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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Порівняльний аналіз сигнатурних та поведінкових підходів при реалізації IPS

Виконав: студент IV курсу, групи СН-42
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

_____ Колдриш В.А.
(підпис) (прізвище та ініціали)

Керівник _____ Никитюк В.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Тимощук Д.І.
(підпис) (прізвище та ініціали)

Тернопіль
2025

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

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

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«___» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Колдришу Вадиму Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Порівняльний аналіз сигнатурних та поведінкових підходів при реалізації IPS

Керівник роботи Никитюк Вячеслав Вячеславович, к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*07*» *травня* *2025* року № *4/7-444*

2. Термін подання студентом завершеної роботи 24 червня 2025р.

3. Вихідні дані до роботи Методи виявлення вторгнень. Сигнатурні та поведінкові підходи. Інструменти pfSense та Suricata. Сценарії атак. Операційні системи Ubuntu Linux та Kali Linux.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1) Теоретичні основи систем запобігання вторгненням
2) Налаштування лабораторного середовища тестування IPS
3) Практичне тестування сигнатурних та поведінкових підходів в IPS
4) Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2. Актуальність дослідження. 3. Мета, Об'єкт, Предмет дослідження. 4. Завдання дослідження. 5. Схема під'єднання елементів системи. 6. Характеристика мікрокомп'ютера та мікроконтролера. 7. Характеристика давачів системи. 8. Характеристика давачів системи (продовження). 9. Вибір мови програмування та налаштування Arduino. 10. Налаштування MQTT та створення Telegram-bot на Raspberry Pi Zero 2 W. 11. Розробка корпусу для монтажу та вставлення системи. 12. Перевірка роботи системи. 13. Висновки. 14. Завершальний.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Окіпний Ігор Богданович, к.т.н. зав. кафедри МТ	12.06.2024	14.06.2024

7. Дата видачі завдання 29 січня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	30.01.2024	*Виконано*
2.	Підбір джерел по темі кваліфікаційної роботи	31.01.2024-03.02.2024	*Виконано*
3.	Опрацювання джерел по темі кваліфікаційної роботи	04.02.2024-06.02.2024	*Виконано*
4.	Виконання дослідження щодо огляду, впровадження	07.02.2024-11.02.2024	*Виконано*
	і тестування сигнатурного та поведінкового підходів		
	в IPS		
5.	Оформлення розділу «Теоретичні основи систем	03.06.2024-05.06.2024	*Виконано*
	запобігання вторгненням»		
6.	Оформлення розділу «Налаштування лабораторного	06.06.2024-08.06.2024	*Виконано*
	середовища тестування IPS»		
6.	Оформлення розділу «Практичне тестування	09.06.2024-11.06.2024	*Виконано*
	сигнатурних та поведінкових підходів в IPS»		
7.	Виконання завдання до розділу «Безпека життєдіяльності»	12.06.2024-13.06.2024	*Виконано*
8.	Виконання завдання до підрозділу «Основи охорони	14.06.2024-15.06.2024	*Виконано*
	праці»		
9.	Оформлення кваліфікаційної роботи	16.06.2024-17.06.2024	*Виконано*
10.	Нормоконтроль	18.06.2024-19.06.2024	*Виконано*
11.	Перевірка на плагіат	20.06.2024	*Виконано*
12.	Попередній захист кваліфікаційної роботи	21.06.2024	*Виконано*
13.	Захист кваліфікаційної роботи	30.06.2024	

Студент _____ Колдриш В.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Никитюк В.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Порівняльний аналіз сигнатурних та поведінкових підходів при реалізації IPS // Кваліфікаційна робота освітнього рівня «Бакалавр» // Колдриш Вадим Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СН-42 // Тернопіль, 2025 // С.73, рис. – 32, табл. – 0, кресл. – 14, додат. – 2, бібліогр. – 35.

Ключові слова: pfSense, IPS, Suricata, Kali Linux, Ubuntu Linux, сигнатури, аномалії.

У кваліфікаційній роботі бакалавра досліджено ефективність сигнатурного та поведінкового підходів до виявлення та запобігання мережевим атакам з використанням системи IPS Suricata, інтегрованої в маршрутизатор pfSense. Робота присвячена аналізу, налаштуванню та практичному тестуванню обох методів у віртуальному лабораторному середовищі на основі VMware Workstation.

У першому розділі розглянуто принципи роботи IDS/IPS, переваги й недоліки сигнатурного та поведінкового підходів, а також функціональні можливості Suricata. У другому розділі детально описано архітектуру та налаштування лабораторного середовища, встановлення pfSense, конфігурацію мережевих інтерфейсів та інтеграцію IPS Suricata. У третьому розділі здійснено практичне моделювання типових мережевих атак і проведено аналіз ефективності виявлення кожним із підходів.

Результати дослідження свідчать про високу точність сигнатурного методу у виявленні відомих атак, а також про гнучкість поведінкового аналізу при фіксації аномальної активності. Обґрунтовано доцільність використання комбінованого підходу як більш ефективного рішення для сучасних мережевих середовищ.

ANNOTATION

Comparative analysis of signature and behavioural approaches to IPS implementation // Qualification work of the educational level "Bachelor" // Vadym Koldrysh // Ternopil Ivan Pulyu National Technical University, Computer and Information Systems and Software Engineering Faculty, Computer Sciences Department, group SN-42 // Ternopil, 2025 // P. 73, fig. - 32, tabl. - 0, drawings - 14, annexes. – 2, references - 35.

Keywords: pfSense, IPS, Suricata, Kali Linux, Ubuntu Linux, signatures, behavioural.

The bachelor's thesis investigates the effectiveness of signature and behavioural approaches to detecting and preventing network attacks using the Suricata IPS system integrated into the pfSense router. The work focuses on the analysis, configuration, and practical testing of both methods in a virtual lab environment based on VMware Workstation.

The first section discusses the principles of IDS/IPS, the advantages and disadvantages of signature and behavioural approaches, and the functional capabilities of Suricata. The second section describes in detail the architecture and setup of the lab environment, installation of pfSense, configuration of network interfaces, and integration of Suricata IPS. The third section provides a practical simulation of typical network attacks and analyses the detection efficiency of each approach.

The results of the study demonstrate the high accuracy of the signature method in detecting known attacks, as well as the flexibility of behavioural analysis in detecting anomalous activity. The expediency of using a combined approach as a more effective solution for modern network environments is substantiated.

ПЕРЕЛІК СКОРОЧЕНЬ

IPS (англ. Intrusion Prevention System) - Система запобігання вторгненням.

IDS (англ. Intrusion Detection System) - Система виявлення вторгнень.

DoS (англ. Denial of Service) - Відмова в обслуговуванні.

DDoS (англ. Distributed Denial of Service) - Розподілена відмова в обслуговуванні.

DNS (англ. Domain Name System) - Система доменних імен.

NTP (англ. Network Time Protocol) - Протокол мережної синхронізації часу.

TCP (англ. Transmission Control Protocol) - Протокол керування передачею

UDP (англ. User Datagram Protocol) - Протокол дейтаграм користувача.

WAN (англ. Wide Area Network) - Глобальна мережа.

LAN (англ. Local Area Network) - Локальна мережа.

HTTP (англ. HyperText Transfer Protocol) — Протокол передавання гіпертексту.

TLS (англ. Transport Layer Security) — Захист транспортного рівня.

ЗМІСТ

ВСТУП 8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ЗАПОБІГАННЯ ВТОРГНЕННЯМ 10
1.1 Типи атак та їх наслідки 10
1.2 Поняття і місце IPS у забезпеченні мережевої безпеки 21
1.3 Огляд сигнатурного та поведінкового підходів в IPS 24
1.4 Висновок до першого розділу 27
РОЗДІЛ 2. НАЛАШТУВАННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА ТЕСТУВАННЯ IPS 29
2.1 Архітектура лабораторного середовища 29
2.2 Компоненти лабораторного середовища 31
2.2.1 Гіпервізор VMware Workstation Professional 31
2.2.2 Маршрутизатор pfSense 33
2.2.3 Система IPS Suricata 37
2.2.4 Операційна система Ubuntu Linux 42
2.2.5 Операційна система Kali Linux 45
2.3 Висновок до другого розділу 47
РОЗДІЛ 3. ПРАКТИЧНЕ ТЕСТУВАННЯ СИГНАТУРНИХ ТА ПОВЕДІНКОВИХ ПІДХОДІВ В IPS 49
3.1 Тестування працездатності лабораторного середовища 49
3.2 Тестування сигнатурного підходу 51
3.3 Тестування поведінкового підходу 57
3.5 Висновок до третього розділу 61
РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ 63
4.1 Природне середовище і його забруднення 63
4.2 Психофізіологічне розвантаження для працівників 65
4.3 Висновок до четвертого розділу 67
ВИСНОВКИ 69

ПЕРЕЛІК ДЖЕРЕЛ 71
ДОДАТКИ

ВСТУП

Актуальність теми. У теперішніх умовах стрімкого розвитку інформаційних технологій та зростання кількості кіберзагроз питання захисту мережевої інфраструктури стає особливо важливим. Системи запобігання вторгненням (IPS) є критичним елементом комплексного захисту, оскільки дозволяють виявляти та блокувати шкідливу активність у режимі реального часу. Серед основних методів роботи IPS-систем виділяють сигнатурний та поведінковий підходи. Кожен із них має свої переваги та обмеження, що визначають їх ефективність у різних сценаріях застосування. Актуальність теми обумовлена необхідністю глибокого аналізу цих підходів, порівняння їх результативності та практичного тестування в умовах, наближених до реальних мережевих середовищ.

Мета і задачі дослідження. Метою кваліфікаційної роботи є аналіз переваг і недоліків сигнатурного та поведінкового підходів у системах запобігання вторгненням, а також оцінка їх ефективності шляхом практичного впровадження та тестування на базі системи Suricata в маршрутизаторі pfSense.

Для досягнення поставленої мети сформульовано такі задачі:

– провести огляд типів мережевих атак і методів захисту від них.

– дослідити принципи функціонування сигнатурного та поведінкового підходів в IPS;

– налаштувати лабораторне середовище для тестування;

– виконати впровадження системи IPS Suricata в маршрутизаторі pfSense;

– виконати практичне тестування сигнатурного та поведінкового підходів до виявлення атак;

– проаналізувати та оцінити результати тестування.

Об’єкт дослідження. Об’єктом дослідження є системи IPS як складова частина комплексного захисту комп’ютерних мереж.

Предмет дослідження. Предметом дослідження є особливості функціонування сигнатурного та поведінкового підходів виявлення атак у системах IPS на прикладі системи Suricata.

Практичне значення одержаних результатів. Практичне значення одержаних результатів полягає у впровадженні IPS-системи на базі відкритого програмного забезпечення. Результати роботи можуть бути використані для підвищення ефективності захисту мереж, а також як основа для подальших досліджень і розробок у сфері інформаційної безпеки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ЗАПОБІГАННЯ ВТОРГНЕННЯМ

1.1 Типи атак та їх наслідки

Атаки на інформаційні системи можуть бути різноманітними за своєю природою, методами реалізації та наслідками для організацій і окремих користувачів. Усі типи атак мають спільну мету - порушити конфіденційність, цілісність або доступність інформації чи ресурсів.

Одним із найбільш поширених типів є атаки на прикладному рівні, до яких належить SQL-ін’єкція [1]. При такій атаці зловмисник вставляє шкідливі SQL-запити у поля вводу веб-додатків, щоб отримати несанкціонований доступ до баз даних (див. рисунок 1.1).

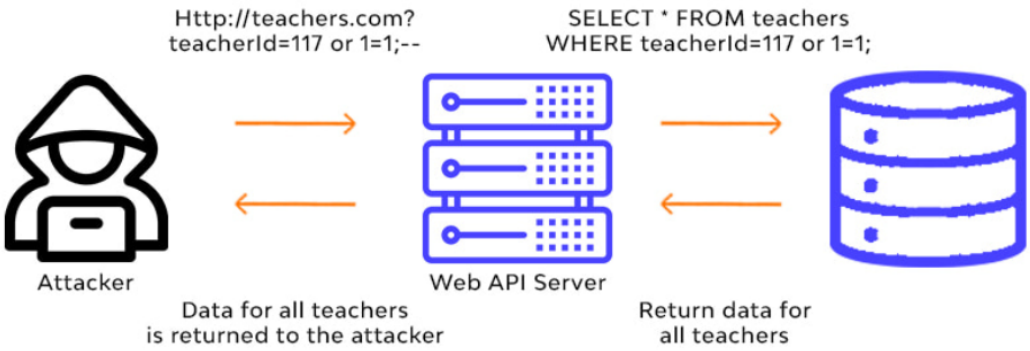

Рисунок 1.1 – Схема виконання атаки SQL-ін’єкція

Це може призвести до витоку персональних даних, знищення чи зміни важливої інформації та серйозної компрометації довіри до організації.

Ще одним поширеним типом атаки є Cross-Site Scripting (XSS) [2]. При XSS атаках зловмисник впроваджує шкідливий скрипт у веб-сторінку, яка потім виконується в браузерах інших користувачів (див. рисунок 1.2).

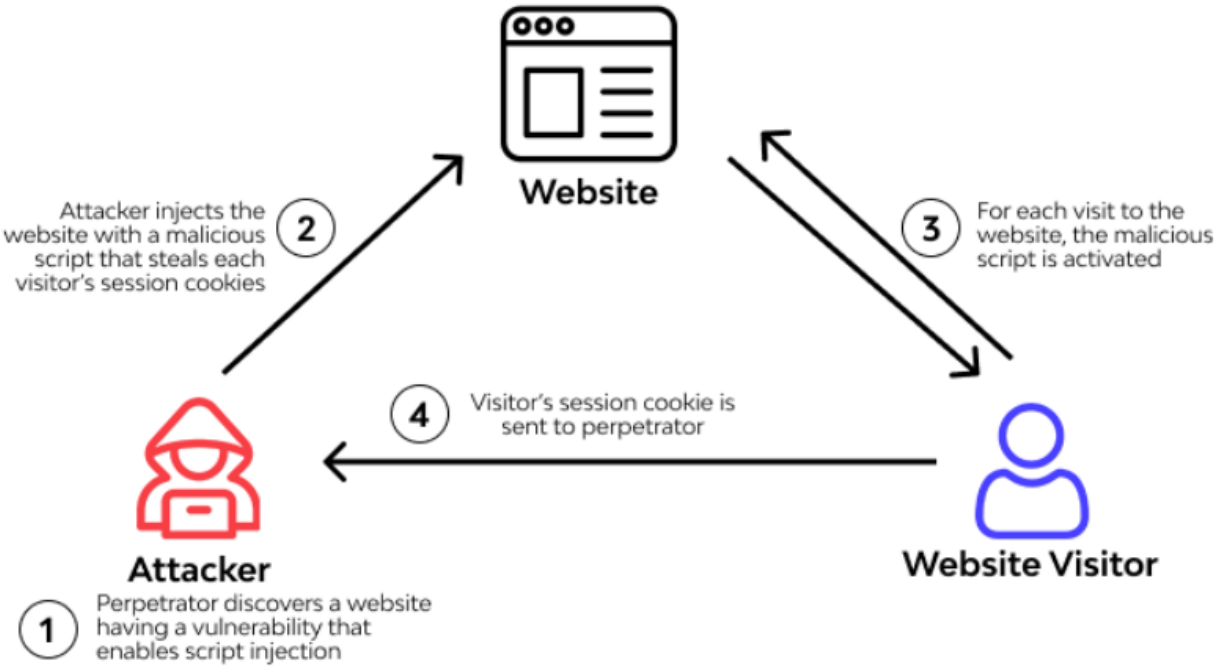

Рисунок 1.2 – Схема виконання атаки Cross-Site Scripting

Це може призвести до крадіжки сесій, облікових даних, перехоплення особистої інформації або перенаправлення користувачів на шкідливі сайти. Такі атаки особливо небезпечні для електронної комерції, банківських платформ і соціальних мереж.

Інший небезпечний тип - атаки типу DoS та DDoS спрямовані на те, щоб вивести з ладу інформаційну систему, мережу або онлайн-сервіс шляхом перевантаження їх запитами або шкідливими діями [3]. У випадку DDoS-атак напад організовується за допомогою великої кількості зламаних пристроїв (ботнетів), що працюють одночасно та координовано (див. рисунок 1.3). Ботнети є одним із найбільш небезпечних і потужних інструментів у сфері кіберзагроз [4]. Вони являють собою мережі заражених пристроїв, які перебувають під контролем зловмисника без відома їхніх власників. До складу ботнетів можуть входити комп'ютери, сервери, смартфони, IoT-пристрої та мережеве обладнання. Кожен заражений пристрій у такій мережі називається ботом або зомбі.

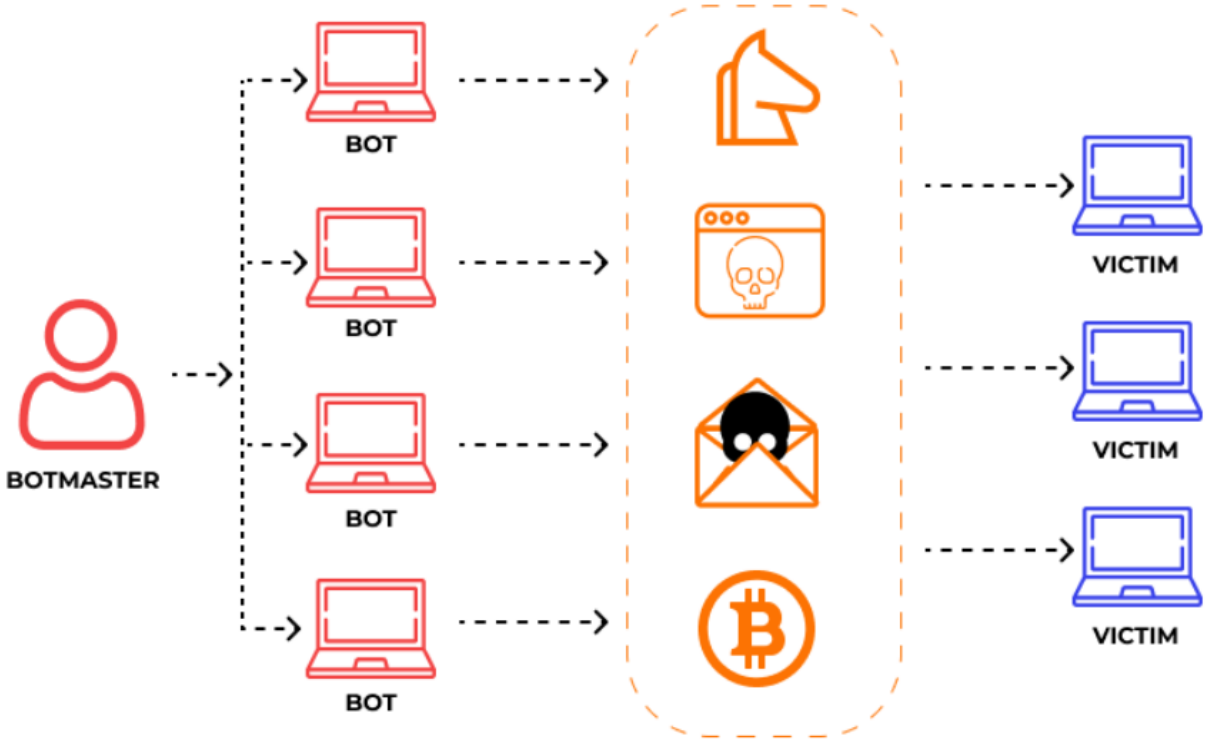

Рисунок 1.3 – Принцип роботи ботнет мережі

Ботнет створюється шляхом розповсюдження шкідливого програмного забезпечення, яке встановлюється на пристрої жертви через фішингові листи, експлойти в додатках або через вразливості в операційних системах. Після зараження пристрій непомітно підключається до командного серверу (Command and Control), який координує дії ботів. У сучасних ботнетах замість централізованих серверів часто використовуються розподілені архітектури типу peer-to-peer або мережі Darknet для підвищення стійкості до виявлення та ліквідації.

Однією з важливих характеристик ботнетів є можливість їх оновлення. Зловмисники можуть надсилати нові команди ботам, змінювати їхню поведінку або завантажувати нові модулі для виконання інших видів атак. Ботнети великого масштабу здатні змінювати правила гри в кіберпросторі, оскільки їх обчислювальна потужність може перевищувати можливості цілого дата-центру.

Прикладами відомих ботнетів є Mirai, який заражав IoT-пристрої та використовував їх для потужних DDoS-атак, і ботнет Emotet, який спочатку

розповсюджував банківські трояни, а згодом еволюціонував у сервіс доставки шкідливого ПЗ для інших кіберзлочинців [5].

Існує кілька основних типів DDoS-атак, які розрізняються за механізмом впливу на цільову систему. Одним із найбільш поширених є атаки на транспортному рівні (Transport Layer 4). Серед них найбільш відомі атаки типу SYN Flood (див. рисунок 1.4) [6,7].

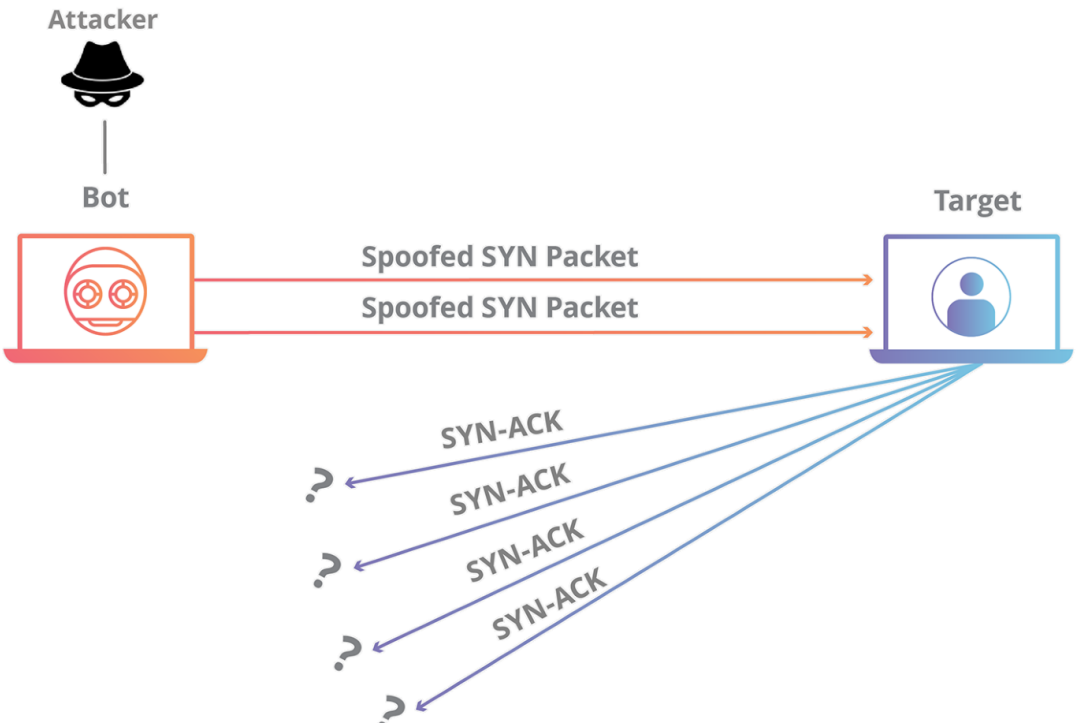

Рисунок 1.4 – Принцип здійснення атаки SYN Flood

Її мета полягає у виснаженні ресурсів сервера або мережевого пристрою шляхом зловживання механізмом встановлення TCP-з'єднань, відомим як триетапне рукостискання (TCP three-way handshake). За стандартною процедурою встановлення з'єднання клієнт надсилає серверу TCP-пакет SYN для ініціації з'єднання. Сервер у відповідь формує SYN-ACK пакет, зберігаючи при цьому інформацію про нове підключення в спеціальній черзі, і чекає фінального підтвердження (ACK) від клієнта. Тільки після отримання ACK-запиту з'єднання вважається повністю встановленим. У випадку SYN Flood зловмисник надсилає велику кількість TCP SYN-запитів, але підробляє адресу

джерела, внаслідок чого відповідь сервера потрапляє неіснуючому або невідповідному хосту. Сервер залишається в очікуванні завершення рукостискання, тримаючи кожне неповне з'єднання у таблиці напіввідкритих сесій. Через обмежену кількість записів у цій таблиці та певні таймаути очікування, надмірна кількість SYN-запитів швидко заповнює ресурси сервера, що призводить до відмови в обслуговуванні нових, легітимних клієнтів.

Інший приклад - UDP Flood атака, коли атакуючий надсилає великий обсяг UDP-пакетів на випадкові порти на сервері (див. рисунок 1.5) [8,9].

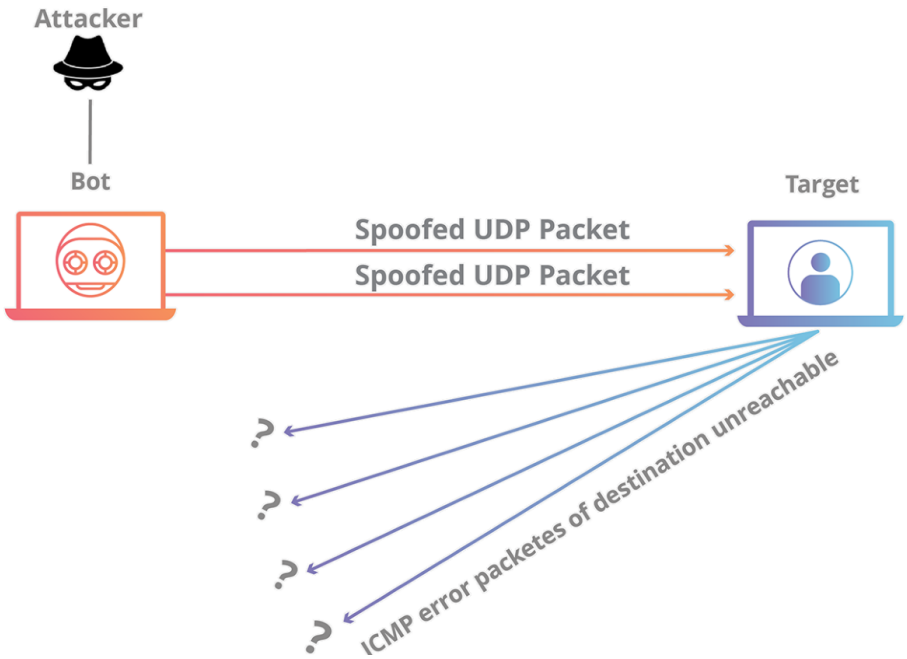

Рисунок 1.5 – Принцип здійснення атаки UDP Flood

Сервер, намагаючись відповісти ICMP-повідомленнями про недоступність портів, витрачає свої ресурси, що може спричинити його перевантаження.

Прикладом DDoS-атаки на мережевому рівні (Network Layer 3) є ICMP Flood (Ping Flood), де величезна кількість запитів ICMP Echo Request ("ping") надсилається для перевантаження каналу зв’язку або процесора цільової машини (див. рисунок 1.6) [10].

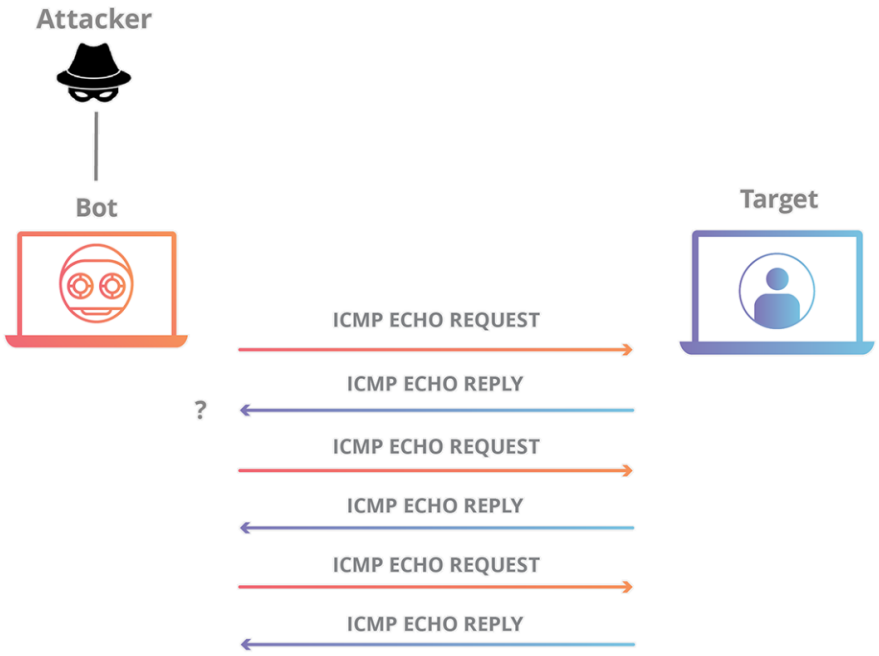

Рисунок 1.6 – Принцип здійснення атаки ICMP Flood

Хоча сучасні сервери краще захищені від простого пінгування, у певних випадках ICMP-атаки можуть бути ефективними.

Окремо виділяють атаки на рівні прикладного протоколу (Application-Layer 7), наприклад HTTP Flood, де ботнет генерує велику кількість HTTP-запитів до веб-сервера (наприклад, запитуючи сторінки, зображення) (див. рисунок 1.7) [12].

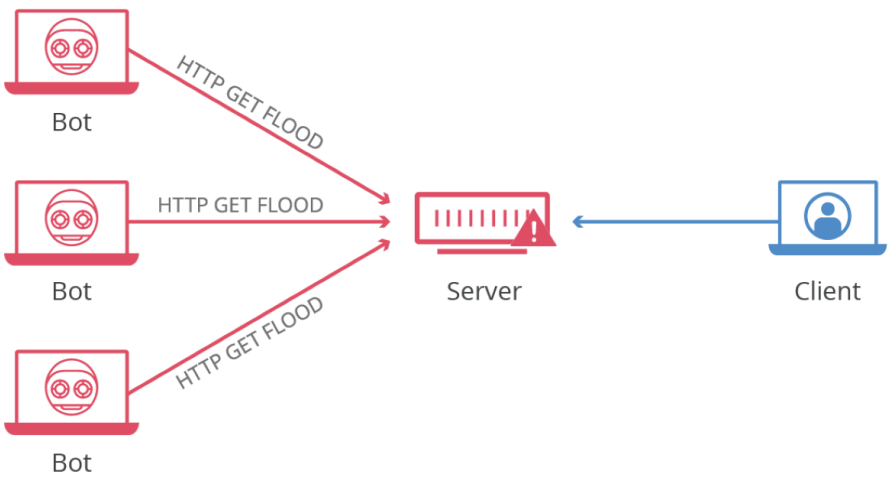

Рисунок 1.7 – Принцип здійснення атаки HTTP Flood

Такі атаки є особливо небезпечними, оскільки їх важко відрізнити від реальної активності користувачів, а навантаження створюється не тільки на мережу, але й на серверні ресурси (пам’ять, процесор, бази даних).

Slowloris атака - це специфічний тип DDoS-атаки на прикладному рівні, який націлений на веб-сервери [12]. На відміну від класичних DDoS-атак, що працюють через масове засилання великої кількості запитів або перенавантаження каналу, Slowloris діє "тихо" і розумно, використовуючи мінімальний обсяг трафіку для виведення сервера з ладу [13].

Суть атаки полягає в тому, що Slowloris надсилає на сервер неповні HTTP-запити, утримуючи TCP-з'єднання відкритими якомога довше. Зловмисник постійно надсилає невеликі частини даних або заголовків HTTP-запиту, але ніколи не завершує їх (див. рисунок 1.8) [14].

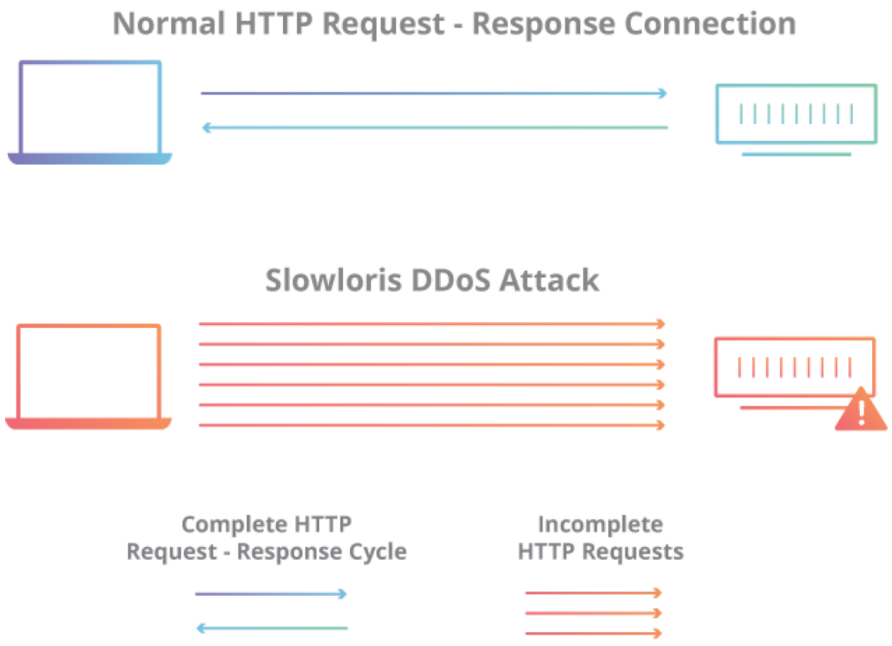

Рисунок 1.8 – Принцип здійснення Slowloris атаки

Сервер, відповідно до протоколу HTTP, змушений зберігати ці неповні з'єднання відкритими, очікуючи завершення запиту, оскільки він не має права закрити його самостійно без відповіді. Як результат, сервер виділяє свої ресурси на обробку численних неповних підключень. Якщо кількість таких

"підвішених" сесій достатньо велика, сервер більше не має змоги обробляти нові легітимні запити від користувачів. Таким чином, сервер перестає бути доступним для реальних клієнтів і фактично відбувається відмова в обслуговуванні.

Існують також атаки підсилення (Amplification Attacks). У цьому випадку зловмисник надсилає невеликий запит до відкритого сервера (DNS-сервера або NTP-сервера), підробляючи IP-адресу жертви, так що відповідь надходить не до атакуючого, а до жертви. Оскільки відповіді у таких протоколах часто у десятки або сотні разів більші за розміром початкового запиту, трафік, який спрямовується до жертви, може бути колосальним. Прикладами є DNS Amplification та NTP Amplification.

Механізм DNS Amplification атаки полягає в тому, що зловмисник використовує відкриті DNS-сервери для створення величезного обсягу трафіку, спрямованого на жертву, при цьому сам генерує лише невелику кількість запитів їх (див. рисунок 1.9) [15].

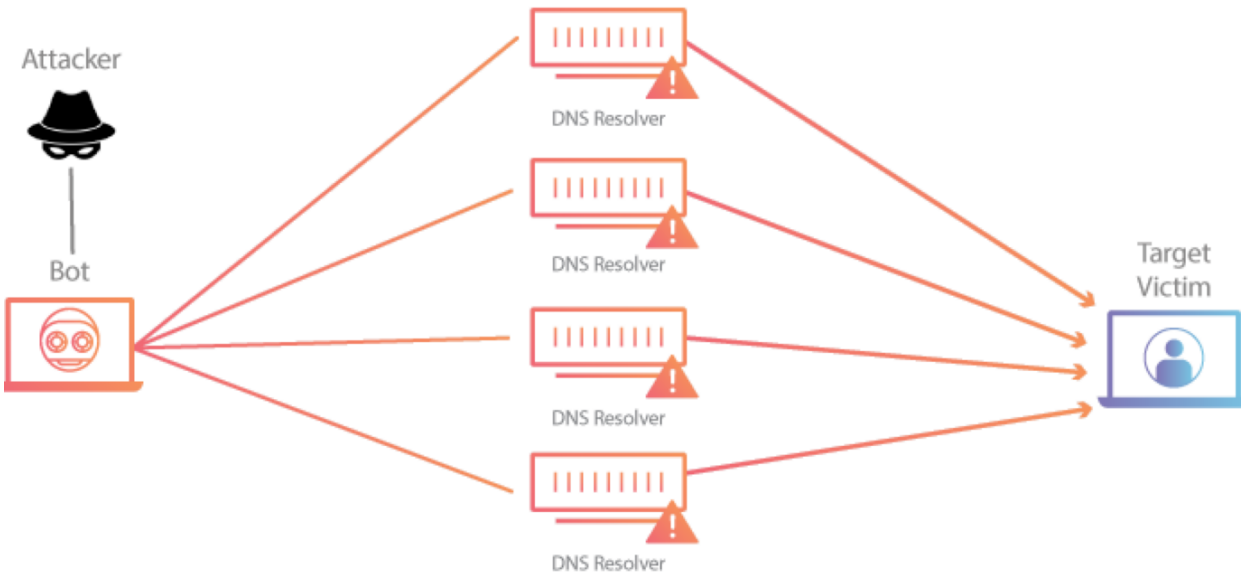

Рисунок 1.9 – Принцип здійснення DNS Amplification атаки

Суть атаки базується на двох ключових особливостях протоколу DNS. По-перше, запити до DNS-серверів є надзвичайно невеликими (кілька байтів),

тоді як відповіді можуть бути значно більшими - у десятки разів. По-друге, протокол DNS працює переважно через UDP, який є протоколом безстану (connectionless) і не вимагає встановлення сесії.

Під час атаки зловмисник надсилає DNS-запити до відкритих рекурсивних DNS-серверів, використовуючи підроблену IP-адресу жертви як джерело запиту. Сервери DNS, нічого не підозрюючи, надсилають об'ємні відповіді безпосередньо на адресу жертви. Оскільки розмір відповіді в багато разів перевищує розмір початкового запиту, обсяг трафіку, що надходить до жертви, зростає експоненційно. Це називається коефіцієнтом ампліфікації, який у випадку DNS може сягати 28 - 54 разів залежно від типу запитів (наприклад, запити типу ANY генерують великі відповіді).

DNS Amplification дозволяє зловмиснику із відносно малими ресурсами створити велике навантаження на мережу або сервер жертви. Ця атака особливо небезпечна тим, що залучає до процесу тисячі сторонніх відкритих DNS-серверів, що значно ускладнює фільтрацію і виявлення джерела первинної атаки. Жертва такої атаки може відчути повне блокування інтернет-каналу через надмірну кількість вхідного UDP-трафіку на порт 53 (DNS), що призводить до недоступності ресурсів, критичних сервісів або навіть виходу з ладу мережевого обладнання.

Основою NTP Amplification атаки є використання відкритих NTP-серверів, які відповідають на специфічні запити надзвичайно великими обсягами інформації [16]. Для цього зловмисник формує спеціальний запит типу monlist або аналогічні команди діагностики, які змушують NTP-сервер надсилати велику кількість інформації у відповідь. Критичним є те, що цей запит надсилається з підробленою IP-адресою, яка вказує на жертву. В результаті сервер направляє свою відповідь не атакуючому, а безпосередньо жертві (див. рисунок 1.10).

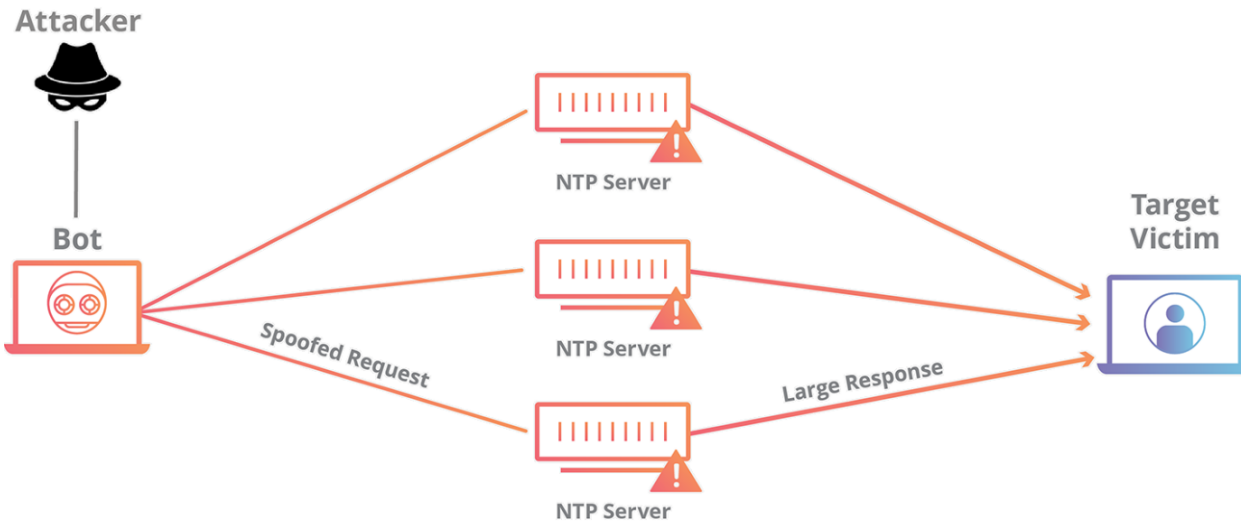

Рисунок 1.10 – Принцип здійснення NTP Amplification атаки

Особливість NTP Amplification полягає в дуже високому коефіцієнті підсилення. Один невеликий за розміром запит (кілька десятків байтів) може генерувати відповідь у десятки або навіть сотні разів більшого розміру. Наприклад, 60-байтний запит може викликати відповідь обсягом понад 4000 байтів. Це дозволяє атакуючим із невеликою кількістю запитів створити надмірне навантаження на канал жертви, що призводить до його перенавантаження, відмови в обслуговуванні і втрати доступності сервісів. NTP Amplification-атаки особливо небезпечні через їхню простоту в реалізації, доступність відкритих NTP-серверів у мережі Інтернет і важкість миттєвого виявлення. Жертва отримує масивний потік легітимних відповідей від реальних серверів, що ускладнює фільтрацію і протидію атаці простими методами.

Наслідком NTP Amplification є істотне перевантаження каналів зв'язку, відмова в обслуговуванні серверів, падіння продуктивності мережевого обладнання або навіть повне припинення роботи інтернет-послуг організації.

Серйозну загрозу становлять атаки типу "людина посередині" (MITM), коли зловмисник перехоплює або змінює комунікацію між двома сторонами без їхнього відома (див. рисунок 1.11) [17].

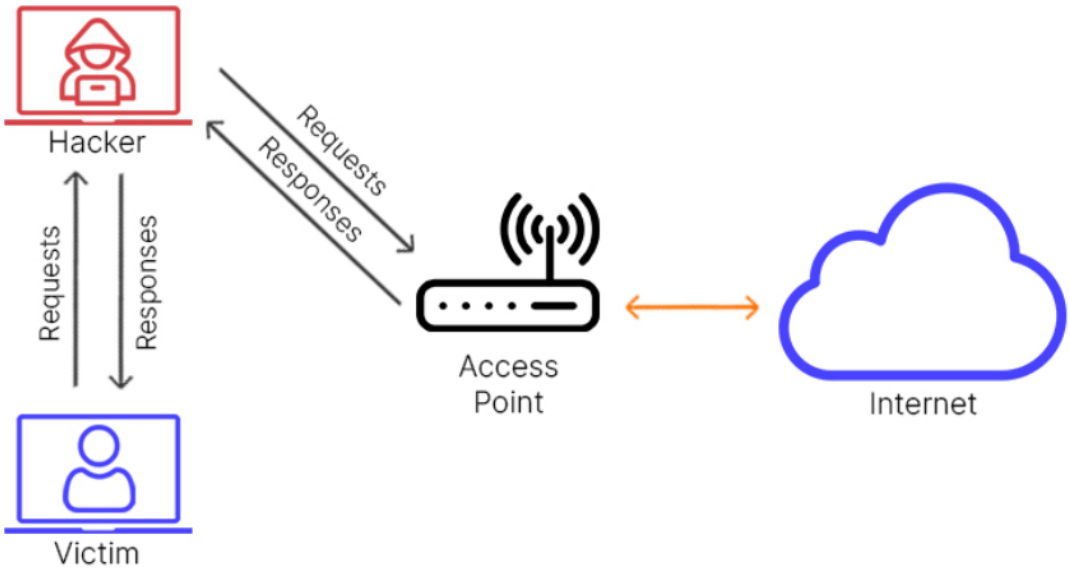

Рисунок 1.11 – Принцип здійснення MITM атаки

Такі атаки часто використовуються для крадіжки облікових даних, фінансової інформації чи інших конфіденційних даних. Наслідками можуть бути не тільки витоки інформації, а й можливість подальших складніших атак, наприклад, несанкціонованого доступу до внутрішніх систем.

Ще одним небезпечним типом є атаки типу brute-force, де автоматизовані скрипти перебирають різні комбінації логінів і паролів для отримання доступу до облікових записів (див. рисунок 1.12) [18,19].

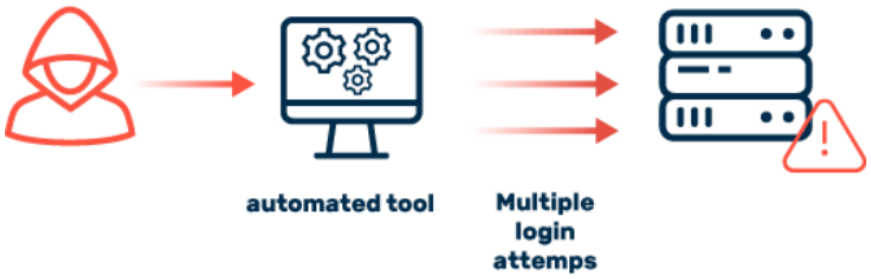

Рисунок 1.12 – Принцип здійснення brute-force атаки

Якщо паролі недостатньо складні, це може призвести до повного контролю над обліковими записами, викрадення службових даних, або навіть розповсюдження шкідливого ПЗ у корпоративній мережі.

Шкідливе програмне забезпечення (malware) - ще одна важлива категорія атак. Віруси, трояни, ransomware, шпигунське ПЗ використовуються для руйнування даних, викрадення інформації, шифрування файлів з метою вимагання викупу або для перетворення зараженої системи в частину великої злочинної мережі. Наслідками таких атак можуть бути втрата критичної інформації, фінансові втрати, тривалі простої роботи систем та значне погіршення репутації компанії.

Фішинг також залишається дуже поширеним методом атак. Зловмисники надсилають електронні листи або повідомлення, які виглядають як офіційні запити від банків, сервісів чи партнерів, змушуючи користувачів передавати конфіденційні дані або встановлювати шкідливе програмне забезпечення. Успішний фішинг може стати початком великого інциденту безпеки, що тягне за собою витік інформації, шахрайство чи подальший розвиток внутрішніх атак.

Наслідки всіх перелічених атак можуть бути катастрофічними для організації. Від прямих фінансових збитків і витрат на відновлення до втрати клієнтів, падіння вартості бренду, юридичних санкцій і кримінальної відповідальності через невиконання нормативних вимог із захисту даних. Тому розуміння типів атак та їхніх потенційних наслідків є основою для побудови ефективної стратегії захисту і мотивує до активного впровадження систем виявлення та запобігання вторгненням у сучасних IT-інфраструктурах.

1.2 Поняття і місце IPS у забезпеченні мережевої безпеки

Системи IDS та системи IPS є важливими складовими мережевої безпеки, проте вони мають різні функціональні призначення та принципи дії [20].

IDS - це система, основною функцією якої є виявлення підозрілої або шкідливої активності в комп’ютерній мережі чи на окремому хості. Вона здійснює моніторинг трафіку або подій у системі та аналізує їх з метою виявлення ознак атак, несанкціонованого доступу або порушення політик

безпеки. IDS зазвичай працює у пасивному режимі: вона лише фіксує підозрілу активність і генерує сповіщення для адміністратора, але не втручається у мережевий трафік чи роботу системи (див. рисунок 1.13) [21].

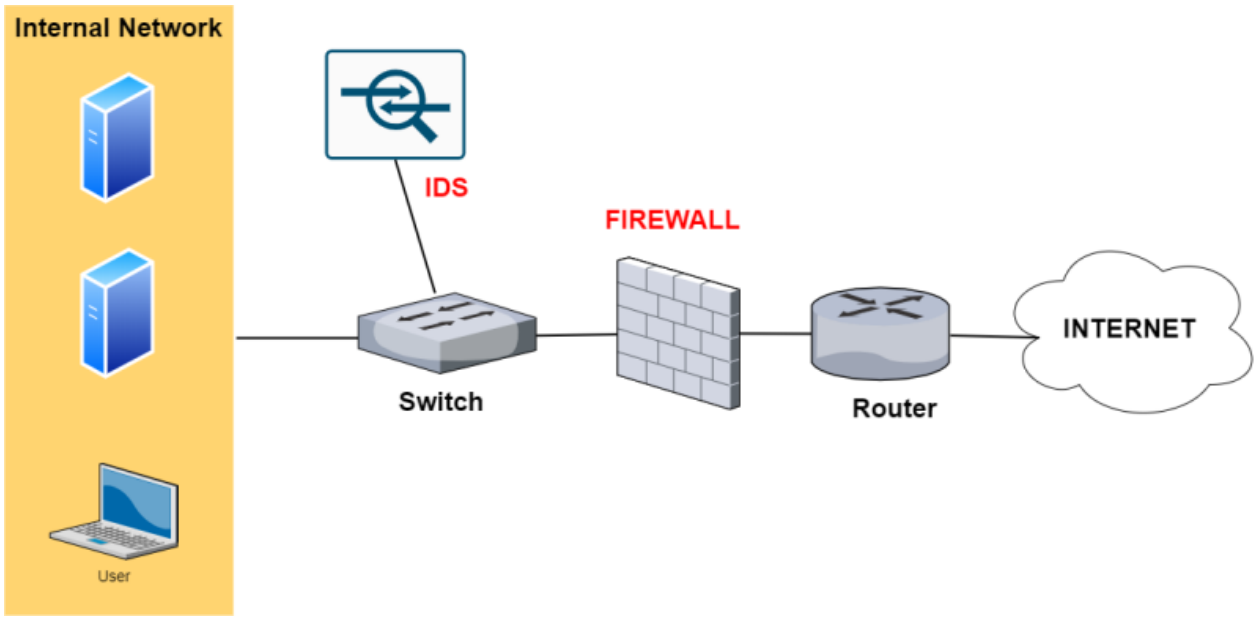

Рисунок 1.13 – Схема розташування IDS

Системи IDS можна поділити на дві основні категорії: мережеві IDS (NIDS), які аналізують мережевий трафік, і хостові IDS (HIDS), що зосереджуються на аналізі подій операційної системи або прикладного ПЗ на конкретних пристроях.

IPS, на відміну від IDS, працює в активному режимі. Система запобігання вторгненням не лише виявляє підозрілу активність, але й автоматично вживає заходів для нейтралізації. IPS встановлюється безпосередньо в ланцюгу передавання даних між пристроями і має змогу припинити сесію, заблокувати IP-адресу атакуючого, змінити політику брандмауера або виконати інші дії для запобігання шкоді (див. рисунок 1.14) [22,23].

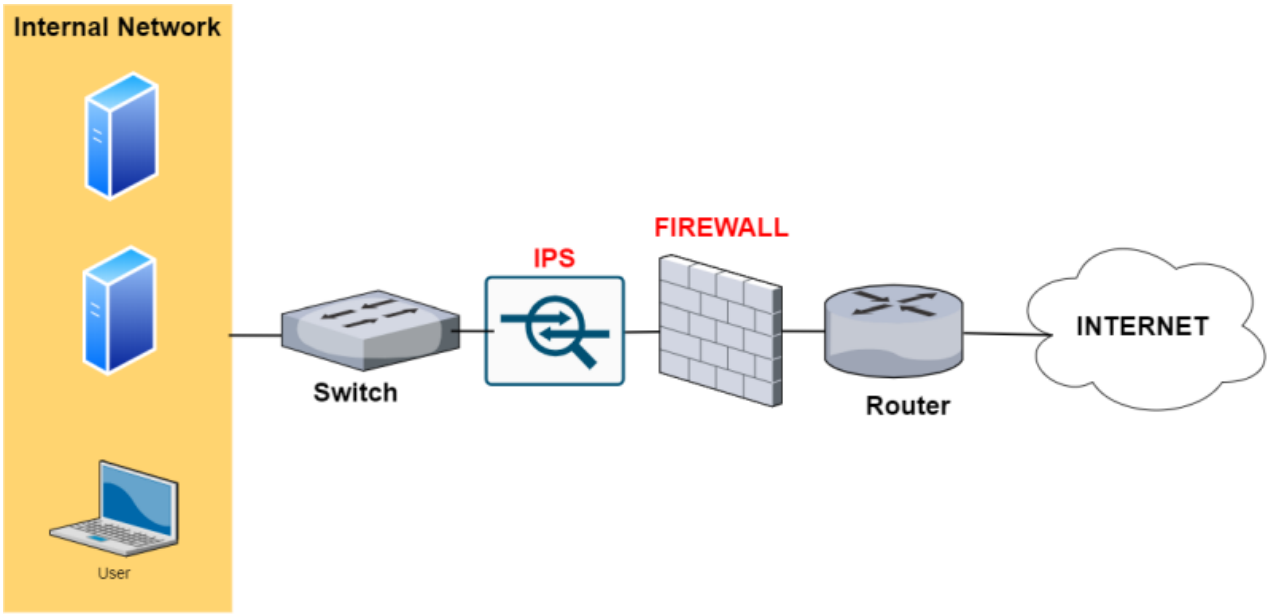

Рисунок 1.14 – Схема розташування IPS

Таким чином, IPS діє як активний захисний механізм, який не лише повідомляє про атаку, а й самостійно зупиняє її в реальному часі.

Незважаючи на те, що IDS і IPS використовують схожі методи аналізу трафіку (сигнатурне виявлення, аналіз аномалій (поведінковий аналіз)), головна різниця полягає у характері їхнього реагування: IDS обмежується виявленням та оповіщенням, тоді як IPS активно втручається для запобігання вторгненням.

Системи IPS виконують ключову роль у забезпеченні проактивного захисту мережі та інформаційних систем. Їх основна функція полягає у виявленні та нейтралізації шкідливої активності ще до того, як вона може завдати шкоди. IPS постійно моніторить мережевий трафік у реальному часі, аналізуючи пакети даних на основі певних правил або моделей поведінки для того, щоб оперативно виявляти ознаки атак, спроб експлуатації вразливостей чи інших підозрілих дій.

Однією з ключових функцій IPS є аналіз і порівняння трафіку з базою відомих сигнатур атак. Це дає змогу системі швидко розпізнавати стандартні атаки, такі як SQL-ін’єкції, спроби отримання несанкціонованого доступу, експлойти операційних систем або мережевого обладнання. Однак IPS не обмежується лише сигнатурним виявленням. Вона також може застосовувати

поведінкові механізми аналізу, які передбачають виявлення аномалій - відхилень від звичайної поведінки користувачів або систем, що можуть свідчити про початок нового типу атаки.

Ще однією важливою функцією є блокування шкідливої активності у режимі реального часу. На відміну від систем IDS, IPS має можливість безпосередньо втручатися в передавання даних. Система може відхилити підозрілий пакет, розірвати з’єднання, змінити маршрутизацію або заборонити доступ певному джерелу. IPS інтегрується з іншими системами безпеки, наприклад, із брандмауерами, і автоматично змінює їхні політики на основі виявлених загроз.

Іншою функцією є ведення журналів і формування сповіщень. Під час роботи IPS записує інформацію про всі виявлені та заблоковані дії, що дає змогу адміністраторам аналізувати інциденти, удосконалювати політики безпеки і планувати подальший захист. Ведення журналів також важливе для відповідності нормативним вимогам (GDPR та PCI DSS), де фіксація подій безпеки є обов'язковою.

IPS також виконує функцію адаптивного захисту. Сучасні системи IPS здатні самостійно оновлювати свої бази правил або поведінкові моделі, базуючись на отриманих даних про нові загрози. Це дозволяє підвищити стійкість мережі навіть у ситуаціях, коли атаки є новими або мають змінений характер.

1.3 Огляд сигнатурного та поведінкового підходів в IPS

Огляд сигнатурного та поведінкового підходів в IPS є важливою частиною розуміння механізмів роботи систем запобігання вторгненням [24]. Кожен із підходів має власні принципи функціонування, переваги та обмеження, що визначають їхню ефективність у різних умовах застосування.

Сигнатурний підхід у системах запобігання вторгненням базується на ідеї ідентифікації атак шляхом порівняння мережевого трафіку або подій із базою

заздалегідь визначених шаблонів, які описують характерні ознаки відомих загроз. Такі шаблони або сигнатури можуть включати в себе конкретні послідовності байтів у пакеті, специфічні патерни запитів, характерні команди протоколів або інші ознаки поведінки атакуючих програм. Принцип роботи сигнатурного підходу нагадує роботу антивірусного програмного забезпечення: система аналізує вхідні дані в реальному часі і шукає збіги з відомими сигнатурами. Якщо збіг знайдено, система реєструє інцидент і заздалегідь визначеним чином реагує - наприклад, блокує з'єднання, сповіщає адміністратора або ізолює атакуючий вузол.

Основною перевагою сигнатурного підходу є його висока швидкість виявлення атак [25]. Оскільки процес аналізу базується на порівнянні із заздалегідь підготовленими шаблонами, обробка запитів є дуже ефективною і не вимагає значних обчислювальних ресурсів. Ще однією важливою перевагою є низький рівень хибних спрацьовувань: оскільки виявлення відбувається на основі точних і специфічних ознак загроз, ризик неправильного визначення легітимного трафіку як шкідливого мінімальний. Це особливо важливо для великих корпоративних мереж, де надмірна кількість помилкових сповіщень може перевантажити персонал служби безпеки і призвести до ігнорування реальних інцидентів. Однак сигнатурний підхід має і свої обмеження. Головним недоліком є його нездатність виявляти нові, невідомі типи атак. Якщо загроза ще не вивчена і її сигнатура не додана до бази даних системи, така атака залишиться непоміченою. Таким чином, ефективність сигнатурного підходу безпосередньо залежить від актуальності і повноти бази сигнатур. Постійне оновлення цієї бази є критичним елементом для підтримання належного рівня захисту, але навіть за умови регулярних оновлень завжди залишається проміжок часу між появою нової загрози і її фіксацією в сигнатурних базах. Це вікно вразливості може бути використане зловмисниками для успішних атак. Крім того, надмірна кількість сигнатур може з часом впливати на продуктивність системи, оскільки кожен запит потрібно перевіряти за зростаючим списком правил.

Поведінковий підхід у системах запобігання вторгненням базується на аналізі поведінки об'єктів у мережі або системі з метою виявлення аномалій, що можуть свідчити про наявність загрози. На відміну від сигнатурного підходу, який шукає чіткі відповідності з відомими шаблонами атак, поведінковий підхід орієнтується на відхилення від встановленої норми. Принцип його роботи полягає в побудові моделей нормальної поведінки для мережевого трафіку, користувачів, серверів чи додатків. Ці моделі формуються на основі спостереження за стандартними операціями упродовж певного часу. Після створення профілю нормальної активності система відстежує всі подальші події, порівнює їх із очікуваною поведінкою та ідентифікує будь-які відхилення як потенційно небезпечні.

Аналіз аномалій може включати в себе моніторинг обсягу трафіку, частоти запитів до певних ресурсів, характеру доступу до файлів, типових маршрутів пересилання даних та інших параметрів. Якщо система фіксує нетипові дії - наприклад, різке зростання обсягу вихідного трафіку, незвичні запити до системних служб або нехарактерну активність у позаробочий час то це розцінюється як сигнал про можливе порушення безпеки. Таким чином, поведінковий підхід не потребує попереднього знання про конкретний тип атаки, що дає йому велику гнучкість у протидії новим загрозам. Основною перевагою поведінкового підходу є його здатність виявляти невідомі атаки, які ще не мають сигнатур або не описані у базах даних. Завдяки аналізу відхилень система може виявити абсолютно нові методи вторгнення, складні атаки нульового дня (zero-day attacks), а також внутрішні загрози, які базуються на зміні поведінки користувачів або систем. Це робить поведінковий підхід незамінним елементом сучасної багаторівневої безпеки, особливо в умовах постійного виникнення нових векторів атак. Водночас поведінковий підхід має низку суттєвих недоліків. Одним із найбільших викликів є висока кількість хибних спрацьовувань. У реальних мережах нормальна поведінка може бути надзвичайно різноманітною і змінюватися залежно від часу доби, типу діяльності чи зовнішніх обставин. Зміни, які не є атаками, але виходять за межі

побудованої моделі, часто сприймаються як загрози, що призводить до великої кількості помилкових попереджень. Це може перевантажити аналітиків безпеки і знизити ефективність реагування на реальні загрози. Ще одним недоліком є складність навчання системи. Побудова адекватних моделей поведінки вимагає значного обсягу даних про нормальну діяльність, що потребує часу і ресурсів. Крім того, потрібно уважно налаштовувати початкові пороги чутливості, щоб уникнути як надлишкового реагування, так і пропуску реальних атак. Підтримка актуальності моделей поведінки також є важливим завданням, оскільки мережеві середовища змінюються, і профілі потрібно адаптувати до нових умов, не втрачаючи при цьому точності виявлення. Використання машинного навчання значно підвищує ефективність поведінкового аналізу. Системи здатні динамічно оновлювати свої моделі у відповідь на зміни в мережевій активності, самонавчатись на основі нових даних та мінімізувати людське втручання у процес налаштування. У багатьох реальних рішеннях поведінковий аналіз поєднується із сигнатурним підходом для досягнення кращого балансу між точністю і здатністю виявляти загрози.

1.4 Висновок до першого розділу

У першому розділі було здійснено теоретичний аналіз основних моментів пов’язаних із системами IPS та сучасними типами кібератак. Огляд типів атак показав, що загрози інформаційним системам можуть мати різноманітний характер. Від атак на прикладному рівні, таких як SQL-ін’єкції та Cross-Site Scripting, до масових DDoS-атак, атак із використанням ботнетів та атак ампліфікації на базі протоколів DNS і NTP. Було розглянуто механізми виконання атак типу SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, Slowloris, а також специфіку атак MITM та brute-force атак. Особлива увага приділена аналізу наслідків атак, які можуть мати критичний вплив на конфіденційність, цілісність і доступність інформаційних ресурсів.

У розділі було розглянуто поняття і місце систем виявлення та запобігання вторгненням у забезпеченні мережевої безпеки. Було показано, що системи IDS виконують пасивний моніторинг і фіксацію підозрілих дій, тоді як IPS негайно блокують виявлені загрози у режимі реального часу. Особливу увагу приділено ключовим функціям IPS: аналізу трафіку за сигнатурами, поведінковому аналізу аномалій, активному втручанню у мережеві процеси для запобігання атакам, а також веденню журналів подій для подальшого аналізу та вдосконалення безпеки. Було детально розглянуто два основні підходи, що використовуються в IPS: сигнатурний та поведінковий. Сигнатурний підхід забезпечує високу швидкість виявлення атак і низький рівень хибних спрацьовувань, але має обмеження у виявленні нових загроз через залежність від актуальності бази сигнатур. Поведінковий підхід базується на аналізі відхилень від нормальної поведінки та дозволяє виявляти невідомі атаки, зокрема атаки нульового дня. Проте поведінкові IPS мають вищий ризик хибних тривог і вимагають складного етапу початкового навчання та постійного вдосконалення моделей.

Таким чином, результати першого розділу створюють теоретичне підґрунтя для подальшого практичного впровадження і тестування IPS-систем із використанням сигнатурних та поведінкових методів виявлення загроз, що буде розглянуто у наступних розділах роботи.

РОЗДІЛ 2. НАЛАШТУВАННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА ТЕСТУВАННЯ IPS

2.1 Архітектура лабораторного середовища

Лабораторне середовище для тестування системи запобігання вторгненням побудоване на базі гіпервізора VMware Workstation і включає кілька віртуальних мережевих компонентів, що взаємодіють між собою для моделювання реальних умов атаки та захисту мережі [26,27]. Вся система розділена на зовнішню і внутрішню мережеві зони, які пов'язані через маршрутизатор pfSense з інтегрованою IPS Suricata (див. рисунок 2.1).

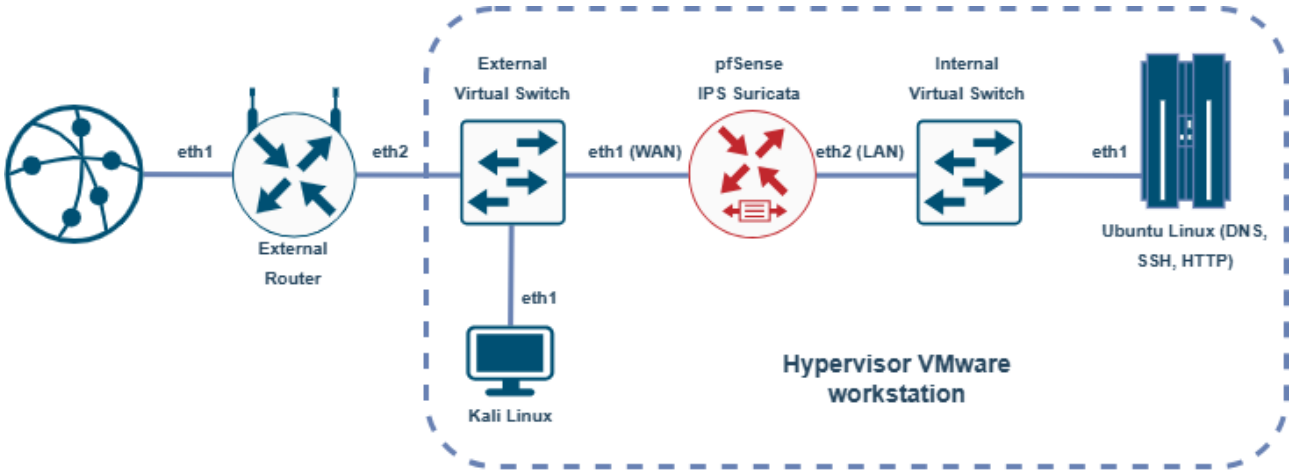

Рисунок 2.1 – Схема лабораторного середовища

На зовнішній стороні мережі розташований зовнішній маршрутизатор, який має два мережевих інтерфейси: eth1 і eth2. Інтерфейс eth1 підключений до глобальної мережі Інтернету, тоді як eth2 підключений до зовнішнього віртуального комутатора (External Virtual Switch) всередині середовища VMware. Цей віртуальний комутатор використовується для об'єднання зовнішніх пристроїв та маршрутизатора у спільну віртуальну мережу.

До зовнішнього комутатора також підключено віртуальну машину Kali Linux через інтерфейс eth1. Kali Linux використовується як атакуюча система,

яка генерує шкідливий трафік і проводить атаки на цільові служби в тестовому середовищі. Це дозволяє проводити практичне тестування роботи системи виявлення і запобігання вторгненням в умовах симульованої атаки.

Головною ланкою захисту в середовищі є віртуальний маршрутизатор pfSense, який виконує роль брандмауера і IPS. pfSense має два мережевих інтерфейси: eth1 (WAN) та eth2 (LAN). Інтерфейс eth1 підключений до зовнішнього віртуального комутатора і приймає трафік із зовнішньої мережі, зокрема атаки від Kali Linux. Інтерфейс eth2 з'єднаний з внутрішнім віртуальним комутатором (Internal Virtual Switch), що забезпечує з'єднання із внутрішньою захищеною мережею.

До внутрішнього комутатора підключена віртуальна машина з операційною системою Ubuntu Linux через інтерфейс eth1. Ця машина виступає як захищений сервер, який надає критичні сервіси: DNS, SSH і HTTP. Вона є безпосередньою ціллю для атак, що дозволяє перевірити, як система pfSense з IPS Suricata ідентифікує та блокує загрози ще на периметрі мережі.

У таблиці 2.1 показано мережеві налаштування елементів лабораторного середовища.

Таблиця 2.1 – Мережеві налаштування елементів лабораторного середовища

Елемент	Інтерфейс	IP-адреса	Мережева маска	Шлюз
External Router	eth1	DHCP	DHCP	DHCP
	eth2	192.168.0.1	255.255.255.0	
pfSense IPS Suricata	eth1	192.168.0.140	255.255.255.0	192.168.0.1
	eth2	192.168.1.1	255.255.255.0	
Kali Linux	eth1	192.168.0.150	255.255.255.0	192.168.0.1
Ubuntu Linux	eth1	192.168.1.110	255.255.255.0	192.168.1.1

Архітектура лабораторного стенду забезпечує повноцінне розмежування середовищ, чітке розділення зон довіри і можливість моделювання повного ланцюга атаки - від її ініціації у зовнішньому середовищі до спроби впливу на

внутрішні сервіси. Використання віртуальних комутаторів і гіпервізора дає змогу ефективно контролювати весь процес взаємодії та безпечно проводити експерименти без ризику для реальної інфраструктури.

2.2 Компоненти лабораторного середовища

2.2.1 Гіпервізор VMware Workstation Professional

Гіпервізор VMware Workstation Professional є одним із найбільш популярних інструментів для створення та керування віртуальними машинами на персональних комп'ютерах [28]. Це програмне забезпечення забезпечує середовище віртуалізації типу 2, що означає його роботу поверх основної операційної системи, яка виступає базовим рівнем підтримки апаратних ресурсів. Workstation Professional дозволяє запускати кілька віртуальних машин одночасно, кожна з яких може працювати під управлінням власної операційної системи - Windows, Linux, BSD або інших підтримуваних систем.

VMware Workstation Professional надає можливість повністю ізолювати віртуальні машини одна від одної та від основної системи, що створює безпечне середовище для тестування нових додатків, операційних систем або потенційно небезпечного програмного забезпечення. Однією з найважливіших характеристик цього гіпервізора є підтримка складної мережевої конфігурації. Workstation Professional дозволяє створювати віртуальні мережеві адаптери (комутатори), моделюючи як прості приватні мережі, так і складні багатосегментні інфраструктури, що ідеально підходить для тестування мережевої безпеки та систем запобігання вторгненням.

Продукт підтримує прив'язку віртуальних машин до фізичних мереж через режим Bridged Networking, організацію окремих приватних мереж через Host-Only Networking або створення ізольованого внутрішнього трафіку за допомогою NAT-режимів. Це дає змогу точно контролювати трафік,

обмежувати або дозволяти доступ до Інтернету, налаштовувати маршрутизацію між сегментами та емулювати реальні мережеві умови для проведення тестів.

VMware Workstation Professional підтримує знімки стану системи (snapshots), що дозволяє швидко повертатись до збережених конфігурацій, експортувати та імпортувати віртуальні машини у форматах, сумісних з іншими платформами VMware або хмарними сервісами. Це особливо корисно при тривалих тестах або експериментах, які можуть призводити до нестабільного стану середовища.

Ще однією перевагою є підтримка апаратної віртуалізації через Intel VT-x або AMD-V технології, що дозволяє ефективно використовувати ресурси процесора і пам’яті, забезпечуючи високу продуктивність віртуальних машин навіть під навантаженням. VMware Workstation також надає розширені функції для професійного середовища розробки і тестування, включаючи інтеграцію з vSphere, можливість клонування віртуальних машин, створення зашифрованих віртуальних середовищ та багаторівневе налаштування ресурсів.

У сфері інформаційної безпеки, тестування мереж і лабораторних експериментів VMware Workstation Professional є незамінним інструментом завдяки своїй стабільності, гнучкості в налаштуванні мереж і зручності в керуванні численними віртуальними машинами у межах одного фізичного комп’ютера. Він дозволяє створити середовище, яке максимально наближене до реальної інфраструктури, із можливістю контролювати всі аспекти віртуальної мережі та системного середовища без ризику для основної операційної системи [29].

На рисунку 2.2 представлений інтерфейс програми VMware Workstation, у якій видно налаштоване лабораторне середовище для тестування системи запобігання вторгненням.

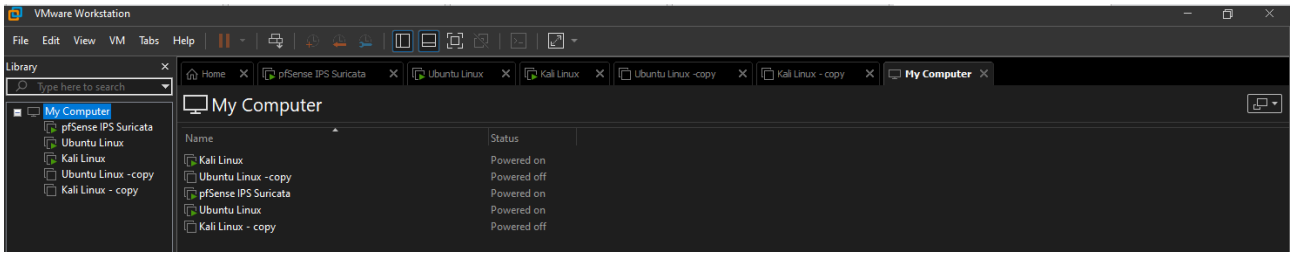

Рисунок 2.2 – Інтерфейс гіпервізора VMware Workstation

Для організації віртуальної мережевої топології використовувалися можливості VMware Workstation зі створення віртуальних комутаторів: зовнішнього та внутрішнього. Інтерфейс WAN на pfSense підключено до зовнішнього віртуального комутатора разом із Kali Linux, тоді як інтерфейс LAN - до внутрішнього віртуального комутатора з під'єднаним Ubuntu Linux. Така схема дозволяє ізолювати захищений сегмент мережі та повністю контролювати трафік, що надходить із зовнішньої мережі через IPS.

Віртуальні машини налаштовані на використання окремих мережевих інтерфейсів, що відповідають вимогам тестування, а їхній стан контролюється через інтерфейс VMware Workstation. Підготовка лабораторного середовища у VMware Workstation забезпечила гнучке, контрольоване і безпечне середовище для моделювання атак і аналізу ефективності різних підходів в системах запобігання вторгненням.

2.2.2 Маршрутизатор pfSense

Маршрутизатор pfSense є відкритою платформою, яка базується на операційній системі FreeBSD [30]. Це комплексне рішення для забезпечення мережевої безпеки, яке дозволяє гнучко налаштовувати маршрутизацію, фільтрацію трафіку, VPN-з'єднання, балансування навантаження, створення віртуальних локальних мереж (VLAN) та інтеграцію систем виявлення і запобігання вторгненням. Завдяки зручному вебінтерфейсу адміністрування (див. рисунок 2.3) pfSense є доступним навіть для користувачів, які не мають глибокої підготовки в роботі з командним рядком Unix-систем.

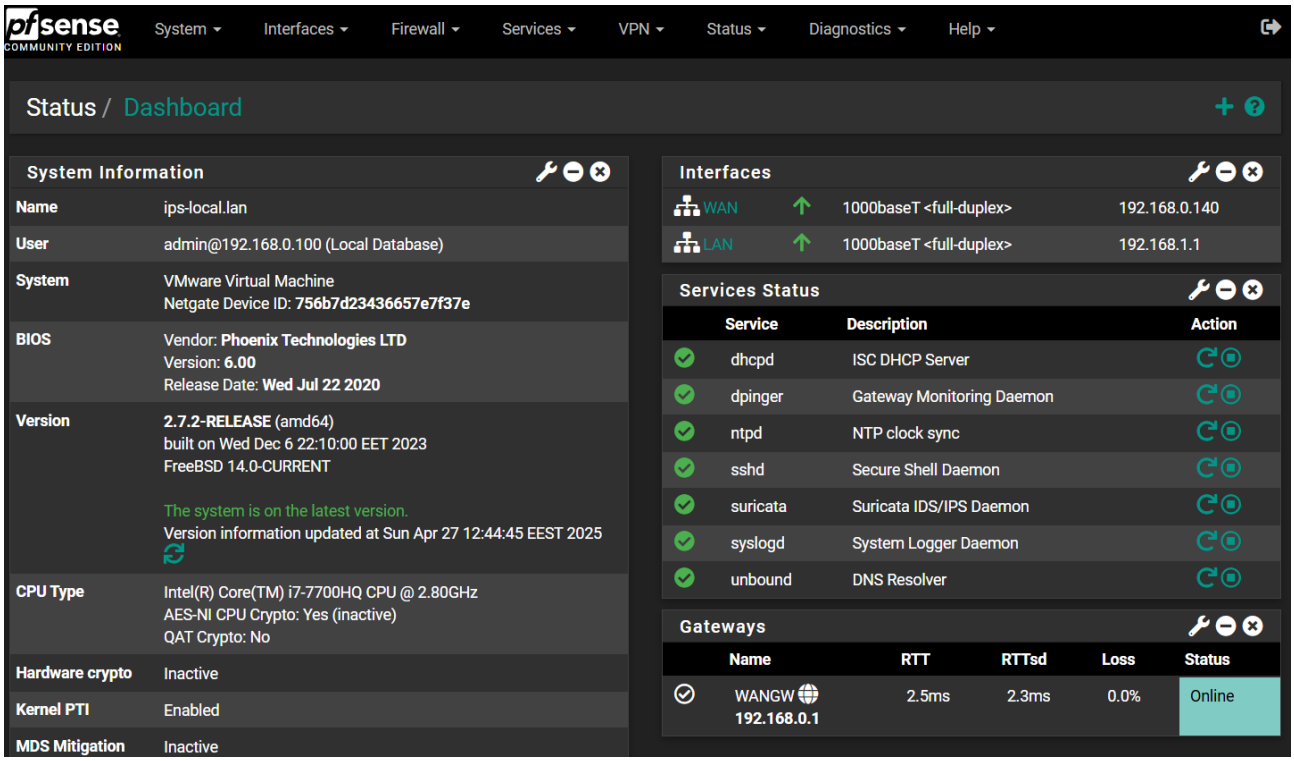

Рисунок 2.4 – Вебінтерфейс адміністрування pfSense

На рисунку 2.5 показане стандартне текстове меню початкового налаштування pfSense після встановлення та першого запуску віртуальної машини.

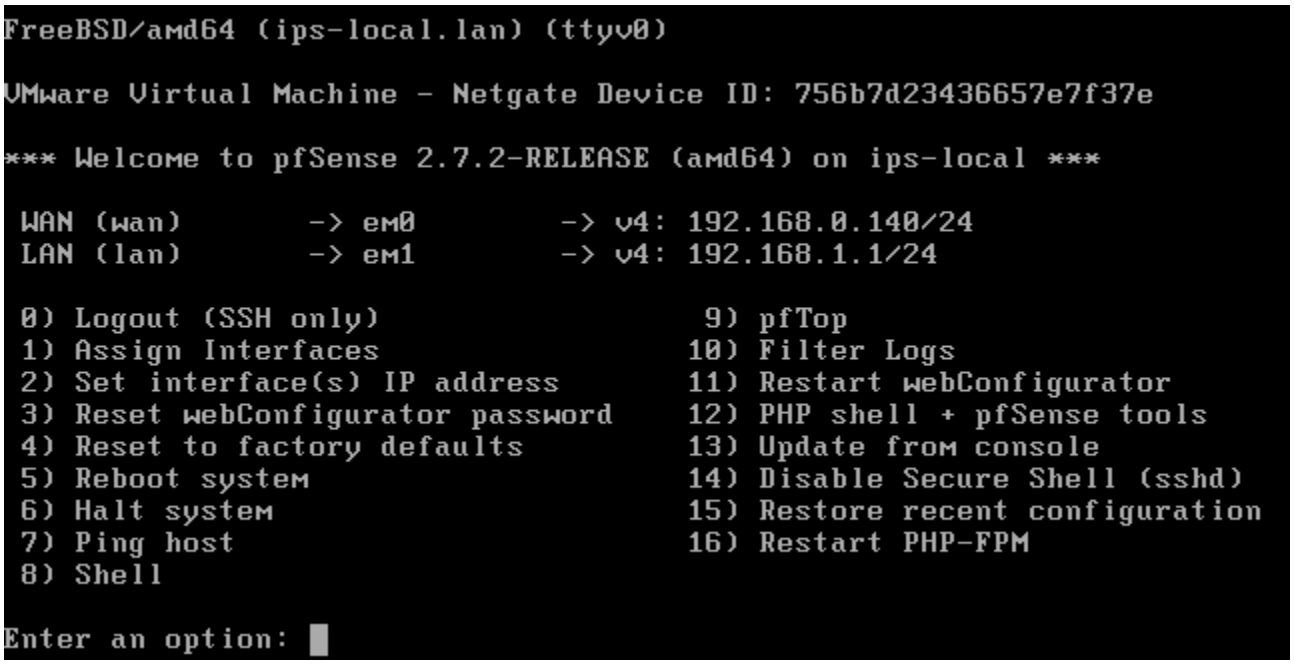

Рисунок 2.5 – Консольний інтерфейс адміністрування pfSense

Маршрутизатор pfSense після завантаження пропонує користувачеві основні інструменти для базової конфігурації системи через консольний інтерфейс.

Окремі пункти меню також дозволяють виконати специфічні задачі, такі як перегляд поточного стану проходження трафіку через утиліту pfTop, перегляд журналів фільтрації трафіку, перезапуск веб-конфігуратора, оновлення системи безпосередньо через консоль або керування службами, такими як PHP-FPM і SSH. Це консольне меню є дуже важливим на початковому етапі, оскільки дозволяє привести pfSense до мінімально працездатного стану навіть у випадку втрати доступу до веб-інтерфейсу або в середовищах, де GUI тимчасово недоступний. Після базового налаштування зазвичай адміністратори переходять до повного конфігурування системи через зручний веб-інтерфейс за допомогою браузера, використовуючи IP-адресу інтерфейсу LAN.

PfSense є повноцінним маршрутизатором, здатним обробляти великі обсяги трафіку та управляти складною мережею. Він підтримує статичну та динамічну маршрутизацію за допомогою протоколів RIP, OSPF, BGP. Це дозволяє інтегрувати pfSense у великі корпоративні мережі або використовувати його в ролі основного шлюзу для малих і середніх підприємств. Однією з важливих функцій pfSense є можливість створення політик фільтрації трафіку на основі правил брандмауера PF. Користувач може визначати, який трафік дозволено або заборонено, задавати пріоритети для різних типів даних, обмежувати швидкість передавання пакетів, налаштовувати правила NAT (Network Address Translation) і порт-форвардинг.

Особливу роль у можливостях pfSense відіграє підтримка інтеграції модулів захисту, таких як Suricata або Snort, які реалізують функціональність IDS/IPS. Завдяки цьому pfSense може не тільки пропускати або блокувати трафік на основі правил брандмауера, але й активно аналізувати вміст трафіку

для виявлення і запобігання атакам, що робить його повноцінною платформою для забезпечення мережевої безпеки.

Маршрутизатор pfSense також забезпечує розширену підтримку VPN-з'єднань, включаючи такі протоколи, як OpenVPN, IPsec, L2TP і WireGuard. Це дає змогу створювати захищені канали зв'язку між офісами, забезпечувати безпечний доступ для віддалених користувачів та організовувати гібридні корпоративні мережі.

У сфері адміністрування pfSense пропонує гнучкі механізми моніторингу та звітності (див. рисунок 2.6). Система підтримує збір статистики трафіку, логування подій безпеки, оповіщення та інтеграцію із зовнішніми системами моніторингу через syslog.

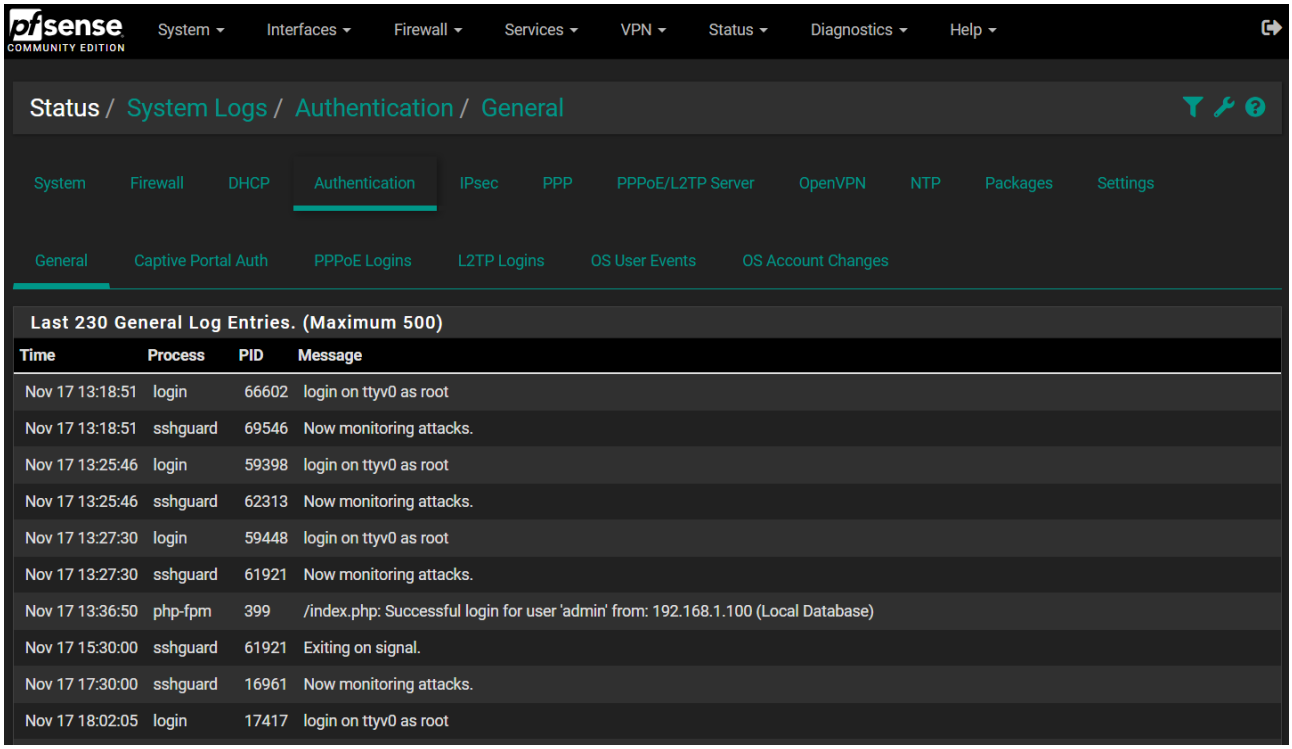

Рисунок 2.6 – Механізми моніторингу та звітності в pfSense

Через вебінтерфейс адміністратор може оперативно контролювати стан мережі, виявляти аномалії та швидко реагувати на інциденти.

Маршрутизатор pfSense підтримує концепцію кількох інтерфейсів, що дозволяє розділяти мережеві сегменти, будувати складні DMZ-зони

(demilitarized zones), впроваджувати ізоляцію для різних груп користувачів або серверів. Завдяки своїй відкритій архітектурі, високій гнучкості налаштувань і надійності, pfSense широко використовується як у лабораторних стендах, так і у реальних виробничих середовищах для забезпечення захисту мереж, організації безпечного доступу до ресурсів та контролю за потоками даних. Його популярність зумовлена тим, що рішення pfSense дозволяє отримати рівень безпеки корпоративного класу без необхідності купувати дороге обладнання.

2.2.3 Система IPS Suricata

Suricata є відкритою системою IDS/IPS, яка активно використовується в галузі кібербезпеки для аналізу мережевого трафіку і виявлення загроз у режимі реального часу [31]. Вона розроблена і підтримується організацією OISF (Open Information Security Foundation) і є одним із найпопулярніших інструментів завдяки своїй високій продуктивності і можливостям розширення.

Основним завданням Suricata є аналіз мережевого трафіку, виявлення атак, шкідливої активності, експлойтів та аномальної поведінки [32]. Система підтримує глибоку інспекцію пакетів (DPI – Deep Packet Inspection), що дозволяє не тільки аналізувати заголовки мережевих пакетів, а й розглядати вміст додатків, таких як HTTP, DNS, SMTP, SMB, TLS. Завдяки цьому Suricata може детально перевіряти трафік на наявність атак навіть на прикладному рівні моделі OSI.

Suricata може працювати у кількох режимах: як IDS, тобто система виявлення вторгнень, яка лише спостерігає за трафіком і створює попередження про підозрілі події, або як IPS, тобто система запобігання вторгненням, яка має можливість блокувати підозрілий трафік на рівні мережевого фільтра у реальному часі. В IPS-режимі Suricata інтегрується з брандмауером системи, що дозволяє їй активно впливати на маршрутизацію або фільтрацію пакетів.

Однією з основних особливостей Suricata є багатопотокова обробка трафіку. Система ефективно використовує багатоядерні процесори,

розподіляючи завдання обробки пакетів між кількома ядрами, що суттєво підвищує її продуктивність і дає змогу працювати із великими обсягами трафіку без помітних затримок.

Suricata підтримує використання правил nf має розширені можливості для написання складних умов виявлення. Бази правил можуть оновлюватися автоматично, що забезпечує актуальність системи перед новими загрозами. Крім того, Suricata має вбудовані механізми для виявлення аномалій у мережевому трафіку, що дає можливість працювати не тільки на основі сигнатур, але й виявляти підозрілі шаблони поведінки.

Система може зберігати детальні журнали про події безпеки у різних форматах, зокрема JSON, що полегшує інтеграцію з системами моніторингу, SIEM-платформами, такими як Splunk, ELK Stack (Elasticsearch, Logstash, Kibana). Також Suricata може зберігати повні копії мережевих сесій у форматі PCAP для подальшого аналізу.

IPS Suricata у складі маршрутизатора pfSense є одним із найефективніших рішень для інтеграції активного захисту мережі. Маршрутизатор pfSense виступає не тільки як маршрутизатор і брандмауер, а й як універсальна система безпеки завдяки можливості розгортання модулів виявлення та запобігання вторгненням. Підключення Suricata у pfSense дає змогу проводити глибокий аналіз трафіку в реальному часі, використовуючи як сигнатурний, так і поведінковий підхід до виявлення атак. IPS Suricata в pfSense працює через спеціальний плагін, який встановлюється безпосередньо через вбудовану систему керування пакетами. Після встановлення адміністратор може налаштовувати Suricata через вебінтерфейс pfSense, що значно спрощує процес конфігурації в порівнянні з використанням Suricata як окремої самостійної системи (див. рисунок 2.7).

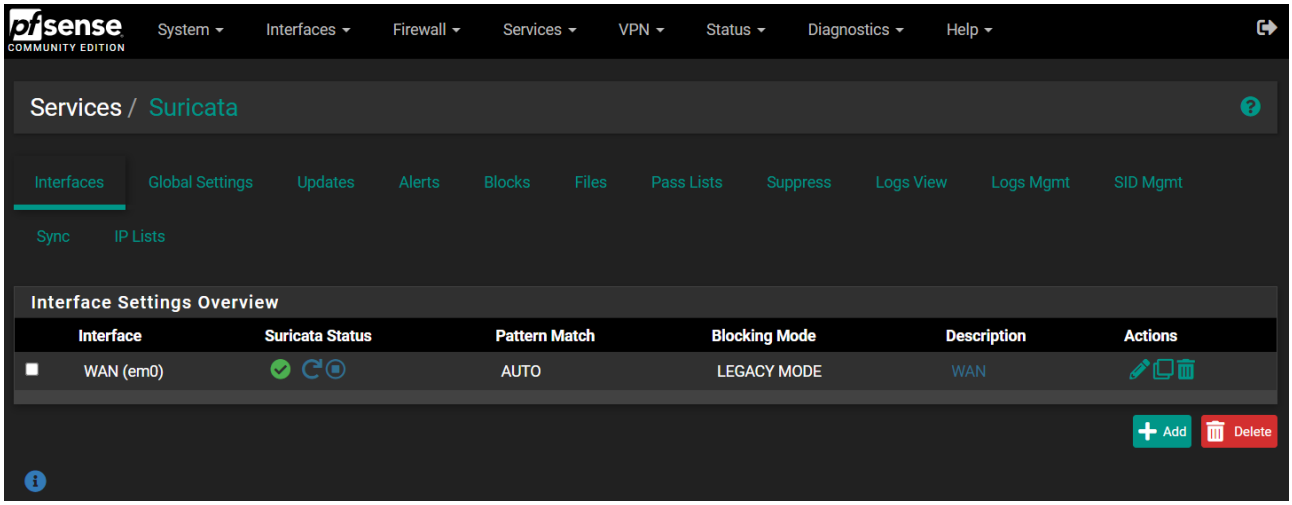

Рисунок 2.7 – Інтерфейс керування IPS Suricata в pfSense

Інтеграція дозволяє прив'язувати моніторинг до конкретних мережевих інтерфейсів, наприклад, до інтерфейсів WAN, LAN або VLAN, що забезпечує гнучкість у захисті різних сегментів мережі.

Однією з важливих особливостей використання Suricata у pfSense є можливість обирати режими роботи - система може бути налаштована на пасивний режим виявлення атак (IDS) або активний режим блокування загроз (IPS). У режимі IPS Suricata у pfSense здатна автоматично блокувати шкідливі пакети за допомогою інтеграції з механізмом netmap, що дозволяє перехоплювати і відхиляти трафік на рівні ядра системи з мінімальними затримками.

Suricata в pfSense підтримує використання декількох джерел правил для виявлення атак та шкідливої активності. Основними джерелами є ETOpen, ETPro, Snort Rules (безкоштовні та платні), Snort GPLv2 Community Rules, а також спеціалізовані списки з ботнетами та шкідливими SSL-сертифікатами.

ETOpen Emerging Threats - це безкоштовний набір правил із відкритим кодом, який надає базове покриття для відомих типів атак і загроз. Він менш повний порівняно з комерційним набором ETPro, але є хорошим стартовим варіантом для більшості користувачів. Можна використовувати власний URL для завантаження ETOpen-правил, якщо потрібно отримувати правила з приватного дзеркала або локального сервера.

ETPro Emerging Threats - це платна підписка на набір правил, яка пропонує щоденні оновлення та розширене покриття актуальних загроз, зокрема експлойтів, нових ботнетів, складних атак і варіацій шкідливого ПЗ. Підписку на ETPro потрібно оформити окремо.

Snort Rules діляться на безкоштовний набір для зареєстрованих користувачів (Registered User Rules) і платний набір для передплатників (Subscriber Rule Set). Зареєстровані користувачі мають доступ до правил із затримкою в кілька днів порівняно з платними користувачами. Також можна вказати власний URL для завантаження правил Snort.

Snort GPLv2 Community Rules - це відкритий набір правил, який безкоштовно розповсюджується під ліцензією GPLv2. Він є частиною платної підписки на Snort, тому для користувачів Snort Subscriber додаткове завантаження Community Rules не потрібне.

Feodo Tracker Botnet C2 IP Rules - це спеціальний набір правил, що включає IP-адреси командних серверів ботнетів Dridex, Emotet і Heodo, які активно відслідковуються проєктом Feodo Tracker. Додаючи ці правила, Suricata може автоматично виявляти і блокувати підключення до відомих ботнет-інфраструктур.

ABUSE.ch SSL Blacklist Rules - цей набір містить відбитки SSL-сертифікатів, що належать шкідливим або небезпечним сайтам. Додавання правил ABUSE.ch дозволяє Suricata виявляти спроби встановити шифровані з’єднання із сумнівними ресурсами.

У розділі General Settings визначається, чи буде увімкнено інспекцію Suricata на конкретному мережевому інтерфейсі. У даному випадку обрано інтерфейс WAN (em0), що означає, що весь вхідний трафік із зовнішньої мережі буде перевірятися на наявність загроз. Logging Settings відповідають за налаштування реєстрації подій Suricata. Активується надсилання сповіщень про тривоги у системний журнал pfSense (див. рисунок 2.8).

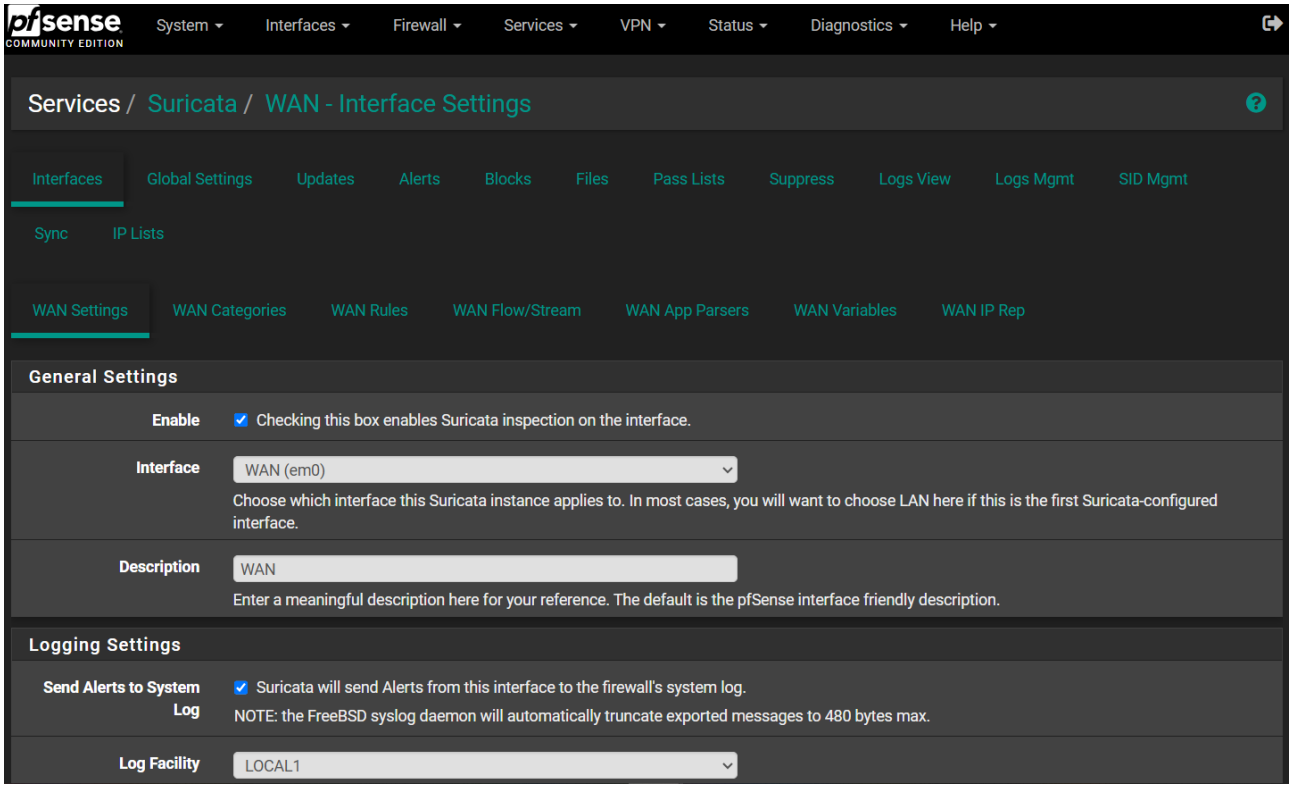

Рисунок 2.8 – Інтерфейс налаштування IPS Suricata в pfSense

Є можливість збирати статистику про продуктивність, логувати HTTP-трафік і додавати розширену інформацію про HTTP-з'єднання. При бажанні можна логувати TLS-рукостискання або навіть зберігати витягнуті файли, що проходять через прикладні потоки, хоча це значно збільшує використання диску. Додатково можна активувати логування усіх оброблених пакетів у форматі PCAP для подальшого аналізу, хоча також із великими витратами простору. Alert and Block Settings дозволяють увімкнути автоматичне блокування джерел шкідливого трафіку. Можна обрати IPS Mode в режимі Legacy Mode, який працює з копіями пакетів (де деякий трафік може пройти до блокування), або Inline Mode, який інтегрується глибше в мережевий стек і блокує пакети ще до їх передачі операційній системі. Важливо врахувати, що для Inline Mode потрібна підтримка драйверами мережевих карт через Netmap. Також можна налаштувати чи потрібно вбивати сесії (Kill States) для заблокованих IP і який саме IP (джерело чи призначення) буде блокуватися. IP Pass List дає змогу створити список винятків (білих списків), IP-адреси з якого

ніколи не будуть заблоковані Suricata. За замовчуванням сюди додаються шлюзи, DNS-сервери, локальні мережі та інші критично важливі IP. Performance and Detection Engine Settings керують тим, як Suricata буде обробляти трафік. Режим виконання AutoFP обирає оптимальну багатопоточну обробку трафіку на основі потоків, що балансуються за допомогою алгоритму Hash або IP Pair. Кількість пакетів для одночасної обробки можна налаштувати через Max Pending Packets (наприклад, 1024 для середніх навантажень). Профіль виявлення Detect-Engine Profile визначає баланс між споживанням пам'яті і швидкістю роботи: Medium - рекомендований варіант для більшості випадків. Promiscuous Mode активується для інтерфейсу за замовчуванням, що дозволяє системі бачити весь трафік на інтерфейсі незалежно від MAC-адреси призначення. Interface PCAP Snaplen визначає максимальний розмір пакета, який зберігається при захопленні трафіку. Значення 1518 байтів є стандартним для захоплення повних Ethernet кадрів без фрагментації. У розділі Networks Suricata Should Inspect and Protect налаштовуються мережі, які вважаються локальними (Home Net) і зовнішніми (External Net). За замовчуванням Home Net включає лише локальні мережі й IP-адреси маршрутизатора.

Використання системи Suricata у середовищі pfSense забезпечує комплексний, високоякісний захист мережі, дозволяючи виявляти і блокувати відомі і нові загрози у реальному часі, при цьому зберігаючи гнучкість налаштування і можливість масштабування під потреби конкретної мережевої архітектури.

2.2.4 Операційна система Ubuntu Linux

Ubuntu Linux є однією з найпопулярніших дистрибутивів операційної системи Linux у світі, розробленою компанією Canonical Ltd. Вона заснована на Debian GNU/Linux і орієнтована на забезпечення простоти використання, стабільності та широкої підтримки як для звичайних користувачів, так і для підприємств [33]. Ubuntu пропонує зручний інтерфейс, стабільні оновлення

безпеки, програмне забезпечення з відкритим кодом та багату інфраструктуру підтримки спільноти.

Система випускається у кількох версіях: для настільних комп’ютерів (Desktop), серверів (Server) та спеціалізованих середовищ, таких як хмарні обчислення, Інтернет речей (IoT) і контейнеризація. Ubuntu має розвинену систему безпеки. За замовчуванням вона включає в себе засоби для регулярного оновлення безпеки, використання фаєрвола UFW (Uncomplicated Firewall), механізми AppArmor для ізоляції процесів, а також можливість швидкої інтеграції шифрування даних за допомогою LUKS. Адміністратори мають доступ до журналів системи через systemd, що дозволяє здійснювати моніторинг подій і пошук несправностей.

У лабораторному середовищі віртуальна машина Ubuntu Linux виступає сервером, на який спрямовуються атаки з метою перевірки ефективності роботи системи запобігання вторгненням Suricata, розгорнутої на маршрутизаторі pfSense. Ubuntu Linux у цьому стенді виконує роль умовної продуктивної системи, що надає базові мережеві сервіси, такі як HTTP, DNS і SSH. Така конфігурація дозволяє змоделювати типовий сервер у реальній корпоративній мережі, який одночасно обробляє запити користувачів і є потенційною ціллю для атак. Основними каналами атаки на Ubuntu Linux є відкриті мережеві сервіси, які відповідають на зовнішні запити. Зокрема, порт 22 використовується для SSH-з'єднань, що робить його потенційною ціллю для brute-force атак зі спробами підібрати логін і пароль до облікових записів системи. Порт 80 на якому працює HTTP-сервер, є об'єктами атак типу SQL-ін'єкцій, XSS.

Важливим завданням тестування є перевірка, наскільки ефективно Suricata, встановлена на межі між зовнішньою і внутрішньою мережею, зможе виявити та заблокувати шкідливу активність до того, як вона досягне Ubuntu-сервера. При цьому аналізується здатність системи реагувати як на класичні сигнатурні атаки, так і на аномальні типи трафіку, що не відповідають звичайній моделі поведінки мережі. Ubuntu Linux у даному середовищі

спеціально налаштована без додаткових підсилень безпеки, що дозволяє виявити базові вектори компрометації. Водночас для достовірності тестів система залишається працездатною і виконує реальні мережеві функції, моделюючи поведінку корпоративного сервера.

На рисунку 2.9 показано вивід команд `ip addr` та `route -n` у терміналі віртуальної машини Ubuntu Linux. Ці команди використовуються для перевірки мережевих налаштувань та таблиці маршрутизації системи.

```
admin@sr-ubuntu:~$ 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:e9:ce:80 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.110/24 brd 192.168.1.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
admin@sr-ubuntu:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    20100  0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 ens33
admin@sr-ubuntu:~$
```

Рисунок 2.9 – Мережеві налаштування Ubuntu Linux

Ці налаштування підтверджують, що віртуальна машина Ubuntu Linux правильно інтегрована у внутрішню мережу лабораторного середовища, підключена до LAN-сегменту pfSense, і має прямий доступ до локальних ресурсів через свою IP-адресу. Водночас, вихід у глобальну мережу чи доступ до інших зовнішніх систем можливий через стандартний шлюз pfSense, який також здійснює моніторинг і захист мережі за допомогою IPS Suricata.

На рисунку 2.10 показано результат виконання команди `netstat -an | more` в віртуальній машині Ubuntu Linux. Ця команда використовується для перегляду відкритих портів у системі.

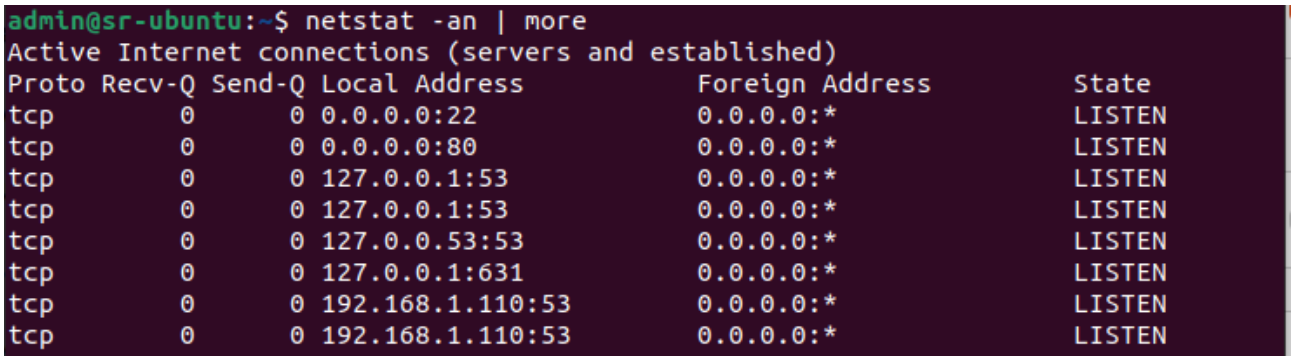

Рисунок 2.10 – Результат виконання команди `netstat -an | more` в Ubuntu Linux

Стан всіх служб LISTEN, що означає готовність до встановлення нових вхідних з'єднань. Такий набір відкритих портів вказує, що Ubuntu Linux у лабораторному середовищі надає критичні сервіси: SSH для віддаленого керування, HTTP для веб-доступу і DNS. Це підтверджує, що система є повноцінною моделлю сервера у корпоративній мережі та є реальною ціллю для різних типів атак під час тестування системи IPS Suricata.

Таким чином, Ubuntu Linux у лабораторному середовищі виконує роль реальної робочої цілі атаки, що дозволяє в контрольованих умовах моделювати реальні загрози, вивчати можливості виявлення і блокування атак системою IPS Suricata і отримувати практичні навички побудови захищеної мережевої інфраструктури.

2.2.5 Операційна система Kali Linux

Kali Linux є спеціалізованою операційною системою на основі Debian GNU/Linux, яка орієнтована на проведення тестування безпеки, аудит інформаційних систем і цифрову криміналістику. Розробником дистрибутива є компанія Offensive Security [34]. Kali Linux позиціонується як професійний інструмент для фахівців з кібербезпеки, дослідників безпеки, системних адміністраторів, а також для освітніх і наукових цілей.

Kali Linux за замовчуванням постачається з величезною кількістю попередньо встановленого спеціалізованого програмного забезпечення для всіх етапів тестування безпеки. У розподілених категоріях містяться інструменти для збору інформації (Nmap), експлуатації вразливостей (Metasploit Framework), атак на паролі (Hydra), перехоплення трафіку (Wireshark) і багато інших засобів для тестування безпеки. Система підтримує архітектури x86, x86_64, ARM і доступна для встановлення на широкий спектр пристроїв, від серверів і настільних ПК до одноплатних комп'ютерів, таких як Raspberry Pi. Kali Linux може працювати у форматі віртуальних машин для VMware або VirtualBox. Це дозволяє легко інтегрувати Kali у лабораторні середовища для тестування.

У лабораторному середовищі Kali Linux використовується як основний засіб для імітації реальних атак на цільові системи з метою перевірки ефективності роботи системи запобігання вторгненням Suricata, розгорнутої на маршрутизаторі pfSense. Віртуальна машина Kali Linux підключена до WAN інтерфейсу мережі, що дозволяє моделювати дії зловмисника, який атакує внутрішні ресурси організації з боку Інтернету або потенційно небезпечної зони.

На рисунку 2.11 показано вивід команд `ip addr` та `route -n` у терміналі віртуальної машини Kali Linux. Ці команди використовуються для перевірки мережевих налаштувань та таблиці маршрутизації системи.

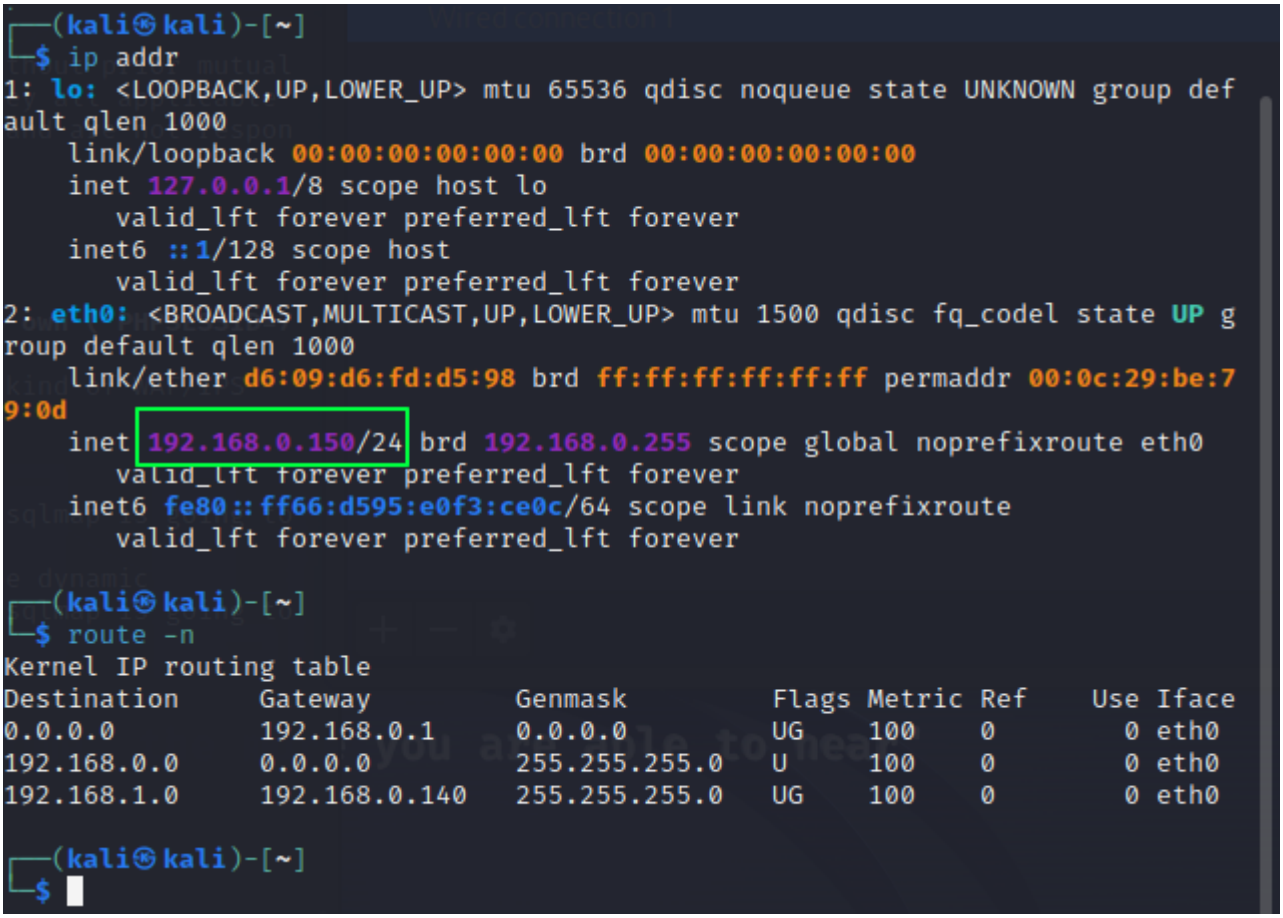

Рисунок 2.11 – Мережеві налаштування Kali Linux

Для доступу до внутрішньої мережі 192.168.1.0/24 лабораторного середовища Kali Linux використовує маршрутизатор pfSense (IP-адреса 192.168.0.140) як проміжний вузол для пересилання пакетів, що імітує реалістичний сценарій доступу до захищеної корпоративної мережі через шлюз. Конфігурація Kali Linux демонструє готовність до виконання практичних тестових атак у межах моделювання кіберзагроз, а також забезпечує реалістичні умови для оцінки можливостей системи запобігання вторгненням Suricata, налаштованої на маршрутизаторі pfSense.

2.3 Висновок до другого розділу

В другому розділі було здійснено побудову та налаштування лабораторного середовища для тестування системи запобігання вторгненням

IPS Suricata. Детально описано архітектуру середовища, яка складається із двох окремих мережевих зон - зовнішньої та внутрішньої, що об'єднані через маршрутизатор pfSense із інтегрованою системою виявлення та запобігання вторгненням. Було створено повноцінну віртуальну інфраструктуру на основі гіпервізора VMware Workstation Professional із використанням віртуальних комутаторів для розмежування мережевого трафіку.

Розглянуто особливості роботи та призначення основних компонентів лабораторного середовища: гіпервізора VMware Workstation Professional, маршрутизатора pfSense, системи IPS Suricata, операційних систем Ubuntu Linux і Kali Linux. Надано докладний опис їхньої конфігурації та мережевих налаштувань. Особлива увага приділена функціональним можливостям pfSense як базового елемента безпеки і маршрутизації, а також інтеграції в нього Suricata для реалізації активного моніторингу та блокування загроз. Було налаштовано Ubuntu Linux як цільову машину, яка надає сервіси HTTP, SSH, DNS і виступає реалістичною моделлю корпоративного сервера для атаки. Kali Linux використовується як інструмент моделювання атак, що дозволяє перевіряти ефективність системи IPS Suricata в умовах реальних сценаріїв загроз. Завдяки ізоляції сегментів і контролю за мережевим трафіком забезпечено безпечне проведення експериментів без ризику для реальної IT-інфраструктури.

Таким чином, створене лабораторне середовище повністю відповідає цілям і задачам дослідження, забезпечуючи контрольованість і реалістичність тестових сценаріїв для оцінки ефективності сигнатурного і поведінкового підходів у системах запобігання вторгненням.

РОЗДІЛ 3. ПРАКТИЧНЕ ТЕСТУВАННЯ СИГНАТУРНИХ ТА ПОВЕДІНКОВИХ ПІДХОДІВ В IPS

3.1 Тестування працездатності лабораторного середовища

Тест працездатності лабораторного середовища полягає у перевірці правильності взаємодії між усіма віртуальними компонентами, коректності маршрутизації, доступності мережевих сервісів.

На рисунку 3.1 показано результат виконання команд ping та traceroute у терміналі Kali Linux для перевірки мережевого з'єднання з сервером Ubuntu Linux з IP-адресою 192.168.1.110.

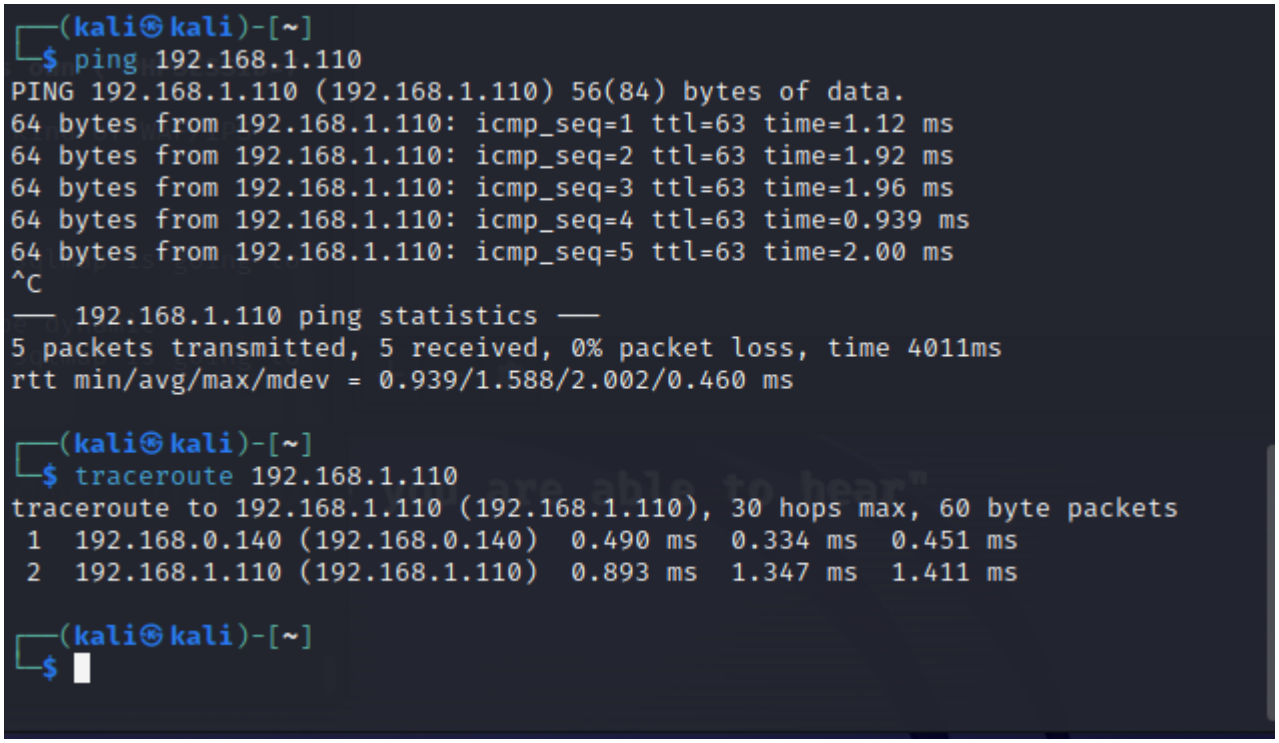

Рисунок 3.1 – Результат перевірки мережевого з'єднання з сервером Ubuntu Linux

Це підтверджує працездатність маршрутизації та доступ до цільового вузла через pfSense. Команда ping 192.168.1.110 надсилає ICMP-запити до Ubuntu Linux. Усі п'ять пакетів отримали відповіді зі стабільним часом відгуку

(приблизно 0.9–2 мс), що свідчить про відсутність втрат пакетів і коректну доставку трафіку через pfSense. Команда traceroute 192.168.1.110 показує маршрут проходження пакетів до цільової IP-адреси. Першим вузлом на шляху є IP-адреса 192.168.0.140, яка належить WAN-інтерфейсу pfSense. Другим вузлом у трасі є безпосередньо Ubuntu Linux. Це підтверджує, що трафік успішно маршрутизується через pfSense у внутрішню мережу 192.168.1.0/24.

Загалом цей вивід демонструє повну працездатність маршрутизації у лабораторному середовищі, правильну взаємодію між зонами WAN і LAN через pfSense, а також наявність стабільного мережевого з'єднання між Kali Linux і Ubuntu Linux.

На рисунку 3.2 представлено результат сканування портів цільового сервера Ubuntu Linux за допомогою утиліти nmap з Kali Linux.

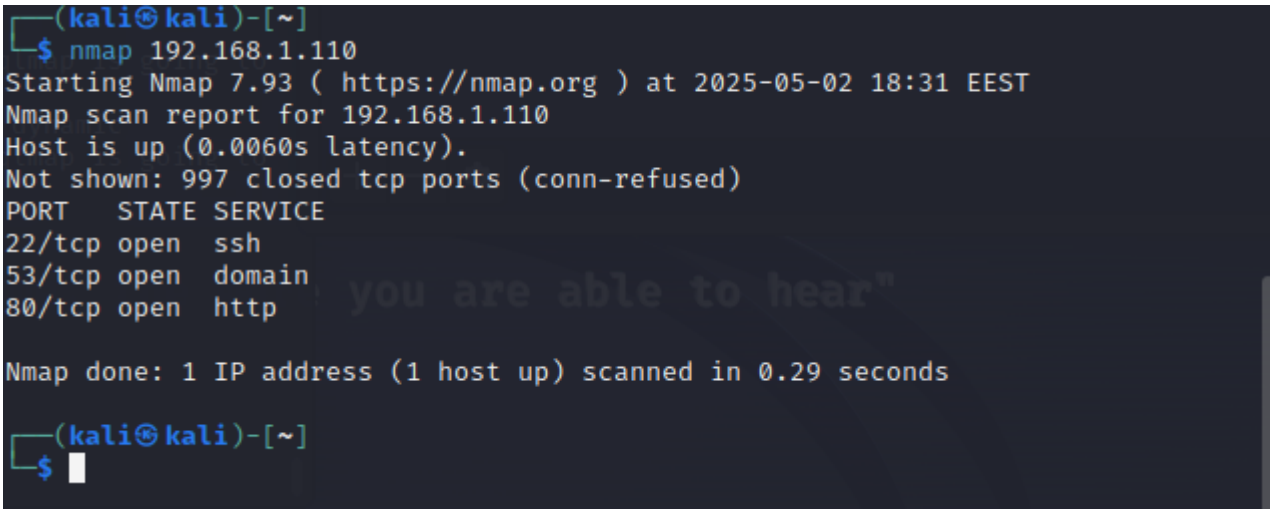

Рисунок 3.2 – Результат сканування портів Ubuntu Linux

Сканування показує, що цільовий хост активний і відповідає на запити. У результаті сканування виявлено три відкриті TCP-порти: порт 22 (SSH), порт 53 (DNS) та порт 80 (HTTP). Усі вони перебувають у стані open, що означає доступність цих сервісів для з'єднання ззовні, зокрема з Kali Linux. Це підтверджує, що цільова система Ubuntu Linux надає необхідні мережеві сервіси й налаштована для тестування різних типів атак.

Таким чином, сканування портів за допомогою nmap показало, що лабораторне середовище працює коректно: сервер Ubuntu Linux доступний, цільові сервіси відповідають, і середовище готове до моделювання атак з боку Kali Linux, а також до подальшої перевірки реакції системи IPS Suricata.

3.2 Тестування сигнатурного підходу

Використання сигнатурного підходу в системах IPS базується на методі порівняння вхідного мережевого трафіку з базою попередньо відомих шаблонів, які описують характерні ознаки конкретних атак. Ці шаблони, або сигнатури, створюються фахівцями з кібербезпеки на основі аналізу реальних інцидентів, досліджень уразливостей програмного забезпечення та поведінки шкідливого коду. Сигнатура може містити специфічні послідовності байтів, командні рядки, ознаки запитів до певних портів, комбінації заголовків мережевих протоколів або інші унікальні характеристики, що дозволяють точно ідентифікувати шкідливу активність.

Коли система IPS працює в сигнатурному режимі, кожен вхідний або вихідний мережевий пакет (або потік пакетів) аналізується в режимі реального часу й порівнюється з базою сигнатур. Якщо знайдено повний або частковий збіг, система ініціює відповідну дію згідно з налаштуваннями політики безпеки - це може бути реєстрація події, сповіщення адміністратора, блокування IP-адреси джерела, завершення сесії або інші заходи захисту.

Основною перевагою сигнатурного підходу є його висока точність при виявленні відомих атак. Оскільки сигнатури ґрунтуються на конкретних прикметах атак, ризик хибнопозитивних спрацювань є мінімальним. Це особливо важливо в умовах великих корпоративних мереж, де велика кількість некоректних тривог може призвести до ігнорування реальних загроз. Крім того, сигнатурний аналіз не потребує тривалого навчання або створення моделей поведінки, що робить його швидким у розгортанні та легким у керуванні.

На рисунку 3.2 показано користувацьке сигнатурне правило для виявлення певної послідовності символів у трафіку по протоколу TCP.

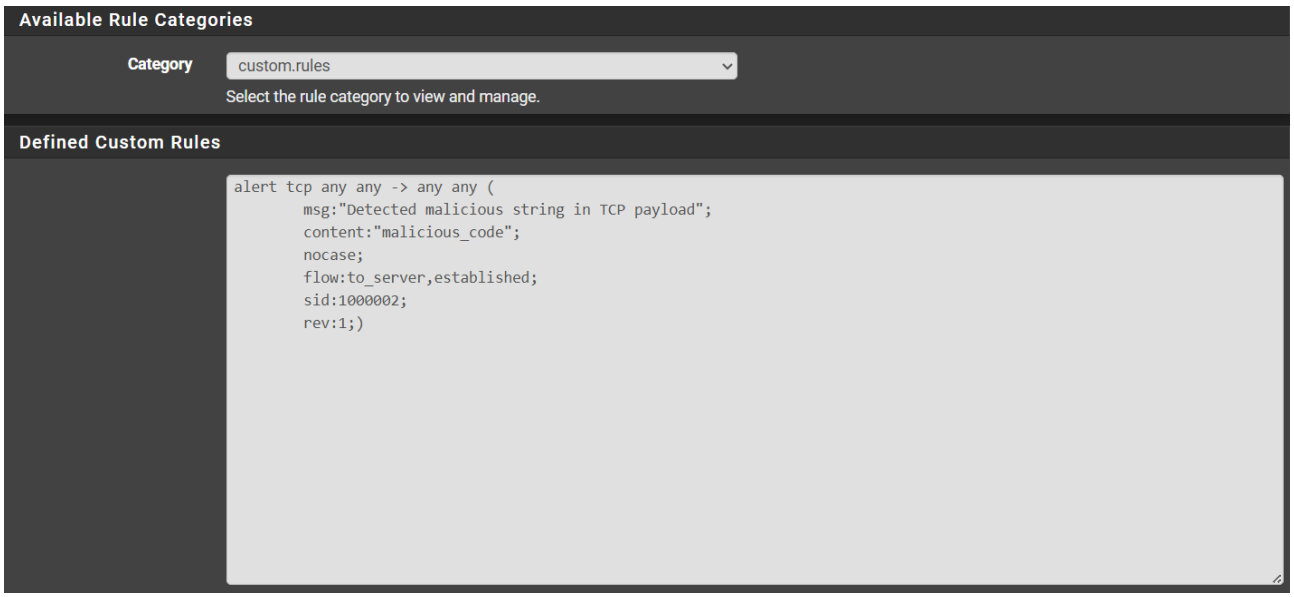

Рисунок 3.3 – Сигнатурне правило IPS Suricata

Елементи правила:

- `alert` — дія, яку виконує Suricata при спрацюванні (запис тривоги);
- `tcp any any -> any any` - правило застосовується до всіх TCP-пакетів між будь-якими джерелами і призначеннями;
- `msg:"Detected malicious string in TCP payload"` - повідомлення, що буде виведене в журналі при спрацюванні;
- `content:"malicious_code"` - ключовий фрагмент тексту, який шукається у тілі трафіку;
- `nocase` - пошук незалежно від регістру;
- `flow:to_server,established` - правило працює на трафік, що йде до сервера і є частиною встановленого TCP-з’єднання;
- `sid:1000002` - унікальний ідентифікатор правила;
- `rev:1` - версія правила;

Це правило спрацює, якщо вхідний TCP-пакет (з’єднання до порту) міститиме текст “malicious_code”. Якщо у потоці знайдеться текст “malicious_code”, буде створено тривогу (alert), яка з'явиться у журналі Suricata.

В Додатку А наведено скрипт на мові програмування python, який використовується для симулювання атаки з надсиланням послідовність символів у вигляді рядка “malicious_code” на порт 80 з метою перевірки працездатності сигнатурного правила в системі IPS. Він не є HTTP-запитом у повному сенсі (не містить заголовків протоколу HTTP), але створює корисне навантаження, яке проходить через мережу в TCP-пакетах, доступне для аналізу Suricata на наявність заданих сигнатур.

На початку скрипт ініціалізує параметри з’єднання, включаючи IP-адресу, порт, кількість повторень (packet_count) і затримку між відправленнями (delay). Потім він формує простий текстовий рядок - послідовність, яку потрібно передати. Весь процес супроводжується логуванням у файл attack_log.txt, куди записуються часові мітки та повідомлення про кожну дію. Після запуску скрипт створює TCP-сокет і намагається встановити з’єднання з цільовим сервером. У разі успішного підключення в циклі for надсилається визначена кількість повідомлень із вмістом “malicious_code”, кожне з яких фіксується у журналі. Після кожної відправки виконується пауза на задану кількість секунд (див. рисунок 3.4).

Після завершення передачі повідомлень скрипт намагається отримати відповідь від сервера. Якщо відповідь надходить, вона також записується у лог. Якщо таймаут перевищено - про це також повідомляється. Обробка винятків включає ситуації, коли сервер недоступний, порт заблокований або з’єднання не вдалося встановити.

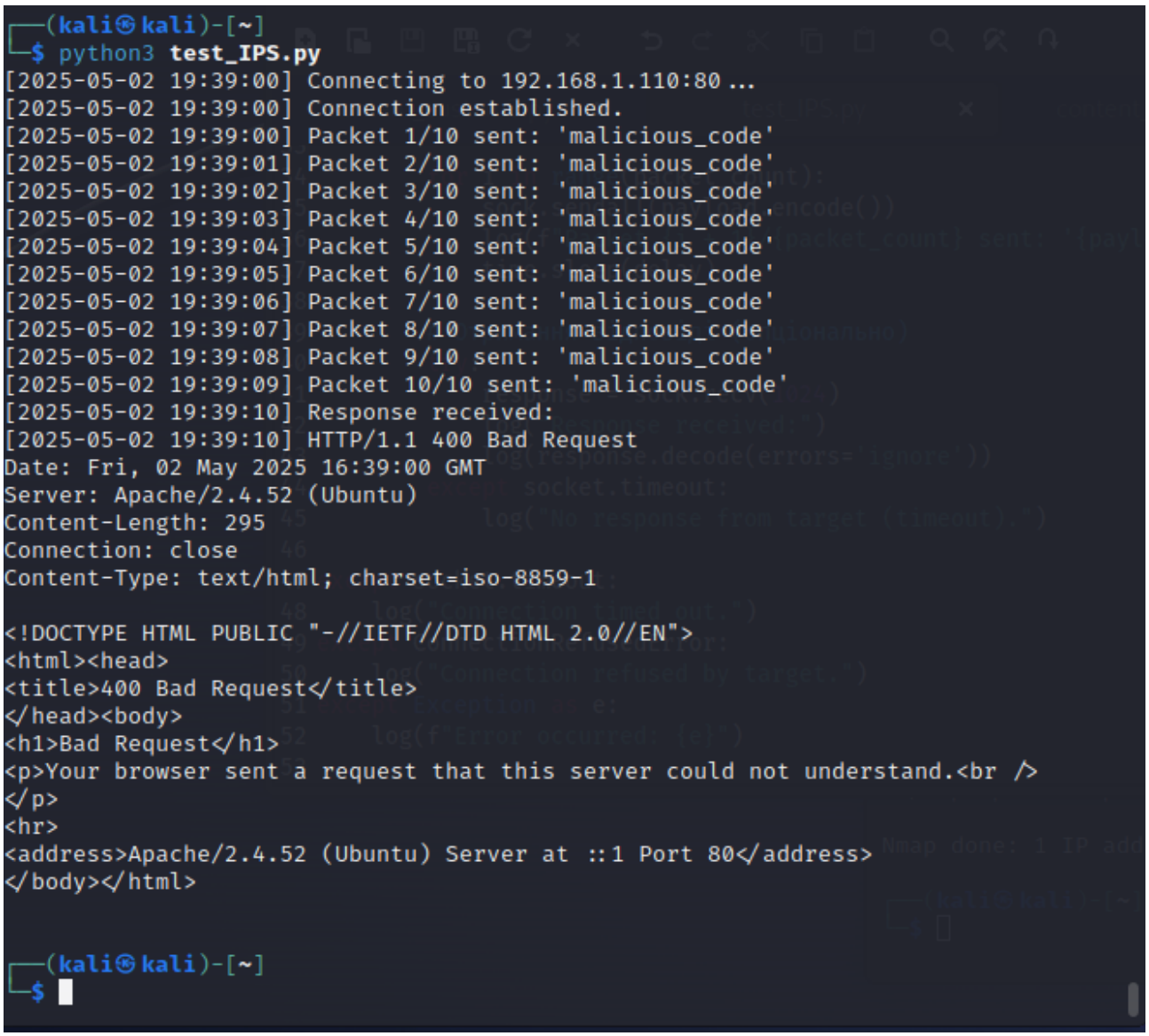

Рисунок 3.4 – Виконання скрипта test_IPS.py

На рисунку 3.5 представлено журнал сповіщень IPS Suricata спрацювання сигнатурного правила, що відбулось у результаті тестової атаки з Kali Linux на HTTP-сервер Ubuntu Linux. Усі спрацювання мають однакову природу та ідентифікуються сигнатурою з SID 1000002, що відповідає користувацькому правилу Suricata, створеному раніше для виявлення фрази "malicious_code" у TCP-пакетах.

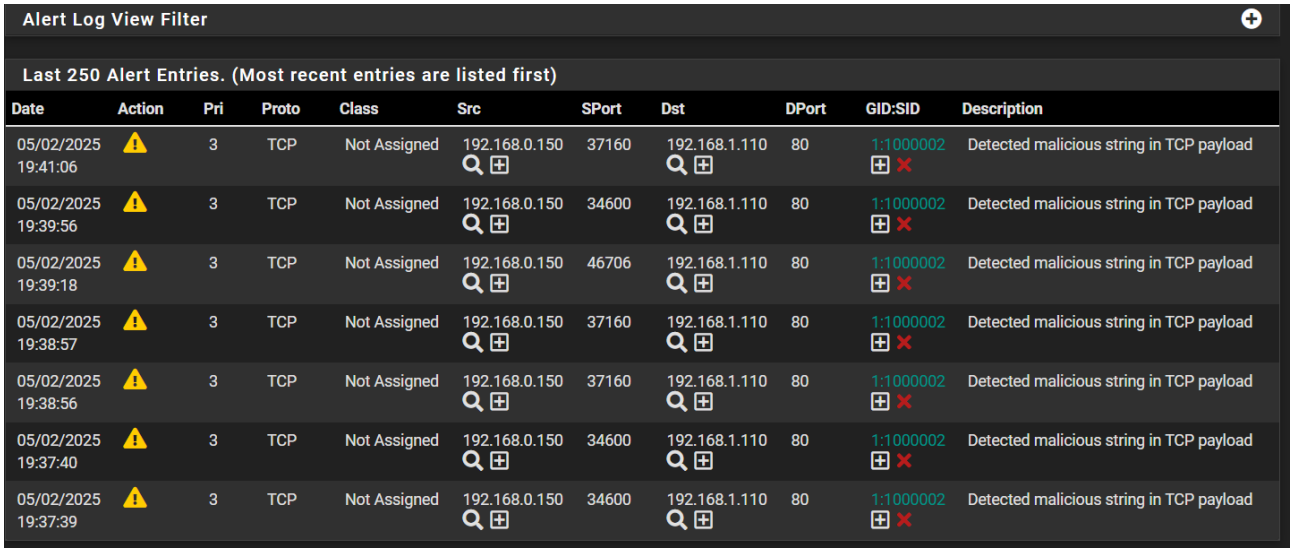

Рисунок 3.5 – Журнал сповіщень IPS Suricata при спрацюванні сигнатурного правила

Це підтверджує, що Suricata успішно ідентифікує визначену сигнатуру, спрацьовує при кожному входженні фрази “malicious_code” у трафік. Такий результат демонструє функціональність сигнатурного підходу в реальних умовах, а також працездатність лабораторного середовища, побудованого для моделювання атак і тестування IPS.

На рисунку 3.6 представлено список IP-адрес, автоматично заблокованих IPS Suricata.

Видно, що IP-адреса 192.168.0.150, яка належить Kali Linux була заблокована. У полі Block Alert Description вказано опис тривоги, що викликала блокування - Detected malicious string in TCP payload. Це означає, що Suricata спрацювала на правило з сигнатурою, яке було раніше додано вручну й налаштоване на виявлення певної послідовності символів у вмісті TCP-пакетів.

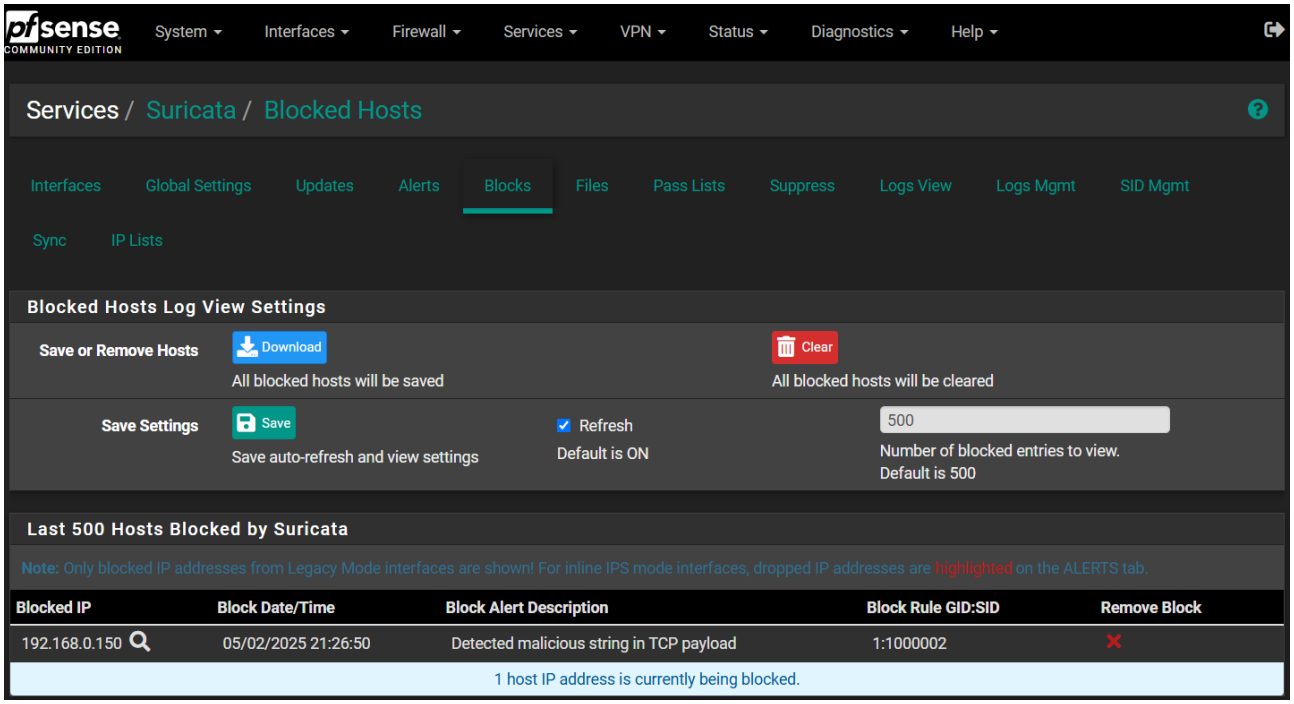

Рисунок 3.6 – Заблокована IP-адреса при спрацюванні сигнатурного правила

IPS Suricata у pfSense успішно виявила шкідливий трафік, згенерований у рамках симуляції атаки з Kali Linux, та автоматично реалізувала політику блокування зловмисника, як передбачено в конфігурації.

Ключовим обмеженням сигнатурного підходу є його неефективність проти нових, раніше невідомих атак, які не мають відповідної сигнатури в базі. У випадку zero-day атак, поліморфного шкідливого ПЗ або цілеспрямованих атак із унікальними параметрами, сигнатурний підхід в IPS не зможе виявити загрозу, якщо вона не була ідентифікована раніше й не внесена до бази. Це означає, що ефективність такого підходу безпосередньо залежить від актуальності, повноти та частоти оновлення сигнатур.

Сигнатурний підхід в IPS є ефективним засобом для виявлення широкого спектра відомих атак з високою точністю, мінімальними хибними спрацюваннями і чіткою логікою реагування.

3.3 Тестування поведінкового підходу

Поведінковий підхід у системах IPS ґрунтується на виявленні аномалій у мережевій чи системній активності на основі порівняння з моделями нормальної поведінки. На відміну від сигнатурного підходу, який спирається на попередньо визначені шаблони відомих атак, поведінковий аналіз намагається виявити невідому або нову загрозу шляхом виявлення відхилень від стандартної активності в мережі чи на хості. Принцип роботи поведінкового підходу базується на етапі навчання, під час якого IPS-система спостерігає за "нормальним" функціонуванням мережі або пристроїв у певний період часу. На основі зібраної інформації створюється поведінкова модель, що охоплює типові шаблони доступу, обсяг і частоту трафіку, використання портів, часові характеристики, комунікаційні канали, зв’язки між вузлами тощо. Після завершення навчання система переходить у режим моніторингу, де всі нові події або трафік порівнюються з цими моделями.

Якщо фіксується відхилення від звичної поведінки (наприклад, зростання обсягу вихідного трафіку з певного вузла, підключення до нетипових портів або встановлення зв’язку з незвичними хостами) система розцінює це як потенційну загрозу і створює попередження або блокує відповідну активність. Особливо цінним є те, що поведінковий підхід дозволяє виявляти атаки нульового дня, невідомі експлойти або внутрішні загрози, які не мають відомих сигнатур.

Для тестування поведінкового підходу в скрипті test_IPS.py було проведено зміни, які показано на рисунку 3.7.

```
 9 # Дані для надсилання
10 payload = "NEW_attack\n"
11
12 # Кількість пакетів і затримка
13 packet_count = 40                # Скільки разів надіслати
14 delay = 0.01                     # Затримка між надсиланнями у секундах
```

Рисунок 3.7 – Фрагмент зміненого скрипту test_IPS.py

Було змінено три ключові параметри:

- `payload` тепер містить рядок "NEW_attack\n" - це нова сигнатура, яка невідома для IPS;
- `packet_count = 40` - скрипт тепер надсилає 40 запитів;
- `delay = 0.01` - затримка між кожним надсиланням становить 1/100 секунди, тобто частота надсилання значно зросла.

Ці зміни імітують аномальну поведінку, характерну для атак типу HTTP Flood, що ма.nm високу інтенсивність у короткий проміжок часу. Таким чином, тестовий скрипт навмисно буде створювати умови для спрацювання поведінкового правила Suricata, яке було визначено на основі частоти запитів (див. рисунок 3.8).

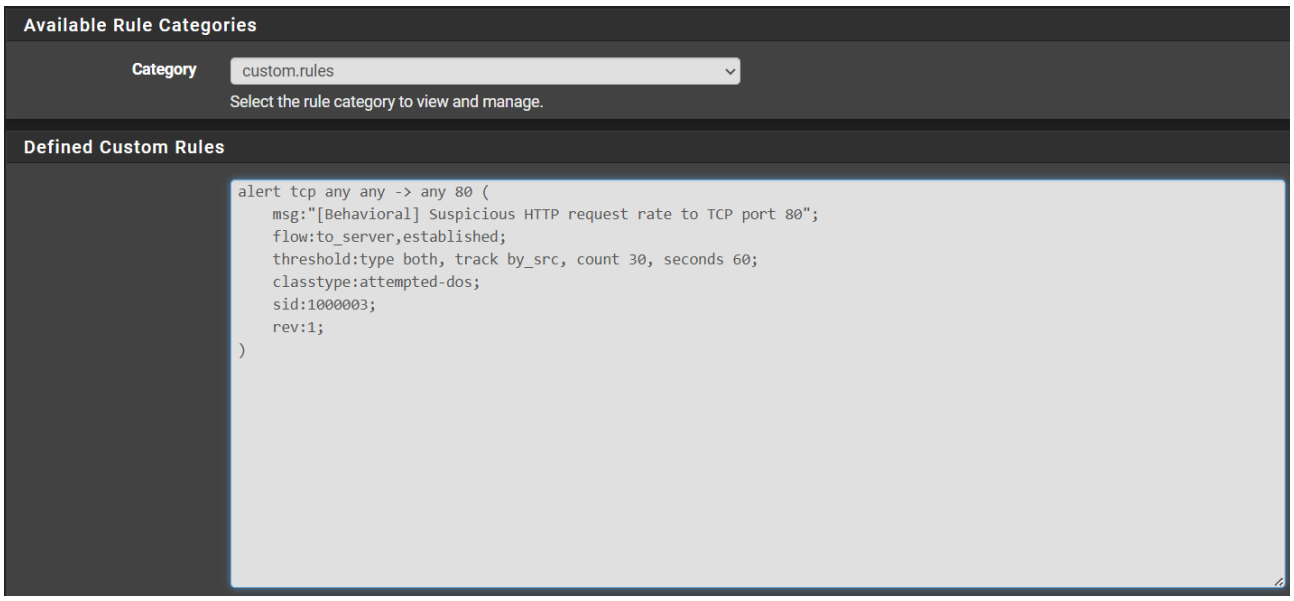

Рисунок 3.8 – Поведінкове правило IPS Suricata

Елементи правила:

- tcp any any -> any 80 - правило застосовується до запитів, що йдуть до TCP порту 80;
- threshold:type both, track by_src, count 30, seconds 60 - спрацьовує, якщо з одного джерела надійшло понад 30 -запитів за 60 секунд;

- classtype:attempted-dos - тип загрози - спроба DoS-атаки.
- sid:1000003- унікальний ідентифікатор правила;
- rev:1 - версія правила.

Це правило реалізує поведінковий аналіз. Воно не прив'язане до фіксованого контенту (як у сигнатурних правилах), а базується на швидкості та частоті трафіку, що характерно для поведінкових аномалій.

На рисунку 3.9 показано вкладку "Alerts", яка використовується для перегляду журналу спрацювань системи IPS.

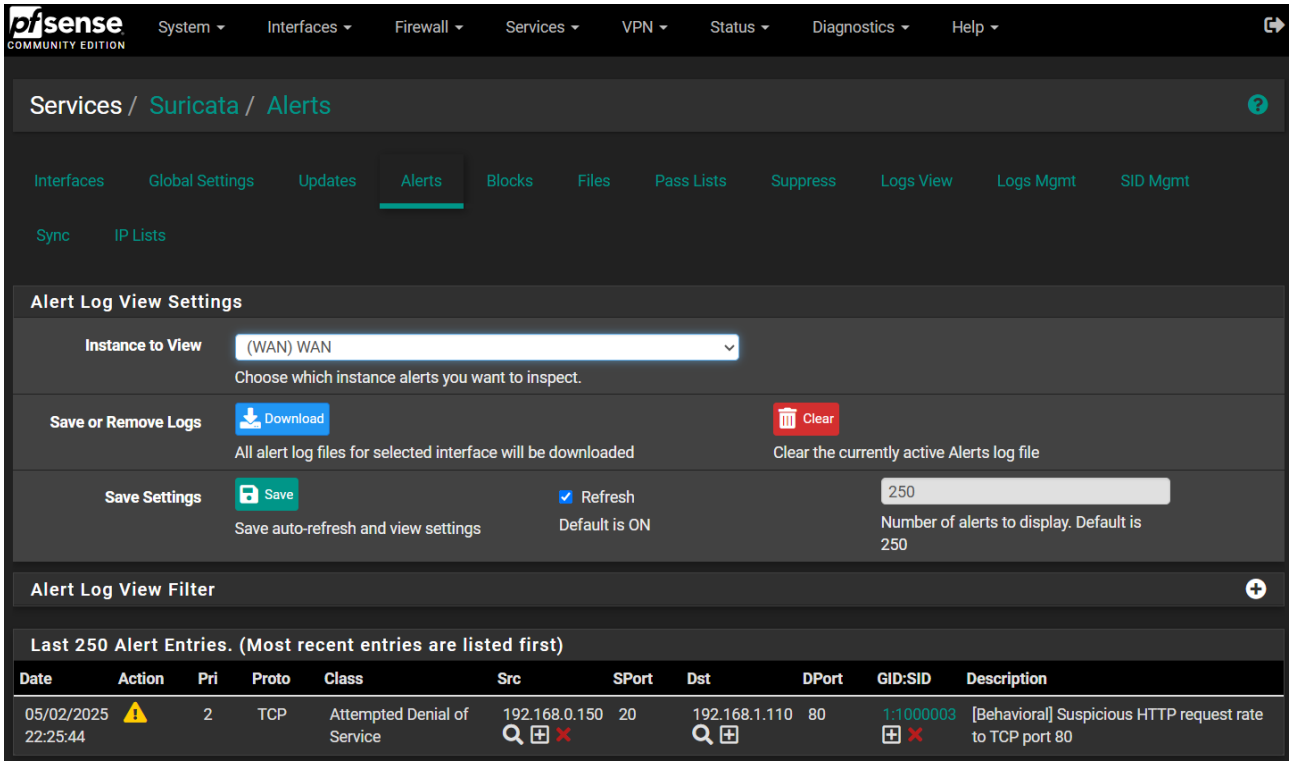

Рисунок 3.9 – Журнал сповіщень IPS Suricata при спрацюванні поведінкового правила

Оскільки нова сигнатура не була прописана в правилах IPS то як можна побачити з рисунку, що спрацювання Suricata було не через сигнатуру з конкретною послідовністю байтів, а внаслідок виявлення аномальної поведінки.

На рисунку 3.10 представлено список IP-адрес, автоматично заблокованих IPS Suricata при спрацюванні поведінкового правила.

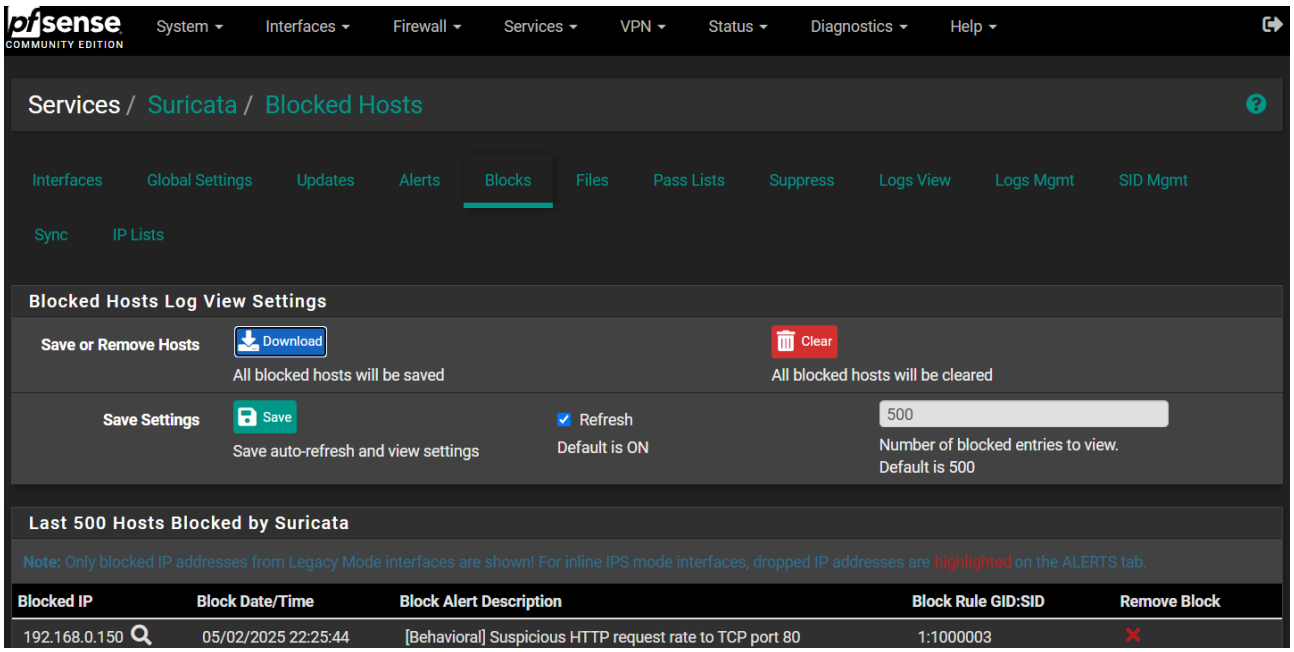

Рисунок 3.10 – Заблокована IP-адреса при спрацюванні поведінкового правила

Suricata не лише виявила аномалію, а й вжила активних заходів - додала IP до списку заблокованих.

Поведінковий аналіз часто реалізується за допомогою алгоритмів машинного навчання [35,36] або статистичного аналізу. Системи можуть самонавчатись у процесі роботи, коригуючи моделі відповідно до нових даних, що покращує їхню адаптивність. Перевагою поведінкового підходу є його здатність ідентифікувати нові й цілеспрямовані атаки, зокрема ті, що маскуються під легітимний трафік. Проте він має і недоліки. Найбільша складність - це високий рівень хибнопозитивних спрацювань, особливо у великих динамічних середовищах, де "нормальна" поведінка постійно змінюється. Налаштування системи може вимагати ретельного калібрування, визначення порогів аномалій щоб уникнути зайвого блокування легального трафіку.

Сучасні IPS часто використовують гібридний підхід, поєднуючи сигнатурне виявлення з поведінковим аналізом, що дозволяє досягати балансу між точністю, продуктивністю і здатністю виявляти невідомі атаки. Поведінкові механізми використовуються також як друга лінія захисту -

спочатку активуються сигнатури, а при їх неефективності включається аналіз аномалій.

3.5 Висновок до третього розділу

В третьому розділі було проведено практичне тестування сигнатурного та поведінкового підходів у системі запобігання вторгненням Suricata, яка працює на маршрутизаторі pfSense. У межах перевірки сигнатурного підходу було реалізовано спеціальне користувацьке правило Suricata, призначене для виявлення у трафіку послідовності символів “malicious_code”. Для генерації відповідного навантаження був створений скрипт на python, який у встановленій кількості з певною частотою надсилав послідовність символів на порт HTTP-сервера Ubuntu. В результаті передача фіксувалась у журналі сповіщень Suricata, що засвідчує повну працездатність сигнатурного механізму виявлення загроз. Крім того, система автоматично заблокувала IP-адресу Kali Linux після фіксації інцидентів згідно з правилами блокування, визначеними в політиках IPS. Далі було проведено тестування поведінкового підходу. Для цього було змінено параметри того ж скрипта – нова послідовність символів, значно зменшена затримка між відправленнями та збільшена кількість пакетів, що імітує інтенсивний мережевий трафік на порт 80. Поведінкове правило Suricata, налаштоване на фіксацію частоти запитів понад встановлений поріг, успішно виявило спробу атаки типу HTTP Flood. Це підтверджено записами у журналі сповіщень з відповідним описом аномалії та автоматичним занесенням IP-адреси атакуючого хоста до списку заблокованих.

Результати тестів демонструють ефективність як сигнатурного, так і поведінкового підходів у виявленні та нейтралізації загроз. Сигнатурний підхід забезпечує високу точність при роботі з відомими атаками і мінімальну кількість хибнопозитивних спрацювань, але вимагає регулярного оновлення бази правил. Поведінковий аналіз, у свою чергу, дозволяє виявляти нові, нетипові загрози, однак є більш чутливим до змін у мережевій активності, що

може призводити до хибних блокувань. Тестування підтвердило, що оптимальним підходом у побудові сучасної системи захисту є поєднання обох методів – сигнатурного для точного виявлення відомих атак і поведінкового для виявлення невідомих або аномальних загроз.

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Природне середовище і його забруднення

Природне середовище включає в себе всі живі і неживі компоненти, які взаємодіють між собою утворюючи унікальні екосистеми. Вода, повітря, ґрунт, рослини, тварини і мікроорганізми є основними елементами. Все починається з атмосфери, яка складається з різних газів таких, як азот, кисень і вуглекислий газ, ці гази необхідні для підтримки життя на Землі.

Атмосфера забезпечує захист від шкідливого ультрафіолетового випромінювання сонця а також підтримує кліматичні умови необхідні для життя. Вода є невід'ємною частиною природного середовища.

Вона присутня у океанах, морях, річках, озерах і підземних водах. Вода є життєво необхідною для всіх живих організмів. Вона використовується для пиття, приготування їжі, сільського господарства та промисловості.

Ґрунт також є важливою частиною природного середовища. Він забезпечує рослини поживними речовинами і підтримує їх ріст. Ґрунт також грає важливу роль у кругообігу води і вуглецю.

Рослини і тварини складають біотичну частину природного середовища. Вони взаємодіють між собою і з неживими компонентами утворюючи складні екосистеми. Рослини забезпечують їжу для тварин і людей, а також відіграють важливу роль у фотосинтезі виробляючи кисень.

Тварини у свою чергу відіграють важливу роль у підтримці екологічного балансу. Природне середовище піддається впливу різних факторів які можуть спричиняти його забруднення.

Забруднення може бути природним або антропогенним тобто спричиненим людською діяльністю. Природні забруднення включають: вулканічні виверження, лісові пожежі і пилові бурі, які можуть викидати в атмосферу велику кількість газів і часток [37]. Проте антропогенні забруднення є найбільш значущими і тривалими. Джерела антропогенного забруднення

включають промисловість, транспорт, сільське господарство і побутову діяльність.

Промислові викиди є одним з основних джерел забруднення повітря і води. Вони включають викиди шкідливих газів таких як, діоксид сірки і оксиди азоту, а також важких металів і органічних речовин.

Транспорт також спричиняє значне забруднення викидаючи в атмосферу велику кількість вихлопних газів, які містять оксиди вуглецю, азоту і інші шкідливі речовини [37].

Сільське господарство спричиняє забруднення ґрунту і води через використання пестицидів і добрив, які можуть потрапляти у водні об'єкти і ґрунт.

Побутові викиди включають: сміття і відходи, які можуть забруднювати ґрунт і водні об'єкти. Наслідки забруднення природного середовища є різноманітними і можуть бути дуже серйозними [38]. Забруднення повітря може спричиняти проблеми зі здоров'ям у людей такі як респіраторні захворювання і серцево-судинні проблеми. Воно також може спричиняти кислотні дощі які пошкоджують рослини, ґрунт і водні об'єкти. Забруднення води може спричиняти загибель водних організмів і зниження якості питної води, що може мати серйозні наслідки для здоров'я людей. Забруднення ґрунту може призводити до зниження родючості ґрунту і зниження врожайності рослин. Боротися із забрудненням природного середовища можна різними способами [38].

Одним з найбільш ефективних способів є зменшення викидів шкідливих речовин через впровадження екологічно чистих технологій і використання альтернативних джерел енергії. Такими джерелами є сонячна вітрова і гідроенергія, які не спричиняють викидів шкідливих речовин. Важливим є також впровадження систем управління відходами, які дозволяють зменшити кількість сміття і забезпечити його правильну утилізацію або переробку. Освіта і підвищення обізнаності громадськості про проблеми забруднення природного середовища також є важливими заходами, які можуть сприяти зміні поведінки

людей і зменшенню забруднення. Іншими заходами є збереження природних ресурсів і захист природних екосистем через створення природоохоронних територій і заповідників ці території забезпечують захист різноманітних видів рослин і тварин і підтримують екологічний баланс [38]. Природне середовище є надзвичайно важливим для життя на Землі і його забруднення може мати серйозні наслідки для здоров'я людей і стану екосистем. Тому важливо вживати заходів для зменшення забруднення і збереження природного середовища для майбутніх поколінь.

4.2 Психофізіологічне розвантаження для працівників

Психофізіологічне розвантаження є важливим аспектом підтримання здоров'я та працездатності працівників, особливо тих, хто працює в умовах підвищеного стресу або фізичного навантаження. Різноманітні методи релаксації та відновлення допомагають знижувати стрес, покращують фізичне самопочуття та сприяють підвищенню продуктивності. Основні заходи психофізіологічного розвантаження включають організацію робочого місця, впровадження регулярних перерв, використання спеціальних технік релаксації та підтримання здорового способу життя.

Перш за все, важливо забезпечити правильну організацію робочого місця. Ергономічні меблі, належне освітлення та достатня кількість простору для рухів сприяють зниженню фізичного та психічного напруження. Працівники повинні мати можливість зручно розташувати всі необхідні інструменти та обладнання, уникати тривалого сидіння в одному положенні та забезпечувати правильну поставу.

Регулярні перерви під час роботи є необхідними для зменшення втоми та напруження. Вони дозволяють працівникам відволіктися від робочих обов'язків, розслабитися та відновити енергію. Під час перерв можна виконувати легкі фізичні вправи, які допомагають зняти м'язове напруження та покращити кровообіг. Також корисним є проведення коротких сеансів

медитації або дихальних вправ, які сприяють заспокоєнню нервової системи та зниженню рівня стресу [39].

Використання спеціальних технік релаксації є ефективним способом зниження стресу та напруги. До них відносяться прогресивна м'язова релаксація, яка полягає в поетапному напруженні та розслабленні різних груп м'язів, та аутогенне тренування, що включає самонавіювання для досягнення стану розслаблення. Також популярними є йога та медитація, які поєднують фізичні вправи з дихальними техніками та концентрацією уваги.

Підтримання здорового способу життя є ключовим фактором для зниження рівня стресу та підтримання загального фізичного та психічного здоров'я. Збалансоване харчування, регулярна фізична активність, достатній сон та відмова від шкідливих звичок (таких як паління та надмірне вживання алкоголю) сприяють підвищенню стійкості до стресу та покращують загальне самопочуття. Важливо також забезпечити працівникам можливість відпочинку та відновлення після робочого дня, включаючи проведення часу на свіжому повітрі та заняття улюбленими справами .

Соціальна підтримка та позитивна атмосфера на робочому місці також є важливими аспектами психофізіологічного розвантаження. Підтримка з боку колег та керівництва, можливість відкрито обговорювати проблеми та ділитися думками сприяють зниженню рівня стресу та покращенню настрою. Організація спільних заходів, таких як тренінги з управління стресом, командні будівельні активності та святкування корпоративних подій, допомагає зміцнити командний дух та покращити взаємодію між працівниками .

Важливим аспектом психофізіологічного розвантаження є забезпечення гнучкості робочого графіка. Гнучкий робочий графік дозволяє працівникам краще управляти своїм часом, що сприяє зниженню стресу та покращенню балансу між роботою та особистим життям. Можливість працювати з дому або мати гнучкі години роботи допомагає працівникам краще адаптуватися до особистих потреб та обов’язків, що позитивно впливає на їхнє психічне здоров'я.

Крім того, впровадження програм фізичних активностей на робочому місці є ефективним способом покращення психофізіологічного стану працівників. Це можуть бути групові заняття спортом, організація спортивних змагань або надання доступу до тренажерних залів. Фізичні вправи сприяють зняттю стресу, покращенню настрою та загальному зміцненню організму. Також важливо проводити регулярні тренінги з правильного виконання фізичних вправ, щоб уникнути травм та забезпечити максимальну користь для здоров'я .

Підтримка ментального здоров'я працівників є ще одним важливим аспектом. Компанії можуть надавати психологічну підтримку через консультації з психологами, тренінги з управління стресом та іншими психотерапевтичними методами. Регулярні зустрічі з фахівцями допомагають працівникам вирішувати особисті та професійні проблеми, знижуючи рівень стресу та покращуючи психічне здоров'я.

4.3 Висновок до четвертого розділу

В четвертому розділі було розглянуто важливі аспекти, пов’язані з безпекою життєдіяльності та охороною праці, зокрема вплив природного середовища на здоров’я людини, а також методи психофізіологічного розвантаження працівників.

Детально проаналізовано структуру та компоненти природного середовища, включаючи атмосферу, воду, ґрунт, флору і фауну, а також визначено основні фактори забруднення довкілля – як природні, так і антропогенні. Особливу увагу приділено впливу промислових, транспортних, сільськогосподарських і побутових джерел забруднення, а також їх негативному впливу на здоров’я людей і стан екосистем. Розглянуто практичні шляхи зменшення забруднення, серед яких впровадження екологічних технологій, альтернативних джерел енергії, систем управління відходами та підвищення екологічної обізнаності населення.

Висвітлено актуальність психофізіологічного розвантаження працівників у контексті підтримання їх здоров’я, підвищення працездатності та зниження рівня стресу. Описано сучасні методи розвантаження, включаючи організацію ергономічного робочого середовища, впровадження регулярних перерв, застосування технік релаксації, фізичну активність, психологічну підтримку та формування сприятливого соціального клімату в колективі. Особливо підкреслено значення гнучкого робочого графіка та комплексного підходу до підтримки ментального та фізичного благополуччя працівників.

Таким чином, розділ демонструє важливість забезпечення екологічної безпеки та належних умов праці як ключових чинників сталого розвитку, охорони здоров’я та ефективності працівників.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було проведено дослідження ефективності сигнатурного та поведінкового підходів для виявлення і запобігання мережевим атакам на прикладі системи IPS Suricata, встановленої в маршрутизаторі в pfSense. Дослідження виконувалося у віртуальному лабораторному середовищі на базі VMware Workstation з використанням операційних систем Kali Linux (як джерело атак) та Ubuntu Linux (як цільовий вузол).

У першому розділі було розглянуто актуальність проблеми захисту комп'ютерних мереж та загальні принципи роботи систем IPS. Надано порівняльний огляд сигнатурного та поведінкового методів виявлення, зокрема їхні переваги, недоліки та можливості комбінованого застосування.

У другому розділі було описано процес створення лабораторного середовища для тестування IPS на базі pfSense. Віртуальне середовище включало операційну систему Kali Linux для запуску атак, цільовий сервер Ubuntu Linux та міжмережевий екран із налаштованою системою IPS Suricata. Проведено початкове налаштування мережевих інтерфейсів, правил фільтрації та журналювання подій у pfSense, а також встановлення й активацію Suricata з розмежуванням внутрішнього й зовнішнього трафіку.

У третьому розділі проведено практичне тестування ефективності обох підходів. У ході дослідження підтверджено, що сигнатурний метод є високоефективним у виявленні відомих атак з мінімальною кількістю хибнопозитивних спрацювань, тоді як поведінковий підхід забезпечує виявлення нетипової активності, у тому числі нових або змінених атак, але потребує ручної оптимізації правил та валідації результатів.

Отримані результати засвідчують доцільність комбінованого підходу, що поєднує точність сигнатурного методу з гнучкістю поведінкового аналізу, особливо у високонавантажених або критичних інформаційних системах. Реалізація такої системи на основі IPS Suricata в pfSense є ефективним

рішенням для побудови відкритої, гнучкої та масштабованої архітектури мережевої безпеки.

Подальші дослідження можуть бути зосереджені на використанні машинного навчання для покращення поведінкового аналізу. Результати дослідження можуть бути застосовані в побудові систем мережевого захисту для малих і середніх підприємств, освітніх установ, державних структур, а також як навчальний матеріал. Завдяки відкритому коду та гнучким налаштуванням, рішення на основі pfSense і IPS Suricata можуть ефективно використовуватись в умовах обмежених бюджетів для забезпечення базового рівня захисту мережевої інфраструктури.

ПЕРЕЛІК ДЖЕРЕЛ

1. What is SQL injection (sqli)? Types & examples. part 1. (n.d.). Retrieved from https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1

2. Cross site scripting (XSS) attack - Types and Examples. (n.d.). Retrieved from https://www.wallarm.com/what/what-is-xss-cross-site-scripting

3. What is a ddos attack? Ddos meaning, definition & types | fortinet. (n.d.). Retrieved from https://www.fortinet.com/resources/cyberglossary/ddos-attack

4. What is a botnet? Definition, types, examples of attack. (n.d.). Retrieved from https://www.wallarm.com/what/what-is-a-botnet

5. What is the Mirai Botnet? Cloudflare. (n.d.). URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

6. SYN flood attack. Cloudflare. (n.d.). URL: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

7. 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.

8. UDP flood attack. Cloudflare. (n.d.). URL: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

9. 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.

10. Ping (ICMP) flood DDoS attack. Cloudflare. (n.d.). URL: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/

11. HTTP flood attack. Cloudflare. (n.d.). URL: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/

12. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

13. What is slowloris ddos attack? Mitigation methods. (n.d.). Retrieved from https://www.wallarm.com/what/what-is-slowloris

14. 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.

15. DNS amplification attack. Cloudflare. (n.d.). URL: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

16. What is NTP amplification DDOS attack? Overview 2025. (n.d.). Retrieved from https://www.wallarm.com/what/ntp-amplification-attack-what-is-it

17. MITM - what is man in the middle attack? How to prevent? (n.d.). Wallarm | Advanced API Security. https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack

18. 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.

19. What is a brute force attack? Definition, types & how it works | fortinet. (n.d.). Retrieved from https://www.fortinet.com/resources/cyberglossary/brute-force-attack

20. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.

21. What is an intrusion detection system? (n.d.). Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids

22. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.

23. What is an intrusion prevention system? (n.d.). Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

24. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

25. Signature based vs anomaly based IDS. (n.d.). Retrieved from https://fidelissecurity.com/cybersecurity-101/learn/signature-based-vs-anomaly-based-ids/

26. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

27. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

28. Inc, C. (2025, April 24). Using VMware Workstation Pro. Retrieved from https://techdocs.broadcom.com/us/en/vmware-cis/desktop-hypervisors/workstation-pro/17-0/using-vmware-workstation-pro.html

29. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146. https://doi.org/10.62731/mcnd-24.05.2024.001

30. PfSense documentation | pfsense documentation. (n.d.). Netgate Documentation | Netgate Documentation. https://docs.netgate.com/pfsense/en/latest/

31. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081

32. Suricata User Guide (n.d.). Suricata documentation. https://docs.suricata.io/en/latest/

33. Ubuntu desktop guide. (n.d.). Retrieved from https://help.ubuntu.com/lts/ubuntu-help/index.html

34. Kali docs | kali linux documentation. (n.d.). Kali Linux. https://www.kali.org/docs/

35. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N. & Tymoshchuk, V.(2024). Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 3842, 184–195.

36. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

37. Вбивча природа: як забруднення навколишнього середовища впливає на здоров'я. Новини України - останні новини України сьогодні - УНІАН. URL: https://www.unian.ua/ecology/1304769-vbivcha-priroda-yak-zabrudnennya-navkolishnogo-seredovischa-vplivae-na-zdorovya.html (date of access: 21.06.2024).

38. Сайт журналу «Геоінформатика» Головна - Сайт журналу «Геоінформатика». URL: https://www.geology.com.ua/wp-content/uploads/2015/05/15_Stakhiv.pdf (date of access: 21.06.2024).

39. Основи психофізіології та фізіології вищої нервової діяльності. Навчально-методичний посібник. URL: https://www.dkpp.com.ua/wp-content/uploads/2024/03/sylabus_psykhofiziolohiia_io_2024.pdf (date of access: 29.05.2024).

ДОДАТКИ

Додаток А

Скрипт test_IPS.py

```
import socket
import time
from datetime import datetime

# Налаштування цілі
target_ip = '192.168.1.110'      # IP-адреса цільового сервера
target_port = 80                 # Порт HTTP
# Кількість пакетів і затримка
packet_count = 10                # Скільки разів надіслати payload
delay = 1.0                          # Затримка між надсиланнями у
секундах

# Дані для надсилання
payload = "malicious_code\n"

# Файл логування
log_file = "attack_log.txt"

# Функція логування у файл
def log(message):
    timestamp = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
    entry = f"[{timestamp}] {message}"
    print(entry)
    with open(log_file, "a") as f:
        f.write(entry + "\n")

try:
    with   socket.socket(socket.AF_INET,   socket.SOCK_STREAM)   as
sock:
        log(f"Connecting to {target_ip}:{target_port}...")
        sock.settimeout(5)
```

```
            sock.connect((target_ip, target_port))
            log("Connection established.")

            for i in range(packet_count):
                sock.sendall(payload.encode())
                log(f"Packet    {i    +    1}/{packet_count}    sent:
'{payload.strip()}'")
                time.sleep(delay)

            # Отримання відповіді від сервера
            try:
                response = sock.recv(1024)
                log("Response received:")
                log(response.decode(errors='ignore'))
            except socket.timeout:
                log("No response from target (timeout).")

    except socket.timeout:
        log("Connection timed out.")
    except ConnectionRefusedError:
        log("Connection refused by target.")
    except Exception as e:
        log(f"Error occurred: {e}")
```