтерфейсів) та net.ipv4.conf.default.rp_filter=1 (встановлює це значення за замовчуванням для усіх майбутніх налаштованих інтерфейсів).

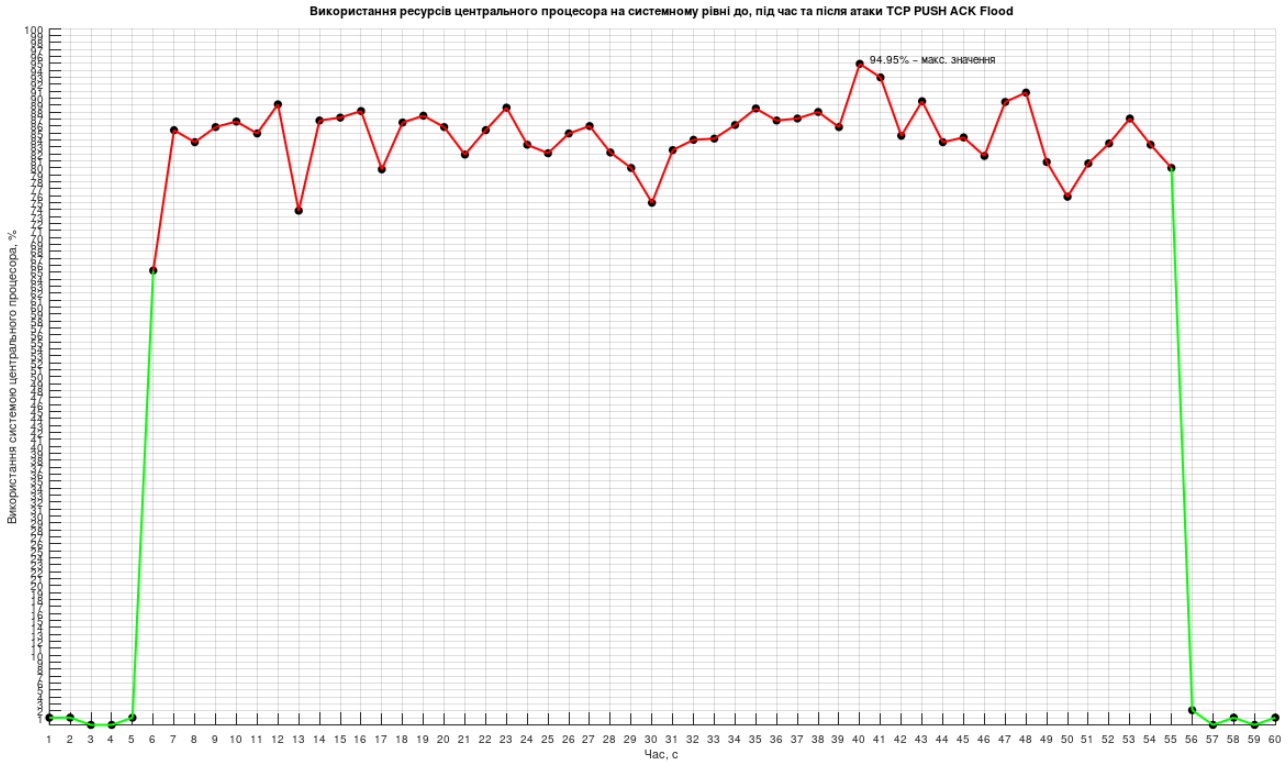

Рис. 4. Використання ресурсів процесора на системному рівні до, під час та після атаки TCP PUSH ACK Flood із впровадженим масштабуванням вікна та вільною зворотною фільтрацією адрес

Графік використання центрального процесора під час виконання команд на системному рівні при суворій зворотній фільтрації надано на рис. 5. Як показано на рис. 5, одразу після початку атаки відсоток використання ресурсів процесора становив 40%. Впродовж атаки відсоток навантаження коливався від 79% до 94,95%, у середньому становлячи 87,03%. Максимальне значення споживання ресурсів центрального процесора дорівнювало 91,92%, що свідчить про кращий результат у порівнянні з першим експериментом. Під час проведеної атаки виведена командою ping статистика вказує на те, що середній час відповіді сервера – 2,239 мс, мінімальний – 0,129 мс, максимальний – 13,217 мс, що є кращим результатом у порівнянні з першим експериментом. Під час атаки показник втрат пакетів становив 0%, а вебсторінка була доступною. Недоліком точності цього експерименту є те, що атака почалась через декілька секунд через розбіжність у часі між віртуальними машинами.

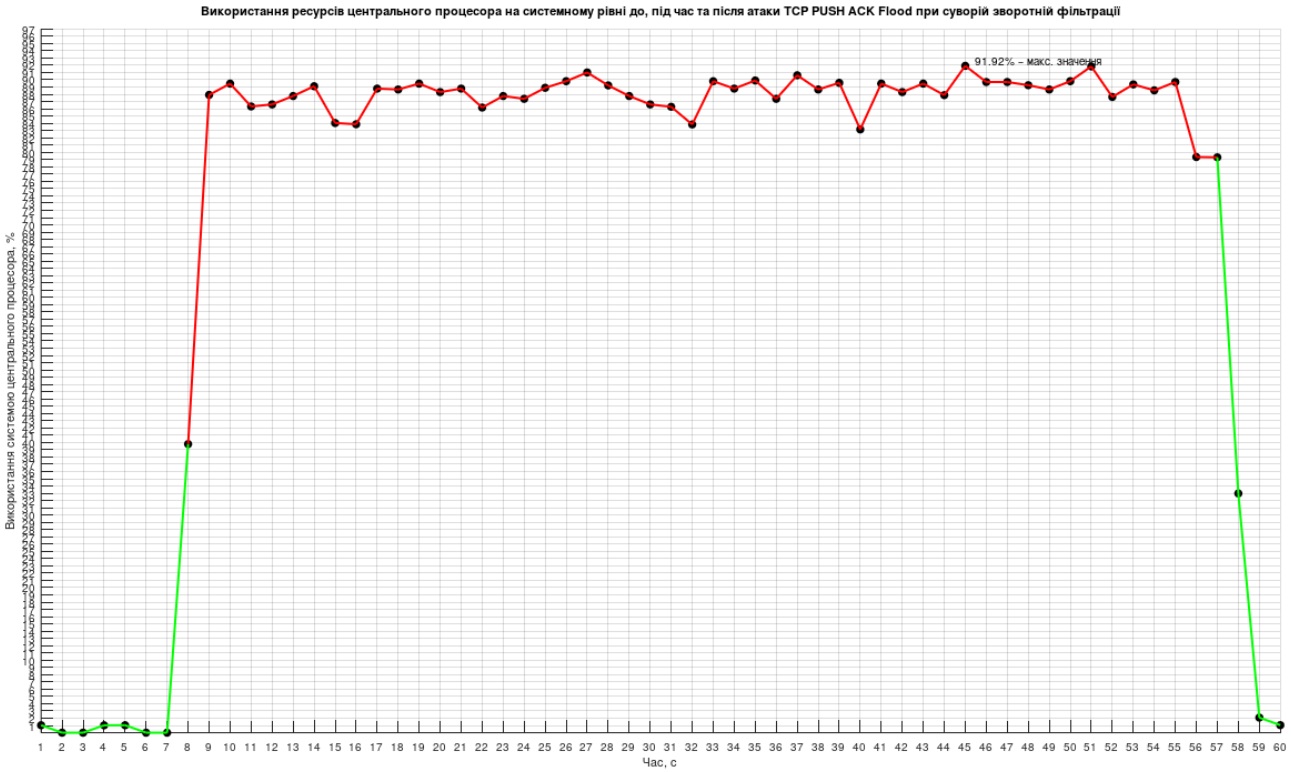

Рис. 5. Використання ресурсів процесора на системному рівні до, під час та після атаки TCP PUSH ACK Flood із впровадженим масштабуванням вікна та суворою зворотною фільтрацією адрес

Відсутність зворотної фільтрації налаштовується параметрами net.ipv4.conf.all.rp_filter=0 та net.ipv4.conf.default.rp_filter=0. Після конфігурації цих параметрів у файлі /etc/sysctl.conf IP-адреса джерела вхідних пакетів жодним чином не буде перевірятись.

Графік використання центрального процесора під час виконання команд на системному рівні при вимкненій зворотній фільтрації зображено на рис. 6. З рис. 6 робимо висновок, що впродовж атаки відсоток навантаження коливався у межах від 79% до 94,85%. Середній відсоток використання ресурсів процесора складав 88,59%, це значення є найбільшим у порівнянні з попередніми експериментами.

Середній час відповіді – 10,776 мс, мінімальний – 0,201 мс, максимальний – 61,783 мс, що є найбільшим результатом серед конфігурацій параметра зворотної фільтрації. З отриманих результатів можна зробити висновок, що відсутність зворотної фільтрації негативно впливає на час відповіді від сервера під час атаки. Водночас показник втрат пакетів склав 2% під час атаки , проте вебсторінка залишалась доступною.

Масштабування вікна використовується для збільшення розміру вікна при надходженні великої кількості запитів за короткий проміжок часу. Цей режим увімкнено за замовчуванням, проте дослідження показників навантаження процесора та часу відповіді за відсутності цієї функції корисні для всебічного дослідження ефективності

значень параметрів. Вимкнення масштабування розміру вікна проводиться за допомогою запису у файл /etc/sysctl.conf рядка net.ipv4.tcp_window_scaling=0.

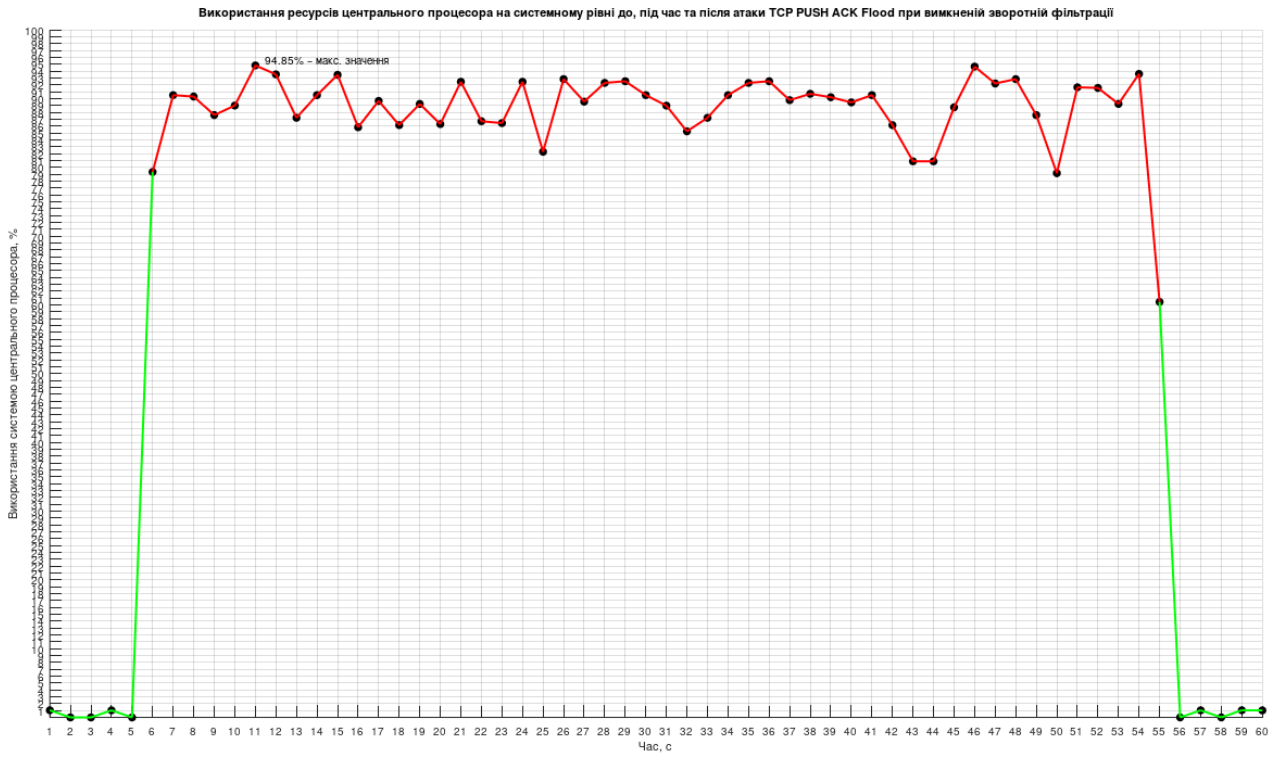

Рис. 6. Використання ресурсів процесора на системному рівні до, під час та після атаки TCP PUSH ACK Flood із впровадженим масштабуванням вікна та відсутньою зворотною фільтрацією адрес

Графік використання центрального процесора під час виконання команд на системному рівні (ядра) при вимкненому масштабуванні вікна представлено на рис. 7. З графіку (рис. 7) можна зробити висновок, що впродовж атаки відсоток навантаження коливався від 72% до 93,94% (за виключенням першої секунди атаки, коли використання ресурсів процесора складало приблизно 39%). Середній відсоток навантаження становив 85,85%. У порівнянні з графіком, зображеним на рис. 5, у цьому експерименті середнє значення навантаження центрального процесора менше, хоча максимальне значення більше на 1,01%. Недоліком точності цього експерименту є те, що атака почалась через декілька секунд через розбіжність у часі між віртуальними машинами.

Після проведеної атаки виведена командою ping статистика повідомляє про те, що середній час відповіді сервера – 7,100 мс, мінімальний – 0,158 мс, максимальний – 203,33 мс. Під час атаки вебсторінка була доступною, а пакети не були втраченими. Показники часу відповіді показали, що після вимкнення масштабування розміру вікна середній час відповіді збільшився з 2,110 мс до 7,100 мс (приблизно у 3,36 рази).

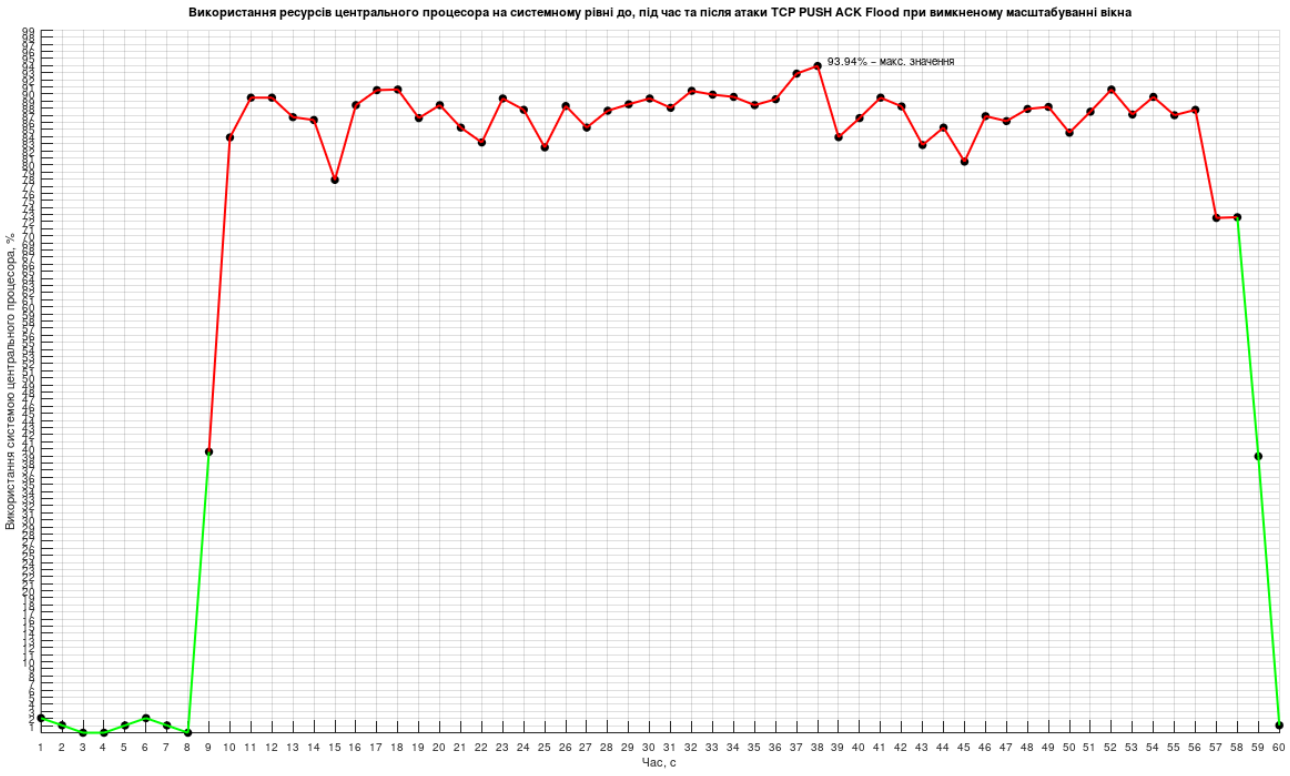

Рис. 7. Використання ресурсів процесора на системному рівні до, під час та після атаки TCP PUSH ACK Flood при вільній зворотній фільтрації адрес та вимкненому масштабуванні вікна

Наступні методи протидії атаці TCP PUSH ACK Flood – обмеження швидкості вхідних пакетів та відкидання пакетів з комбінацією прапорів – налаштовуються за допомогою утиліти iptables, що управляє мережним екраном netfilter.

Графік використання центрального процесора під час виконання команд на системному рівні (ядра) при обмеженні швидкості вхідних пакетів зображено на рис. 8.

З рис. 8 видно, що впродовж атаки відсоток навантаження процесора був високим та досяг свого максимуму (94,68%) на сьомій секунді після початку атаки. Середній відсоток використання ресурсів процесора на системному рівні склав 87,39%. На час проведення атаки середній час відповіді склав 8,652 мс, мінімальний – 0,112 мс, максимальний – 71,486 мс. Пакети під час перевірки не було втрачено, вебсторінка була доступною. Відкидання мережним екраном пакетів полягало у відкиданні пакетів на підставі наявності у сегментах певних прапорів (PSH та ACK).

Графік використання центрального процесора під час виконання команд на системному рівні (ядра) при відкиданні вхідних пакетів задля протидії атаці TCP PUSH ACK Flood зображено на рис. 9. На рис. 9 видно, що впродовж атаки середній відсоток навантаження процесора був найнижчим серед усіх попередніх експериментів – 52,63%. Максимальне значення використання ресурсів центрального процесора становило 69,74%. Під час проведення атаки середній час відповіді склав 0,189 мс, мінімальний – 0,126 мс, максимальний – 0,415 мс. Пакети під час перевірки не було втрачено, вебсторінка також була доступною.

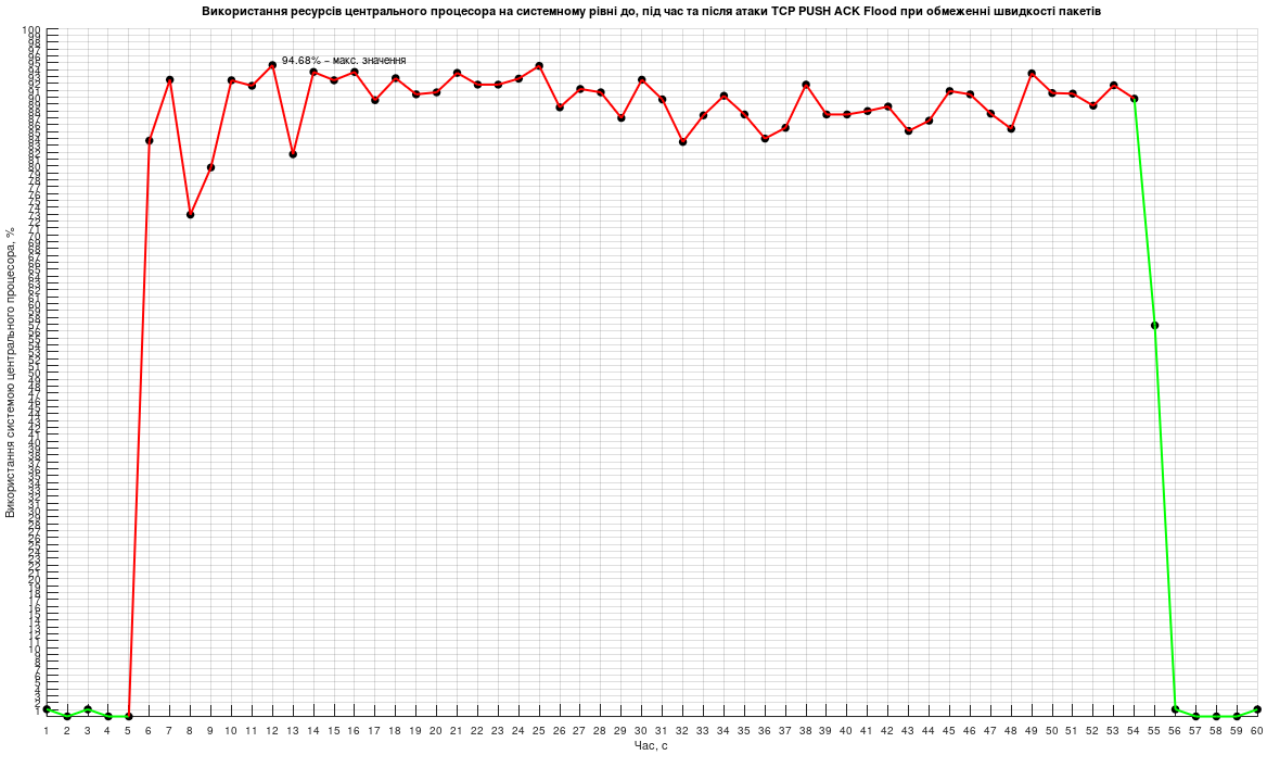

Рис. 8. Використання ресурсів процесора на системному рівні до, під час та після атаки TCP PUSH ACK Flood при обмеженні швидкості надходження вхідних пакетів

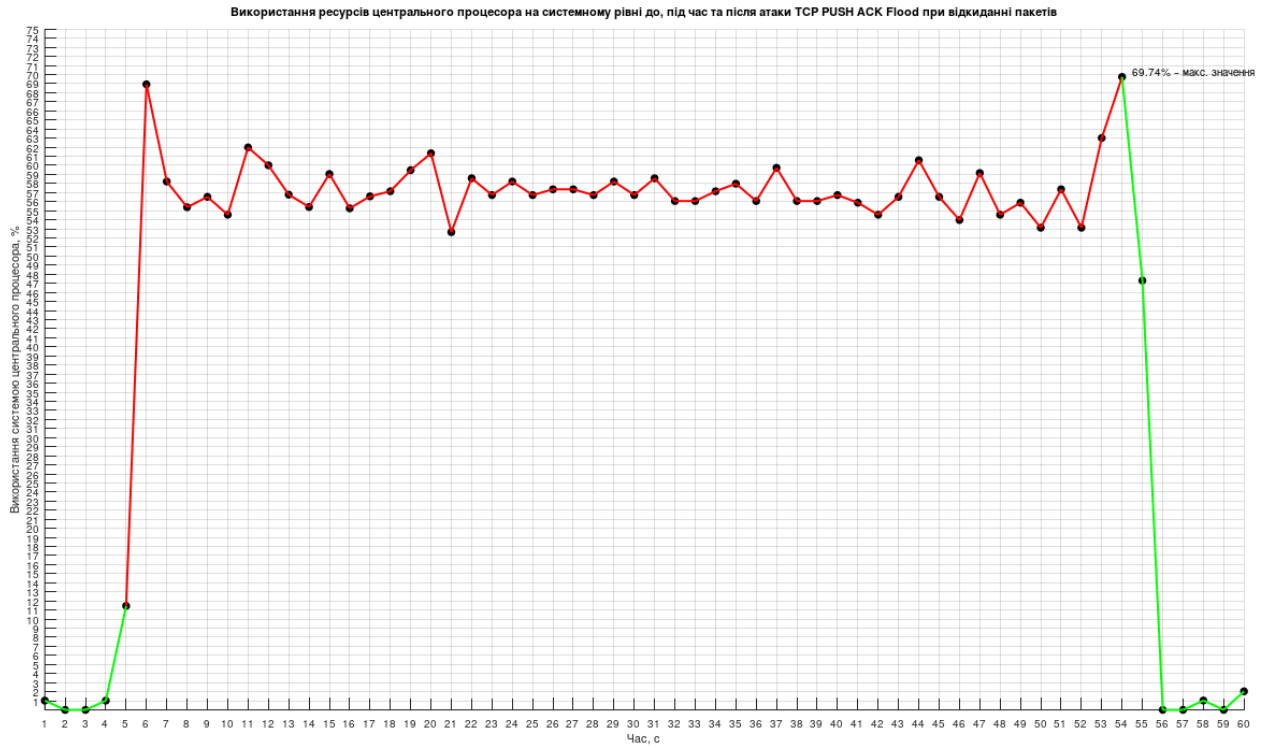

Рис. 9. Використання ресурсів процесора на системному рівні до, під час та після атаки TCP PUSH ACK Flood при впровадженому відкиданні вхідних пакетів

З отриманих кількісних показників можна зробити висновок, що цей метод був найбільш ефективним та економним стосовно значень використання ресурсів центрального процесора. Комбінований графік, що містить отримані графіки в результаті проведення усіх попередніх експериментів, представлено на рис. 10.

З рис. 10 можна зробити висновок, що хоча кількісні показники рівня використання ресурсів центрального процесора постійно змінюються, існує тенденція до того, що під час атаки значення цих показників знаходяться у межах від 73% до 95% для усіх методів захисту, окрім відкидання пакетів мережним екраном. Максимальний відсоток використання ресурсів для методу відкидання пакетів мережним екраном (графік чорного кольору) не перевищує 70%, водночас для інших методів протидії мінімальне значення впродовж основної частини атаки складало 73%.

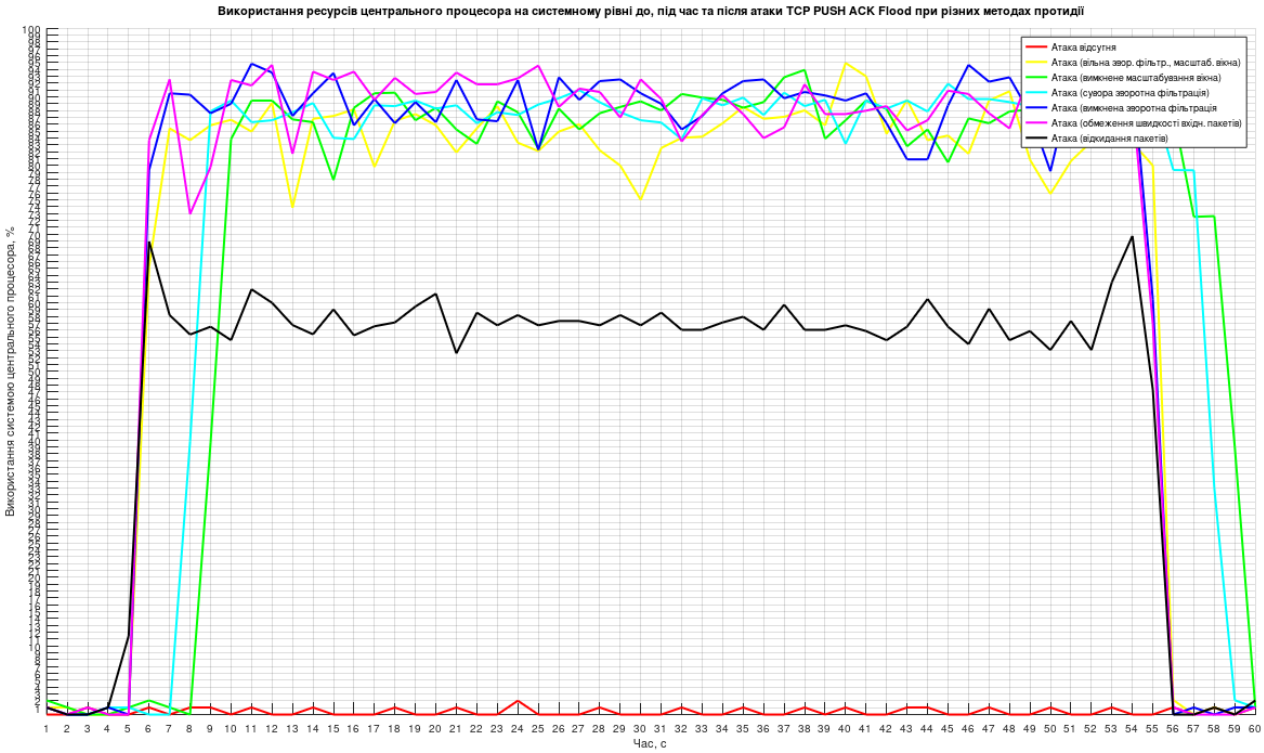

Рис. 10. Результати порівняльного аналізу отриманих результатів під час впровадження досліджених методів захисту

Результати порівняння ефективності впроваджених методів протидії атаці TCP PUSH ACK Flood за якісними та кількісними показниками представлено у табл. 3. У табл. 3 можна побачити, що найефективніше протидіяти загрозі вдалось за допомогою відкидання пакетів з комбінацією прапорів PUSH та ACK. Незважаючи на ефективність цього методу, слід зауважити, що у цьому випадку існує ймовірність блокування запитів не тільки від зловмисників, а і від легітимних клієнтів. Під час усіх експериментів вебсторінка була доступною. При перевірці з'єднання пакети було втрачено лише один раз – при вимкненні зворотної фільтрації адрес.

Таблиця 3. Порівняння ефективності впроваджених методів протидії атаці TCP PUSH ACK Flood

Експеримент	Середнє значення використання ресурсів процесором, %	Максимальне значення використання ресурсів процесором, %	Відсоток втрачених пакетів, %	Середній час відповіді ресурсу, мс	Максимальний час відповіді ресурсу, мс	Наявність доступу до вебсторінки
Нормальна робота	0,4	2,02	0	0,333	0,512	Так
Налаштування за замовчуванням	84,47	94,95	0	2,110	21,673	Так
Відсутнє масштабування розміру вікна	85,85	93,94	0	7,100	203,333	Так
Сувора зворотна фільтрація адрес	87,03	91,92	0	2,239	13,217	Так
Відсутня зворотна фільтрація адрес	88,59	94,85	2	10,776	61,783	Так
Обмеження швидкості вхідних пакетів	87,39	94,68	0	8,652	71,486	Так
Відкидання пакетів	56,64	69,74	0	0,189	0,415	Так

Як висновок, у даних експериментах було доведено, що атака TCP PUSH ACK Flood хоч і не була загрозою доступності вебсторінки, проте мала великий вплив на затримку при з'єднанні, через яку процесор на рівні системи витрачав до 94,95% ресурсів на обробку вхідних запитів.

Програмна утиліта hping3 не дає користувачу можливості проведення процедури тристороннього рукостискання та після цього почати надсилання пакетів PUSH ACK. Після отримання пакету з сегментами SYN та ACK від сервера клієнт надсилає у відповідь пакет з прапором RST. Наявність можливості створювати підробні сесії була б більш руйнівною, адже без додаткових засобів захисту у випадку вже встановленого з'єднання сервер мусив би приймати та обробляти усі пакети з прапорами PUSH ACK.

IV. Розробка рекомендацій щодо вдосконалення програмного забезпечення серверів і протоколів транспортного рівня для підвищення рівня їхньої безпеки

Двома недоліками протоколу TCP, виявленими під час вивчення відомих рішень та проведення експериментів, є можливість створення пакетів з нетиповими комбінаціями прапорів та відсутність перевірки сегментів при їхньому надсиланні. Завдання перевірки вмісту сегментів виконується отримувачем, проте не відправником; сегменти з будь-якими прапорами без перешкод надсилаються відправником.

Рекомендацією є створення списку дозволених комбінацій прапорів, перевірка цього значення у сегменті та запис у новостворене поле CHK (Check) значення 0, якщо послідовність заборонена, та 1, якщо вона прийнятна. Отже, пакет буде дозволено до надсилання або обробки у випадку, якщо сегмент не містить заборонених комбінацій прапорів (наприклад, URG, FIN та PSH), включно з 111111 та 000000 (всі прапори водночас присутні або відсутні).

При наявності у полі CHK значення 0, сегмент одразу відкидається, якщо 1 – комбінація прапорів ще раз перевіряється на прийнятність для унеможливлення підміни значення у цьому полі. Дозволені комбінації прапорів: SYN, ACK, SYN та ACK, RST, RST та ACK, FIN, FIN та ACK, PUSH та ACK, URG, PUSH.

Приклад полів прапорів та поля CHK у заголовку представлено у табл. 4.

Таблиця 4. Поля прапорів та поле CHK

Прапор	URG	ACK	PSH	RST	SYN	FIN	CHK
Значення	1	0	1	0	0	1	0

З табл. 4 видно, що використання цієї комбінації прапорів недопустиме, тому сегмент буде відкинуто. Використання цього підходу на стороні відправника при перевірці сформованих сегментів дозволить зменшити навантаження на мережний екран отримувача, сконфігурований відкидати пакети з певними прапорами. Таким чином, стає можливим захист від атак з використанням нестандартних (заборонених) комбінацій прапорів і суттєве зниження кількості ймовірних методів атак. Недоліками цього підходу є використання додаткового біта у заголовку, що сигналізуватиме про допустимість або недопустимість прапорів у сегменті.

Атак типу Flood з використанням протоколів TCP та UDP існує велика кількість [1]. Зловмисники використовують для цих атак підміну адреси відправника з двох причин: для уникнення поширення своєї IP-адреси та для того, щоб обробка запитів з кожного сокета відправника створювала навантаження як на сам вебсервер, так і на мережний екран.

Як підмінені адреси можна використовувати IP-адреси для спеціального використання, що складають так звані «марсіянські пакети». Наприклад, до таких IP-адрес відносяться 10.0.0.0/8, 172.16.0.0/12 та 192.168.0.0/16, що призначені для приватного використання [23]. Наприклад, при отриманні пакету з прапором SYN та недоступною адресою джерела, вебсервер не відкидає його, а надсилає у відповідь пакет з прапорами SYN та ACK декілька разів протягом деякого часу, так і не отримуючи відповіді. Використання зворотної фільтрації адрес (параметр net.ipv4.conf.all.rp_filter) не завершує з'єднання з такими адресами, а параметр net.ipv4.conf.all.log_martians [21] дозволяє лише записувати пакети до файлу журналу. Таким чином, методи захисту від «марсіянських пакетів» не є впровадженими. Рекомендацією є визначення за замовчуванням адрес, наявність яких у сокетах, що знаходяться у черзі з'єднань, буде забороненою.

Висновки

Під час атаки параметри зі значеннями net.ipv4.conf.default.rp_filter=1, net.ipv4.conf.all.rp_filter=1 та net.ipv4.tcp_window_scaling=1 показали кращий результат у порівнянні з іншими значеннями для цих параметрів. Відповідно, найбільш ефективним методом протидії атаці TCP PUSH ACK Flood виявилось блокування пакетів мережним екраном. Під час атаки при використанні цього методу захисту використання процесора на рівні системи не перевищувало 70 %.

З кожним рівнем моделі OSI зростає площа атаки та спостерігається тенденція до використання програмного забезпечення та експлуатації вразливостей у механізмах роботи протоколів. І хоча атаки на прикладному рівні є найбільш небезпечними, адже зловмисник має можливість вивести з ладу не тільки мережний пристрій, а скомпрометувати безліч прикладних програм і вебсервісів, якими користуються десятки мільйонів людей кожного дня, саме атаки на транспортному рівні є підготовчим етапом до атак на протоколи верхніх рівнів. На додачу до атак, спрямованих на сканування портів та перехоплення повідомлень, найпоширенішими атаками на цьому рівні моделі OSI є саме розподілені атаки на відмову в обслуговуванні.

Атаки на транспортному рівні пов'язані з особливостями функціонування прикладного та мережного рівнів. Цей зв'язок виражений у використанні портів прикладними програмами і вебсерверами та у використанні механізму підміни IP-адрес.

Вибір методів протидії атакам повинен бути економічно адекватним можливим загрозам безпеці інфокомунікаційних мереж і базуватись насамперед на атаці, захист від якої повинен бути впроваджений. На прикладі описаних методів протидії атакам транспортного рівня було доведено, що найбільша кількість методів можуть бути застосованими до атаки TCP SYN Flood. Кількість цих методів пояснюється поширеністю самої атаки, серйозністю шкоди системі та вразливостями процесу тристороннього рукостискання. Внаслідок проведених експериментів було встановлено, що за замовчуванням в операційній системі Xubuntu на рівні ядра встановлено параметри, які впливають на продуктивність системи та надають захист від атак, проте його рівень не є достатнім.

Список літератури

1. *Бондарчук А.П., Срочинська Г.С., Твердохліб М.Г.* (2015), Основи інфокомунікаційних технологій. Навчальний посібник: ДУТ, 76 с.

2. *Yoachimik O., Pacheco J.* (2024), "DDoS threat report for 2024 Q1", The Cloudflare Blog. **URL**: https://blog.cloudflare.com/ddos-threat-report-for-2024-q1.

3. *Yoachimik O.* (2022), "DDoS attack trends for 2022 Q2", The Cloudflare Blog. **URL**: https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2.

4. Державна служба спеціального зв'язку та захисту інформації України (2024), "Російські кібероперації. Аналітика за II півріччя 2023 року". С. 1–33. **URL**: https://cip.gov.ua/services/cm/api/attachment/download?id=64621.

5. *Васильєв Ю.* (2015), "Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури", Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, No. 29, С. 56 – 61.

6. ENISA Threat Landscape 2023 (2023). **URL**: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

7. *Barabanov R., Kowalski S., Yngström L.* (2011), Information Security Metrics, State of the Art, 62 p.

8. *Axelrod W.* (2008), "Accounting for Value and Uncertainty in Security Metrics", Information Systems Control Journal, No. 6, P. 1–6.

9. *Obaid H., Abeed E.* (2020), "DoS and DDoS Attacks at OSI Layers", International Journal of Multidisciplinary Research and publications, Vol. 2, P. 1–9. **DOI**: http://doi.org/10.5281/zenodo.3610833.

10. Layer 4. Knowledge Base. MazeBolt. **URL**: https://kb.mazebolt.com/kbe_taxonomy/layer-4/.

11. Attack Events – IBM Documentation. **URL**: https://www.ibm.com/docs/en/i/7.3?topic=types-attack-events/.

12. LAND Attacks. Imperva. **URL**: https://www.imperva.com/learn/ddos/land-attacks/.

13. Types of DDoS Attacks. Knowledge Base. **URL**: https://ddos-guard.net/en/terms/ddos-attack-types.

14. *Gont F., Bellovin S.* (2012), RFC 6528: Defending against Sequence. **URL**: https://datatracker.ietf.org/doc/html/rfc6528.

15. *Postel J.* (1981), RFC 793: Transmission Control Protocol. **URL**: https://datatracker.ietf.org/doc/html/rfc793.

16. Description of Windows TCP features. **URL**: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/description-tcp-features.

17. Nmap – Switches and Scan Types in Nmap. **URL**: https://www.digitalocean.com/community/tutorials/nmap-switches-scan-types.

18. *Villing J.* (2019), "Investigating TCP SYN Flood Mitigation Techniques in the Wild", Network Architectures and Services, Seminar IITM WS 18/19, May 2019, P. 67–70. **DOI**: https://www.doi.org/10.2313/NET-2019-06-1_14.

19. Security Configuration Guide: Denial of Service Attack Prevention, Cisco IOS Release 15M&T. **URL**: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_dos_atprvn/configuration/15-mt/sec-data-dos-atprvn-15-mt-book/sec-cfg-tcp-intercpt.html.

20. Spectrum. DDoS Protection for Apps. **URL**: https://www.cloudflare.com/application-services/products/cloudflare-spectrum.

21. IP Sysctl – The Linux Kernel documentation. **URL**: https://docs.kernel.org/networking/ip-sysctl.html.

22. Mitigate TCP SYN Flood Attacks with Red Hat Enterprise Linux 7 Beta. **URL**: https://www.redhat.com/en/blog/mitigate-tcp-syn-flood-attacks-red-hat-enterprise-linux-7-beta.

23. IANA IPv4 Special-Purpose Address Registry. **URL**: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml.