Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп’ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: " Розробка системи пом’якшення DDoS атак на базі Mikrotik"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Трофимчук Олег Миколайович
підпис (прізвище та ініціали)

Керівник Оробчук О.Р.
підпис (прізвище та ініціали)
Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Трофимчуку Олегу Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка системи помякшення DDoS атак на базі Mikrotik

Керівник роботи Оробчук Олександра Романівна, доктор філософії, старший викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «15» 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 12.06.2024

3. Вихідні дані до роботи Вимоги до системи пом'якшення DDoS атак. Маршрутизатор Mikrotik CHR. Операційні системи Ubuntu Linux, Windows, Kali Linux

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд DDoS атак на сервіси та їх наслідків
2. Тестове середовище для моделювання DDoS атак
3. Налаштування та тестування механізму пом'якшення DDoS атак
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета, задачі. Поняття DDoS атаки. Атаки на прикладному рівні. Атаки на транспортному рівні. Атаки на мережевому рівні. Методи захисту від DDoS атак. Схема середовища моделювання DDoS атаки. Налаштування компонентів лабораторного середовища. Маршрутизатор Mikrotik CHR. Сервер Ubuntu Linux. Операційна система Windows. Операційна система Parrot Security. Моделювання Ping Flood атаки. Моделювання SYN Flood атаки. Моделювання UDP flood атаки. Налаштування механізму пом'якшення DDoS атаки. Тестування захисного механізму. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2024	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд DDoS атак на сервіси та їх наслідків»	21.02 – 10.03	
4.	Оформлення розділу «Тестове середовище для моделювання DDoS атак»	11.03 – 25.03	
5.	Оформлення розділу «Налаштування та тестування механізму пом’якшення DDoS атак»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	26.06.2024	

Студент _____ Трофимчук О. М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Оробчук О.Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка системи пом’якшення DDoS атак на базі Mikrotik. // Кваліфікаційна робота ОР «Бакалавр» // Трофимчук Олег Миколайович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2024 // С. 63, рис. – 39, табл. – 0, кресл. – 15, додат. – 1.

Ключові слова: DDoS, Mikrotik, Linux, Ubuntu, Windows, Parrot Security, брандмауер.

У кваліфікаційній роботі бакалавра було розроблено та проведено тестування системи для зменшення впливу DDoS-атак. Основою даної системи є маршрутизатор Mikrotik CHR. В роботі було проведено аналіз різноманітних типів DDoS-атак, їхніх характеристик та впливу на мережеву інфраструктуру.

Було досліджено HTTP Flood, DNS Amplification, TCP SYN Flood, UDP Flood, Ping Flood та IP Fragmentation, розглянуті їхні особливості, впливу на окремі рівні моделі OSI. та методи протидії.

Розроблено та проведено налаштування тестового середовища для моделювання DDoS-атак, включаючи віртуальний маршрутизатор Mikrotik CHR, віртуальну машину Ubuntu Linux з вебсервером, а також віртуальні машини Windows 10, Windows 11 та Parrot Security для моделювання DDoS атак.

Було проведено моделювання DDoS-атак з використанням утиліти hping3 в операційній системі Parrot Security та налаштовано заходи захисту на маршрутизаторі Mikrotik. Результати досліджень підтвердили ефективність розроблених механізмів захисту для зменшення впливу DDoS-атак на мережеву інфраструктуру.

ANNOTATION

Development of a DDoS attack mitigation system based on Mikrotik. // Thesis of educational level "Bachelor"// Oleh Trofymchuk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-41 // Ternopil, 2024 // P. 63, fig. - 39, tab. - 0, chair. - 15, added. - 1.

Keywords: DDoS, Mikrotik, Linux, Ubuntu, Windows, Parrot Security, firewall.

In the bachelor's thesis, a system was developed and tested to reduce the impact of DDoS attacks. The basis of this system is the Mikrotik CHR router. The work analysed various types of DDoS attacks, their characteristics and impact on the network infrastructure.

HTTP Flood, DNS Amplification, TCP SYN Flood, UDP Flood, Ping Flood and IP Fragmentation were investigated, their features, impact on individual layers of the OSI model and methods of counteraction were considered.

A test environment for modelling DDoS attacks was developed and configured, including a Mikrotik CHR virtual router, an Ubuntu Linux virtual machine with a web server, as well as Windows 10, Windows 11 and Parrot Security virtual machines for modelling DDoS attacks.

The DDoS attacks were simulated using the hping3 utility in the Parrot Security operating system and security measures were configured on the Mikrotik router. The research results confirmed the effectiveness of the developed protection mechanisms to reduce the impact of DDoS attacks on the network infrastructure.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8
ВСТУП..... 9
РОЗДІЛ 1 ОГЛЯД DDOS АТАК НА СЕРВІСИ ТА ЇХ НАСЛІДКІВ 11
1.1 Поняття DDoS атаки 11
1.1.1 Атаки на прикладному рівні 11
1.1.2 Атаки на транспортному рівні. 14
1.1.3 Атаки на мережевому рівні 16
1.2 Методи захисту від DDoS атак 19
1.3 Наслідки DDoS атак 22
1.4 Висновки до розділу 24
РОЗДІЛ 2 ТЕСТОВЕ СЕРЕДОВИЩЕ ДЛЯ МОДЕЛЮВАННЯ DDOS АТАК.. 25
2.1 Схема середовища моделювання DDoS атаки 25
2.2 Налаштування компонентів лабораторного середовища..... 27
2.2.1 Маршрутизатор Mikrotik CHR..... 27
2.2.2 Сервер Ubuntu Linux 31
2.2.3 Операційна система Windows..... 34
2.2.4 Операційна система Parrot Security 37
2.4 Висновки до розділу 39
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕХАНІЗМУ ПОМ’ЯКШЕННЯ DDOS АТАК 41
3.1 Засіб здійснення DDoS атаки 41
3.1.1 Моделювання Ping Flood атаки 41
3.1.2 Моделювання SYN Flood атаки..... 43
3.1.3 Моделювання UDP flood атаки..... 46
3.2 Налаштування механізму пом’якшення DDoS атаки..... 48
3.3 Тестування захисного механізму..... 51
3.4 Висновки до розділу 54
РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ 55
4.1 Долікарська допомога при ураженні електричним струмом..... 55

4.2 Зниження стресу та покращення психологічного благополуччя працівників 57
ВИСНОВКИ 59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 60
ДОДАТКИ 62
Додаток А Параметри налаштування Mikrotik для пом’якшення DDoS атак 62

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DDoS	—	Distributed Denial of Service
OSI	—	Open Systems Interconnection
TCP	—	Transmission Control Protocol
UDP	—	User Datagram Protocol
ICMP	—	Internet Control Message Protocol
ISP	—	Internet Service Provider
WAF	—	Web Application Firewall
IDS	—	Intrusion Detection Systems
IPS	—	Intrusion Prevention Systems
SSH	—	Secure Shell
CHR	—	Cloud Hosted Router
DMZ	—	Demilitarized Zone
DHCP	—	Dynamic Host Configuration Protocol
LTS	—	Long-Term Support
TTL	—	Time to Live
ОС	—	Операційна система

ВСТУП

З кожним роком зростає загроза кібератак, серед яких особливе місце посідають DDoS-атаки. Ця проблема особливо загострилась після нападу росії на Україну. Ці атаки стають все більш складними та руйнівними для мережевої інфраструктури і серверів, що призводить до великих фінансових втрат та порушення діяльності підприємств. В цьому контексті розробка та вдосконалення систем пом’якшення DDoS-атак набуває надзвичайної важливості.

Метою цього дослідження є розробка та апробація системи пом'якшення DDoS-атак на базі маршрутизатора Mikrotik CHR у комплексі зі створенням DMZ-сегменту з вебсервером на основі Ubuntu Linux та LAN-сегменту операційними систем Windows 11 та Windows 10.

Задачі дослідження включають:

- аналіз атак та їхнього впливу на мережеву інфраструктуру;
- огляд існуючих методів захисту від DDoS-атак;
- розробка та налаштування системи захисту на базі Mikrotik CHR для виявлення та фільтрації DDoS-трафіку;
- проведення практичних експериментів для тестування ефективності заходів захисту за допомогою інструментів, таких як Parrot Security.

Об'єктом дослідження є мережева інфраструктура з основним елементом маршрутизатором Mikrotik CHR, вебсервером на базі Ubuntu Linux та робочими станціями під управлінням Windows 10 та Windows 11.

Предметом дослідження є розробка та апробація системи захисту від DDoS-атак на базі Mikrotik CHR, а також аналіз її ефективності в умовах моделювання DDoS-атак.

Результати дослідження матимуть практичне значення для організацій. Розроблена система захисту може бути використана для забезпечення безпеки мережевих інфраструктур, підвищення доступності сервісів та мінімізації наслідків атак для бізнесу. Також, отримані під час дослідження результати

можуть послужити основою для проведення подальших досліджень у галузі кібербезпеки.

РОЗДІЛ 1 ОГЛЯД DDOS АТАК НА СЕРВІСИ ТА ЇХ НАСЛІДКІВ

1.1 Поняття DDoS атаки

DDoS атака, або атака на відмову в обслуговуванні - це вид кібератаки, який полягає в спробі зробити недоступними онлайн-сервіси, комп'ютери або мережі, переповнюючи їхні ресурси запитами з багатьох джерел одночасно [1]. У DDoS атаках зазвичай використовуються ботнети - мережі комп'ютерів, що контролюються зловмисниками без відома їхніх власників, для створення великого обсягу трафіку, який перевантажує цільовий сервер або мережу, призводячи до припинення або обмеження доступу для законних користувачів.

1.1.1 Атаки на прикладному рівні

DDoS атаки на прикладному рівні (application layer), також відомі як Layer 7 атаки, спрямовані на перенавантаження або використання ресурсів на рівні застосунків, наприклад, вебсерверів, електронної пошти або баз даних [2]. Основною метою таких атак є вичерпання доступних обчислювальних ресурсів на рівні застосунків, що призводить до недоступності сервісу для легітимних користувачів.

HTTP Flood - це одна з найпоширеніших та ефективних форм DDoS атак на прикладному рівні. Вона полягає у масовому відправленні вебзапитів на цільовий вебсервер з метою перевантаження його ресурсів та відмови в обслуговуванні легітимних користувачів [3]. Зловмисники використовують ботнети або спеціально налаштовані комп'ютери для масового відправлення HTTP запитів на цільовий вебсервер (див.рисунок 1.1).

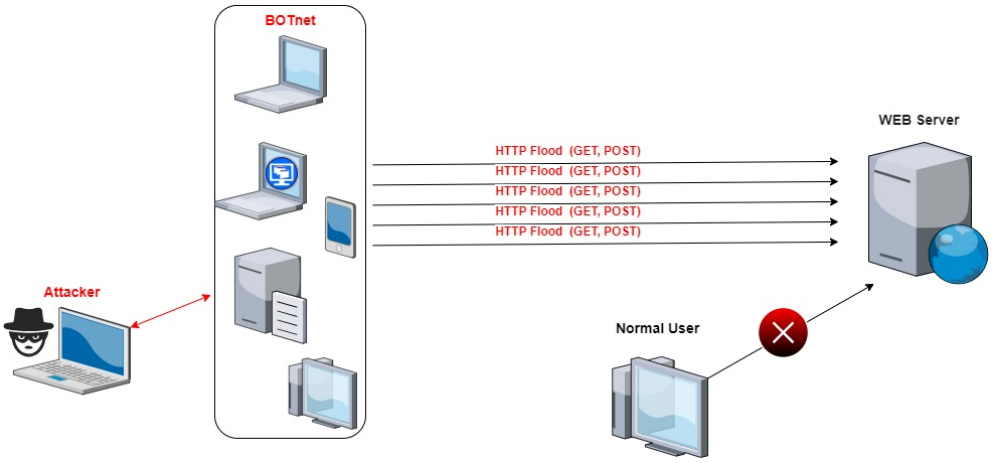

Рисунок 1.1 – Схема HTTP Flood атаки

HTTP Flood атаки можуть бути направлені на будь-яку частину вебсайту. Зловмисники можуть підробляти агентів користувачів у своїх HTTP запитах, щоб сховати свою ідентичність або створити враження, що запити надходять від реальних користувачів. Нападники можуть вносити зміни в HTTP запити, такі як зміна методу запиту, додавання додаткових заголовків або параметрів, щоб ускладнити виявлення та блокування атаки. Для проведення HTTP Flood атак можуть використовуватися різноманітні інструменти та скрипти, які дозволяють зловмисникам автоматизувати процес генерації та надсилання великого обсягу HTTP запитів.

Атака HTTP GET - це форма атаки, при якій кілька комп'ютерів або інших пристроїв спільно надсилають багато запитів на ресурси, такі як зображення чи файли, з цільового сервера. Це призводить до перевантаження сервера вхідними запитами та відповідями, що може спричинити відмову в обслуговуванні для легітимного трафіку.

Атака HTTP POST - це форма атаки, яка полягає в надсиланні багатьох запитів POST на вебсайт, який обробляє дані форми та передає їх як правило до бази даних. Обробка даних форми та виконання необхідних команд бази даних є процесом, який вимагає значних обчислювальних ресурсів порівняно з потужністю обробки та пропускною здатністю, необхідною для надсилання запитів POST. Ця атака використовує різницю у споживанні ресурсів, відправляючи багато запитів POST, щоб перевантажити сервер та спричинити відмову в обслуговуванні.

Наслідки HTTP Flood атак можуть бути серйозними для цільового вебсервера, такі як перевантаження обчислювальних ресурсів, відмова у обслуговуванні а також репутаційна шкода.

Після виявлення ці атаки можна зупинити та відстежити до певного джерела легше, ніж інші типи DDoS-атак.

DNS Amplification (DNS підсилення) - це форма DDoS атаки, яка використовує вразливості протоколу DNS для перенаправлення великої кількості трафіку на цільовий сервер. Основним принципом цієї атаки є підміна IP-адреси відправника запитів до DNS сервера, щоб відповіді надсилались на адресу цільового сервера замість адреси, з якої був зроблений запит (див.рисунок 1.2).

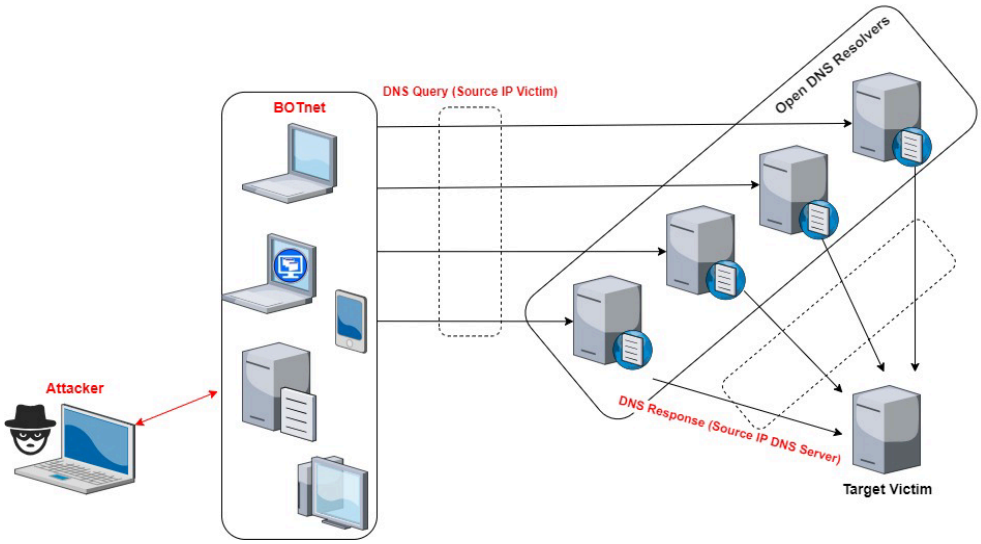

Рисунок 1.2 – Схема DNS Amplification атаки

Зловмисники використовують відкриті DNS сервери для надсилання трафіку на цільовий сервер. Відкриті DNS сервери можуть відправляти відповіді на запити із збільшеним розміром, порівняно з розміром запиту. Це забезпечує високий ступінь посилення (amplification factor), оскільки велика кількість вихідного трафіку здійснюється на адресу цільового сервера. Велика кількість відповідей DNS, спрямованих на цільовий сервер, перевантажує його мережеві ресурси та призводить до відмови в обслуговуванні для легітимного трафіку.

Ця атака є ефективним методом перенаправлення великого обсягу трафіку на цільовий сервер, що дозволяє зловмисникам спричиняти значні завади в роботі мережі та сервісів.

1.1.2 Атаки на транспортному рівні

Атаки DDoS на транспортному рівні (transport layer) відносяться до категорії кібератак, які спрямовані на зрив надання послуг шляхом перевантаження мережевої інфраструктури цілі. Транспортний рівень, згідно з моделлю OSI, включає протоколи, такі як TCP та UDP, які забезпечують передачу даних між вузлами в мережі. Основною метою атак на транспортному рівні є перешкоджання або повне блокування доступу до сервісів.

TCP SYN Flood - це одна з найпоширеніших і ефективних форм DDoS атак, яка використовується для перевантаження цільового сервера та призводить до відмови в обслуговуванні легітимного трафіку. Вона використовує уразливість протоколу TCP, пов'язану з процесом встановлення з'єднання [4].

SYN-флуд використовує потоки SYN-пакетів для атаки на систему. Пакет SYN є першим кроком у встановленні TCP-з'єднання. Коли клієнт надсилає SYN-пакет на сервер, він очікує підтвердження (SYN-ACK). Після отримання SYN-ACK від сервера, клієнт надсилає пакет ACK, і тим самим встановлюється TCP-з'єднання. Однак, в SYN-флуді клієнти намагаються не завершити процес рукостискання, переповнюючи черги сервера. Якщо кількість підключень вичерпано, сервер стає недоступним для нормальних запитів. Таким чином, зловмисники використовують цей механізм для виконання SYN-флуду.

Зловмисники зазвичай відправляють на сервер велику кількість SYN-пакетів із підробленими вихідними IP-адресами та портами для ініціації TCP-з'єднань [5]. Це призводить до створення великої кількості напіввідкритих з'єднань на сервері, оскільки реальні клієнти ніколи не отримають SYN-ACK відповідь від сервера (див.рисунок 1.3).

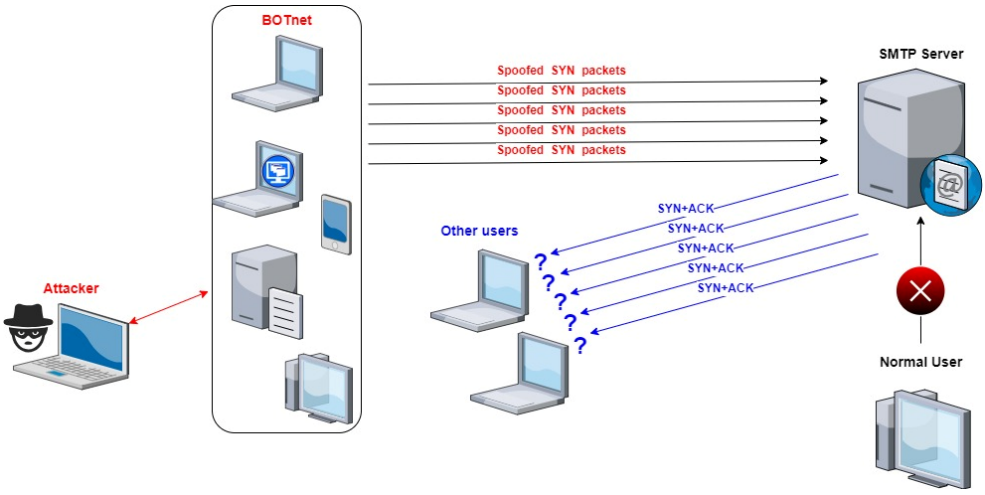

Рисунок 1.3 – Схема TCP SYN Flood атаки

В таких випадках сервер повинен підтримувати великий список очікування та намагатися повторно надіслати SYN-ACK пакети, що споживає велику кількість ресурсів. В результаті, звичайні користувачі можуть мати проблеми із встановленням TCP-з'єднань через те, що сервер зайнятий обробкою шкідливих напіввідкритих з'єднань.

UDP Flood - це ще одна з поширених форм DDoS атак, що полягає у надсиланні великого обсягу UDP пакетів на цільовий сервер з метою перевантаження його мережевих ресурсів [6].

У порівнянні з TCP, UDP є протоколом без з’єднання, що означає, що він не вимагає встановлення з'єднання перед передачею даних. У порівнянні з TCP, UDP не має механізму виявлення втрати пакетів і не передає повідомлення про втрату пакетів під час комунікації між клієнтом та сервером. Це робить UDP менш вимогливим до ресурсів і забезпечує високу швидкість обробки. Ці переваги роблять UDP привабливим для використання, але також надають можливість зловмисникам ініціювати атаки UDP flood.

Атака UDP Flood також може призвести до перевантаження брандмауера, який захищає цільовий сервер, і це може призвести до відмови в обслуговуванні легітимного трафіку [7].

UDP-флуд працює завдяки процесам, які виконує сервер при отриманні UDP-пакетів, що надсилаються на один з його портів. Коли сервер отримує UDP-пакет на певному порту, він пройде через два кроки відповіді. Спочатку сервер

перевіряє, чи існують активні програми, які слухають запити на цьому порті. Якщо жодна програма не очікує пакети на цьому порті, сервер може відповісти пакетом ICMP, щоб повідомити відправника, що отримувач недоступний.

Під час атаки DDoS типу UDP Flood кожен новий UDP-пакет, що надсилається на сервер, вимагає обробки, що використовує ресурси сервера. Зловмисники зазвичай підробляють IP-адресу джерела пакетів, ускладнюючи виявлення їхнього справжнього місцезнаходження (див.рисунок 1.4).

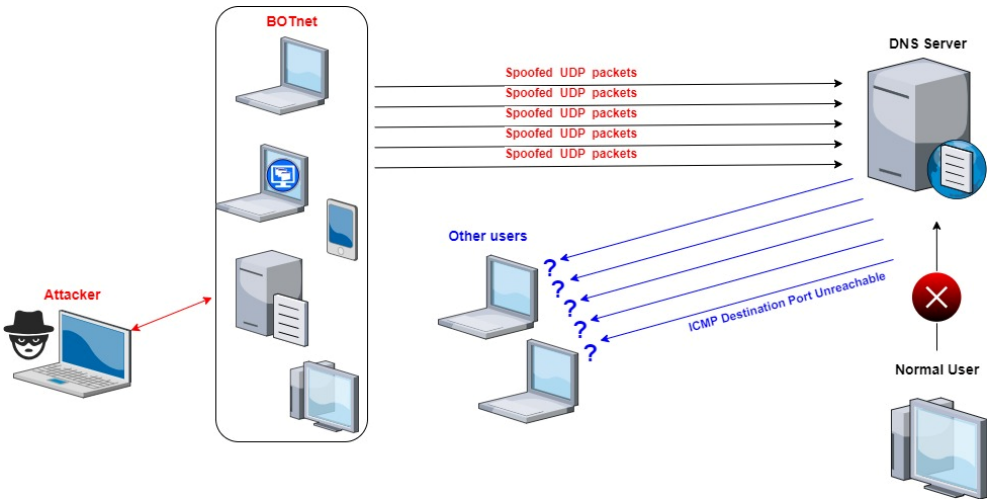

Рисунок 1.4 – Схема UDP Flood атаки

Оскільки цільовий сервер витрачає ресурси на обробку кожного UDP-пакета, при масштабних атаках ресурси сервера можуть швидко вичерпатися, що може призвести до відмови в обслуговуванні для легітимного трафіку.

1.1.3 Атаки на мережевому рівні

Атаки DDoS на мережевому рівні (network layer), також відомі як L3 атаки, це форма кібератак, спрямованих на перевантаження мережевого рівня інфраструктури цільового об'єкта [8]. Ці атаки зазвичай використовуються для перевантаження пропускної здатності мережі та вичерпують великі обсяги ресурсів на маршрутизаторах.

Ping Flood - це атака на відмову в обслуговуванні, при якій зловмисник намагається перевантажити цільовий пристрій пакетами ICMP echo-request. Це

призводить до того, що сервер стає недоступним для звичайного трафіку. Якщо трафік атаки надходить з кількох пристроїв, ця атака стає DDoS або розподіленою атакою на відмову в обслуговуванні. Хоча цей вид атаки втратив популярність як основний метод нападу, його часто використовують поряд з іншими методами для створення дуже складних атак, які важче подолати, відомих як багатовекторні атаки. Протокол ICMP, який використовується під час атаки Ping Flood, є протоколом на мережевому рівні, що використовується мережевими пристроями для комунікації. Інструменти мережевої діагностики, такі як traceroute і ping, використовують ICMP. Зазвичай повідомлення ICMP echo-request та echo-reply використовуються для перевірки зв'язку між відправником і отримувачем пакетів.

Запит ICMP потребує від сервера певних ресурсів для обробки кожного запиту та відправлення відповіді. Цей запит також вимагає пропускної здатності як для вхідного повідомлення (echo-request), так і для відповіді (echo-reply). Атака Ping Flood націлено на те, щоб заставити ціль відповідати на велику кількість запитів та перевантажувати мережеве з'єднання фальшивим трафіком. З огляду на те, що багато пристроїв у ботнеті можуть атакувати одну й ту саму ціль, обсяг трафіку атаки значно зростає, що може призвести до порушення нормальної активності мережі. Історично зловмисники часто використовували фіктивні IP-адреси для маскування пристрою-відправника. Однак сучасні атаки ботнетів рідко потребують маскування IP-адреси, а замість цього використовують велику мережу непідроблених ботів, щоб наситити пропускну здатність цільового пристрою.

Ping Flood атаку можна розглядати як процес, який складається з двох основних кроків, що повторюються. У першому кроці зловмисник використовує багато пакетів ICMP echo-request для надсилання на цільовий сервер за допомогою ботнету. У другому кроці цільовий сервер відправляє пакети ICMP echo-reply на IP-адреси кожного запитуючого пристрою як відповідь (див.рисунок 1.5).

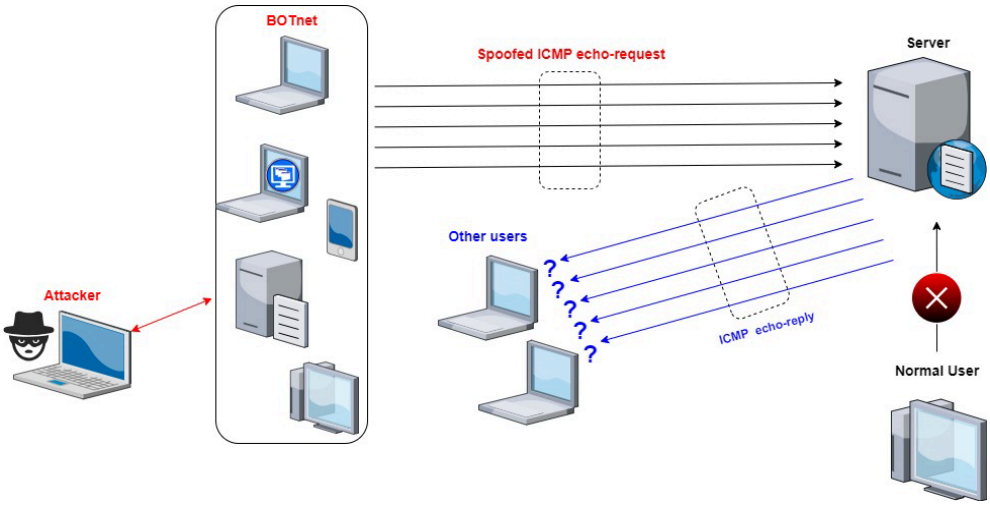

Рисунок 1.5 – Схема ICMP Flood атаки

Шкідливий ефект Ping Flood безпосередньо залежить від кількості запитів, що надсилаються до цільового сервера. На відміну від DDoS-атак на основі відображення, наприклад DNS Amplification, трафік Ping Flood атаки є симетричним. Пропускна здатність, яку отримує цільовий пристрій, є просто сумою загального трафіку, надісланого від кожного бота.

Атака з фрагментацією IP (IP Fragmentation) - це метод DDoS атаки, в якій зловмисник намагається перевантажити цільовий пристрій шляхом надсилання великої кількості фрагментованих IP-пакетів [9]. Фрагментація IP дозволяє розділити великий IP-пакет на менші частини для передачі по мережі, а отримувач відновлює оригінальний пакет із фрагментів. Зловмисники використовують цю функцію для створення навантаження, яке може перешкоджати нормальному функціонуванню цільового пристрою.

Атаки фрагментації часто використовують підроблені фрагменти, які неможливо зібрати в оригінальний пакет. Це можна досягти шляхом надсилання фрагментів, які є або занадто малими, або занадто великими для обробки, або які зосереджені на накладенні на вже існуючі фрагменти, щоб перевантажити сервер. В результаті фрагменти можуть застрягати в тимчасовому сховищі, витрачаючи пам'ять та вичерпуючи доступні ресурси пам'яті. Це може призвести до перевантаження сервера і, в кінцевому підсумку, до відмови в обслуговуванні. Такі атаки можуть бути особливо ефективними, оскільки вони використовують вразливість у способі обробки фрагментованих пакетів сервером.

1.2 Методи захисту від DDoS атак

Одним з основних симптомів DDoS-атаки є раптове збільшення навантаження на сайт або сервіс, що призводить до повільної роботи або недоступності [10]. Проте важливо відрізняти це від нормального підвищення трафіку. Для виявлення можливої DDoS-атаки можуть бути використані наступні показники:

- надмірний обсяг трафіку з однієї IP-адреси або діапазону IP-адрес;
- трафік від користувачів з подібними характеристиками, такими як тип пристрою, геолокація або версія браузера;
- неочікуваний ріст запитів до конкретної сторінки або ресурсу;
- незвичайні моделі трафіку, такі як стрибки в активності у непарні години або неприродні патерни (наприклад, стрибки кожні 20 хвилин).

Використання інструментів аналізу трафіку може допомогти вчасно виявити ці показники і вжити відповідних заходів для захисту від атаки [11].

Однією з ключових задач у протидії DDoS-атакам є розрізнення легітимного трафіку і зловмисного. Проблема полягає в тому, що існує велика різноманітність типів DDoS-атак, від атак з одного джерела до складних атак, які використовують кілька джерел одночасно.

Складні DDoS-атаки можуть використовувати різні методи, щоб завдати шкоди цілі, використовуючи різні шляхи для нападу на різні частини мережі. Наприклад може бути використане комбінування атак DNS Amplification і HTTP Flood. Загалом, чим складніше атака, тим важче виявити та відрізнити трафік атаки від легітимного.

Злочинці прагнуть залишатися непоміченими, щоб ускладнити заходи протидії. Для ефективного протистояння цим складним DDoS-атакам необхідно впровадити багаторівневі заходи захисту, які враховують різноманітність шляхів нападу. Ці заходи повинні бути масштабовані, з резервуванням та можливістю моніторингу трафіку та ефективного управління вразливими точками.

Однією з ключових складових загальної стратегії кібербезпеки є навчання персоналу. DDoS-ботнет - це мережа комп'ютерів або інших пристроїв, які були скомпрометовані зловмисниками і використовуються для здійснення DDoS атаки [12]. Зловмисники отримують доступ до цих пристроїв, зазвичай за допомогою шкідливого програмного забезпечення або вразливостей безпеки, і об'єднують їх в ботнет, щоб вони могли виконувати команди з централізованого керівництва. Після цього зловмисники можуть використовувати цей ботнет для виконання DDoS-атак, спрямованих на цільові ресурси, переповнюючи їх трафіком і призводячи до відмови в обслуговуванні. Співробітники можуть ненавмисно стати часткою таких ботнетів, якщо їх пристрої скомпрометовані. Проте співробітники можуть значно знизити цей ризик, регулярно оновлюючи програмне забезпечення на своїх пристроях, використовуючи багатофакторну аутентифікацію для захисту облікових записів, встановлюючи надійне антивірусне програмне забезпечення та уважно поводячись з електронними листами та вкладеннями, особливо якщо вони виглядають підозріло.

Один з варіантів, доступних практично для всіх ISP, полягає у створенні маршруту blackhole (чорна діра) та перенаправленні трафіку на цей маршрут. У своїй найпростішій формі, коли використовується фільтрація blackhole без конкретних обмежень, як легітимний, так і зловмисний мережевий трафік направляється на нульовий маршрут (null route), або blackhole, і видаляється з мережі.

У випадку DDoS-атаки на інтернет-ресурс, постачальник послуг Інтернету (ISP) може спрямовувати весь трафік сайту в blackhole як захисний захід. Проте це рішення не є ідеальним, оскільки фактично воно відповідає бажанню зловмисника зробити сервіс недоступним.

Хоча DDoS blackhole може бути корисним інструментом для захисту мережі від неприємностей, пов'язаних зі спробами атак, варто розглядати його як крайній захід у боротьбі з такими загрозами. Використання цієї стратегії може досягти основної мети атаки, якою є зробити мережу недоступною, що потенційно може завдати шкоди бізнесу. Проте, необхідно розуміти, що атаки DDoS часто спрямовані не лише на окремий вебсайт, а й на всю мережу в цілому.

У таких ситуаціях направлення трафіку в blackhole може виявитися ефективним заходом для захисту мережі від негативних наслідків атаки.

Ще одним методом боротьби з DDoS-атаками є обмеження швидкості або тимчасове блокування трафіку з конкретної IP-адреси протягом певного періоду. Це буде сприяти зменшенню кількості запитів, які сервер мусить обробляти, та буде запобігати перевантаженню системних ресурсів під час атаки. Такий підхід дозволяє забезпечити доступ до системних ресурсів для законних користувачів, але не є гарантією повного захисту від складних DDoS-атак. Втім, це може бути корисним елементом у загальній стратегії боротьби з такими атаками, особливо для малих бізнесів, оскільки він не вимагає значних фінансових витрат.

Брандмауер вебпрограм (WAF) - це захисний інструмент, який використовується для пом'якшення DDoS-атак на рівні додатків. Він функціонує як зворотній проксі-сервер, розміщений між Інтернетом та програмами, і створює бар'єр для захисту вебсервісів. WAF допомагає виявляти зловмисний трафік, спрямований на порушення нормальної роботи служб. Цей інструмент дозволяє контролювати вхідний трафік, використовуючи заздалегідь встановлені правила безпеки для дозволу або блокування доступу.

Постійний моніторинг і аналіз мережевого трафіку в реальному часі мають кілька переваг у виявленні та пом'якшенні потенційних DDoS-атак. Запровадження IDS і IPS для неперервного моніторингу мережевого трафіку є ефективними для розпізнавання та блокування підозрілих моделей трафіку, пов'язаних з DDoS. Використання таких інструментів аналізу дозволяє вчасно виявляти DDoS-атаки, що дозволяє швидко реагувати перед ескалацією атак. Моніторинг допомагає створити базову лінію нормальної активності в мережі або комп'ютерних системах, охоплюючи як періоди середнього, так і періоди пікового трафіку. Це також сприяє розумінню типової мережевої активності і моделей трафіку, допомагаючи відрізняти законний від зловмисного трафіку та ідентифікувати незвичні або підозрілі дії.

Маршрутизація unicast є широко використовуваною у мережевих комунікаціях через свою простоту та універсальність. У моделі unicast кожному вузлу мережі або пристрою призначається унікальна IP-адреса, що сприяє

прямому та ефективному зв'язку в мережі. Проте, не зважаючи на свою простоту, unicast передача може бути уразливою до DDoS-атак. Оскільки трафік направляється прямо до конкретного центру обробки даних, DDoS-атака може перевантажити цей центр або навколишню інфраструктуру надмірним трафіком. Це може призвести до відмови в обслуговуванні, що ускладнює обробку законних запитів.

На відміну від unicast маршрутизації, мережі anycast є більш стійкими завдяки їх унікальним характеристикам маршрутизації та адресації. Anycast розподіляє вхідний трафік по мережі серверів, розташованих у різних місцях, використовуючи одну і ту ж IP-адресу. Цей метод розширює покриття мережі, запобігаючи переповненню будь-якого окремого місця зловмисними запитами. Коли на адресу надходить надмірний обсяг трафіку, наприклад під час DDoS-атаки, трафік автоматично перенаправляється до найближчого доступного розташування мережі, таким чином мінімізуючи вплив на первинну інфраструктуру.

Маршрутизація anycast покращує стійкість мережі, оскільки робить атаки менш ефективними та зменшує їх потенціал для спричинення збоїв. Ця розгалужена мережева конфігурація ускладнює здійснення DDoS-атак зловмисниками, оскільки вона вимагає значних ресурсів для ефективного надсилання шкідливого трафіку через ботнет.

1.3 Наслідки DDoS атак

DDoS-атаки можуть мати різноманітні наслідки, як для постраждалих організацій і компаній, так і для користувачів Інтернету.

Одним з основних наслідків DDoS-атак є те, що цільовий вебсайт або онлайн-сервіс може стати недоступним для користувачів. Це може спричинити зменшення прибутку компанії, негативно вплинути на репутацію та призвести до втрати клієнтів. DDoS-атаки можуть призвести до припинення роботи організацій та підприємств, що викликає порушення робочих процесів. Деякі DDoS-атаки можуть бути використані як відволікаюча тактика для злому

серверів, щоб отримати доступ до конфіденційної інформації. Постійна недоступність сервісу може призвести до втрати довіри користувачів до компанії.

DDoS-атаки, як і будь-які інші кібератаки, мають серйозні правові наслідки, і зловмисники можуть бути піддані кримінальній відповідальності за свої дії. В Україні кіберзлочини, включаючи DDoS-атаки, підпадають під дію Кримінального кодексу України [13].

Стаття 363-1 Кримінального кодексу України визначає відповідальність за широкий спектр протиправних дій в мережі, від надсилання небажаних електронних повідомлень (спаму) і розсилки SMS-повідомлень до проведення масових та цілеспрямованих DDoS-атак, які можуть призвести до зупинки або відмови в роботі комп'ютерних систем, мереж або обладнання. Основним критерієм для класифікації злочину за цією статтею є виникнення таких наслідків, як порушення або припинення роботи електронно-обчислювальних систем, які повинні бути обов'язково документовані під час досудового розслідування. У зв'язку з високим рівнем анонімності в Інтернеті такі злочини рідко фіксуються правоохоронцями і можуть бути вчинені спільно з іншими кіберзлочинами або злочинами економічного характеру.

Перша частина статті 363-1 визначає відповідальність при вчиненні злочину вперше у вигляді штрафу у розмірі від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

Друга частина статті 363-1 застосовується у випадках, коли такі дії вчинені повторно і також з попередньою змовою групою осіб, якщо вони спричинили значну шкоду. У такому разі покарання може бути більш суворим, з обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, із позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

Загалом DDoS-атаки можуть мати серйозні віддалені наслідки для всіх сторін, що беруть участь, і вимагають ефективних заходів захисту та реагування

для запобігання їхньому виникненню і мінімізації шкоди, яку вони можуть завдати.

1.4 Висновки до розділу

В першому розділі було здійснено огляд механізмів здійснення DDoS атак включно з використання мережі ботнет. Проаналізовано типи DDoS атак в залежності від рівня моделі OSI. Наведено приклади та проаналізовано механізм здійснення атак на прикладному рівні, а саме HTTP Flood та DNS Amplification атак. Показано приклади та механізм здійснення атак на транспортному рівні, а саме TCP SYN Flood та UDP Flood атак. Проаналізовано вразливості мережевого рівня що до здійснення DDoS атак на прикладі атак Ping Flood та IP Fragmentation.

Показано що основними симптомами DDoS-атаки є раптове збільшення навантаження на сайт або сервіс, що призводить до повільної роботи або недоступності. Показано, що для виявлення можливої DDoS-атаки слід звернути увагу на надмірний обсяг трафіку з однієї IP-адреси або діапазону IP-адрес, спостерігати за трафіком від користувачів з подібними характеристиками, збільшенням кількості запитів до конкретної сторінки або ресурсу, а також незвичайними моделями трафіку, такими як стрибки в активності у непарні години або неприродні патерни.

Розглянуто методи захисту від DDoS-атак, а саме: використання маршруту blackhole для IP-адреси цілі, обмеження швидкості або тимчасове блокування трафіку з атакуючих IP-адрес протягом певного періоду, використання брандмауера веб-програм (WAF), використання мережі anycast.

Зазначено що DDoS-атаки можуть призвести до недоступності вебсайтів та сервісів, втрати прибутку та репутації компаній, а також порушення робочих процесів. Ці атаки також мають серйозні правові наслідки згідно статті 363-1 Кримінального кодексу України.

РОЗДІЛ 2 ТЕСТОВЕ СЕРЕДОВИЩЕ ДЛЯ МОДЕЛЮВАННЯ DDOS АТАК

2.1 Схема середовища моделювання DDoS атаки

Для моделювання DDoS атаки оптимальним рішенням є використання лабораторного тестового середовища.

На рисунку 2.1 показана схема тестового середовища на основі гіпервізора VMware та маршрутизатора Mikrotik для моделювання DDoS атаки.

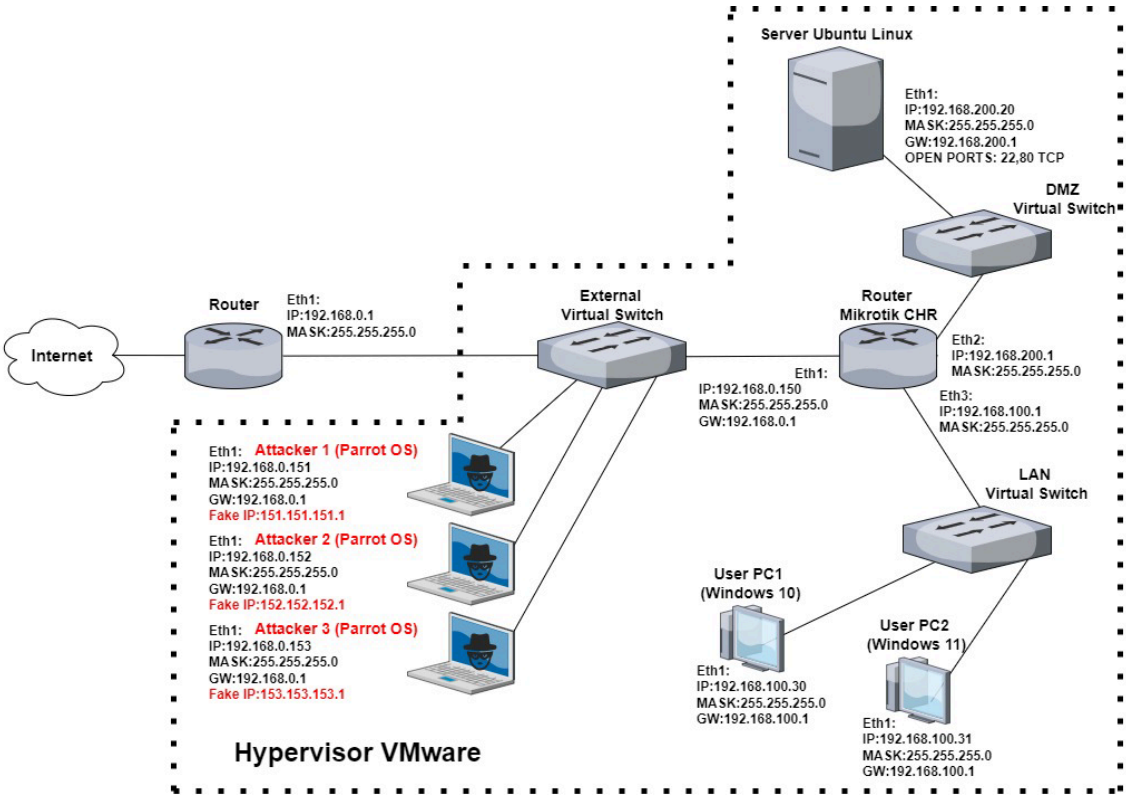

Рисунок 2.1 – Тестове лабораторне середовище для моделювання DDoS атаки

На рисунку показано різні компоненти мережі та їх конфігурації.

Опис мережевих налаштувань наступний:

1) Фізичний маршрутизатор (Router) має підключення до Інтернету та до локальної мережі з інтерфейсом Eth1 з IP-адресою 192.168.0.1 і маскою підмережі 255.255.255.0. Він відокремлює внутрішню мережу від зовнішньої.

2) Зовнішній віртуальний комутатор (External Virtual Switch) в гіпервізорі VMware служить для підключення до зовнішньої фізичної мережі.

3) Маршрутизатор Mikrotik CHR (Router Mikrotik CHR) має три інтерфейси, Eth1 з IP-адресою 192.168.0.150 і маскою 255.255.255.0, Eth2 з IP-адресою 192.168.200.1 і маскою 255.255.255.0 та Eth3 з IP-адресою 192.168.100.1 і маскою 255.255.255.0.

4) LAN віртуальний комутатор (LAN Virtual Switch): використовується в гіпервізорі VMware для підключення внутрішніх користувацьких ПК до віртуальної LAN мережі.

5) Користувацькі ПК (User PC1 і User PC2) - це дві віртуальних машини з операційними системами Windows 10 і Windows 11 відповідно. PC1 має IP-адресу 192.168.100.30, а PC2 - 192.168.100.31, обидва з маскою підмережі 255.255.255.0 і шлюзом 192.168.100.1.

6) DMZ віртуальний комутатор (DMZ Virtual Switch): використовується для підключення серверів в гіпервізорі VMware до віртуальної демілітаризованої зони (DMZ).

7) Сервер (Server Ubuntu Linux) знаходиться в DMZ з IP-адресою 192.168.200.20, маскою 255.255.255.0 і шлюзом 192.168.200.1. На сервері відкриті порти 22 і 80 TCP. Порт 22 TCP - це порт, який використовується для з'єднання з сервером за допомогою протоколу SSH. SSH використовується для безпечного та шифрованого з'єднання з сервером для адміністративних цілей, таких як віддалене керування та адміністрування. Порт 80 TCP - це стандартний порт для вебтрафіку за протоколом HTTP. Він використовується для доступу до вебсайтів. Сервер, який слухає порт 80, може обробляти HTTP-запити та надсилати вебсторінки клієнтам.

8) Атакуючі (Attacker 1, Attacker 2, Attacker 3): три віртуальні машини з операційною системою Parrot OS. Мають наступні IP-адреси: 192.168.0.151, 192.168.0.152, 192.168.0.153, та підроблені (Fake IP) адреси відповідно: 151.151.151.1, 152.152.152.1, 153.153.153.1. Всі мають маску підмережі 255.255.255.0 і шлюз 192.168.0.1.

Гіпервізор VMware є основою для створення віртуальних машин, таких як атакуючі, користувацькі ПК, сервер та маршрутизатор Mikrotik CHR. Ця схема

відображає мережеве тестове середовище, де можна відтворити DDoS-атаку, щоб перевірити реакцію мережі та її компонентів на такий вид атаки.

2.2 Налаштування компонентів лабораторного середовища

2.2.1 Маршрутизатор Mikrotik CHR

Mikrotik CHR - це маршрутизатор, який можна встановити в хмарних середовищах або в гіпервізорах типу 1 або 2 [14]. Цей маршрутизатор може бути встановлений на різні типи віртуальних платформ, таких як VMware, Hyper-V, XEN та KVM. MikroTik CHR працює на базі операційної системи RouterOS, яка надає широкі можливості налаштування і управління мережею. CHR може бути використаний як для розгортання власної мережі, так і для надання хмарних послуг. Основні функції Mikrotik CHR включають в себе маршрутизацію, комутацію, брандмауер, VPN, керування доступом, безпеку мережі, моніторинг і управління мережею. Це робить CHR універсальним інструментом для будь-якої мережевої інфраструктури. Інтерфейс управління CHR дозволяє адміністраторам налаштовувати та контролювати роботу маршрутизатора через вебінтерфейс, SSH або Winbox.

На рисунку 2.2 показано вивід команди `interface print`, яка показує список інтерфейсів разом із типом, MTU та MAC-адресами.

```
[admin@MikroTik] > interface print
Flags: R - RUNNING
Columns: NAME, TYPE, ACTUAL-MTU, MAC-ADDRESS
#    NAME     TYPE    ACTUAL-MTU  MAC-ADDRESS
;;; External
0 R ether1   ether        1500   00:0C:29:B8:9F:6E
;;; DMZ
1 R ether2   ether        1500   00:0C:29:B8:9F:78
;;; LAN
2 R ether3   ether        1500   00:0C:29:B8:9F:82
[admin@MikroTik] >
```

Рисунок 2.2 – Вивід команди `interface print` в операційної системи RouterOS

На рисунку 2.3 зображено вивід команди `ip address print detail` у консолі RouterOS MikroTik, яка надає детальну інформацію про IP-адреси на кожному інтерфейсі.

```
[admin@MikroTik] >  ip address print detail
Flags: X - disabled, I - invalid, D - dynamic
 0   address=192.168.0.150/24 network=192.168.0.0 interface=ether1
     actual-interface=ether1

 1   address=192.168.200.1/24 network=192.168.200.0 interface=ether2
     actual-interface=ether2

 2   address=192.168.100.1/24 network=192.168.100.0 interface=ether3
     actual-interface=ether3
[admin@MikroTik] >
```

Рисунок 2.3 – Вивід команди `ip address print detail` в операційної системи RouterOS

На рисунку 2.4 зображено правила брандмауера Mikrotik для забезпечення базового захисту.

#		Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Interf...
;;; accept established											
0		accept	input								
;;; accept related											
1		accept	input								
;;; allow Winbox											
2		accept	input					6 (tcp)			ether1
;;; allow ICMP											
3		accept	input					1 (icm...			ether1
;;; drop invalid											
4		drop	input								
;;; allow SSH											
5		accept	input					6 (tcp)			ether1
;;; allow HTTP											
6		accept	input					6 (tcp)			ether1
;;; allow HTTPS											
7		accept	input					6 (tcp)			ether1
;;; block everything else											
8		drop	input								ether1
;;; accept established											
9		accept	forward								
;;; accept related											
10		accept	forward								
;;; drop invalid											
11		drop	forward								
;;; DMZ allow											
12		accept	forward	192.168.0.0/...	192.168.200.0/24						ether1
;;; allow from parrot OS to DMZ											
13		accept	forward	151.151.151.1	192.168.200.0/24						ether1
14		accept	forward	152.152.152.1	192.168.200.0/24						ether1
15		accept	forward	153.153.153.1	192.168.200.0/24						ether1
;;; drop access to clients behind NAT from WAN											
16		drop	forward								ether1

Рисунок 2.4 – Базові правила брандмауера Mikrotik

Налаштування брандмауера мають наступні значення:

- правило 0 дозволяє пакети, які належать встановленим з'єднанням (connection-state=established);

- правило 1 дозволяє пакети, які пов'язані із встановленим з'єднанням (connection-state=related);

- правило 2 дозволяє доступ до сервісу Winbox порт 8291 TCP на інтерфейсі ether1;

- правило 3 дозволяє ICMP-пакети на інтерфейс ether1;

- правило 4 відкидає пакети, які не відповідають правилам стану з'єднання (connection-state=invalid);

- правило 5 дозволяє доступ до сервісу SSH на інтерфейсі ether1;

-правило 6 дозволяє доступ до сервісу HTTP порт 80 TCP на інтерфейсі ether1;

-правило 7 дозволяє доступ до сервісу HTTPS порт 443 TCP на інтерфейсі ether1;

- правило 8 відкидає всі інші пакети, які приходять на інтерфейс ether1;

- правило 9 дозволяє пакетам, що належать встановленим з'єднанням (connection-state=established), проходити через маршрутизатор;

- правило 10 дозволяє пакетам, які пов'язані з встановленим з'єднанням (connection-state=related), проходити через маршрутизатор;

- правило 11 відкидає пакети, які не відповідають правилам стану з'єднання (connection-state=invalid);

- правило 12 дозволяє пакетам з мережі 192.168.0.0/24, що прийшли на інтерфейс ether1 і призначені для мережі 192.168.200.0/24, проходити через маршрутизатор;

- правила 13-15 дозволяють пакетам з IP-адрес операційних систем Parrot Security пройти через маршрутизатор до мережі DMZ;

- правило 16 відкидає нові вхідні з'єднання, які намагаються встановитись з клієнтами за маршрутизатором через інтерфейс ether1;

Ця конфігурація брандмауера реалізує базовий захист та фільтрацію трафіку на маршрутизаторі Mikrotik. Правила 2-7 використовуються для зручності налаштування маршрутизатора Mikrotik в лабораторному середовищі.

На рисунку 2.5 зображено правила NAT в Mikrotik.

```
[admin@MikroTik] >  ip firewall nat  print detail
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=accept src-address=192.168.200.0/24 dst-address=192.168.0.0/24
      out-interface=ether1 log=no log-prefix=""

 1    chain=srcnat action=accept src-address=192.168.200.0/24 dst-address=151.151.151.1
      out-interface=ether1 log=no log-prefix=""

 2    chain=srcnat action=accept src-address=192.168.200.0/24 dst-address=152.152.152.1
      out-interface=ether1

 3    chain=srcnat action=accept src-address=192.168.200.0/24 dst-address=153.153.153.1
      out-interface=ether1

 4    chain=srcnat action=masquerade src-address=192.168.100.0/24 out-interface=ether1
      log=no log-prefix=""

 5    chain=srcnat action=masquerade src-address=192.168.200.0/24 out-interface=ether1
      log=no log-prefix=""
[admin@MikroTik] >
```

Рисунок 2.5 – Правила NAT в Mikrotik

Налаштування NAT мають наступні значення:

- правило 0 дозволяє вихідним пакетам з мережі 192.168.200.0/24 до мережі 192.168.0.0/24 проходити інтерфейс ether1 без застосування NAT;

- правила 1-3 дозволяє вихідним пакетам з мережі 192.168.200.0/24 до IP-адрес 151.151.151.1, 152.152.152.1 та 153.153.153.1 проходити інтерфейс ether1 без застосування NAT;

- правила 4-5 застосовує NAT до пакетів з мережі 192.168.100.0/24 та 192.168.200.0/24 на інтерфейсі ether1.

На рисунку 2.6 показано конфігурацію DHCP-сервера на маршрутизаторі Mikrotik.

```
[admin@MikroTik] > ip dhcp-server print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TIME
# NAME        INTERFACE  ADDRESS-POOL  LEASE-TIME
0 DHCPserver  ether3     DHCPpool      10m
[admin@MikroTik] > ip dhcp-server network print
Columns: ADDRESS, GATEWAY, DNS-SERVER, DOMAIN
# ADDRESS           GATEWAY        DNS-SERVER     DOMAIN
0 192.168.100.0/24  192.168.100.1  192.168.100.1  local.lan
                                   192.168.0.1
[admin@MikroTik] > ip pool print
Columns: NAME, RANGES
#  NAME      RANGES
0  DHCPpool  192.168.100.20-192.168.100.50
[admin@MikroTik] > ip dhcp-server lease print
Columns: ADDRESS, MAC-ADDRESS, HOST-NAME, SERVER, STATUS, LAST-SEEN
# ADDRESS         MAC-ADDRESS        HOST-NAME          SERVER      STATUS   LAST-SEEN
0 192.168.100.30  00:0C:29:53:51:39  Win10Education     DHCPserver  waiting  4h4m41s
1 192.168.100.31  00:0C:29:74:C3:15  WIN11EnterpriseEN  DHCPserver  waiting  3h56m26s
[admin@MikroTik] >
```

Рисунок 2.6 – Конфігурація DHCP-сервера в Mikrotik

Створений DHCP-сервер має ім'я "DHCPserver" і прив'язаний до інтерфейсу ether3. Він використовує пул адрес "DHCPpool" для надання IP-адрес клієнтам. Тривалість оренди становить 10 хвилин. DHCP-сервер надає IP-адреси з пулу 192.168.100.20-192.168.100.50 клієнтам з мережі 192.168.100.0/24. IP-адреса інтерфейсу ether3 192.168.100.1 використовується як шлюз за замовчуванням а також DNS-сервером.

В DHCP-сервер прописано дві статичних оренди IP-адрес 192.168.100.30 для пристрою з MAC-адресою 00:0C:29:53:51:39 та 192.168.100.31 для пристрою з MAC-адресою 00:0C:29:74:C3:15. Статус цих адрес є "waiting", що означає, що вони ще не були прийняті пристроями.

Ця конфігурація забезпечує автоматичне надання IP-адрес пристроям, які підключаються до мережі через інтерфейс ether3 маршрутизатора MikroTik.

2.2.2 Сервер Ubuntu Linux

Ubuntu Linux - це один з найпопулярніших дистрибутивів операційної системи Linux. Вона є відкритою операційною системою, що означає, що можна вільно використовувати, модифікувати та поширювати її [15]. Ubuntu Linux може бути ідеальним вибором для використання в якості серверної операційної системи завдяки своїм багатим функціоналом, стабільністю, безпекою та зручністю у використанні. Операційна система славиться своєю надійністю та

стабільністю. Вона має регулярні оновлення безпеки та опцію довгострокової підтримки (LTS), що забезпечує стабільність і безпеку системи протягом тривалого часу. Ubuntu проста у встановленні та налаштуванні, що робить її ідеальним вибором для адміністраторів серверів. Вона має широкий набір інструментів для налаштування.

Ubuntu має широкий вибір програмного забезпечення, що можна встановити на сервер. Від вебсерверів таких як Apache, Nginx та баз даних таких як MySQL, PostgreSQL до систем віртуалізації таких як Docker та Kubernetes, Ubuntu має усе необхідне для побудови потужних серверних рішень. Ubuntu Linux має активну спільноту розробників та користувачів, яка надає підтримку, консультації та працює над новими рішеннями для серверів. Операційна система має вбудовані інструменти для забезпечення безпеки серверів, такі як брандмауер, механізми автоматичного оновлення та інші що допомагають захистити сервер від потенційних загроз. Ubuntu широко використовується у хмарних обчисленнях, оскільки вона є популярним вибором для створення віртуальних серверів у публічних та приватних хмарних сервісах.

В лабораторному середовищі буде використано віртуальну машину Ubuntu Linux, як цільовий сервер для імітації DDoS атаки на вебсервер.

На рисунку 2.7 показано налаштування мережі в Ubuntu Linux.

```
root@ubuntu-server:~# nmcli
ens33: connected to Wired connection 1
        "Intel 82545EM"
        ethernet (e1000), 00:0C:29:9E:F2:E0, hw, mtu 1500
        ip4 default
        inet4 192.168.200.20/24
        route4 192.168.200.0/24 metric 100
        route4 169.254.0.0/16 metric 1000
        route4 default via 192.168.200.1 metric 100

lo: unmanaged
        "lo"
        loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536

DNS configuration:
        servers: 192.168.200.1
        interface: ens33
```

Рисунок 2.7 – Налаштування мережі в Ubuntu Linux

Утиліта nmcli є інструментом для управління мережею NetworkManager через командний рядок. Вивід вказує на інформацію про мережевий інтерфейс ens33, який підключений до "Wired connection 1". Цей інтерфейс використовує адаптер Intel e1000e, який є віртуальним адаптером.

На рисунку 2.8 показано частину вивід команди `netstat -an` в терміналі Ubuntu Linux.

```
root@ubuntu-server:~# netstat -an | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:34364           0.0.0.0:*
udp6       0      0 :::35776                :::*
udp6       0      0 :::5353                 :::*
```

Рисунок 2.8 – Вивід команди `netstat -an` в терміналі Ubuntu Linux

Команда `netstat` використовується для виводу активних з'єднань та виявлення відкритих портів, які слухають відповідні сервіси.

У переліку показано TCP порт 80, що прослуховуються (статус LISTEN) на сервері та використовується для HTTP-з'єднань. Також TCP порт 22, що використовується для SSH-з'єднань прослуховується на всіх інтерфейсах.

Вивід команди `mtr` (див.рисунок 2.9) підтверджує коректність налаштувань Ubuntu Linux та маршрутизатора Mikrotik для сегменту DMZ.

```
root@ubuntu-server: ~
                              My traceroute  [v0.95]
ubuntu-server (192.168.200.20) -> meta.ua (104.22.65.142024-03-26T14:21:34+0200
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                     Packets               Pings
 Host                              Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 192.168.200.1                   0.0%    19    0.4   0.5   0.4   1.0   0.2
 2. 192.168.0.1                     0.0%    18    3.3   2.7   1.9   9.8   1.8
 3.                                 0.0%    18    2.2   3.6   1.9  14.5   3.3
 4.                                 0.0%    18    4.2   5.8   2.8  14.4   3.3
 5.                                 0.0%    18    3.6   3.4   2.6   7.7   1.2
 6. 194.146.198.192                 0.0%    18    9.7  11.8   8.7  38.1   6.7
 7. 185.1.50.68                    61.1%    18   16.5  11.4   9.5  16.5   2.6
 8. 104.22.65.144                   0.0%    18   12.1  11.3   8.9  21.3   3.4
```

Рисунок 2.9 – Вивід команди `mtr` в терміналі Ubuntu Linux

Ця інформація є корисною для діагностування проблем з мережею, зокрема виявлення точок, де відбуваються затримки або втрати пакетів. В цьому трасуванні видно, що на шостому стрибку відбувається значна втрата пакетів (61.1%), що може свідчити про обмеження пакетів ICMP на маршрутизаторі. Усі інші хости не показують втрати пакетів, а час відгуку є різний і змінюється від мінімуму до максимуму, що є нормальним явищем при трасуванні маршрутів.

2.2.3 Операційна система Windows

Як робочі станції в лабораторному середовищі використовуються Windows 10 та Windows 11. Вони знаходяться в віртуальному LAN сегменті мережі.

На рисунку 2.10 показано мережеві налаштування в Windows 10.

```
Command Prompt
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 520099165
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-77-69-64-00-0C-29-53-51-39
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter vEthernet (External Virtual Switch):

   Connection-specific DNS Suffix  . : local.lan
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-0C-29-53-51-39
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ca6f:f5a4:ebab:ca2c%25(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.100.30(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, March 26, 2024 2:43:12 PM
   Lease Expires . . . . . . . . . . : Tuesday, March 26, 2024 2:53:12 PM
   Default Gateway . . . . . . . . . : 192.168.100.1
   DHCP Server . . . . . . . . . . . : 192.168.100.1
   DHCPv6 IAID . . . . . . . . . . . : 419433513
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-77-69-64-00-0C-29-53-51-39
   DNS Servers . . . . . . . . . . . : 192.168.100.1
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\admin>
```

Рисунок 2.10 – Налаштування мережеві в Windows 10

На рисунку 2.11 показано мережеві налаштування в Windows 11.

```
Administrator: Command Prompt
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : local.lan
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-74-C3-15
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fcfb:f868:c738:9bc2%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.100.31(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 25 березня 2024 р. 13:53:42
   Lease Expires . . . . . . . . . . : 25 березня 2024 р. 14:03:42
   Default Gateway . . . . . . . . . : 192.168.100.1
   DHCP Server . . . . . . . . . . . : 192.168.100.1
   DHCPv6 IAID . . . . . . . . . . . : 100666409
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-6E-C6-39-00-0C-29-74-C3-15
   DNS Servers . . . . . . . . . . . : 192.168.100.1
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Рисунок 2.11 – Налаштування мережеві в Windows 11

На рисунку 2.12 показано результат виконання команди `ip dhcp-server lease print` у командному рядку MikroTik RouterOS. Ця команда використовується для перегляду інформації про надані в оренду (leased) IP-адреси від DHCP-сервера.

```
[admin@MikroTik] > ip dhcp-server lease print
Columns: ADDRESS, MAC-ADDRESS, HOST-NAME, SERVER, STATUS
# ADDRESS          MAC-ADDRESS         HOST-NAME          SERVER      STATUS
0 192.168.100.30   00:0C:29:53:51:39   Win10Education     DHCPserver  bound
1 192.168.100.31   00:0C:29:74:C3:15   WIN11EnterpriseEN  DHCPserver  bound
[admin@MikroTik] >
```

Рисунок 2.12 – Виконання команди `ip dhcp-server lease print` у командному рядку MikroTik

Клієнт з IP-адресою 192.168.100.30, MAC-адресою 00:0C:29:53:51:39, ім'ям хоста Win10Education має статус bound, що означає, що IP-адресу клієнт успішно отримав. Клієнт з IP-адресою 192.168.100.31, MAC-адресою 00:0C:29:74:C3:15, ім'ям хоста WIN11EnterpriseEN також має статус bound.

Вивід утиліти WinMTR в Windows 10 підтверджує коректність налаштувань Windows 10 та маршрутизатора Mikrotik для сегменту LAN (див.рисунок 2.13).

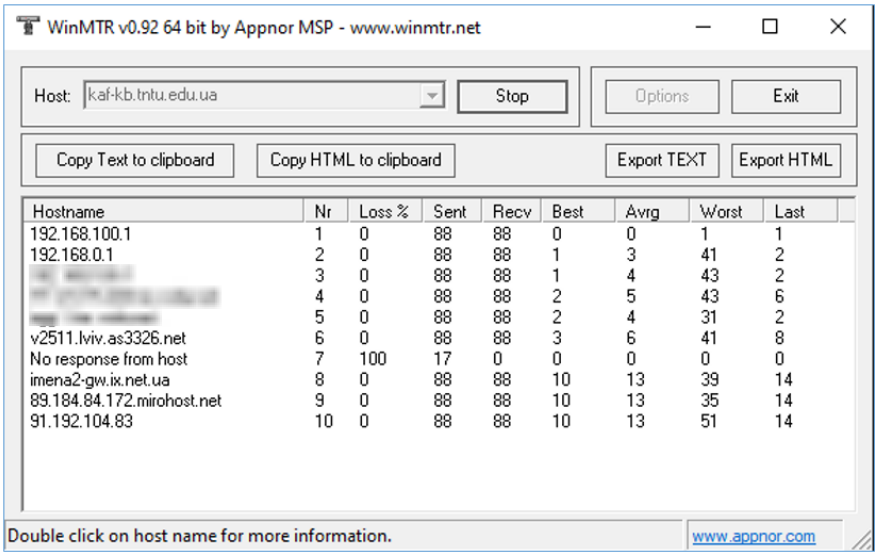

Рисунок 2.13 – Вивід утиліти WinMTR в Windows 10

Кінцевий хост kaf-kb.tntu.edu.ua не показує втрати пакетів, час відгуку є різний і змінюється від мінімуму до максимуму, що є нормальним явищем при трасуванні маршрутів.

2.2.4 Операційна система Parrot Security

Parrot Security - це дистрибутив Linux, спеціально розроблений для тестування безпеки [16]. Він базується на Debian Linux та включає в себе широкий спектр інструментів для перевірки безпеки, таких як сканери вразливостей, інструменти для аналізу безпеки мережі, інструменти для тестування на проникнення та багато іншого.

Операційна система включає в себе велику кількість інструментів безпеки, таких як Metasploit, Wireshark, Nmap та інші, які допомагають у виявленні і виправленні вразливостей. Також Parrot Security містить інструменти для забезпечення анонімності та приватності, такі як Tor та інші інструменти шифрування та анонімного вебперегляду. Підтримує розробку та тестування безпеки шляхом надання різноманітних інструментів, серед яких засоби аналізу вебдодатків, інструменти для аудиту безпеки мережі.

Ця операційна система призначена для фахівців з кібербезпеки, етичних хакерів та інших спеціалістів у сфері безпеки, які шукають потужний інструментарій для роботи у сфері безпеки і тестування.

В лабораторному середовищі ОС Parrot Security буде використовуватись для моделювання DDoS атаки за допомогою утиліти hping3.

На рисунку 2.14 показано мережеві налаштування та статичні маршрути в Parrot Security.

```
route -n - Parrot Terminal (as superuser)
route -n - Parrot Terminal 80x26
┌─[root@parrot]─[/usr/share/wordlists]
└──╼ #ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:ec:d4:05 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.0.151/24 brd 192.168.0.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::c2fd:5519:d2b:7f8b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
┌─[root@parrot]─[/usr/share/wordlists]
└──╼ #route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    100    0        0 ens33
192.168.0.0     0.0.0.0         255.255.255.0   U     100    0        0 ens33
192.168.200.0   192.168.0.150   255.255.255.0   UG    100    0        0 ens33
┌─[root@parrot]─[/usr/share/wordlists]
└──╼ #
```

Рисунок 2.14 – Налаштування мережеві в Parrot Security

Команда route -n показує, що мережа 192.168.200.0/24 доступна через шлюз з IP-адресою 192.168.0.150.

На рисунку 2.15 показано перевірка доступності Ubuntu Linux з Parrot Security Atacker1.

```
┌─[root@parrot]─[/usr/share/wordlists]
└──╼ #ping 192.168.200.20
PING 192.168.200.20 (192.168.200.20) 56(84) bytes of data.
64 bytes from 192.168.200.20: icmp_seq=1 ttl=63 time=3.62 ms
64 bytes from 192.168.200.20: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 192.168.200.20: icmp_seq=3 ttl=63 time=0.745 ms
64 bytes from 192.168.200.20: icmp_seq=4 ttl=63 time=0.727 ms
^C
--- 192.168.200.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 0.727/1.597/3.623/1.191 ms
┌─[root@parrot]─[/usr/share/wordlists]
└──╼ #traceroute 192.168.200.20
traceroute to 192.168.200.20 (192.168.200.20), 30 hops max, 60 byte packets
 1  192.168.0.150 (192.168.0.150)  0.316 ms  0.207 ms  0.164 ms
 2  192.168.200.20 (192.168.200.20)  0.377 ms  0.495 ms  0.455 ms
┌─[root@parrot]─[/usr/share/wordlists]
└──╼ #
```

Рисунок 2.15 – Перевірка доступності Ubuntu Linux з Parrot Security Atacker1

Результати команд ping та traceroute показують, що пакети, які надіслані з Parrot Security Atacker1 успішно досягають сервера Ubuntu Linux.

На рисунку 2.16 показано сканування за допомогою `nmap` з Parrot Security Atacker1 IP-адреси сервера Ubuntu Linux.

```
┌─[root@parrot]─[/usr/share/wordlists]
└──╼ #nmap 192.168.200.20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-26 16:08 UTC
Nmap scan report for 192.168.200.20
Host is up (0.00061s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
┌─[root@parrot]─[/usr/share/wordlists]
└──╼ #
```

Рисунок 2.16 – Сканування за допомогою `nmap` IP-адреси сервера Ubuntu Linux

Результати сканування за допомогою nmap показують, що на пристрої з IP-адресою 192.168.200.20 запущені дві служби: SSH та HTTP.

Доступність служб SSH та HTTP підтверджує коректність налаштувань Parrot Security та маршрутизатора Mikrotik для з’єднання External сегменту та DMZ.

2.4 Висновки до розділу

У другому розділі було розроблено та налаштовано тестове середовище для моделювання DDoS атак. Тестовт середовище розгорнуто на основі гіпервізора VMware з основним елементом маршрутизатором Mikrotik CHR.

Встановлено та налаштовано Mikrotik CHR з брандмауером, NAT та DHCP сервером. Зроблено налаштування LAN та DMZ сегментів віртуальної мережі. Встановлено та налаштовано віртуальну машину Ubuntu Linux з вебсервером в DMZ сегменті віртуальної мережі. Встановлено та налаштовано віртуальні машини Windows 10 та Windows 11 в LAN сегменті віртуальної мережі.

Встановлено та налаштовано віртуальні машини Parrot Security Atacker1, Atacker2 та Atacker3 з відповідними засобами для здійснення DDoS атак.

Перевірено коректність роботи тестового лабораторного середовища та взаємодію усіх елементів схеми.

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕХАНІЗМУ ПОМ'ЯКШЕННЯ DDOS АТАК

3.1 Засіб здійснення DDoS атаки

Моделювання DDoS-атак є важливою частиною процесу забезпечення безпеки мережі, щоб розуміти їхні наслідки та розробити ефективні заходи захисту.

Існує багато інструментів для генерації мережевого трафіку, які можна використовувати для моделювання DDoS-атак. Для моделювання DDoS атак в даній роботі буде використано утиліту hping3 [17]. Ця утиліта є одним з інструментів, які включені до Parrot Security. hping3 - це інструмент командного рядка для тестування мереж та виконання різних мережевих операцій, таких як сканування портів, відправка пакетів з різними типами трафіку тощо. Він надає можливість взаємодії з мережевим стеком операційної системи та надсилати специфічно налаштовані пакети на вказані адреси та порти.

hping3 дозволяє надсилати пакети з різними протоколами, такими як TCP, UDP та ICMP. Є можливість налаштувати різні параметри пакетів, такі як джерело та призначення, порти, прапори TCP, розмір даних тощо. Генерація пакетів з вказаними значеннями полів заголовків дозволяє створювати власні пакети з встановленим значенням TTL, фрагментів, прапорів TCP тощо. Це дозволяє тестувати реакцію мережевих пристроїв на різні ситуації. hping3 може використовуватись для сканування портів на цільових хостах, шукаючи відкриті сервіси.

3.1.1 Моделювання Ping Flood атаки

Здійснимо Ping Flood атаку за допомогою hping3 на IP-адресу Mikrotik. На рисунку 3.1 показано використання hping3 в Parrot Security для здійснення Ping Flood атаки.

```
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo hping3 --icmp --flood -a 151.151.151.1 192.168.0.150
HPING 192.168.0.150 (ens33 192.168.0.150): icmp mode set, 28 headers + 0 data by
tes
hping in flood mode, no replies will be shown
```

Рисунок 3.1 – Використання hping3 в Parrot Security для здійснення Ping Flood атаки на IP-адресу Mikrotik

Утиліта hping3 була використана для надсилання пакетів ICMP Echo Request на IP-адресу 192.168.0.150 з використанням IP-адреси джерела 151.151.151.1. Флаг `--icmp` вказує на використання ICMP протоколу, а `--flood` вказує на те, що треба відправити пакети з максимальною можливою швидкістю. Параметр `-a` встановлює IP-адресу джерела для відправлених пакетів.

Ця команда надсилає пакети ICMP Echo Request на цільову IP-адресу з IP-адресою джерела 151.151.151.1 без зупинки, що спричиняє значне використання ресурсів обладнання на цільовій стороні (див. рисунок 3.2).

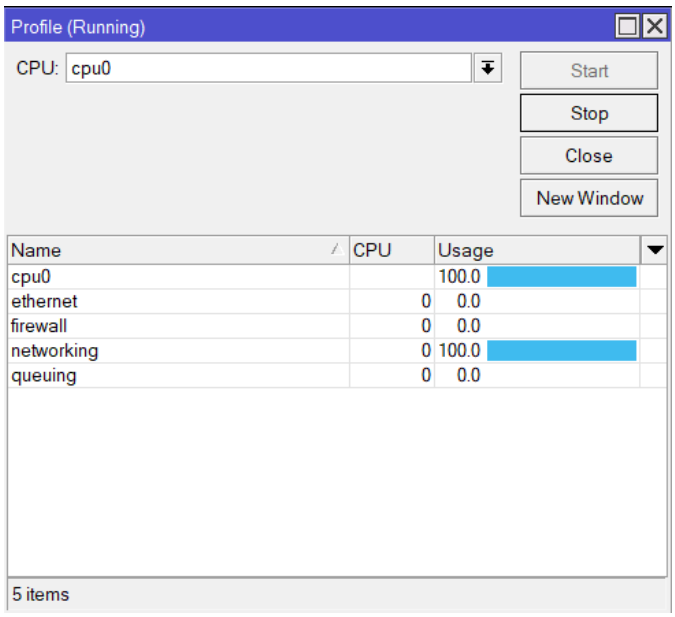

Рисунок 3.2 – Використання ресурсів CPU Mikrotik при здійсненні Ping Flood атаки

На маршрутизаторі спостерігається 100% використання ресурсів CPU зв’язане з мережевою активністю. Це є наслідком здійснення Ping Flood атаки.

На рисунку 3.3 показано перевірку якості зв’язку з віртуальної машини Windows 10 при здійсненні Ping Flood атаки на IP-адресу Mikrotik.

```
Command Prompt
C:\Users\admin>ping 192.168.0.1 -t

Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.0.1: bytes=32 time=3277ms TTL=63
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 24, Received = 1, Lost = 23 (95% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3277ms, Maximum = 3277ms, Average = 3277ms
Control-C
^C
C:\Users\admin>
```

Рисунок 3.3 – Перевірка якості зв’язку з віртуальної машини Windows 10 при здійсненні Ping Flood атаки

Втрати пакетів при виконанні команди ping та великі затримки є наслідком 100% використання ресурсів CPU маршрутизатора Mikrotik.

3.1.2 Моделювання SYN Flood атаки

Здійснимо SYN Flood атаку за допомогою hping3 на вебсервер Ubuntu Linux. На рисунку 3.4 показано використання hping3 в Parrot Security для здійснення SYN Flood атаки.

```
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo hping3 -S --flood -a 152.152.152.1  -p 80 192.168.200.20
HPING 192.168.200.20 (ens33 192.168.200.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Рисунок 3.4 – Використання hping3 в Parrot Security для здійснення SYN Flood атаки на вебсервер Ubuntu Linux

Прапорець `-S` вказує на те, що потрібно надіслати пакети TCP SYN. Прапорець `-flood` вказує на те, що потрібно надсилати пакети якомога швидше без очікування відповідей. Прапорець `-p` вказує порт призначення, в даному випадку, порт 80 (HTTP).

Ця команда відправляє велику кількість пакетів TCP SYN на порт 80 цільової системи, що спричиняє значне використання ресурсів маршрутизатора Mikrotik (див. рисунок 3.5).

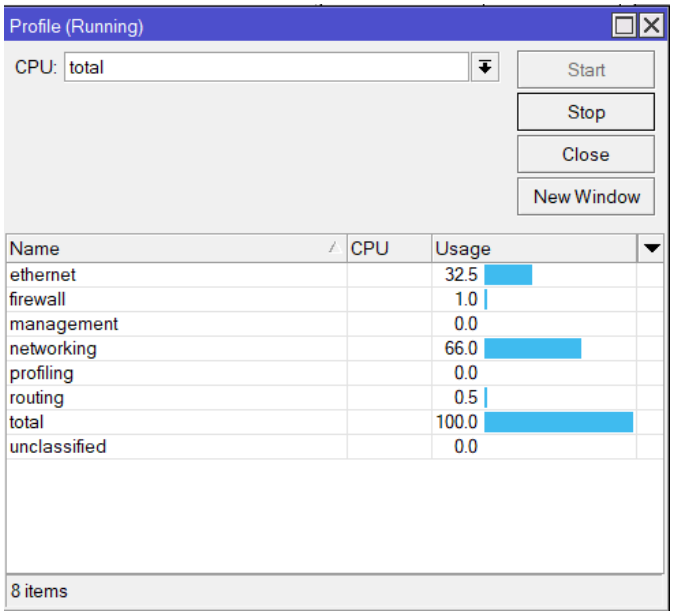

Рисунок 3.5 – Використання ресурсів CPU Mikrotik при здійсненні SYN Flood атаки

На маршрутизаторі, як і у випадку Ping Flood спостерігається 100% використання ресурсів CPU зв’язане з мережевою активністю. Це є наслідком здійснення SYN flood атаки. Також очевидно, що перевірка якості зв’язку з віртуальної машини Windows 10 покаже результат аналогічний що і при здійсненні Ping Flood атаки (див. рисунок 3.3).

На рисунку 3.6 показано вікно терміналу програми iptraf-ng в Ubuntu Linux, інструменту для моніторингу мережевого трафіку в реальному часі.

```
root@ubuntu-server: ~
root@ubuntu-server: ~        root@ubuntu-server: ~
iptraf-ng 1.2.1
Statistics for ens33

                Total      Total    Incoming   Incoming    Outgoing   Outgoing
              Packets      Bytes     Packets      Bytes     Packets      Bytes
Total:        2589531    116485k     1290567   59367018     1298964   57118100
IPv4:         2589531    108741k     1290567   51623820     1298964   57118100
IPv6:               0          0           0          0           0          0
TCP:          2589491    108739k     1290533   51621320     1298958   57117716
UDP:               11        796           5        412           6        384
ICMP:              29       2088          29       2088           0          0
Other IP:           0          0           0          0           0          0
Non-IP:             0          0           0          0           0          0
Broadcast:          1        156           1        156           0          0

Total rates:      13626,98 kbps          Broadcast rates:        0,00 kbps
                     37868 pps                                       0 pps

Incoming rates:    6940,08 kbps
                     18858 pps
                                         IP checksum errors:        0
Outgoing rates:    6686,90 kbps
Time:   0:01 ---     19009 pps------------------ Drops:         0 ----------
X-exit
```

Рисунок 3.6 – Вікно терміналу програми iptraf-ng в Ubuntu Linux при здійсненні SYN Flood атаки

За одну секунду на інтерфейс ens33 надходить приблизно 21509 вхідних пакетів, які вичерпують ресурси Ubuntu Linux. Це в свою чергу призводить до відмови в обслуговуванні та недоступності вебсервера.

На рисунку 3.7 зображено результат виклику команди `netstat`, яка була використана для моніторингу мережевих з'єднань в операційній системі Ubuntu Linux під час проведення атаки типу SYN Flood.

```
root@ubuntu-server: ~
root@ubuntu-server: ~        root@ubuntu-server: ~
root@ubuntu-server:~# netstat -an | grep :80  | more
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 192.168.200.20:80       152.152.152.1:16551     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16491     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16409     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16541     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16459     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16418     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:9995      SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:10111     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16568     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16549     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16432     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:9659      SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16594     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:10020     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:10037     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16431     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16499     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:10200     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16570     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:10016     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:16603     SYN_RECV
tcp        0      0 192.168.200.20:80       152.152.152.1:10085     SYN_RECV
--More--
```

Рисунок 3.7 Дані виводу `netstat` в Ubuntu Linux при здійсненні SYN Flood атаки

Можна побачити, що є багато з'єднань TCP, що чекають на завершення встановлення TCP з’єднання (SYN_RECV статус). Сервер отримує багато одночасних запитів на з'єднання, що є ознакою SYN Flood атаки, при якій атакуючий надсилає швидко послідовність запитів на з'єднання до цільового серверу, не завершуючи з’єднання. Це призводить до переповнення черги для вхідних з'єднань, роблячи вебсервер неспроможним обробити легітимні запити.

3.1.3 Моделювання UDP flood атаки

Здійснимо UDP flood атаку за допомогою hping3 на Ubuntu Linux. На рисунку 3.8 показано використання hping3 в Parrot Security Atacker1 для здійснення UDP Flood атаки.

```
┌─[x]─[root@parrot]─[/home/user]
└──╼ #sudo hping3 --flood -a 153.153.153.1 -2 -p 53 192.168.200.20
HPING 192.168.200.20 (ens33 192.168.200.20): udp mode set, 28 headers + 0 data b
ytes
hping in flood mode, no replies will be shown
```

Рисунок 3.8 – Використання hping3 в Parrot Security для здійснення UDP Flood атаки на Ubuntu Linux

Прапорець `-2` вказує на те, що потрібно надіслати UDP пакети. Прапорець `-flood` вказує на те, що потрібно надсилати пакети якомога швидше без очікування відповідей. Прапорець `-p` вказує порт призначення, в даному випадку, порт 53 (DNS). Аналогічні команди були використані на Parrot Security Atacker2 та Atacker3.

Ця команда відправляє велику кількість пакетів UDP на порт 53 Ubuntu Linux. В Ubuntu Linux немає сервісу, що прослуховує 53 UDP порт, але знову можна спостерігати надмірне використання ресурсів маршрутизатора Mikrotik (див. рисунок 3.9).

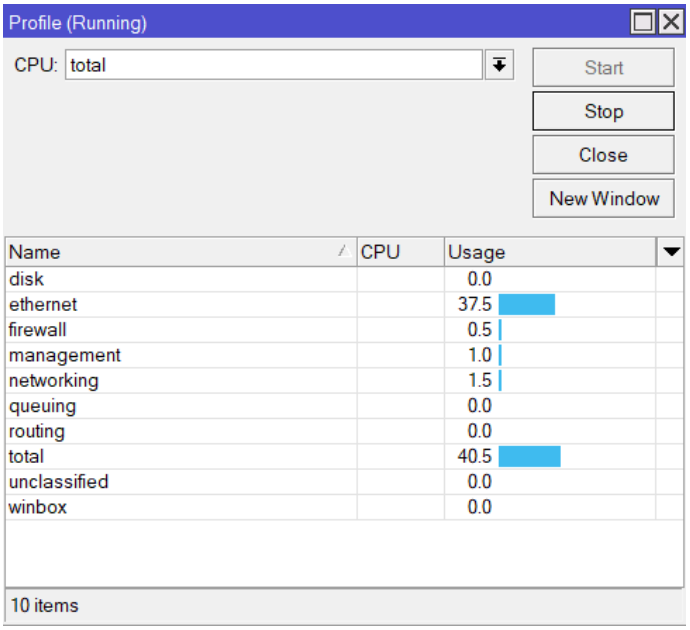

Рисунок 3.9 – Використання ресурсів CPU Mikrotik при здійсненні UDP Flood атаки

Також за одну секунду на інтерфейс ens33 надходить приблизно 15460 вхідних пакетів, які вичерпують ресурси Ubuntu Linux (див. рисунок 3.10). Це в свою чергу призводить до нестабільної роботи сервера.

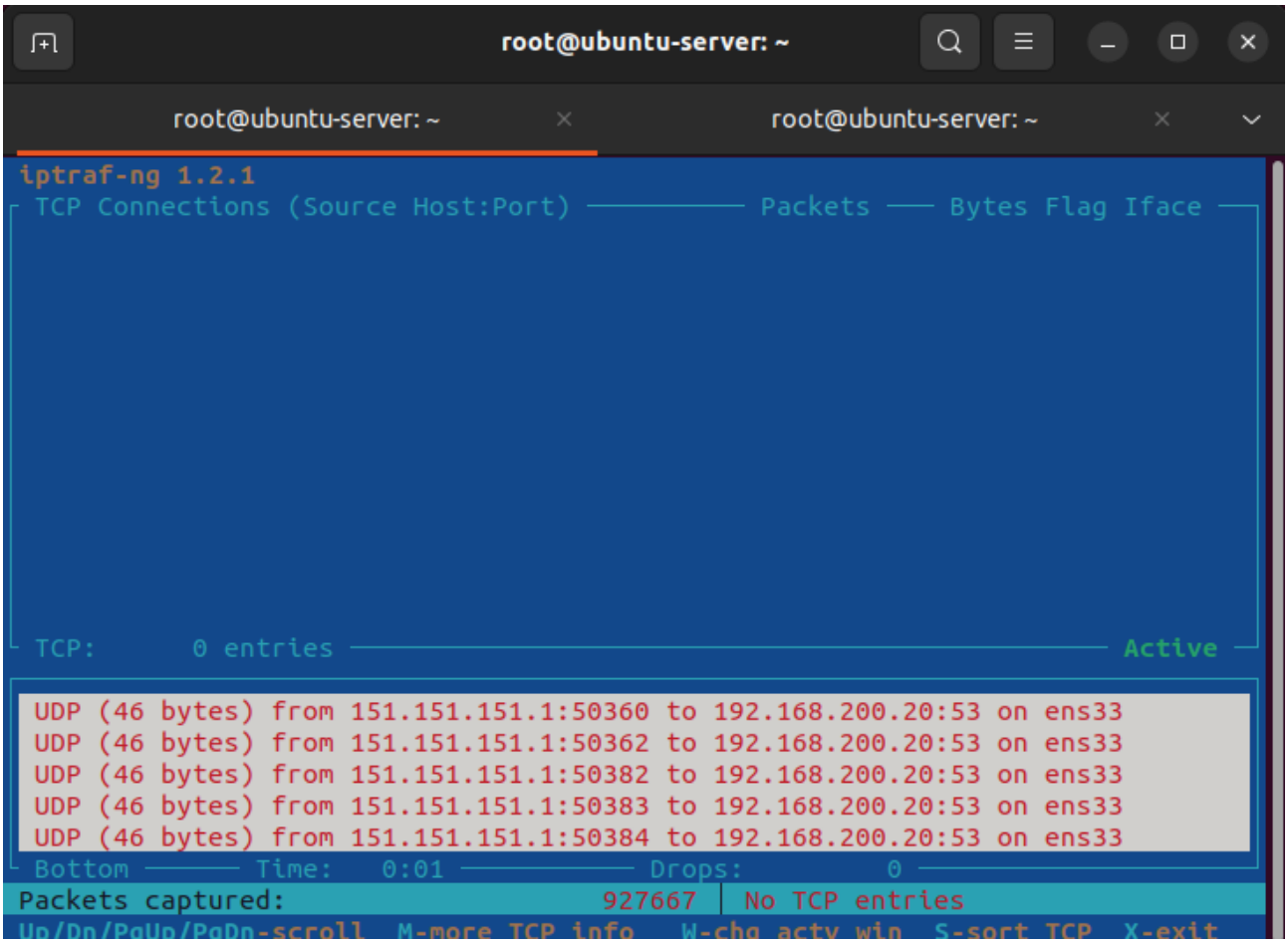

Рисунок 3.10 – Вікно терміналу програми iptraf-ng в Ubuntu Linux при здійсненні UDP Flood атаки

Також в терміналі команди iptraf-ng можна побачити, що UDP пакети мають розмір лише 46 байт.

3.2 Налаштування механізму пом’якшення DDoS атаки

Для налаштування механізмів пом'якшення DDoS атак на маршрутизаторі MikroTik використаємо брандмауер [18].

На рисунку 3.11 показано правила фільтрації пакетів брандмауера Mikrotik для пом’якшення DDoS атак.

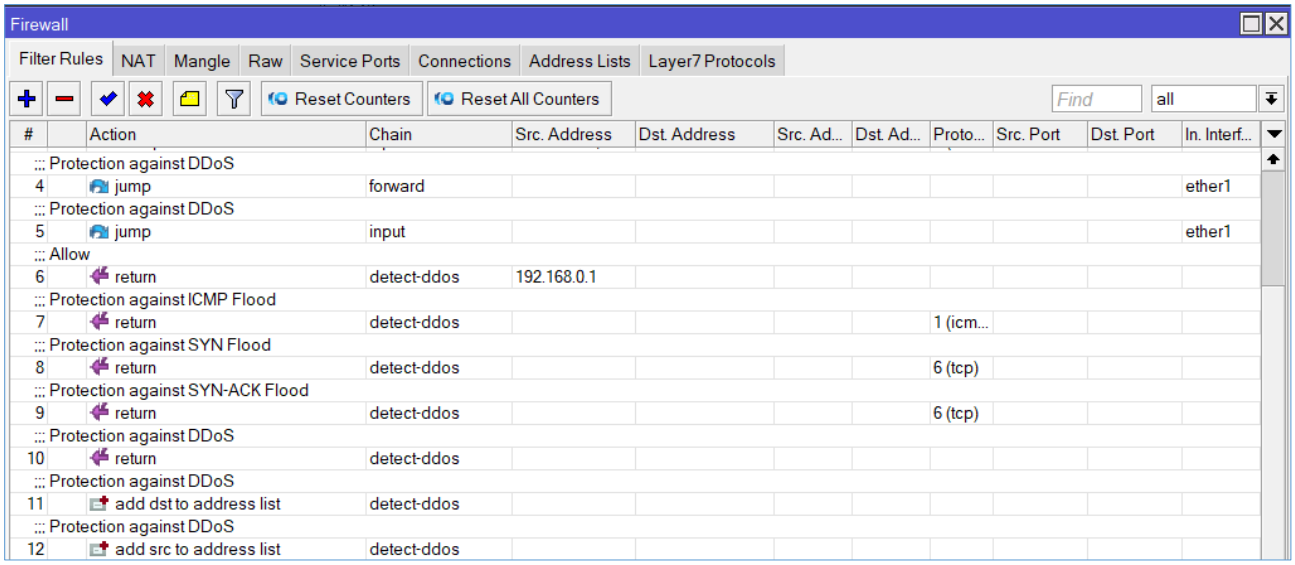

Рисунок 3.11 – Правила фільтрації пакетів для пом’якшення DDoS атак

Ці правила налаштовують механізм пом’якшення DDoS атак на маршрутизаторі MikroTik.

Правило номер 4 встановлює фільтрацію мережевого трафіку та буде застосовуватися до пакетів, які проходять через маршрутизатор. Правило буде застосовуватися тільки до нових з'єднань, що надходять через інтерфейс ether1. Пакети, які відповідають умовам правила, будуть перенаправлені до цільового механізму обробки DDoS атак з іменем detect-ddos для подальшої обробки.

Правило номер 5 встановлює правило фільтрації, яке перенаправляє нові з'єднання, що надходять на інтерфейс ether1, до механізму виявлення DDoS атак для подальшої обробки.

Правило номер 7 встановлює правило фільтрації мережевого трафіку на маршрутизатор Mikrotik для захисту від Ping Flood. Обмеження використовується для визначення, як швидко можуть надходити ICMP пакети. В даному випадку, до 2000 пакетів за 10 секунд не буде вважатися Ping Flood. Пакети, які відповідають умовам правила, будуть повернуті до основного потоку обробки.

Правила 8-10 виконують схожу дію, але для інших типів трафіку і відповідно типів атак.

Правила 11 та 12 додають правила фільтрації мережевого трафіку на маршрутизаторі Mikrotik для обробки потенційних атак DDoS і додавання адрес до списків адрес для подальшої обробки. В даному випадку додається адреса призначення (destination) до списку адрес з назвою ddos-targets. Час, на який адреса буде додана до списку становить 10 хвилин. Також додається джерело (source) до списку адрес з назвою ddos-attackers. Час, на який адреса буде додана до списку становить 10 хвилин.

На рисунку 3.12 показано два списки адрес, які використовуються для зберігання IP-адрес зловмисників та цілей DDoS атаки у правилах фільтрації мережевого трафіку.

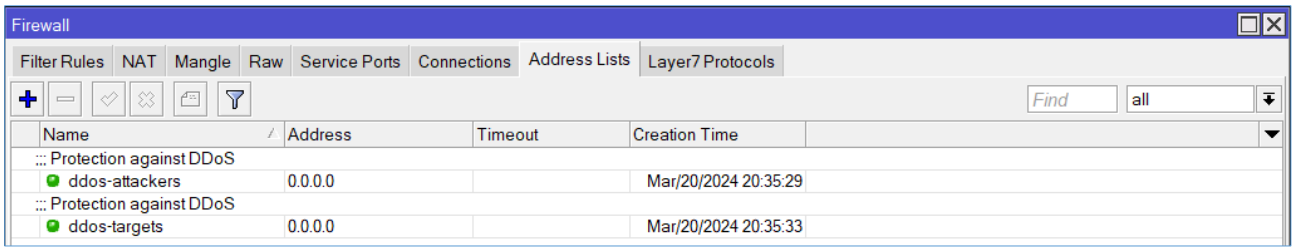

Рисунок 3.12 – Списки адрес в Mikrotik

На рисунку 3.13 показано правило для ланцюга "prerouting" у таблиці "raw" для фільтрації мережевого трафіку на рівні IP-пакетів на маршрутизаторі Mikrotik, яке використовується для блокування IP-адрес зловмисників.

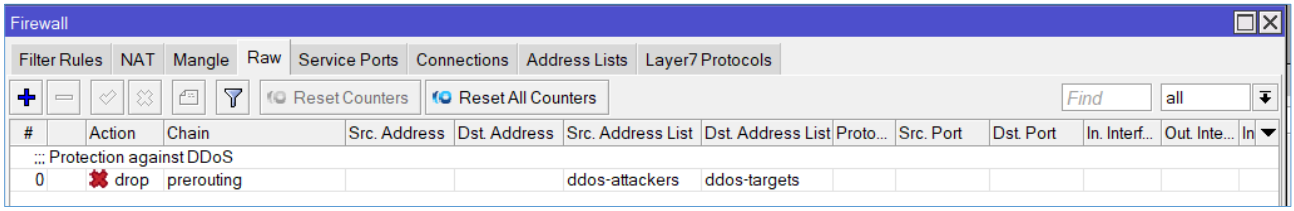

Рисунок 3.13 – Правило для блокування IP-адрес зловмисників в Mikrotik

Використання chain=prerouting вказує на те, що правило буде застосовано до трафіку перед маршрутизацією. Дія drop означає, що пакети, які відповідають цьому правилу, будуть видалені. Тільки пакети з джерелом, яке знаходиться в списку адрес "ddos-attackers та з призначенням, яке знаходиться в списку адрес

"ddos-targets", будуть оброблені цим правилом. В додатку А показано усі параметри налаштування брандмауера в Mikrotik для пом’якшення DDoS атак.

3.3 Тестування захисного механізму

Щоб протестувати захисні механізми проти DDoS атак на маршрутизаторі Mikrotik було використано утиліту hping3 з генерацією максимального обсягу трафіку (велика кількість запитів за одиницю часу). Було здійснено одночасно Ping Flood, SYN Flood та UDP Flood атаки з Parrot Security Atacker1, Atacker2 та Atacker3.

На рисунку 3.14 показано списки адрес в яких збережені IP-адреси атакуючих.

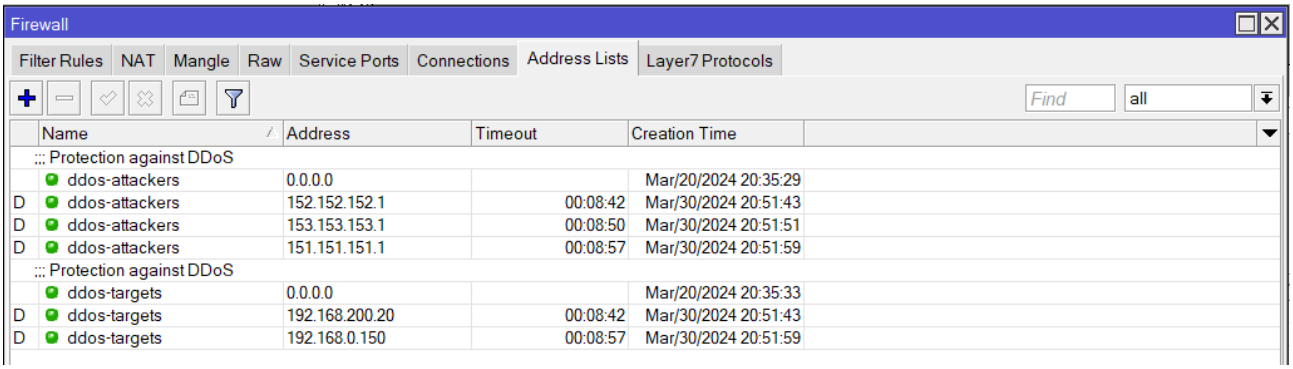

Рисунок 3.14 – Списки адрес в Mikrotik при тестуванні захисту від DDoS атак

Список "ddos-attackers" містить IP-адреси, які визначені як джерела атак. Список "ddos-targets" містить IP-адреси, які були цілями атак.

Ці списки адрес були використані для автоматизованого керування мережевим трафіком, дозволяючи брандмауеру динамічно блокувати IP-адреси визначених джерел атак та захищати визначені цілі.

На рисунку 3.15 можна побачити, що DDoS атаки не спричинили перевантаження та надмірного використання ресурсів маршрутизатора Mikrotik.

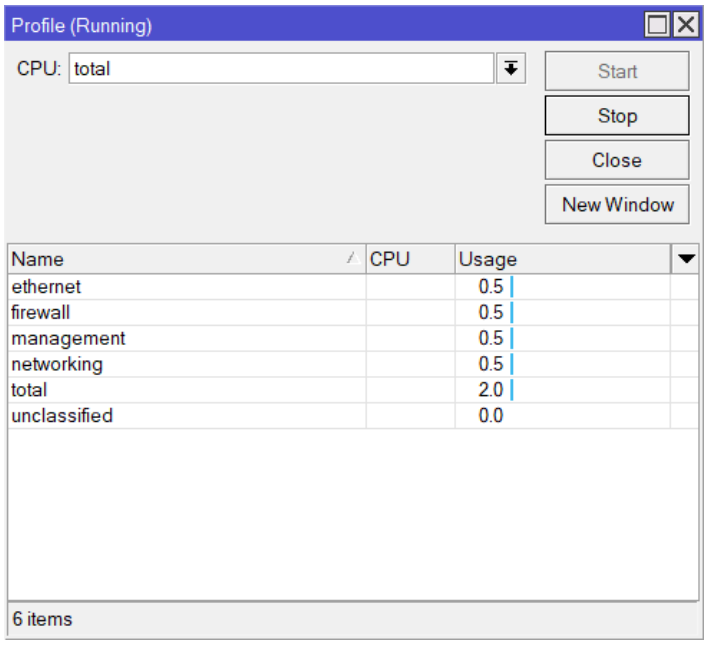

Рисунок 3.15 – Використання ресурсів CPU Mikrotik при здійсненні DDoS атак

На рисунку 3.16, 3.17 та 3.18 показано перевірку якості зв’язку з віртуальної машини Windows 10, Windows 11 та Ubuntu Linux при здійсненні DDoS атак на IP-адресу Mikrotik та IP-адресу Ubuntu Linux.

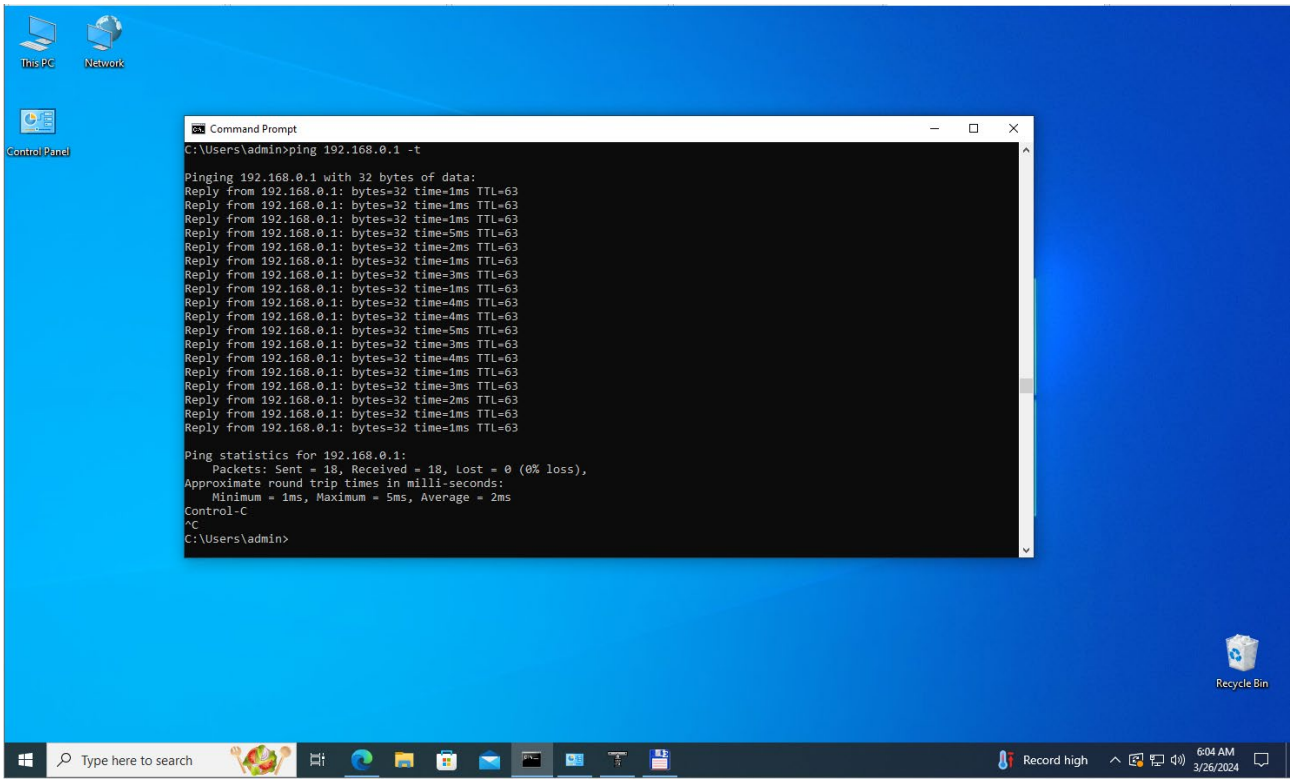

Рисунок 3.16 – Перевірка якості зв’язку з віртуальної машини Windows 10 при активованому захисному механізмі від DDoS

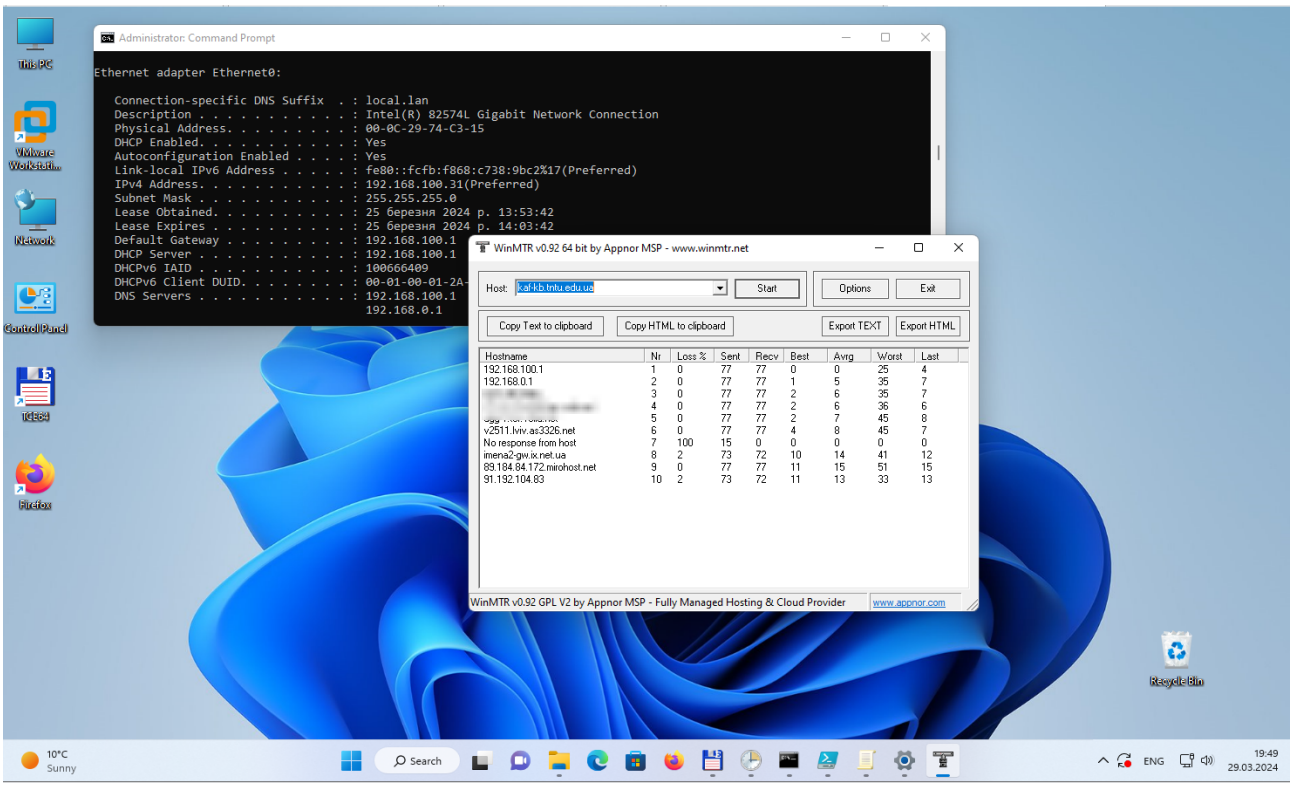

Рисунок 3.17 – Перевірка якості зв’язку з віртуальної машини Windows 11 при активованому захисному механізмі від DDoS

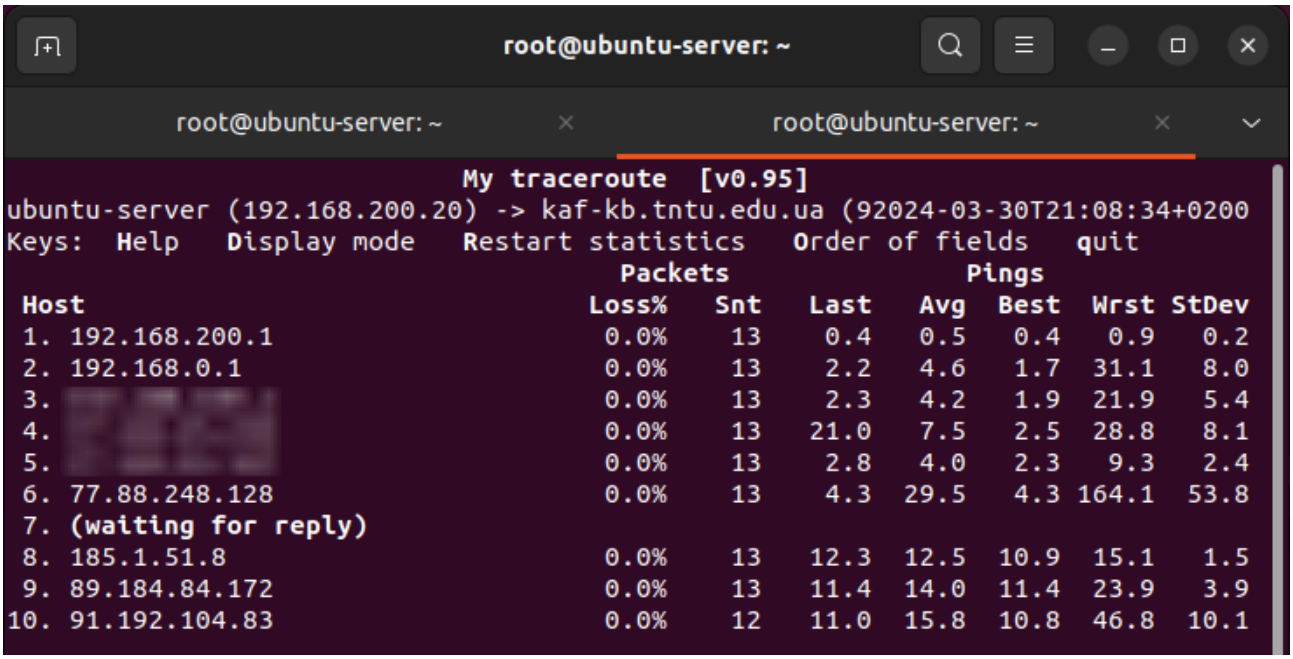

Рисунок 3.18 – Перевірка якості зв’язку з віртуальної машини Ubuntu Linux при активованому захисному механізмі від DDoS

Перевірки показали, що налаштований на маршрутизаторі Mikrotik механізм пом’якшення DDoS атак працює коректно.

3.4 Висновки до розділу

В третьому розділі було проведено моделювання DDoS атак за допомогою утиліту hping3 в операційній системі Parrot Security. Було здійснено Ping Flood атаку на IP-адресу маршрутизатора Mikrotik, SYN Flood атаку на вебсервер Ubuntu Linux та UDP Flood атаку на IP-адресу Ubuntu Linux. У всіх трьох випадках спостерігалось значне використання ресурсів CPU маршрутизатора Mikrotik та відсутність зв’язку з мережею Інтернет з тестових віртуальних машин Windows 10, Windows 11 та Ubuntu Linux. У випадку SYN Flood атаки на вебсервер Ubuntu Linux була переповнена черга для вхідних з’єднань, що призвело до неможливості вебсервером обробляти легітимні запити.

Було налаштовано механізм пом'якшення DDoS атак на маршрутизаторі MikroTik за допомогою брандмауера. Проведено тестування налаштовувань за допомогою одночасного здійснення Ping Flood, SYN Flood та UDP Flood атаки з Parrot Security Atacker1, Atacker2 та Atacker3.

Перевірки показали, що налаштований на маршрутизаторі Mikrotik механізм пом’якшення DDoS атак працює коректно.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при ураженні електричним струмом

Українське законодавство містить низку положень, що регулюють питання долікарської допомоги при ураженні електричним струмом.

Зокрема, Закон України "Про охорону праці" від 14.10.1992 № 2694-XII зобов'язує роботодавців забезпечувати безпеку та охорону праці працівників, в тому числі і при роботі з електроустановками. Роботодавець має забезпечити належний стан та регулярну перевірку електроустановок, використовувати електрообладнання, яке відповідає вимогам безпеки та має сертифікат відповідності [19].

Для забезпечення безпеки під час роботи з ПК, на робочому місці повинні бути встановлені заходи технічного захисту від електричного струму. Закон України "Про охорону праці" встановлює вимоги щодо надання працівникам інструктажу з охорони праці та безпеки під час роботи з електроустановками.

У випадку, коли в результаті ураження електричним струмом сталася смерть або тілесні ушкодження потерпілого, винна особа може бути притягнута до кримінальної відповідальності відповідно до Кримінального кодексу України.

Наказ Міністерства охорони здоров'я України від 09.03.2022 р. № 441 " Про затвердження порядків надання домедичної допомоги особам при невідкладних станах" встановлює порядки надання долікарської допомоги особам при невідкладних станах, в тому числі у разі ураження електричним струмом [20].

Отже, у випадку ураження електричним струмом, долікарська допомога має невідкладний характер та повинна надаватися на місці події.

Ось послідовність дій, які потрібно виконати:

1) Припинити контакт з джерелом струму. Для цього можна вимкнути лінію живлення, виключити пристрій, що спричиняє ураження або від'єднати жертву від джерела струму за допомогою ізольованого предмета (наприклад, дерев'яної палиці, резинової шини).

2) Перед наданням допомоги переконатися у відсутності небезпеки для себе, оточуючих, постраждалого та тільки за її відсутності перейти до наступного кроку.

3) Якщо постраждалий у свідомості, заспокоїти та пояснити свої наступні дії.

4) Здійснити виклик екстреної медичної допомоги та дотримуватись вказівок диспетчера прийому виклику.

5) Забезпечити постійний нагляд за постраждалим до приїзду бригади екстреної (швидкої) медичної допомоги.

6) При погіршенні стану постраждалого до приїзду бригади екстреної (швидкої) медичної допомоги повторно здійснити виклик екстреної медичної допомоги.

7) За можливості зібрати у постраждалого чи оточуючих максимально можливу інформацію стосовно обставин отримання травми. Всю отриману інформацію передати працівникам бригади екстреної (швидкої) медичної допомоги або диспетчеру служби екстреної медичної допомоги.

8) Якщо до приїзду бригади екстреної (швидкої) медичної допомоги постраждалий втратив свідомість, слід перейти до Порядку надання домедичної допомоги дорослим при раптовій зупинці кровообігу або Порядку надання домедичної допомоги дітям при раптовій зупинці кровообігу, затверджених наказом Міністерства охорони здоров’я України від 09 березня 2022 року № 441.

Потерпілий може мати різні види ушкоджень: від легких опіків до серйозних травм та порушень функцій внутрішніх органів. Необхідність подальшого лікування та реабілітації залежить від ступеня тяжкості ушкодження.

Отже, долікарська допомога при ураженні електричним струмом має важливе значення для збереження життя та здоров'я потерпілого. Важливо дотримуватися вимог законодавства та правил безпеки праці при роботі з електричними установками, щоб запобігти подібним випадкам та забезпечити безпеку праці на виробництві.

4.2 Зниження стресу та покращення психологічного благополуччя працівників

Психофізіологічне розвантаження є одним з варіантів зменшення стресу.

Дана практика включає в себе застосування методу аутогенного тренування, що передбачає свідоме використання комплексу прийомів психічної саморегуляції та виконання простих фізичних вправ зі словесним самонавіюванням. Основна увага приділяється розслабленню м'язів (релаксації).

Під час сеансів психофізіологічного розвантаження рекомендується використовувати три періоди, що відповідають фазам відновлення:

Перший період - абстрагування від виробничого середовища, що відповідає фазі залишкового збудження. В цей час відтворюється повільна мелодійна музика та звуки пташиного співу. Працівники знаходять зручну позу та психологічно готуються до наступних періодів.

Другий період - заспокоєння, що відповідає фазі відновлювального гальмування. Показуються фотослайди з зображеннями природи, таких як квітучі луки, березові гаї, ставки і т.д. Звуковий супровід включає спокійну музику та заспокійливі формули аутогенного тренування.

Третій період - активізація, що відповідає фазі підвищеної збудженості. Спочатку світло повністю вимикається, а потім на екрані появляється червона пляма, розмір і яскравість якої поступово збільшуються. В кінці періоду звучить бадьора музика, а працівники виконують мобілізуючі формули аутогенного тренування, попередньо зробивши глибоке вдихання та видихання.

Сеанси психофізіологічного розвантаження можуть проводитись за єдиною програмою через індивідуальні навушники і складатись із двох періодів по 5 хвилин кожний: повне розслаблення та активізація працездатності. При необхідності, на фоні музики можуть використовуватись фрази, що сприяють відпочинку, покращенню самопочуття та бадьорості на заключному етапі. Після сеансів психофізіологічного розвантаження працівники відчувають зменшення втоми, з'являється бадьорість та гарний настрій, а загальний стан помітно поліпшується.

Додатково до сеансів психофізіологічного розвантаження, працівники також можуть скористатись іншими методами для зниження стресу та покращення психологічного благополуччя.

Одним з ефективних підходів є впровадження регулярних перерв під час робочого дня. Це можуть бути короткі паузи, під час яких працівники займаються розслаблюючими вправами, дихальними техніками або просто відпочивають. Це допомагає знизити напругу і покращити фокусування під час робочого процесу.

Також важливо створити комфортне робоче середовище для працівників. Це може включати забезпечення комфортних стільців і столів, добре освітлення та достатню вентиляцію. Природне освітлення та наявність рослин у приміщенні також можуть позитивно вплинути на настрій та самопочуття працівників.

Підтримка від керівництва та колег також має важливе значення. Створення сприятливого та підтримуючого робочого середовища, де працівники можуть відчути підтримку та співпрацю, сприяє зниженню стресу та покращує загальний настрій в колективі.

Крім того, особисте самоуправління і здібність до саморегуляції є важливими навичками для працівників. Це включає уміння регулювати власні емоції, реагувати на стресові ситуації та знаходити способи їх подолання, наприклад, за допомогою медитації, йоги або інших релаксаційних технік.

Усі ці підходи сприяють створенню здорової та продуктивної робочої атмосфери, де працівники можуть ефективно керувати стресом, забезпечуючи своє фізичне та емоційне благополуччя.

ВИСНОВКИ

Під час написання бакалаврської кваліфікаційної роботи була створена та протестована система для зменшення впливу DDoS-атак, що базується на маршрутизаторі Mikrotik CHR. Робота включала аналіз різноманітних методів DDoS-атак, вивчення їхнього впливу на мережеву інфраструктуру та виявлення методів захисту, які можуть ефективно пом'якшити ці атаки.

В першому розділі роботи було проведено детальний аналіз різних типів DDoS-атак, їхніх характеристик та впливу на окремі рівні моделі OSI. Було досліджено HTTP Flood, DNS Amplification, TCP SYN Flood, UDP Flood, Ping Flood та IP Fragmentation, розглянуті їхні особливості та методи протидії.

У другому розділі було розроблено та налаштовано тестове середовище на основі гіпервізора VMware для моделювання DDoS атак з маршрутизатором Mikrotik CHR, як базовим компонентом. Створена інфраструктура включала в себе такі додаткові компоненти, як віртуальна машина Ubuntu Linux з вебсервером, а також віртуальні машини Windows 10, Windows 11 та Parrot Security для моделювання DDoS атак.

У третьому розділі було проведено моделювання DDoS атак за допомогою утиліти hping3 в операційній системі Parrot Security. Було здійснено ping flood, SYN flood та UDP flood атаки на інфраструктуру, а також налаштовано механізми захисту на маршрутизаторі Mikrotik для пом'якшення впливу цих атак.

Результати тестування показали, що розроблені та налаштовані механізми захисту на маршрутизаторі Mikrotik CHR є достатньо ефективними для зменшення впливу DDoS атак. Вони дозволяють виявляти та фільтрувати небезпечний трафік, що допомагає забезпечити стабільну та безпечну роботу мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is a DDoS Attack. URL: https://aws.amazon.com/shield/ddos-attack-protection/ (дата звернення: 04.02.2024).
2. Application layer DDoS attack URL: https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/.html (дата звернення: 04.02.2024).
3. Ванца, В., Тимощук, В., Стебельський, М., & Тимощук, Д. (2023). МЕТОДИ МІНІМІЗАЦІЇ ВПЛИВУ SLOWLORIS АТАК НА ВЕБСЕРВЕР. Матеріали конференцій МЦНД, (03.11. 2023; Суми, Україна), 119-120.
4. SYN flood attack URL: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/ (дата звернення: 04.02.2024).
5. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków, Poland), 130-130.
6. UDP flood attack. URL: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/ (дата звернення: 04.02.2024).
7. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.
8. How do layer 3 DDoS attacks work. URL: https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/ (дата звернення: 04.02.2024).
9. What Is a DDoS Attack. URL: https://info.support.huawei.com/info-finder/encyclopedia/en/DDoS+Attack.html (дата звернення: 04.02.2024).
10. Nataliya Zagorodna, Iryna Kramar (2020). Economics, Business and Security: Review of Relations. Business Risk in Changing Dynamics of Global Village BRCDGV-2020: Monograph / Edited by Pradeep Kumar, Mahammad Sharif. India, Patna: Novelty & Co., Ashok Rajpath,. 446 p., pp.25-39.

11. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276.

12. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.

13. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 04.02.2024).

14. Cloud Hosted Router, CHR. URL: https://help.mikrotik.com/docs/display/ROS/Cloud+Hosted+Router%2C+CHR (дата звернення: 04.02.2024).

15. Ubuntu Server documentation. URL: https://ubuntu.com/server/docs (дата звернення: 04.02.2024).

16. What is ParrotOS. URL: https://www.parrotsec.org/docs/introduction/what-is-parrot (дата звернення: 04.02.2024).

17. hping3 – Active Network Smashing Tool. URL: https://securiumsolutions.com/hping3-active-network-smashing-tool/ (дата звернення: 04.02.2024).

18. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). СИСТЕМА ЗМЕНШЕННЯ ВПЛИВУ DOS-АТАК НА ОСНОВІ MIKROTIK. Матеріали конференцій МЦНД, (17.05. 2024; Ужгород, Україна), 198-200.

19. Закон України "Про охорону праці" від 14.10.1992 № 2694-XII, Version 1. URL: https://zakon.rada.gov.ua/laws/show/2694-12#Text (дата звернення: 04.02.2024).

20. Про затвердження порядків надання домедичної допомоги особам при невідкладних станах. URL: https://zakon.rada.gov.ua/laws/show/z0356-22#n769 (дата звернення: 04.02.2024).

ДОДАТКИ

Додаток А Параметри налаштування Mikrotik для пом’якшення DDoS атак

```
[admin@MikroTik] > ip firewall filter print detail
Flags: X - disabled, I - invalid; D - dynamic
 0     ;;; accept established
       chain=input action=accept connection-state=established

 1     ;;; accept related
       chain=input action=accept connection-state=related

 2     ;;; allow Winbox
       chain=input action=accept protocol=tcp in-interface=ether1 port=8291 log=no
       log-prefix=""

 3     ;;; allow ICMP
       chain=input action=accept protocol=icmp src-address=192.168.0.0/24
       in-interface=ether1 log=no log-prefix=""

 4     ;;; Protection against DDoS
       chain=forward action=jump jump-target=detect-ddos connection-state=new
       in-interface=ether1 log=no log-prefix=""

 5     ;;; Protection against DDoS
       chain=input action=jump jump-target=detect-ddos connection-state=new
       in-interface=ether1 log=no log-prefix=""

 6     ;;; Allow
       chain=detect-ddos action=return src-address=192.168.0.1

 7     ;;; Protection against ICMP Flood
       chain=detect-ddos action=return protocol=icmp
       dst-limit=2000,2000,src-and-dst-addresses/10s log=no log-prefix=""

 8     ;;; Protection against SYN Flood
       chain=detect-ddos action=return tcp-flags=syn protocol=tcp
       dst-limit=200,300,src-and-dst-addresses/10s log=no log-prefix=""

 9     ;;; Protection against SYN-ACK Flood
       chain=detect-ddos action=return tcp-flags=syn,ack protocol=tcp
       dst-limit=200,300,src-and-dst-addresses/10s log=no log-prefix=""

10     ;;; Protection against DDoS
       chain=detect-ddos action=return dst-limit=200,300,src-and-dst-addresses/10s
       log=no log-prefix=""

11     ;;; Protection against DDoS
       chain=detect-ddos action=add-dst-to-address-list address-list=ddos-targets
       address-list-timeout=10m

12     ;;; Protection against DDoS
       chain=detect-ddos action=add-src-to-address-list address-list=ddos-attackers
       address-list-timeout=10m

13     ;;; drop invalid
       chain=input action=drop connection-state=invalid

14     ;;; allow SSH
       chain=input action=accept protocol=tcp in-interface=ether1 port=22

15     ;;; allow HTTP
       chain=input action=accept protocol=tcp in-interface=ether1 port=80
```

```
16    ;;; allow HTTPS
      chain=input action=accept protocol=tcp in-interface=ether1 port=443

17    ;;; block everything else
      chain=input action=drop in-interface=ether1

18    ;;; accept established
      chain=forward action=accept connection-state=established

19    ;;; accept related
      chain=forward action=accept connection-state=related

20    ;;; drop invalid
      chain=forward action=drop connection-state=invalid

21    ;;; DMZ allow
      chain=forward action=accept src-address=192.168.0.0/24
      dst-address=192.168.200.0/24 in-interface=ether1 log=no log-prefix=""

22    ;;; allow from parrot OS to DMZ
      chain=forward action=accept src-address=151.151.151.1
      dst-address=192.168.200.0/24 in-interface=ether1

23    chain=forward action=accept src-address=152.152.152.1 dst-address=192.168.200.0/2>
      in-interface=ether1

24    chain=forward action=accept src-address=153.153.153.1 dst-address=192.168.200.0/2>
      in-interface=ether1

25    ;;; drop access to clients behind NAT from WAN
      chain=forward action=drop connection-state=new in-interface=ether1

[admin@MikroTik] >

[admin@MikroTik] > ip firewall raw  print detail
Flags: X - disabled, I - invalid; D - dynamic
 0    ;;; Protection against DDoS
      chain=prerouting action=drop log=no log-prefix=""
      src-address-list=ddos-attackers dst-address-list=ddos-targets
[admin@MikroTik] >
```

```
[admin@MikroTik] > ip firewall address-list print detail
Flags: X - disabled, D - dynamic
 0   ;;; Protection against DDoS
     list=ddos-attackers address=0.0.0.0 creation-time=mar/20/2024 20:35:29

 1   ;;; Protection against DDoS
     list=ddos-targets address=0.0.0.0 creation-time=mar/20/2024 20:35:33
[admin@MikroTik] >
```