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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Дослідження ефективності IPS у виявленні та запобіганні SQL Injection атакам"

Виконав: студент (ка) IV курсу, групи СБ-42
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Пакош Андрій Володимирович
підпис (прізвище та ініціали)

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

Нормоконтроль Дроздова Т. В.
підпис (прізвище та ініціали)

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

Рецензент
підпис (прізвище та ініціали)

м. 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 кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Пакошу Андрію Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження ефективності IPS у виявленні та запобіганні SQL Injection атакам

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

Затверджені наказом ректора від « 02 » 05 2025 року № 4/7-361

2. Термін подання студентом завершеної роботи 12.06.2025

3. Вихідні дані до роботи Документація pfSense, Snort, Suricata. Вимоги до IPS.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд предметної області
2. Розробка середовища тестування сценаріїв SQL injection атак
3. Тестування та оцінка ефективності IPS Suricata та Snort
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. 5. Принцип виконання SQL Injection атаки. 6. Схема класифікації SQL Injection атак. 7. Схема тестового середовища. 8. Елементи тестового середовища. 9. Сценарій перший з IPS Suricata. 10. Оцінка ефективності IPS Suricata. 11. Сценарій другий з IPS Snort. 12. Оцінка ефективності IPS Snort. 13. Висновки. 14. Завершальний.

6. Консультанти розділів роботи

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

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2025	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд предметної області»	21.02 – 10.03	
4.	Оформлення розділу «Розробка середовища тестування сценаріїв SQL injection атак»	11.03 – 25.03	
5.	Оформлення розділу «Тестування та оцінка ефективності IPS Suricata та Snort»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	26.06.2025	

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

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

АНОТАЦІЯ

Дослідження ефективності IPS у виявленні та запобіганні SQL Injection атакам // Кваліфікаційна робота ОР «Бакалавр» // Пакош Андрій Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-42 // Тернопіль, 2025 // С. 60, рис. – 20, табл. – - , кресл. – 14, додат. – 0.

Ключові слова: SQL Injection, pfSense, Snort, Suricata, IPS.

У кваліфікаційній роботі бакалавра було розглянуто одну з найбільш небезпечних для веб-застосунків атак – SQL Injection. Розкрито суть і механізми здійснення різновидів SQL-ін'єкцій, проаналізовано їхні наслідки для безпеки баз даних. Розроблено й протестовано спеціальне віртуальне середовище на базі VMware в основі якого є pfSense, де впроваджено системи виявлення та запобігання вторгненням Snort і Suricata. Досліджено їхню здатність виявляти та блокувати SQL Injection атаки за допомогою інструмента sqlmap на вразливому веб-додатку Mutillidae. У ході експериментів оцінено ефективність різних режимів роботи (IDS та IPS) і проведено аналіз результатів. Результати підтвердили високу точність обох IPS-систем у блокуванні несанкціонованих SQL-запитів та можуть бути корисними для фахівців у галузі кібербезпеки й адміністрування мереж з метою підвищення безпеки веб-застосунків.

ANNOTATION

Study of IPS Effectiveness in Detecting and Preventing SQL Injection Attacks // Thesis of educational level "Bachelor"// Andrii Pakosh // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-42 // Ternopil, 2025 // P. 60, figs. 20, tables -, drawings 14, added. 0.

Keywords: SQL Injection, pfSense, Snort, Suricata, IPS.

In the bachelor's thesis, one of the most dangerous attacks for web applications - SQL Injection - was considered. The essence and mechanisms of various types of SQL injections were revealed, and their consequences for database security were analysed. A special VMware-based virtual environment powered by pfSense has been developed and tested, where Snort and Suricata intrusion detection and prevention systems have been implemented. Their ability to detect and block SQL Injection attacks using the sqlmap tool on the vulnerable Mutillidae web application was investigated. During the experiments, the effectiveness of different modes of operation (IDS and IPS) was evaluated and the results were analysed. The results confirmed the high accuracy of both IPS systems in blocking unauthorised SQL queries and can be useful for cybersecurity and network administration professionals to improve the security of web applications.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IPS	—	Intrusion Prevention System
IDS	—	Intrusion Detection System
SQL	—	Structured Query Language
DNS	—	Domain Name System
HTTP	—	HyperText Transfer Protocol
SIEM	—	Security Information and Event Management
NIPS	—	Network-based IPS
HIPS	—	Host-based IPS
WIPS	—	Wireless IPS
WAN	—	Wide Area Network
NAT	—	Network Address Translation
VPN	—	Virtual Private Network
LAN	—	Local Area Network
DHCP	—	Dynamic Host Configuration Protocol

ВСТУП

Актуальність теми. З розвитком веб-технологій і зростанням кількості онлайн-сервісів підвищується ризик кіберзагроз, спрямованих на порушення цілісності, доступності та конфіденційності даних. Однією з найпоширеніших та найнебезпечніших атак є SQL Injection, що дозволяє зловмисникам отримати несанкціонований доступ до баз даних, викрадати конфіденційну інформацію або змінювати її вміст. Для ефективного захисту від подібних атак використовуються системи виявлення та запобігання вторгненням, які здатні аналізувати мережевий трафік і виявляти підозрілі дії. Серед найпоширеніших рішень у цій сфері є Snort і Suricata - відкриті системи, що використовуються для моніторингу та захисту мережевих середовищ. Актуальність даної роботи полягає в необхідності дослідження ефективності IPS у виявленні та запобіганні SQL Injection атакам. Отримані результати допоможуть визначити, наскільки ефективними є такі системи у реальних умовах.

Мета і задачі дослідження. Метою дослідження є аналіз ефективності IPS Snort і Suricata у виявленні SQL Injection атак.

Для досягнення цієї мети необхідно вирішити такі завдання:

- провести огляд SQL Injection атак та наслідків;
- дослідити принципи роботи систем IPS та їхню класифікацію;
- розробити сценарії SQL Injection атак для тестування IPS;
- налаштувати тестове середовище, що включає pfSense (IPS Suricata та Snort), Metasploitable VM та Kali Linux;
- провести експериментальне тестування IPS у реальному середовищі та проаналізувати результати;
- оцінити ефективність Snort і Suricata у виявленні SQL Injection атак.

Об’єкт дослідження. Об’єктом дослідження є системи виявлення та запобігання вторгненням, що використовуються для захисту інформаційних систем від атак.

Предмет дослідження. Предметом дослідження є ефективність IPS Suricata та Snort у виявленні та запобіганні SQL Injection атакам у реальному мережевому середовищі.

Практичне значення одержаних результатів. Результати дослідження можуть бути корисними для системних адміністраторів, фахівців з кібербезпеки та організацій, які займаються захистом веб-додатків. Оцінка ефективності IPS дозволить обрати оптимальне рішення для забезпечення безпеки інформаційних систем, а також розробити рекомендації щодо підвищення ефективності захисту від SQL Injection атак. Дослідження також сприятиме покращенню підходів до налаштування та використання IPS, що дозволить мінімізувати ризики атак та підвищити рівень безпеки веб-додатків.

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 SQL injection атаки

1.1.1 Огляд SQL Injection атак

SQL Injection - це тип атаки на веб-додатки, що використовують бази даних. Вона відбувається, коли зловмисник вводить шкідливий SQL-код у поле вводу або запит, який виконується на сервері [1]. Якщо система недостатньо захищена, атака дозволяє отримати доступ до конфіденційних даних, змінювати або видаляти їх, а іноді виконувати адміністративні команди на сервері. Ця атака базується на маніпуляції SQL-запитами, які використовуються веб-додатками для взаємодії з базами даних (див. рисунок 1.1).

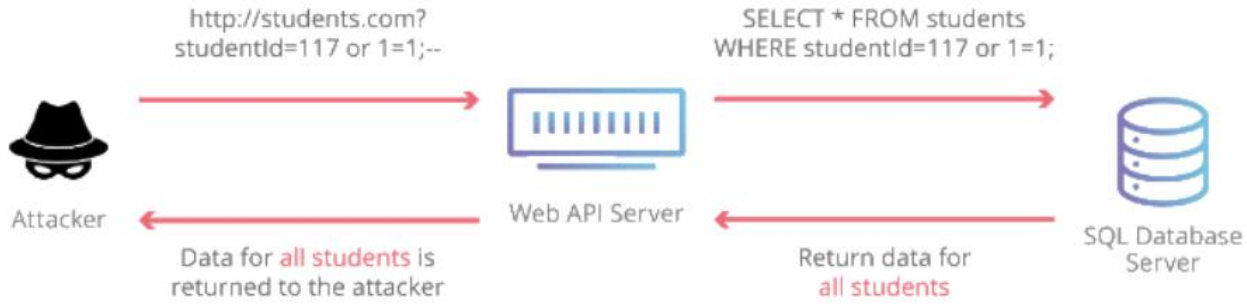

Рисунок 1.1 – Принцип виконання SQL Injection атаки

Вразливі додатки зазвичай використовують динамічне формування SQL-запитів без належної перевірки введених даних, що дозволяє зловмиснику змінювати їхню структуру та виконувати небажані команди.

На рисунку 1.2 представлено схему класифікації SQL-Injection атак [2].

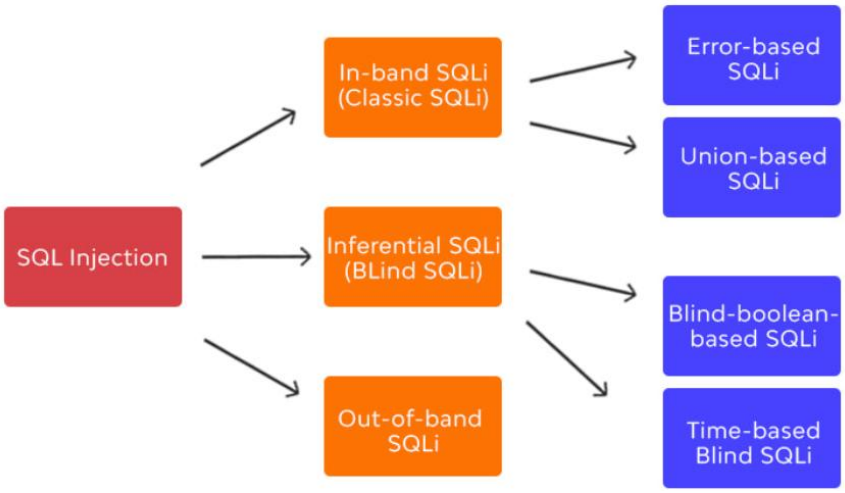

Рисунок 1.2 – Схема класифікації SQL Injection атак

Зазвичай веб-додатки отримують дані від користувача через форми, параметри URL або HTTP-запити [3]. Додавання SQL-коду в користувацьке введення є одним із найпоширеніших механізмів SQL Injection атак. Ця техніка базується на тому, що веб-додатки приймають введені користувачем дані і вставляють їх у SQL-запити без належної перевірки. Якщо введене значення потрапляє до запиту без обробки, зловмисник може модифікувати його структуру і виконати довільні SQL-команди.

Наприклад, веб-додаток може використовувати SQL-запит для автентифікації користувача на основі його імені та пароля `SELECT * FROM users WHERE username = '$user' AND password = '$pass';`

Якщо користувач вводить своє ім'я та пароль, система підставляє їх у запит і виконує його. Однак, якщо введене значення містить шкідливий SQL-код, запит може змінитися так, що дозволить обійти систему автентифікації.

Наприклад, якщо зловмисник у поле пароля введе такий рядок `'OR '1'='1`, то підставлений SQL-запит виглядатиме як `SELECT * FROM users WHERE username = 'admin' AND password = '' OR '1'='1';`

У цьому випадку `'1'='1'` завжди істинне, що дозволяє обійти перевірку пароля і авторизуватися без нього.

Використання логічних операторів у SQL-запитах дозволяє змінювати логіку виконання SQL-запиту шляхом введення додаткових умов, які завжди дають істинне значення або впливають на отримані результати. Найчастіше

використовуються оператори OR, AND, UNION, які можуть змінити очікувану поведінку запиту та дозволити зловмиснику отримати доступ до конфіденційних даних або обійти механізми автентифікації.

Наприклад, якщо веб-додаток формує такий SQL-запит для отримання інформації про користувача `SELECT id, username FROM users WHERE username = '$user';`

Зловмисник може ввести в поле введення такий рядок `' UNION SELECT null, version() --`

Що змінить запит на `SELECT id, username FROM users WHERE username = '' UNION SELECT null, version() --';`

В результаті веб-додаток поверне інформацію про версію бази даних.

Додавання SQL-коду в користувацьке введення також може використовуватися для виконання шкідливих команд, наприклад, видалення таблиць `'; DROP TABLE users; --,` що призведе до виконання такого запиту `SELECT * FROM users WHERE username = ''; DROP TABLE users; --';`

Якщо база даних дозволяє виконання кількох команд у запиті, таблиця `users` буде повністю видалена.

Використання коментарів для обходу перевірок дозволяє зловмиснику ігнорувати частину SQL-запиту, що може бути критично важливим для автентифікації або обмеження доступу. У різних системах управління базами даних використовуються різні символи коментування, зокрема --, # та /* ... */, що дозволяють ігнорувати частину вихідного коду запиту.

Експлуатація помилок у SQL-запитах (Error-based SQL Injection) є одним із ефективних методів SQL Injection, який дозволяє зловмиснику отримувати інформацію про структуру бази даних, типи її полів, кількість колонок у таблиці та інші деталі, які можуть бути використані для подальших атак [4]. Цей метод заснований на тому, що багато веб-додатків недостатньо добре обробляють помилки, які повертає база даних, і відображають їх безпосередньо користувачеві. Якщо веб-додаток будує SQL-запити динамічно і не застосовує механізми обробки помилок, будь-яка невірна зміна структури запиту може

викликати повідомлення про помилку, що дозволяє атакуючому визначити критичні параметри бази даних.

Використання Time-based SQL Injection є однією з технік Blind SQL Injection, що застосовується в ситуаціях, коли сервер не повертає помилки чи інші явні відповіді, які можуть допомогти атакуючому отримати інформацію про базу даних. Замість цього зловмисник вводить SQL-запит, який впливає на час виконання операції, а потім аналізує затримку відповіді від сервера. Якщо сервер реагує з певною затримкою, це свідчить про те, що запит успішно виконано, що дозволяє зловмиснику отримувати інформацію навіть без прямого доступу до результатів запитів. Одним із основних способів реалізації такої атаки є використання функції SLEEP() у MySQL, pg_sleep() у PostgreSQL або WAITFOR DELAY у Microsoft SQL Server. Ці функції дозволяють затримати виконання SQL-запиту на заданий період часу, що дає можливість зловмиснику визначати наявність вразливості.

Boolean-Based (Content-Based) Blind SQL Injection – це метод який використовується в ситуаціях, коли сервер не повертає явних помилок або даних у відповідь, але змінює поведінку або вміст сторінки залежно від результату виконання SQL-запиту. Ця техніка дозволяє атакуючому визначити істинність або хибність певного твердження у SQL-запиті та поступово витягувати дані з бази даних, аналізуючи зміни у відповіді сервера.

Використання Out-of-band SQL Injection є однією з технік SQL-ін'єкції, яка застосовується у випадках, коли зловмисник не може отримати дані безпосередньо через стандартні відповіді сервера або не може використовувати традиційні методи Blind SQL Injection, такі як Error-based чи Time-based. Цей метод передбачає передачу інформації на зовнішні сервери, які контролює атакуючий, через альтернативні канали зв’язку, зокрема DNS-запити або HTTP-запити. Основна ідея Out-of-band SQL Injection полягає в тому, що атакуючий змушує базу даних або сервер додатка робити запити до сторонніх ресурсів, що дозволяє йому отримати дані, навіть якщо безпосередній вивід на веб-сторінку або консоль заблокований. Цей метод ефективний у випадках, коли сервер має вихідне з'єднання з інтернетом і може виконувати зовнішні запити. Out-of-band

SQL Injection є складнішою у виконанні, ніж інші методи SQL-ін'єкції, але вона дуже ефективна у випадках, коли атакуючий не може отримати безпосередній доступ до відповідей сервера. Це робить її популярним інструментом у руках досвідчених кіберзлочинців.

Використання підзапитів для обходу захисту є однією з технік SQL Injection, яка дозволяє атакуючому отримувати дані навіть у випадках, коли основний SQL-запит містить перевірки або обмеження. Підзапити (subqueries) використовуються для вкладених запитів у межах основного SQL-запиту, що дозволяє обходити фільтрацію введених даних, а також отримувати додаткову інформацію про структуру бази даних.

1.1.2 Наслідки SQL Injection атак

Наслідки атак SQL Injection можуть бути вкрай руйнівними для організацій, оскільки вони безпосередньо впливають на цілісність та доступність даних у базах даних. Одним із найсерйозніших наслідків є несанкціонований доступ до конфіденційної інформації [5]. Зловмисники можуть отримати доступ до чутливих даних, таких як особисті дані користувачів, паролі, фінансова інформація та інші критично важливі записи. Це може призвести до витоку інформації, порушення законодавства щодо захисту персональних даних та значних фінансових втрат через штрафи та компенсації постраждалим користувачам. Ще одним важливим наслідком є зміна або видалення даних. Використовуючи SQL-ін'єкції, атакуючі можуть модифікувати вміст бази даних, видаляти важливі записи або повністю знищувати інформацію, що може паралізувати роботу бізнесу або призвести до серйозних операційних збоїв. У випадку, якщо база даних містить фінансові транзакції, зміна інформації може привести до шахрайства або значних фінансових втрат. Атаки SQL Injection також можуть використовуватися для отримання адміністративного контролю над базою даних або навіть над усією системою. Зловмисники можуть виконати довільні команди, створюючи нові облікові записи з підвищеними привілеями або отримуючи контроль над існуючими адміністративними акаунтами. Це дає

їм змогу маніпулювати даними, видаляти або змінювати інформацію та поширювати шкідливе програмне забезпечення в мережі організації. Ще одним серйозним наслідком є компрометація цілісності веб-додатку або сайту. Якщо атакуючий може змінювати дані в базі, він може підмінити вміст веб-сторінок, вставити шкідливі посилання або впровадити вразливості для подальших атак. Це не тільки шкодить репутації компанії, але й може поставити під загрозу користувачів, які відвідують сайт. Якщо зловмисник генерує ресурсоємні SQL-запити або блокує доступ до важливих таблиць, це може спричинити повне припинення роботи бази даних та порушення функціонування сервісу. Це особливо небезпечно для компаній, які покладаються на постійний доступ до своїх даних, наприклад, онлайн-магазинів або банківських установ.

Репутаційні та фінансові втрати є ще одним серйозним наслідком атак SQL Injection. Витік даних або порушення безпеки можуть суттєво вплинути на довіру клієнтів та партнерів до компанії. Втрата репутації може привести до зниження кількості користувачів, падіння продажів та необхідності витрачати значні ресурси на відновлення довіри. Крім того, компанія може зазнати фінансових втрат через судові позови, штрафи від регуляторних органів та витрати на усунення наслідків атаки.

Наслідки атак SQL Injection можуть бути катастрофічними, охоплюючи фінансові, технічні та репутаційні втрати. Вони можуть впливати не лише на компанії, а й на кінцевих користувачів, які довірили свої дані. Саме тому захист від SQL-ін'єкцій є критично важливим для будь-якої організації, що працює з базами даних.

1.2 Системи IPS

1.2.1 Визначення та принципи роботи IPS

Система виявлення та запобігання вторгненням є рішенням, яке використовується для моніторингу трафіку, виявлення потенційних загроз і активного блокування шкідливої активності в реальному часі. Вона є

розширенням системи виявлення вторгнень, з тією відмінністю, що IPS не лише ідентифікує загрози, а й автоматично вживає заходів для їх нейтралізації [6].

На рисунку 1.3 представлено схему розташування IPS та IDS систем [7] в мережевій інфраструктурі.

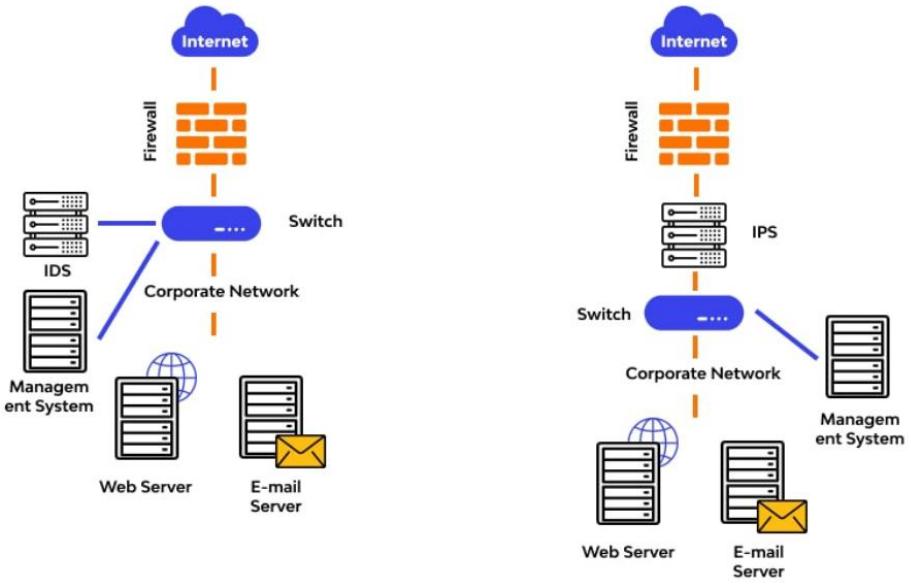

Рисунок 1.3 – Схема розташування IPS та IDS систем в мережевій інфраструктурі

Основна мета IPS - забезпечити захист від кіберзагроз, таких як атаки нульового дня, експлойти вразливостей, DoS-атаки [8] [9] та інші форми несанкціонованого доступу.

Принцип роботи системи запобігання вторгненням полягає в безперервному моніторингу мережевого трафіку або активності хостів з метою виявлення, аналізу та блокування потенційних кіберзагроз у реальному часі. Система IPS відіграє важливу роль у захисті від атак SQL Injection. IPS використовується для виявлення та запобігання таким атакам шляхом аналізу мережевого трафіку та запитів до бази даних у реальному часі. Основним методом захисту є сигнатурний аналіз [10], коли IPS порівнює вхідні SQL-запити з відомими шаблонами атак. Наприклад, якщо виявлено спробу виконання запиту з використанням операторів `OR 1=1` або інших характерних конструкцій SQL Injection, система блокує підозрілий запит та відкидає відповідний трафік. Крім

сигнатурного аналізу, IPS також використовує поведінковий аналіз для виявлення нетипової активності в мережі. Якщо система помічає раптове збільшення складних SQL-запитів, незвичну частоту доступу до бази даних або спроби виконати адміністративні команди через SQL, вона може розцінити це як потенційну атаку. У таких випадках IPS може автоматично закривати сесії підозрілих користувачів, блокувати доступ до веб-додатків та генерувати попередження для адміністраторів.

Однак IPS має певні обмеження у боротьбі з атаками SQL Injection, особливо якщо атака використовує нові, невідомі техніки обходу сигнатур або складно замасковані запити. Тому ефективний захист від SQL Injection повинен включати не лише IPS, але й заходи безпечного програмування, такі як використання параметризованих запитів, валідація введених даних, обмеження прав доступу до бази даних та регулярне оновлення програмного забезпечення. IPS є потужним інструментом у запобіганні атакам SQL Injection, проте його ефективність значно зростає у поєднанні з іншими методами захисту, що допомагає створити комплексну систему безпеки для веб-додатків та баз даних.

Система IPS може бути реалізована у вигляді апаратного або програмного рішення. Апаратні IPS працюють на рівні мережевого обладнання і встановлюються між зовнішніми та внутрішніми мережами для фільтрації трафіку. Вони забезпечують низьку затримку та високу продуктивність, що є критично важливим для великих підприємств та дата-центрів. Програмні IPS можуть бути розгорнуті як окремі додатки або вбудовані в існуючі мережеві пристрої, такі як брандмауери. Вони є більш гнучкими, але можуть мати вищі затримки через програмну обробку даних.

Основні дії, які виконує IPS у разі виявлення загрози, включають блокування трафіку [11], завершення сеансів підозрілих з'єднань, зміну конфігурації мережевих пристроїв для обмеження доступу, а також надсилання сповіщень адміністраторам для подальшого аналізу інциденту. У деяких випадках IPS може також інтегруватися з SIEM-системами для централізованого збору даних та кореляції подій безпеки.

Завдяки постійному оновленню сигнатур і застосуванню штучного інтелекту для аналізу загроз сучасні IPS-системи здатні ефективно виявляти складні атаки, включаючи атаки нульового дня. Водночас важливим аспектом є правильне налаштування та оптимізація IPS, оскільки занадто агресивна фільтрація трафіку може призвести до блокування легітимного трафіку, а надто слабкі правила можуть дозволити проникнення загроз.

Системи IPS є важливим елементом сучасної стратегії кібербезпеки, який працює на перехресті між виявленням і запобіганням загрозам, забезпечуючи захист мереж від широкого спектра атак.

1.2.2 Класифікація IPS

Класифікація IPS базується на різних критеріях, таких як спосіб розгортання, область моніторингу, методи аналізу трафіку та рівень інтеграції з іншими системами безпеки. Основними типами IPS є мережеві, хостові, тв бездротові системи, кожна з яких має власні унікальні характеристики та сценарії використання [12].

Мережева система запобігання вторгненням (NIPS) розгортається на рівні мережевої інфраструктури та аналізує весь вхідний і вихідний трафік у реальному часі [13]. Вона працює як вбудований захисний шлюз, що фільтрує пакети перед тим, як вони досягають кінцевих хостів або серверів. NIPS здатна запобігати атакам, спрямованим на мережеві сервіси, такі як DoS-атаки, експлойти вразливостей у протоколах, сканування портів та атаки на веб-додатки. Ці системи часто інтегруються з брандмауерами та іншими засобами безпеки для забезпечення комплексного захисту мережі.

Хостова система запобігання вторгненням (HIPS) встановлюється безпосередньо на окремих серверах або робочих станціях, забезпечуючи захист конкретного хоста [13] [14]. Вона контролює процеси, реєстри, файлову систему, системні виклики та мережеву активність для виявлення та блокування підозрілих дій. HIPS є особливо ефективною для виявлення атак, спрямованих на конкретні операційні системи або програмне забезпечення, таких як

експлойти нульового дня, спроби отримання прав адміністратора або модифікація важливих системних файлів. Основною перевагою HIPS є його здатність забезпечувати глибоку перевірку активності хоста, але її недоліком може бути високе навантаження на систему.

Бездротова система запобігання вторгненням (WIPS) призначена для моніторингу та захисту бездротових мереж від атак, спрямованих на Wi-Fi протоколи та пристрої [13]. Вона виявляє та блокує несанкціоновані точки доступу, перехоплення трафіку, атаки типу "зловмисна точка доступу" (Evil Twin) та експлойти вразливостей шифрування (наприклад, атаки на WPA2). WIPS зазвичай працює разом із мережевими засобами безпеки, контролюючи бездротове середовище та автоматично ізолюючи потенційні загрози.

За методами аналізу трафіку IPS-системи поділяються на сигнатурні, поведінкові [15] та гібридні (див. рисунок 1.4).

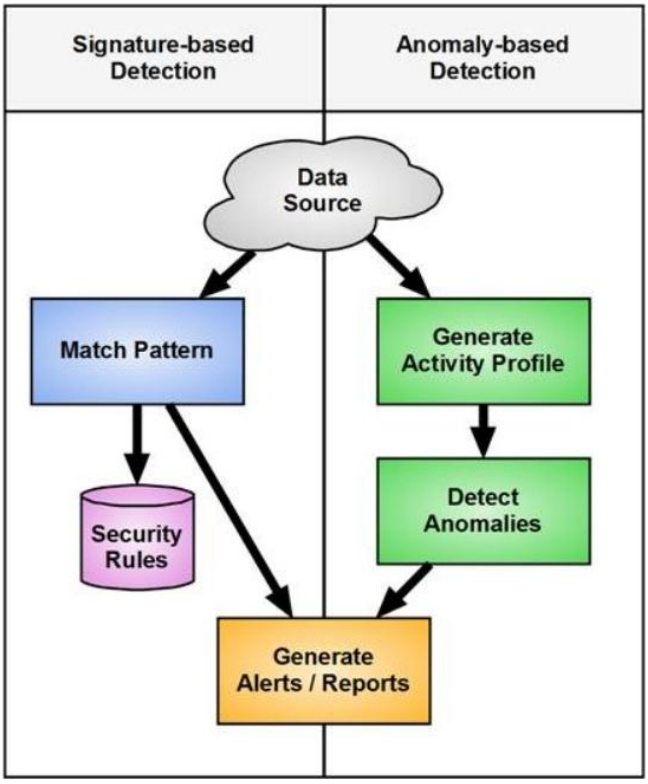

Рисунок 1.4 – Принцип роботи сигнатурних та поведінкових систем IPS

Сигнатурні IPS працюють на основі відомих шаблонів атак, використовуючи бази даних сигнатур для швидкого виявлення загроз. Вони

ефективні проти добре задокументованих атак, але менш корисні проти нових або модифікованих атак. Поведінкові IPS аналізують мережевий трафік і визначають аномальні дії, що дозволяє їм виявляти навіть невідомі загрози. Гібридні IPS комбінують ці два підходи, забезпечуючи баланс між точністю виявлення та швидкістю реакції на загрози.

1.4 Висновки до першого розділу

В першому розділі було розглянуто основні поняття, пов’язані з атаками SQL Injection та системами запобігання вторгненням. Детально проаналізовано принципи роботи SQL Injection атак, їх класифікацію та механізми експлуатації вразливостей веб-додатків. Розглянуто різні типи SQL-ін'єкцій, включаючи Error-based, Union-based, Blind SQL Injection (Boolean-based та Time-based), Out-of-band SQL Injection та використання підзапитів для обходу захисту. Було проілюстровано, як зловмисники можуть отримати несанкціонований доступ до баз даних, змінювати інформацію, обходити механізми автентифікації та впливати на роботу веб-додатків. Також у розділі висвітлено наслідки SQL Injection атак, які можуть мати руйнівний вплив на організації. Витік конфіденційних даних, порушення цілісності баз даних, отримання адміністративного контролю над системою та фінансові втрати є основними загрозами, з якими можуть зіткнутися компанії в результаті таких атак. Крім технічних ризиків, значну роль відіграють репутаційні та юридичні наслідки, що можуть призвести до штрафів, втрати довіри користувачів та великих фінансових витрат на усунення наслідків атак.

Окрім цього, у першому розділі розглянуто системи виявлення та запобігання вторгненням, які відіграють важливу роль у захисті від SQL Injection атак та інших кіберзагроз. Показано принципи роботи IPS, методи аналізу трафіку та механізми реагування на потенційні загрози. Було представлено класифікацію IPS, яка включає мережеві, хостові та бездротові системи. Описано особливості їхньої роботи. Було підкреслено, що для ефективного захисту від атак SQL Injection важливо використовувати комплексні рішення, поєднуючи

IPS із правильними підходами до розробки веб-додатків, такими як параметризовані запити, валідація введених даних та обмеження прав доступу до бази даних.

Таким чином, у розділі розглянуто ключові моменти атак SQL Injection, їх наслідки та заходи захисту за допомогою IPS. Отримані результати показують, що для ефективного захисту інформаційних систем необхідно використовувати багаторівневий підхід, що включає як превентивні методи безпеки, так і активні системи моніторингу та запобігання загрозам.

РОЗДІЛ 2 РОЗРОБКА СЕРЕДОВИЩА ТЕСТУВАННЯ СЦЕНАРІЇВ SQL INJECTION АТАК

2.1 Схема тестового середовища

Схема тестового середовища побудована на основі віртуалізації [16] [17] з використанням гіпервізора типу 2 VMware Workstation на Windows 10, що дозволяє імітувати реальну корпоративну мережу з підключеними до неї системами IPS (див. рисунок 2.1).

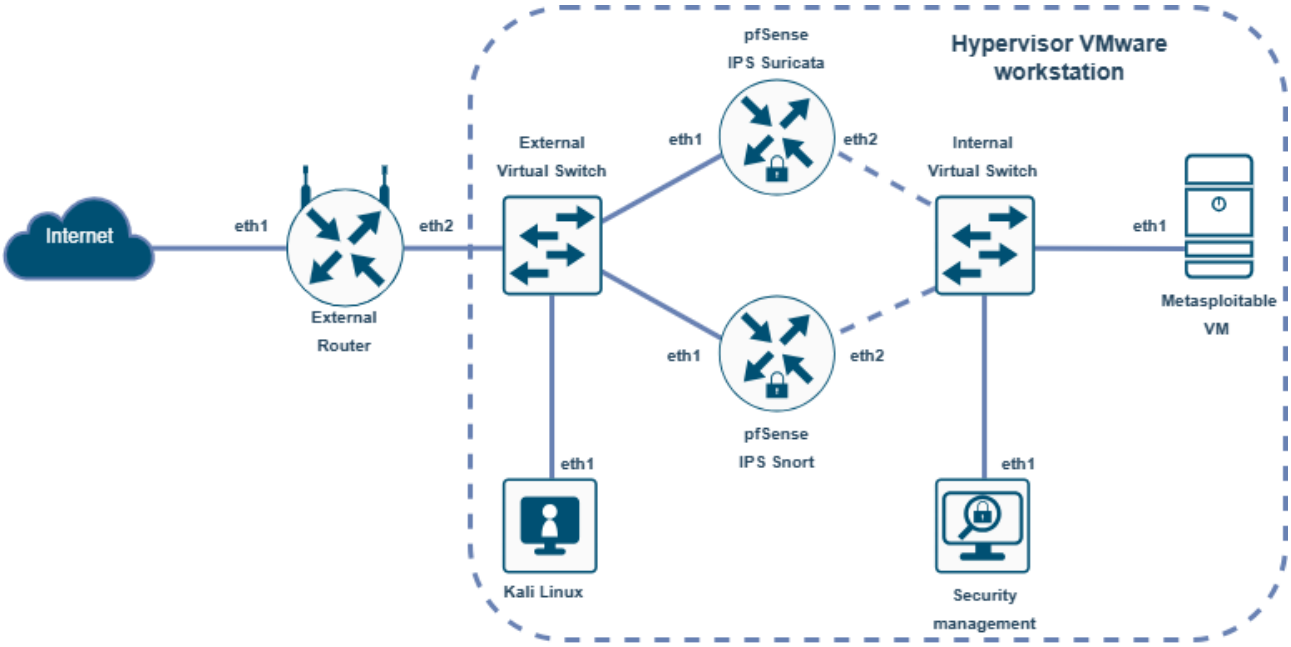

Рисунок 2.1 – Схема тестового середовища

Основна мета цього середовища - протестувати ефективність Suricata та Snort у виявленні та запобіганні SQL Injection атакам.

У цьому середовищі існує два рівні комунікації: зовнішня мережа (WAN), що представляє сегмент, до якого підключений атакуючий, і внутрішня мережа (LAN), в якій знаходиться вразливий сервер. Всі компоненти підключені через віртуальні комутатори, що імітують реальні мережеві зв’язки.

Зовнішній маршрутизатор (External Router) є першою точкою входу в середовище. Він має два мережеві інтерфейси: eth1 підключений до інтернету, а

eth2 з’єднаний із зовнішнім віртуальним комутатором (External Virtual Switch), який забезпечує зв’язок між зовнішнім середовищем і IPS-системами.

В зовнішній мережі працює Kali Linux, яка виконує роль атакуючого. Вона підключена до зовнішнього комутатора і використовується для проведення SQL Injection атак на вразливий сервер. Атакуючий надсилає зловмисні запити через WAN, і трафік проходить через один із двох сценаріїв тестування IPS.

В середовищі розгорнуті два pfSense-шлюзи, кожен із яких грає роль фільтра мережевого трафіку та IPS. У першому сценарії використовується pfSense з IPS Suricata, а в другому - pfSense з IPS Snort. Обидва шлюзи мають два мережеві інтерфейси: eth1 підключений до зовнішнього віртуального комутатора, а eth2 підключений до внутрішнього віртуального комутатора. Ці шлюзи аналізують мережевий трафік у реальному часі та перевіряють запити на предмет SQL Injection атак.

Усередині мережі, підключеної до внутрішнього віртуального комутатора (Internal Virtual Switch), знаходиться Metasploitable VM. Це вразливий сервер, що містить веб-додаток Mutillidae, який спеціально створений для тестування веб-вразливостей, включаючи SQL Injection. На цей сервер спрямовані атаки з Kali Linux через IPS.

Також до внутрішнього комутатора підключена віртуальна машина Windows 10 для управління безпекою (Security Management), яка використовується для аналізу логів IPS, налаштування правил Suricata і Snort, а також моніторингу ефективності виявлення атак. Вона допомагає визначити, які SQL-запити були заблоковані, чи є хибнопозитивні спрацьовування та наскільки ефективно працюють IPS-системи.

Схема дозволяє протестувати обидва варіанти IPS у схожих умовах, оскільки в кожному випадку атакуючий з Kali Linux надсилає запити через один із двох IPS перед тим, як вони досягнуть цільового сервера. Це забезпечує можливість порівняння ефективності Suricata та Snort при виявленні SQL Injection атак.

Усі ці компоненти працюють у віртуальному середовищі [18] VMware Workstation на Windows 10, що дозволяє створити ізольовану тестову мережу без

ризику впливу на реальну інфраструктуру. Кожна віртуальна машина має свої мережеві адаптери, налаштовані відповідно до логічної схеми підключень. VMware Workstation дозволяє використовувати віртуальні комутатори для побудови складних мереж, аналогічних фізичним, що дає можливість тестувати різні варіанти розгортання IPS у лабораторних умовах.

У таблиці 2.1 показано мережеві налаштування пристроїв елементів тестового середовища.

Таблиця 2.1 – Мережеві налаштування елементів тестового 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 Snort	eth1	192.168.0.121	255.255.255.0	192.168.0.1
	eth2	192.168.1.1	255.255.255.0	
pfSense IPS Suricata	eth1	192.168.0.125	255.255.255.0	192.168.0.1
	eth2	192.168.1.1	255.255.255.0	
Kali Linux	eth1	192.168.0.135	255.255.255.0	192.168.0.1
Metasploitable VM	eth1	192.168.1.103	255.255.255.0	192.168.1.1
Security management	eth1	192.168.1.2	255.255.255.0	192.168.1.1

Завдяки такій схемі можливо імітувати реальні атаки та отримати точні результати щодо ефективності IPS у виявленні та запобіганні SQL Injection атакам, що є ключовим завданням тестового середовища.

Таким чином, тестове середовище побудоване так, щоб дозволити чітке розділення зовнішньої та внутрішньої мереж, з можливістю тестування різних IPS-систем у реальних умовах. Усі елементи налаштовані відповідно до своєї ролі, а використання двох pfSense із різними IPS дозволяє безпосередньо порівняти їхню ефективність при схожих мережевих параметрах.

2.2 Елементи тестового середовища

2.2.1 Гіпервізор VMware Workstation

Гіпервізор VMware Workstation Pro є однією з платформ для створення, управління та запуску віртуальних машин у середовищі операційної системи Windows або Linux [19]. Це тип 2 гіпервізора (hosted), що означає, що він встановлюється як окреме програмне забезпечення в існуючій операційній системи, а не працює безпосередньо на апаратному рівні, як bare-metal гіпервізори.

Однією з ключових можливостей VMware Workstation Pro є створення віртуалізованих середовищ, які можуть складатися з декількох віртуальних машин, що взаємодіють між собою через налаштовані мережеві інтерфейси. Це дозволяє створювати тестові та навчальні лабораторії, а також розробляти та тестувати складні корпоративні рішення без необхідності використання фізичного обладнання. Основні функціональні можливості VMware Workstation Pro включають підтримку 64-бітної віртуалізації, що дозволяє запускати сучасні операційні системи як гостьові, включаючи Windows, Linux, macOS (обмежено), BSD та навіть спеціалізовані вбудовані ОС. Програма забезпечує апаратну віртуалізацію через технології Intel VT-x або AMD-V, що значно покращує продуктивність віртуальних машин, дозволяючи їм безпосередньо взаємодіяти з процесором. Гіпервізор підтримує миттєві знімки (Snapshots), що дозволяє зберігати стан віртуальної машини у певний момент часу та відновлювати його у разі необхідності. Це особливо корисно для тестування, оскільки дає змогу швидко повернутися до попередньої конфігурації після виконання експериментів. Мережеві можливості VMware Workstation Pro включають створення віртуальних комутаторів (Virtual Switches), що дозволяє налаштовувати складні мережеві топології. Доступні режими мережевого підключення, зокрема Bridged (підключення типу міст), NAT, Host-Only (ізольована мережа). Це робить VMware Workstation Pro ідеальним середовищем для моделювання корпоративних мереж і тестування систем безпеки. Безпекові

функції включають шифрування віртуальних дисків (AES-256) для захисту даних та можливість інтеграції з апаратними модулями TPM (Trusted Platform Module). Продуктивність у VMware Workstation Pro оптимізована за рахунок апаратного прискорення графіки, включаючи DirectX та OpenGL, що дозволяє запускати графічно вимогливі програми та емулятори в межах віртуальних машин. Завдяки можливості імітації різних апаратних конфігурацій, таких як кількість процесорних ядер, об'єм оперативної пам'яті, тип дискових накопичувачів, VMware Workstation Pro дозволяє створювати реалістичні середовища для тестування продуктивності, безпеки та стабільності операційних систем і додатків. Гіпервізор VMware Workstation Pro у Windows 10 дозволяє побудувати ізольовану, керовану та масштабовану інфраструктуру для тестування ефективності систем IPS у виявленні та блокуванні SQL Injection атак.

На рисунку 2.2 відображено інтерфейс VMware Workstation, в якому запущене тестове середовище для оцінки ефективності систем IPS у контексті атак SQL Injection.

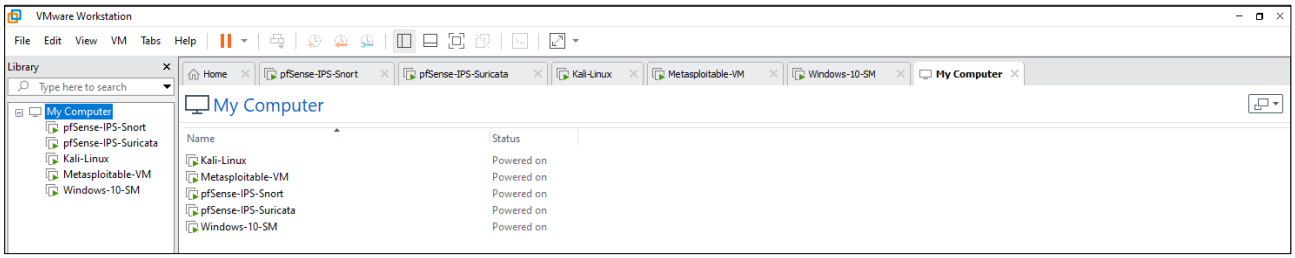

Рисунок 2.2 – Інтерфейс VMware Workstation

Основні компоненти тестового середовища запущені та функціонують, що дозволяє виконувати експерименти з мережевими атаками та оцінювати, як IPS-системи справляються з виявленням SQL Injection атак.

2.2.2 Маршрутизатор pfSense

Маршрутизатор pfSense – це програмне рішення для керування мережею, яке виконує функції мережевого екрану, маршрутизатора та системи запобігання

вторгненням [20]. Він базується на операційній системі FreeBSD і використовується для побудови безпечних мережевих рішень, включаючи корпоративні мережі, VPN-з'єднання. pfSense забезпечує надійне керування мережевим трафіком, дозволяючи застосовувати політики маршрутизації, фільтрації пакетів та моніторингу з'єднань. Він підтримує NAT, що дозволяє організовувати доступ до інтернету для внутрішніх пристроїв без розкриття їхніх реальних IP-адрес. У тестовому середовищі pfSense використовується як шлюз між зовнішньою та внутрішньою мережею. Він має два мережеві інтерфейси: WAN та LAN. Маршрутизатор pfSense також виконує функцію системи запобігання вторгненням за допомогою Suricata або Snort, залежно від конфігурації. У режимі IPS він активно фільтрує трафік та блокує шкідливі пакети. Адміністрування pfSense здійснюється через веб-інтерфейс, який дозволяє налаштовувати брандмауер, маршрутизацію, VPN-з'єднання, балансування навантаження та IDS/IPS-конфігурації. На рисунку 2.3 відображено веб-інтерфейс керування pfSense IPS Snort.

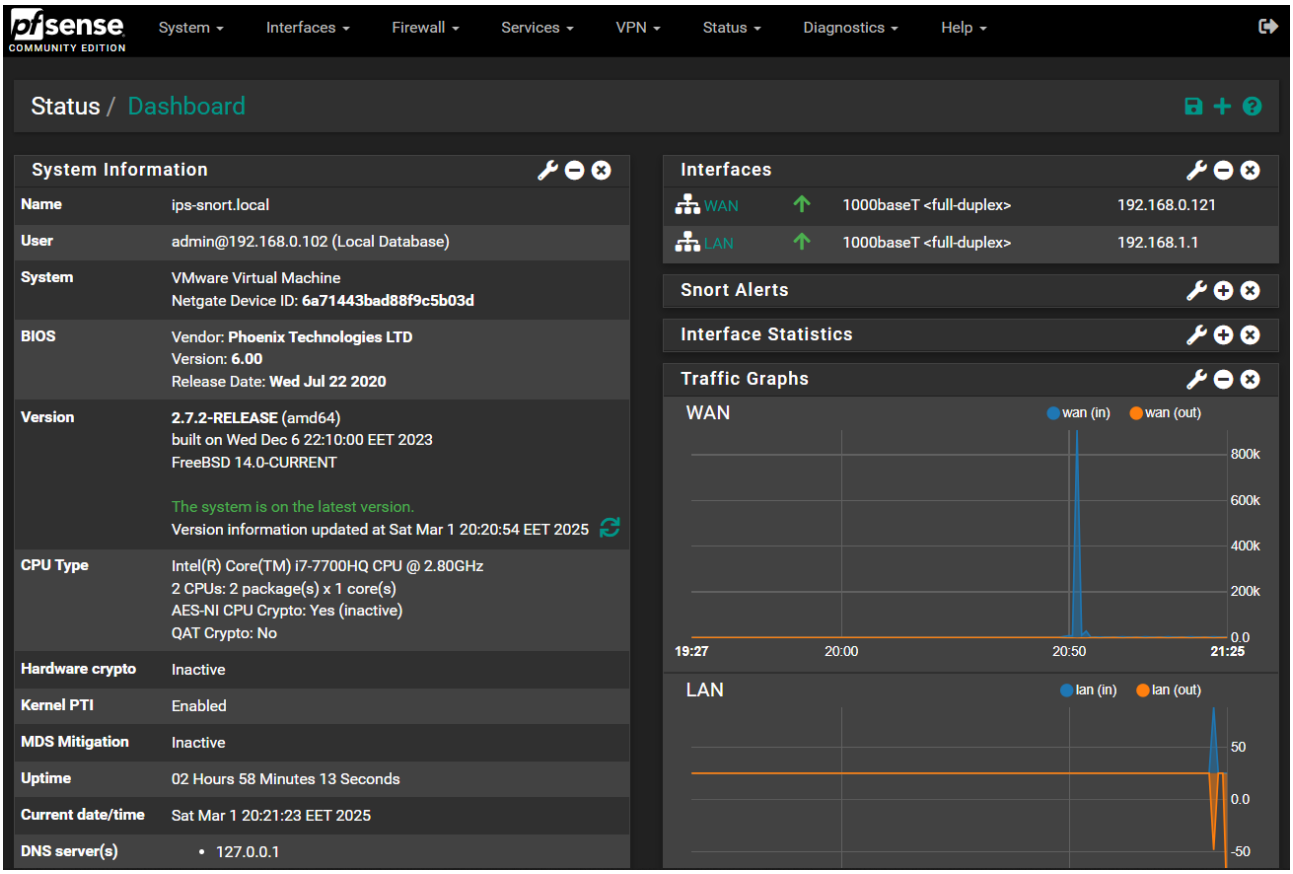

Рисунок 2.3 – Інтерфейс керування pfSense IPS Snort

Вбудовані графіки трафіку та журнали подій допомагають аналізувати поточний стан мережі та оцінювати ефективність виявлення атак.

Також маршрутизатор pfSense підтримує інтеграцію з RADIUS та LDAP, що дозволяє використовувати автентифікацію користувачів для доступу до мережі. Також є можливість реалізації Captive Portal, який вимагає авторизації перед наданням доступу до інтернету.

Завдяки високій стабільності, відкритому коду та широкому набору функцій pfSense є ефективним рішенням для мережевого захисту [21]. У тестовому середовищі його використання дозволяє імітувати реальні мережеві атаки, оцінювати ефективність IPS-систем та проводити експерименти із захисту інформаційних систем від SQL Injection та інших загроз.

2.2.3 Системи виявлення та запобігання вторгненням Snort та Suricata

Системи виявлення та запобігання вторгненням Snort та Suricata є двома найбільш популярними відкритими рішеннями для моніторингу мережевого трафіку та виявлення кіберзагроз. Вони виконують функції IDS та IPS, що дозволяє їм аналізувати потік даних у мережі, розпізнавати шкідливі дії та, у випадку режиму IPS, блокувати потенційно небезпечний трафік у реальному часі.

Snort є одним із найстаріших і найвідоміших механізмів виявлення вторгнень [22]. На даний час його розробником є компанія Cisco, що забезпечує постійну підтримку та оновлення сигнатур загроз. Snort використовує сигнатурний метод аналізу, що означає, що він порівнює трафік із базою відомих атак за допомогою спеціальних правил. Також він підтримує аналіз аномалій, який може виявляти підозрілу активність на основі відхилень від нормальної поведінки мережі.

На рисунку 3.4 показано інтерфейс управління Snort у pfSense Community Edition, де налаштоване мережеве середовище для моніторингу та аналізу трафіку. У цьому розділі відображаються налаштування інтерфейсів, на яких

запущений Snort, а також параметри, що визначають його поведінку під час виявлення загроз.

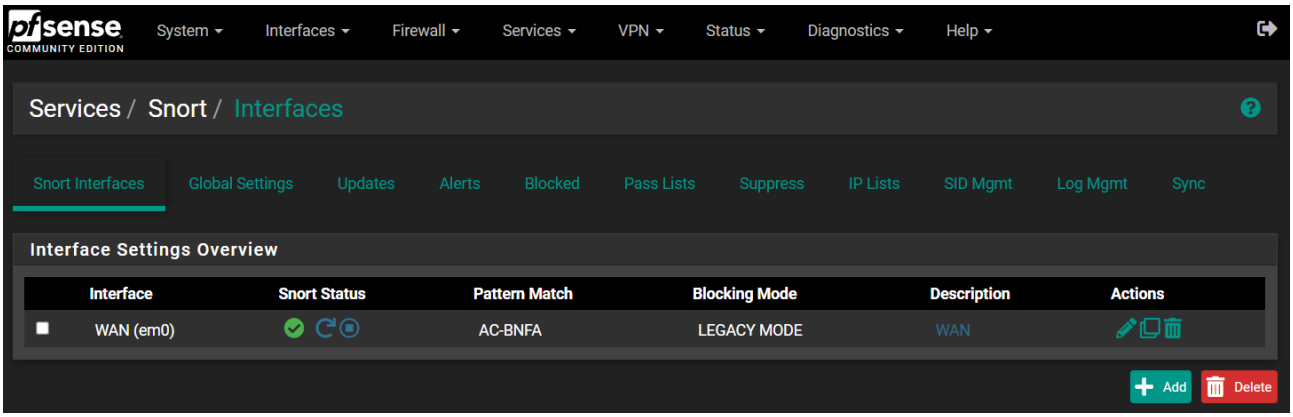

Рисунок 2.4 – Інтерфейс управління Snort в pfSense

Blocking Mode встановлено в LEGACY MODE, що означає, що Snort працює у класичному режимі блокування виявлених загроз (див. рисунок 3.5).

На рисунку 2.5 показано налаштування блокування (Block Settings) у Snort, що визначають, як система IPS буде реагувати на виявлені загрози.

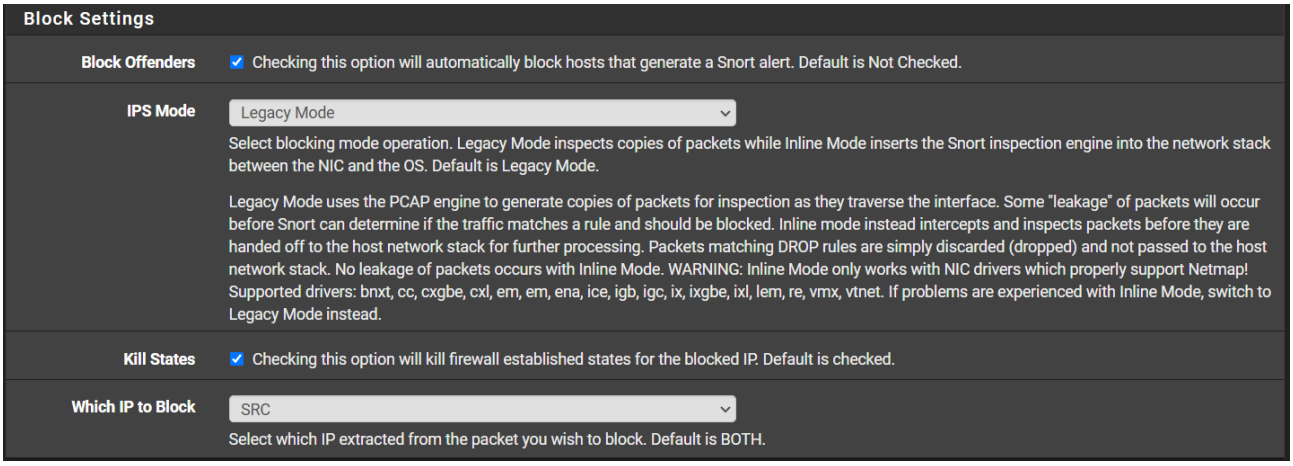

Рисунок 2.5 – Налаштування блокування в Snort

Параметр Block Offenders увімкнено, що означає, що Snort автоматично блокує хости, які викликають спрацьовування правил. Якщо Snort виявить підозрілу активність, він додасть IP-адресу джерела до списку блокування. IPS Mode налаштований на Legacy Mode. Це означає, що Snort працює у режимі, який використовує PCAP для створення копій пакетів, що проходять через інтерфейс.

У такому режимі можлива часткове проходження пакетів в систему до моменту їх обробки, оскільки Snort перевіряє пакети після того, як вони вже передані в систему. Альтернативний варіант – Inline Mode, у якому Snort інтегрується безпосередньо в мережевий стек і може блокувати шкідливі пакети ще до їх потрапляння в ОС, проте Inline Mode підтримується не всіма мережевими драйверами. Опція Kill States увімкнена, що означає, що якщо Snort блокує IP-адресу через виявлену загрозу, всі існуючі з'єднання цього хоста будуть негайно закриті у брандмауері PF. Це запобігає можливому збереженню активних сесій атакуючого навіть після його блокування. Which IP to Block встановлено на SRC (Source IP), що означає, що у разі виявлення загрози Snort буде блокувати IP-адресу джерела трафіку, тобто хоста, який надсилає шкідливі пакети.

Розділ конфігурації Global Settings в Snort містить налаштування завантаження та оновлення правил виявлення загроз, а також керування оновленнями сигнатур та блокуванням хостів. Snort Subscriber Rules надають можливість увімкнення Snort VRT (Vulnerability Research Team) правил, які можна отримати після реєстрації на snort.org. Snort GPLv2 Community Rules – це набір правил, який поширюється без обмежень під ліцензією GPLv2. Ці правила сертифіковані Talos і доступні безкоштовно. Вони оновлюються щоденно та є підмножиною повного комерційного пакету Snort. Emerging Threats (ET) Rules дозволяє завантажувати два різні набори правил. ET Open – це безкоштовний набір правил із меншою кількістю сигнатур у порівнянні з ET Pro, який є платною послугою з розширеним покриттям актуальних загроз, включаючи шкідливі програми, ботнети та експлойти. Sourcefire OpenAppID Detectors дозволяє активувати OpenAppID, що використовується для ідентифікації додатків у мережевому трафіку. Пакет OpenAppID Detectors містить сигнатури для аналізу трафіку додатків, а також можливість завантаження AppID Open Text Rules, які підтримуються спільнотою. FEODO Tracker Botnet C2 IP Rules забезпечує завантаження спеціальних правил для виявлення ботнетів Feodo та його похідних (Cridex, Dridex, Geodo, Heodo, Emotet). Цей механізм дозволяє автоматично блокувати підозрілі IP-адреси, що використовуються командно-контрольними (C2) серверами ботнетів.

Suricata є альтернативою Snort, яка була розроблена для забезпечення вищої продуктивності та розширених можливостей аналізу трафіку [23]. Вона підтримує багатопотокову обробку [24], що дозволяє їй працювати швидше на багато-ядерних системах у порівнянні зі Snort. Suricata також використовує сигнатурний аналіз, але, на відміну від Snort, вона має вбудовану підтримку розширеного аналізу протоколів, включаючи HTTP, TLS, FTP, SMB, що дає змогу отримувати глибшу інформацію про трафік.

На рисунку 2.6показано інтерфейс керування Suricata у pfSense Community Edition.

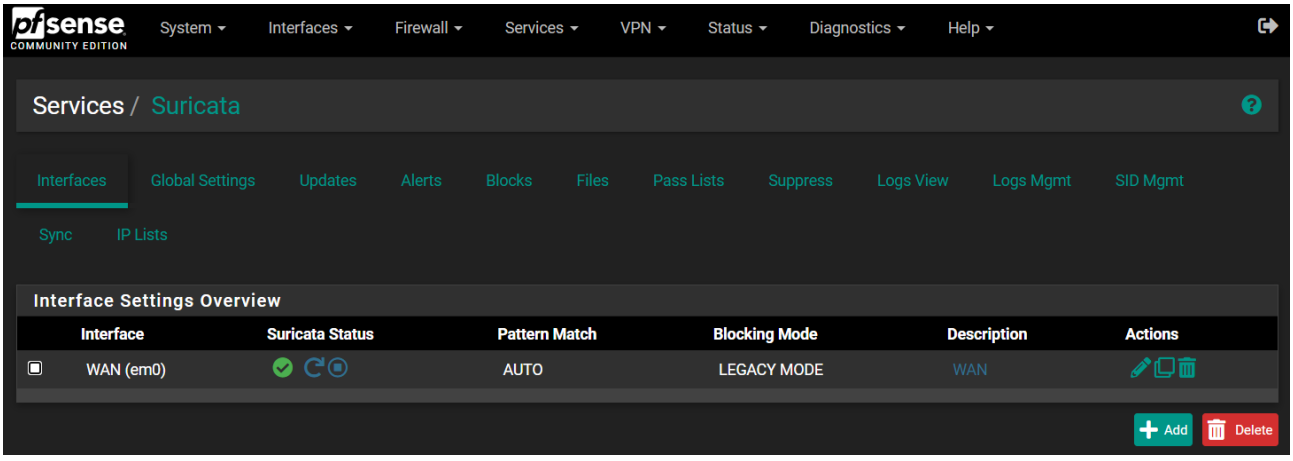

Рисунок 2.6 – Інтерфейс управління Suricata в pfSense

Розділ конфігурації Global Settings в Suricata містить налаштування завантаження та оновлення правил виявлення загроз, а також керування оновленнями сигнатур та блокуванням хостів. У розділі Emerging Threats (ET) Rules встановлено ETOpen правила. Додатково активувано Snort GPLv2 Community Rules, який є безкоштовним сертифікованим набором правил від Talos. Feodo Tracker Botnet C2 IP Rules дозволяє увімкнути список ботнет-командних серверів (C2), які використовуються для атак Dridex, Emotet, Heodo та інших шкідливих програм. Це дозволяє Suricata блокувати відомі IP-адреси ботнетів та запобігати їхньому зв’язку з інфікованими пристроями. ABUSE.ch SSL Blacklist Rules містить чорний список SSL-сертифікатів, які використовуються в кіберзлочинцями. Suricata використовує фінгерпринти SSL для виявлення небезпечних з’єднань і блокує їх на рівні трафіку.

У розділі General Settings можна налаштувати тривалість блокування хостів. Поточне значення встановлено на 6 годин, що означає, що IP-адреси, які потрапили під блокування через Suricata, залишаться заблокованими протягом 6 годин, перш ніж бути автоматично розблокованими.

У тестовому середовищі Snort та Suricata використовуються окремо на двох віртуальних машинах pfSense для порівняння їхньої ефективності у виявленні SQL Injection атак. Використання обох систем у схожих сценаріях дозволяє оцінити їхню продуктивність, точність визначення атак та ефективність у реальних умовах мережевого трафіку.

2.2.4 Операційна система Kali Linux

Операційна система Kali Linux є спеціалізованим дистрибутивом на базі Debian Linux, призначеним для етичного хакінгу, тестування безпеки, цифрової криміналістики та реверс-інжинірингу [25]. Вона містить велику кількість попередньо встановлених інструментів для тестування на проникнення (penetration testing), аналізу вразливостей, зламування паролів, аналізу трафіку, атак і збирання інформації. Розробником Kali Linux є Offensive Security, що забезпечує постійну підтримку, оновлення та розширення функціоналу. Операційна система орієнтована на фахівців із кібербезпеки, аналітиків загроз, дослідників безпеки та тестувальників на проникнення, а також широко використовується в навчальних цілях для вивчення методів злому та захисту інформаційних систем. Kali Linux має адаптивну архітектуру, яка дозволяє працювати як на фізичних пристроях, так і у віртуальних середовищах.

На рисунку 2.7 показано робочий стіл та мережеві налаштування Kali Linux.

Рисунок 2.7 – Мережеві налаштування Kali Linux

Kali Linux містить широкий набір інструментів для аналізу, тестування та експлуатації вразливостей, включаючи SQL Injection. Основні інструменти для SQL Injection у Kali Linux це SQLmap та jSQL Injection.

2.2.5 Операційна система Metasploitable VM

Операційна система Metasploitable VM є спеціалізованим віртуальним середовищем, створеним для тестування кібербезпеки, навчання етичному хакінгу та перевірки ефективності захисту інформаційних систем [26]. Вона розроблена командою Rapid7, що також відповідає за Metasploit Framework, один із найпопулярніших інструментів для експлуатації вразливостей та тестування на проникнення. Metasploitable базується на Ubuntu Linux і містить штучно створені вразливості, що дозволяють фахівцям із безпеки та студентам вивчати методи атак та способи їхнього виявлення та запобігання. Вона використовується в лабораторіях з кібербезпеки, курсах етичного хакінгу та для тестування систем IDS/IPS, таких як Suricata або Snort. Metasploitable має набір сервісів і додатків, які містять відомі вразливості, що дозволяє проводити тести.

Mutillidae – це спеціально створений вразливий веб-додаток, призначений для навчання тестуванню на проникнення (penetration testing) та аналізу веб-безпеки. Він побудований на базі PHP та MySQL і містить широкий набір вразливостей, які дозволяють досліджувати методи атак та способи їхнього виявлення та запобігання. Mutillidae входить до складу Metasploitable VM і використовується разом із інструментами Kali Linux для навчальних і тестових цілей. Mutillidae містить вразливості до найпоширеніших веб-атак, що дозволяє тестувати механізми захисту та ефективність WAF (Web Application Firewall), IPS/IDS та інших систем кібербезпеки.

Серед основних вразливостей, що містяться у Mutillidae: SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Command Injection (див. рисунок 2.8).

Рисунок 2.8 – Веб-інтерфейс керування Mutillidae

Mutillidae містить документацію та навчальні матеріали, що пояснюють суть кожної вразливості та дають можливість виконати її експлуатацію вручну або за допомогою інструментів, таких як SQLmap.

Mutillidae є одним із найкращих навчальних інструментів для вивчення веб-безпеки, оскільки дозволяє практично освоїти принципи атак та механізми їхнього усунення у реальних умовах. У тестових середовищах Mutillidae буде використано для аналізу ефективності засобів захисту, таких як Suricata та Snort.

2.3 Висновки до другого розділу

В другому розділі було розглянуто процес розробки тестового середовища для аналізу ефективності системи IPS Suricata та Snort у виявленні та запобіганні атакам SQL Injection. Було розроблено та описано архітектуру тестового середовища, яке побудоване на базі гіпервізора VMware Workstation Pro у Windows 10, що дозволяє моделювати реальну корпоративну мережу з розділенням зовнішнього та внутрішнього сегментів.

Запропонована схема передбачає наявність зовнішньої WAN та внутрішньої LAN мережі, що дає змогу протестувати роботу IPS у реальних умовах атак. У зовнішній мережі функціонує Kali Linux, який виконує роль атакуючого та використовується для проведення SQL Injection атак. У внутрішній мережі розміщено Metasploitable VM, що містить вразливий веб-додаток Mutillidae, який є ціллю атак.

Для аналізу ефективності різних IPS-систем у тестовому середовищі реалізовано два сценарії:

- сценарій 1 з використанням pfSense із Suricata, яка аналізує трафік і блокує SQL Injection атаки;
- сценарій 2 з використання pfSense із Snort, що виконує аналогічні функції.

Таке середовище дозволяє порівняти продуктивність, точність визначення загроз та загальну ефективність роботи IPS у боротьбі з атаками на веб-додатки.

Було детально описано всі елементи середовища, включаючи гіпервізор VMware Workstation, маршрутизатор pfSense, системи Snort та Suricata, Kali Linux і Metasploitable VM. Особливу увагу приділено конфігурації мережевих

з’єднань, що забезпечують правильну маршрутизацію трафіку та дозволяють точно оцінити ефективність IPS у реальних умовах.

Результати розробки середовища свідчать про його повну відповідність цілям дослідження, що дозволяє імітувати реальні атаки SQL Injection, оцінювати ефективність засобів захисту та надавати рекомендації щодо покращення безпеки веб-додатків. Створена інфраструктура дозволяє в майбутньому модифікувати її для тестування інших типів атак або впровадження додаткових механізмів кіберзахисту.

РОЗДІЛ 3 ТЕСТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ IPS SURICATA ТА SNORT

3.1 Сценарій перший з IPS Suricata

У цьому сценарії тестується ефективність системи запобігання вторгненням Suricata у виявленні та запобіганні атакам SQL Injection. Атака здійснюється з Kali Linux за допомогою sqlmap, а ціллю є веб-додаток Mutillidae, розміщений на вразливому сервері Metasploitable VM, який підключений до LAN-інтерфейсу pfSense.

3.1.1 Проведення SQL Injection атак

Використання sqlmap для проведення SQL Injection атак є одним із ефективних методів автоматизованого тестування безпеки веб-додатків [27]. sqlmap – це інструмент з відкритим вихідним кодом, який дозволяє виявляти, експлуатувати та автоматизувати атаки SQL Injection. Його основна функція – перевірка вразливих веб-додатків, отримання доступу до баз даних і вилучення конфіденційної інформації. Основні можливості sqlmap включають автоматичне виявлення SQL Injection, підтримку різних типів ін’єкцій, зокрема Boolean-Based, Error-Based, Time-Based, UNION-Based та Out-of-Band SQL Injection. Він підтримує роботу з багатьма СУБД, включаючи MySQL, PostgreSQL, Microsoft SQL Server, Oracle, SQLite, DB2, Firebird, Sybase та інші.

Для використання sqlmap достатньо знати URL-адресу веб-додатка, у якому є параметри для маніпуляції запитами. Якщо сторінка містить вразливий параметр у рядку запиту, sqlmap спробує виконати автоматичну SQL-ін’єкцію та отримати доступ до бази даних.

На першому етапі тестування сценарію 1 проведемо SQL Injection атаку при роботі Suricata в режимі IDS. Це дасть можливість відслідкувати послідовність атаки та побачити реакцію Suricata.

На рисунку 3.1 показано термінал Kali Linux, у якому запущено sqlmap для проведення SQL Injection атаки на веб-додаток Mutillidae, що працює на сервері Metasploitable VM.

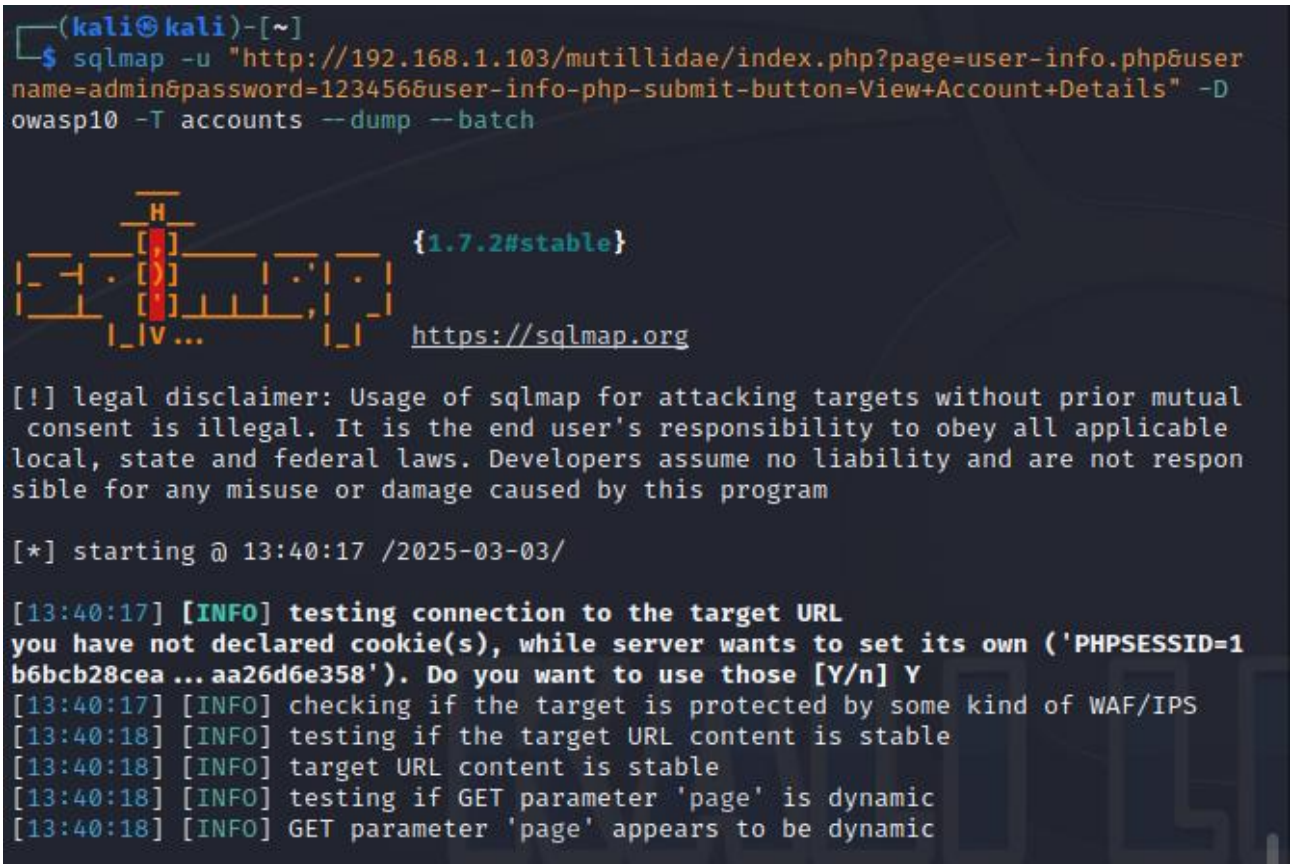

Рисунок 3.1 – Проведення SQL Injection атаки при тестування Suricata

Результати SQL Injection атаки за допомогою sqlmap показують успішне виявлення та експлуатацію вразливості у веб-додатку Mutillidae, який працює на сервері Metasploitable VM. Вразливий параметр знаходиться в GET запиті до сторінки user-info.php, а база даних, яку атакували, має назву owasp10.

Спочатку sqlmap перевіряє можливість ін'єкції в різних параметрах запиту (page, username, password). Параметр page не виявився вразливим до SQL Injection, але sqlmap визначив, що параметр username може бути вразливим. Після проведення автоматичних тестів sqlmap виявив чотири види вразливостей:

- Boolean-based blind SQL Injection;
- Error-based SQL Injection;
- Time-based blind SQL Injection;

– UNION-based SQL Injection.

Серверна база даних виявилася MySQL >= 4.1, що підтвердилося в ході атаки. sqlmap також отримав інформацію про веб-сервер – він працює на Linux Ubuntu 8.04 (Hardy Heron), а веб-додаток використовує Apache 2.2.8 та PHP 5.2.4.

Після визначення вразливості sqlmap виконав команду --dump, що дозволило отримати повний вміст таблиці accounts з бази даних owasp10. У результаті були вивантажені 17 записів користувачів, включаючи імена користувачів (username), паролі (password) та рівень доступу (is_admin). Деякі користувачі мають паролі у вигляді звичайного тексту, що свідчить про відсутність безпечного зберігання паролів у базі даних (див. рисунок 3.2).

```
Database: owasp10
Table: accounts
[17 entries]
+-----+----------+---------------+----------+-------------------------------+
| cid | is_admin | password      | username | mysignature                   |
+-----+----------+---------------+----------+-------------------------------+
| 1   | TRUE     | adminpass     | admin    | Monkey!                       |
| 2   | TRUE     | somepassword  | adrian   | Zombie Films Rock!            |
| 3   | FALSE    | monkey        | john     | I like the smell of confunk   |
| 4   | FALSE    | password      | jeremy   | d1373 1337 speak              |
| 5   | FALSE    | password      | bryce    | I Love SANS                   |
| 6   | FALSE    | samurai       | samurai  | Carving Fools                 |
| 7   | FALSE    | password      | jim      | Jim Rome is Burning           |
| 8   | FALSE    | password      | bobby    | Hank is my dad                |
| 9   | FALSE    | password      | simba    | I am a cat                    |
| 10  | FALSE    | password      | dreveil  | Preparation H                 |
| 11  | FALSE    | password      | scotty   | Scotty Do                     |
| 12  | FALSE    | password      | cal      | Go Wildcats                   |
| 13  | FALSE    | password      | john     | Do the Duggie!                |
| 14  | FALSE    | 42            | kevin    | Doug Adams rocks              |
| 15  | FALSE    | set           | dave     | Bet on S.E.T. FTW             |
| 16  | FALSE    | pentest       | ed       | Commandline KungFu anyone?    |
| 17  | NULL     | 1234          | a_pakosh | SB-42     Andrii Pakosh       |
+-----+----------+---------------+----------+-------------------------------+
```

Рисунок 3.2 – Результати проведення SQL Injection атаки

Sqlmap також зберіг отримані дані у вигляді CSV-файлу /home/kali/.local/share/sqlmap/output/192.168.1.103/dump/owasp10/accounts.csv, що дозволяє згодом проаналізувати результати атаки.

SQL Injection на цьому веб-додатку є критичною загрозою, оскільки дозволяє зловмисникам отримати конфіденційні дані, включаючи імена користувачів та паролі, без авторизації. Крім того, відсутність хешування паролів

означає, що навіть після їхнього отримання зловмисник може відразу використати їх для входу без необхідності розшифрування.

Після переведення режиму роботи Suricata в IPS було повторно здійснено SQL Injection атаку (див. рисунок 3.3).

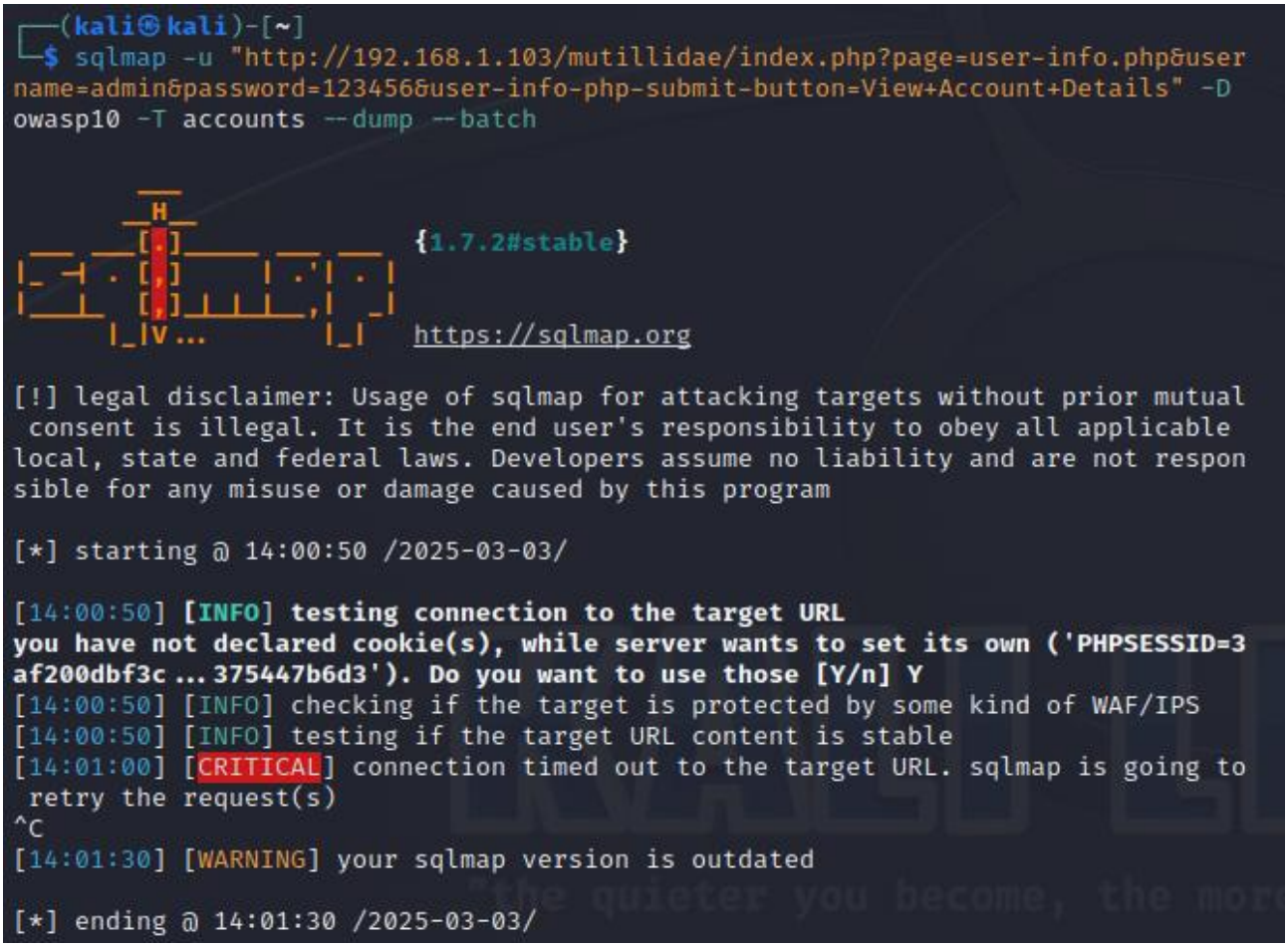

Рисунок 3.3 – Результати проведення SQL Injection атаки при режимі IPS в Suricata

Під час виконання тесту з’явилося критичне повідомлення, що з’єднання з цільовою URL-адресою зірвалося через тайм-аут. Це означає, що Suricata виявила SQL Injection атаку та заблокувала її, перервавши з’єднання між Kali Linux і цільовим веб-додатком.

3.1.2 Оцінка ефективності IPS

Оцінка ефективності IPS Suricata при виявленні та блокуванні SQL Injection атаки базується на аналізі поведінки системи при виконанні атаки та оцінці її здатності виявляти та запобігати несанкціонованим SQL-запитам. Весь трафік проходить через IPS Suricata, яка працює на pfSense та виконує моніторинг та аналіз пакетів на предмет атаки.

Перший етап атаки передбачав сканування вразливих параметрів за допомогою sqlmap. Suricata змогла виявити характерні ознаки SQL Injection, проте на цьому етапі запити ще проходили через систему, дозволяючи sqlmap збирати інформацію про можливі вразливі точки (див. рисунок 3.4).

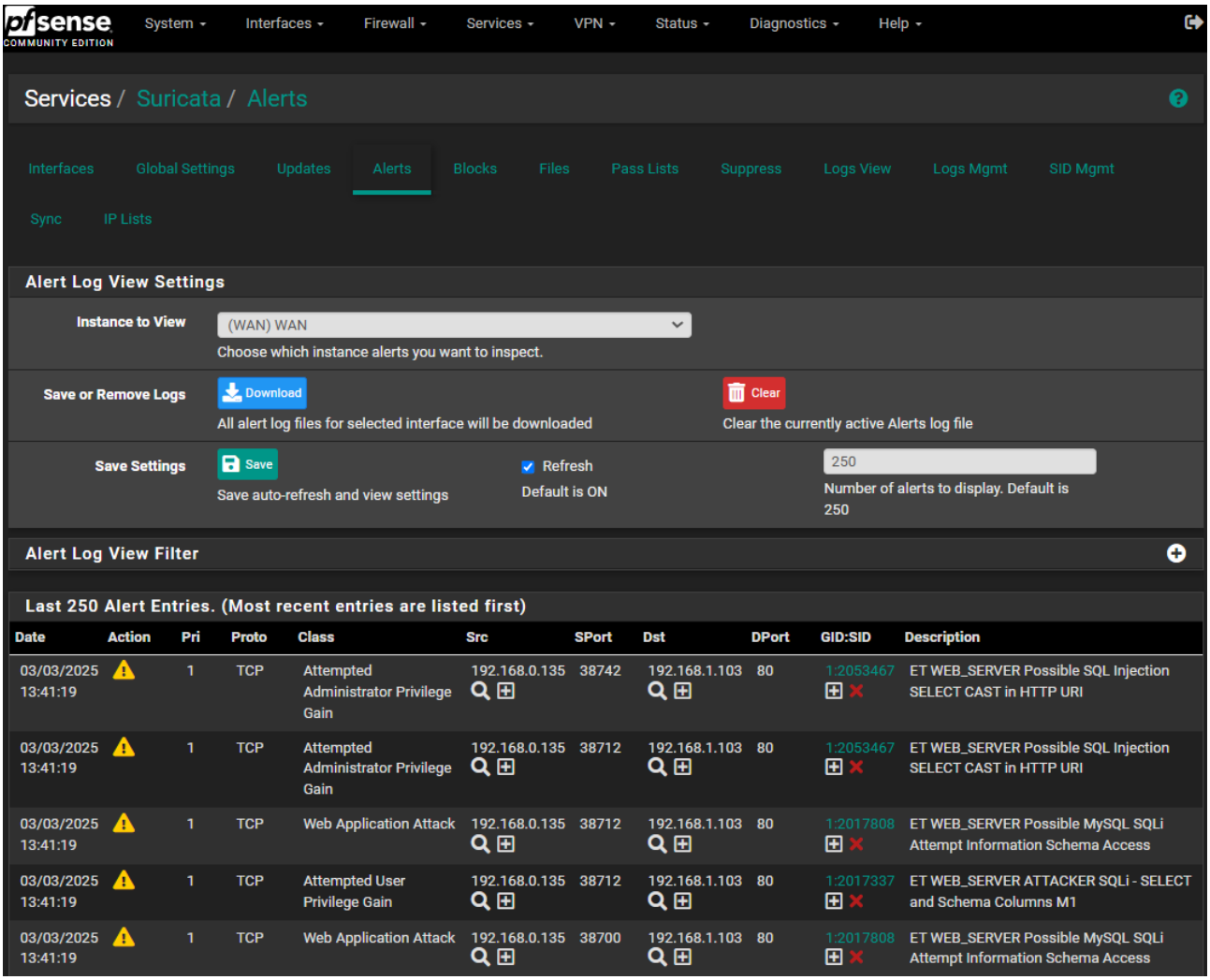

Рисунок 3.4 – Виявлення SQL Injection атаки при режимі IPS в Suricata

Під час проведення тестів Suricata розпізнала спроби SQL Injection у запитах HTTP, що містять параметри UNION SELECT, SELECT CAST, SELECT VERSION(), INFORMATION_SCHEMA, SLEEP(), BENCHMARK() та xp_cmdshell. Було зафіксовано спроби експлуатації вразливостей у MySQL, MSSQL та інших базах даних, включаючи доступ до критично важливих таблиць та команд системи. Записи містять ідентифікатор сигнатури 1:2008538, який відповідає виявленню автоматизованих SQL Injection атак, що використовуються sqlmap. Suricata виявила численні спроби ескалації привілеїв, коли атакуючий намагався отримати доступ до адміністративних функцій бази даних. Це включає запити на виконання команд бази даних, що дозволяють управляти привілеями користувачів. Окремі події в логах вказують на атаки типу Blind SQL Injection, коли атакуючий використовує затримки виконання (SLEEP(), BENCHMARK()) для перевірки вразливості. Suricata виявила ці атаки завдяки сигнатурам, що відповідають поведінковим особливостям time-based атак. Система показала ефективне виявлення атак, але важливим аспектом є рівень реакції.

На другому етапі Suricata в режимі роботи IPS виявила аномальний трафік та заблокувала IP-адресу атакуючого (див. рисунок 3.5).

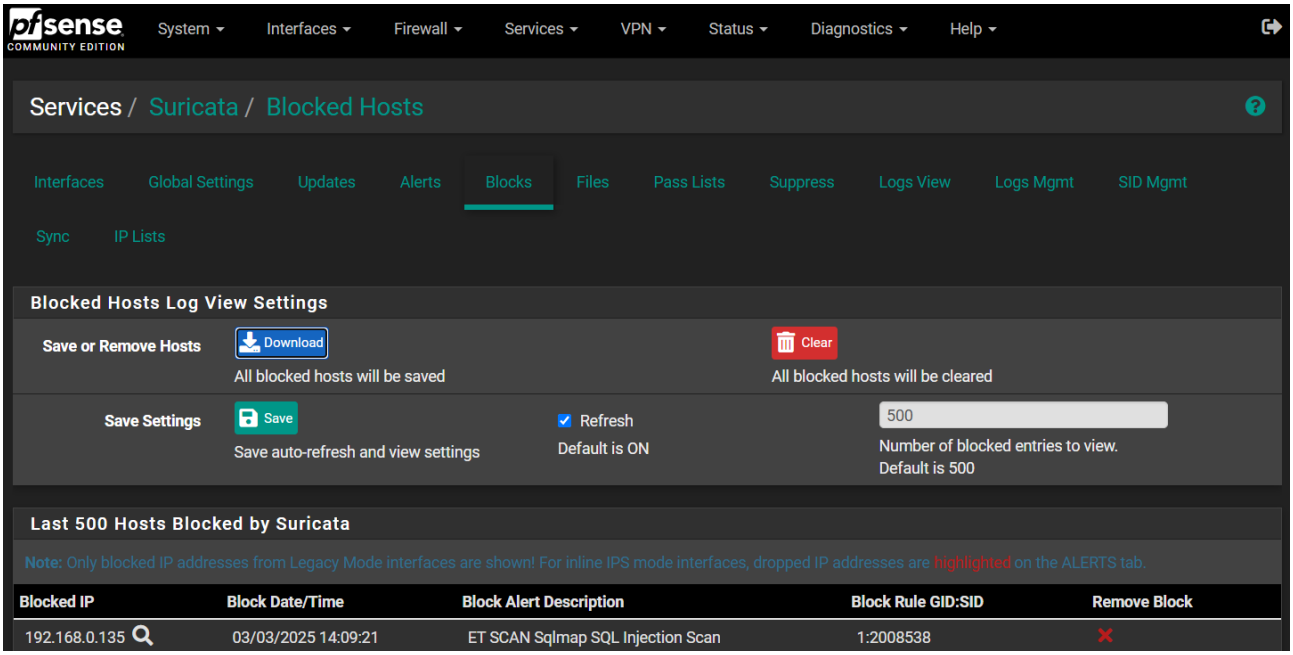

Рисунок 3.5 – Блокування SQL Injection атаки при режимі IPS в Suricata

Це підтвердило ефективність налаштувань режиму IPS та можливість блокування трафіку.

Оцінка ефективності показала, що Suricata має високу точність у виявленні SQL Injection атак, успішно блокує шкідливі SQL-запити. Під час тестування не було зафіксовано хибнопозитивних спрацювань.

3.2 Сценарій другий з IPS Snort

Для тестування можливостей IPS Snort щодо виявлення та блокування атак SQL Injection атакуюча машина Kali Linux використовує sqlmap для виконання SQL Injection атак. sqlmap сканує цільовий веб-сайт, виявляє вразливі параметри у формах введення та GET-запитах і виконує атаку. Мета атаки - отримати інформацію про базу даних, її структуру та можливі облікові записи.

3.2.1 Проведення SQL Injection атак

На першому етапі тестування сценарію 2 було проведемо SQL Injection атаку при роботі Snort в режимі IDS. Це дало можливість відслідкувати послідовність атаки та побачити реакцію Snort. Атаку проводили аналогічно, як на рисунку 3.1. Отримані результати атаки аналогічні, як в пункті 3.1.1.

На другому етапі тестування сценарію 2 було проведемо SQL Injection атаку при роботі Snort в режимі IPS (див. рисунок 3.6).

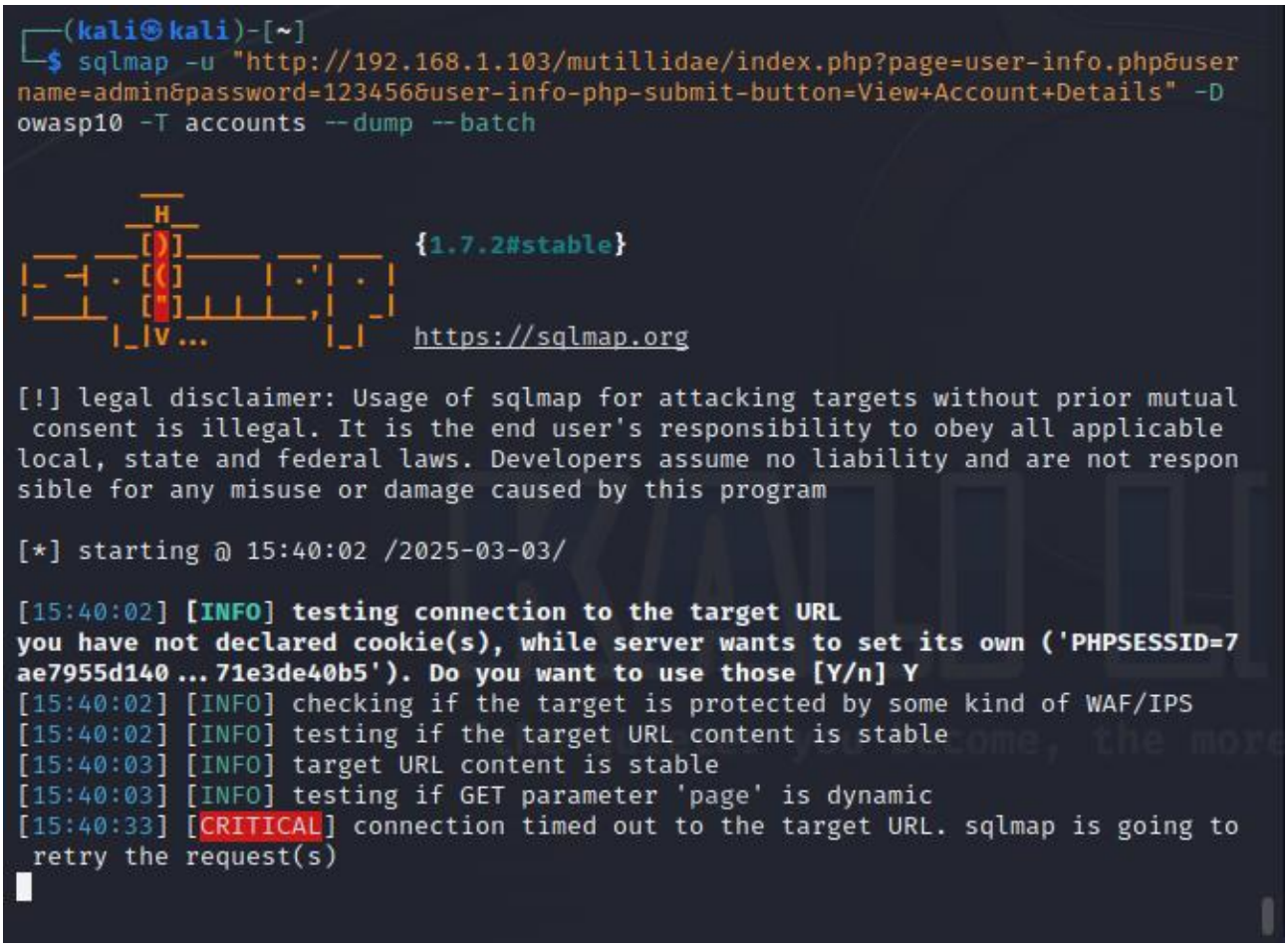

Рисунок 3.6 – Результати проведення SQL Injection атаки при режимі IPS в Snort

Атакуюча машина Kali Linux запустила команду sqlmap для автоматизованого виявлення вразливості у веб-додатку Mutillidae, розміщеному на Metasploitable VM. sqlmap розпочав тестування підключення до цільового веб-сайту, перевірку його стабільності та можливого впливу WAF/IPS. Однак у процесі атаки було зафіксовано переривання з'єднання. Це вказує на те, що з'єднання з цільовим сервером було заблоковано, що є типовим результатом дії IPS Snort. У режимі IPS Snort не просто реєструє шкідливі запити, а активно перешкоджає їх виконанню блокуючи сесію атакуючого.

3.2.2 Оцінка ефективності IPS

Snort, працюючи в режимі IDS, продемонстрував ефективне виявлення SQL Injection атак (див. рисунок 3.7).

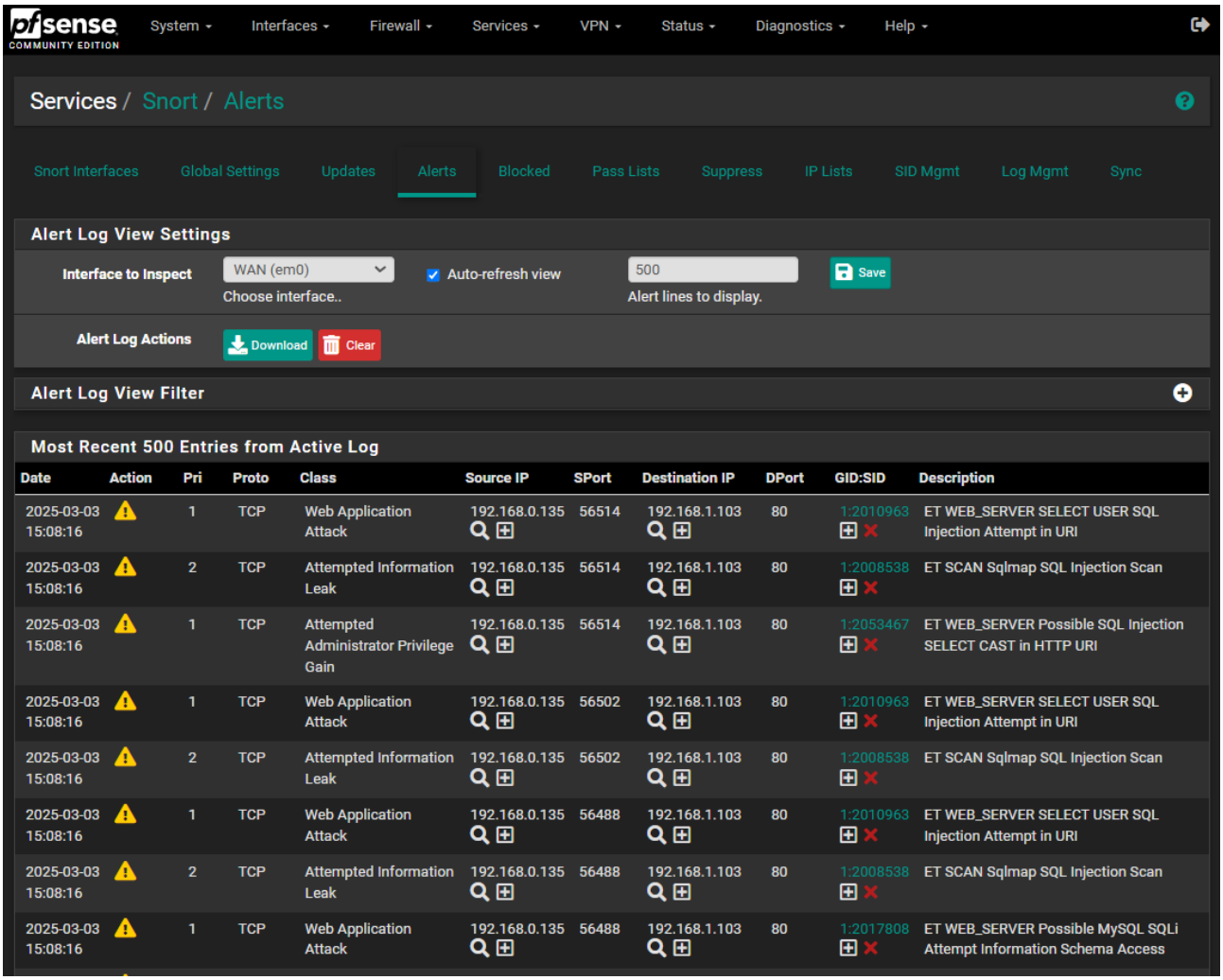

Рисунок 3.7 – Виявлення SQL Injection атаки при режимі IDS в Snort

Аналіз логів свідчить про здійснення SQL Injection атаки. Це підтверджують численні сповіщення про ET SCAN Sqlmap SQL Injection Scan та спроби отримання інформації про користувачів бази даних (наприклад, SELECT USER SQL Injection Attempt in URI). Крім того, спостерігаються спроби отримати версію сервера баз даних (SELECT VERSION) та звернення до системних файлів, таких як /etc/passwd, що може свідчити про спроби подальшого отримання адміністративного доступу до системи. Також є використання методів blind SQL Injection, де відбувається спроба обійти механізми захисту, використовуючи запити з SELECT SLEEP() та іншими техніками вимірювання часу відповіді сервера. Це підтверджує використання методів SQL Injection Time Delay, коли сервер реагує із затримкою, дозволяючи атакуючому визначити, чи є веб-додаток вразливим.

Snort, працюючи в режимі IPS, продемонстрував ефективне виявлення та запобігання спробам SQL Injection атак (див. рисунок 3.8).

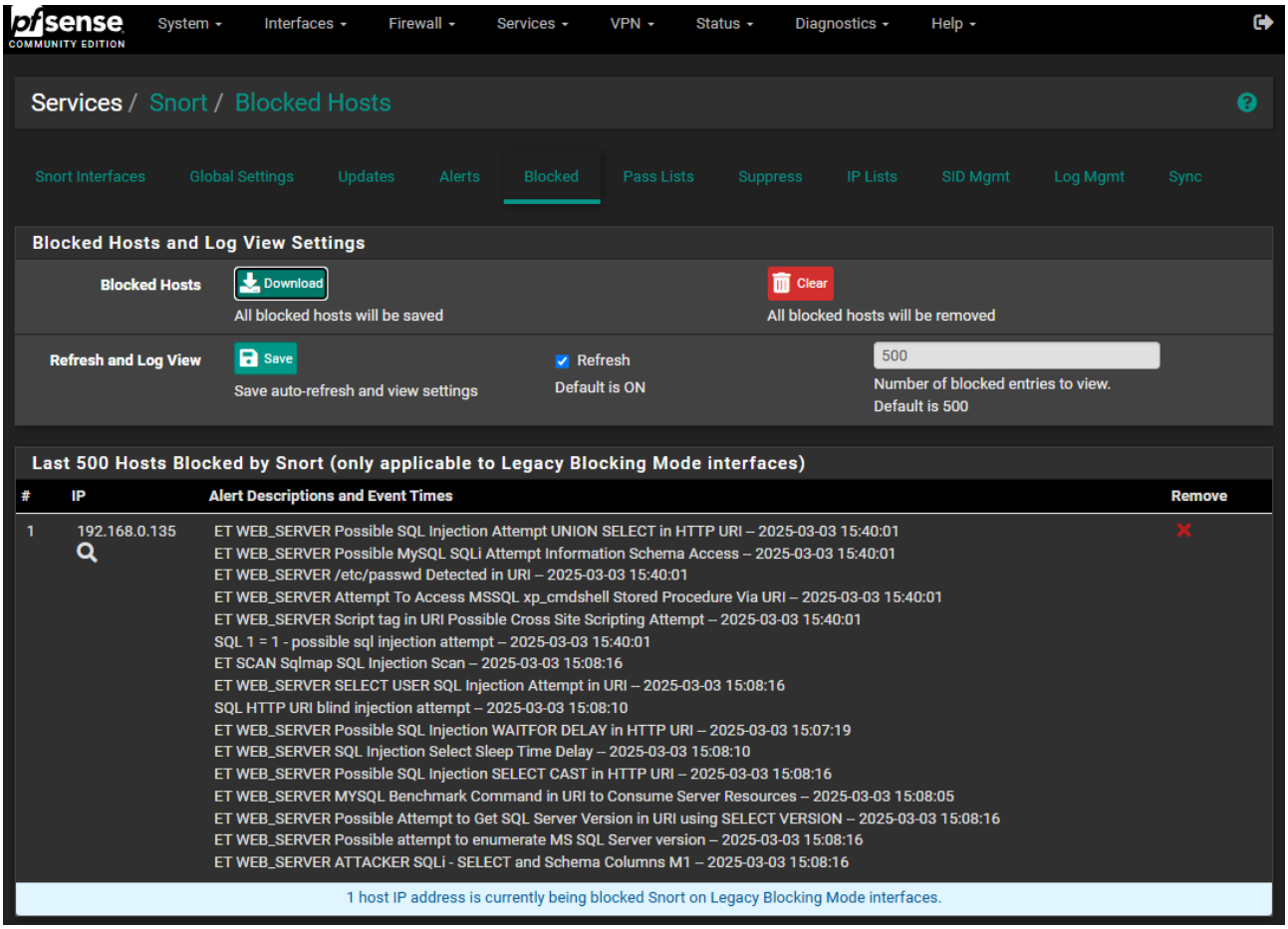

Рисунок 3.8 – Блокування SQL Injection атаки при режимі IPS в Snort

Блокування sqlmap-запитів унеможливило отримання будь-яких результатів щодо структури бази даних, таблиць чи користувачів, що є ознакою ефективного запобігання атаці. Результати тестування показують, що Snort у режимі IPS забезпечує надійний захист від SQL Injection атак, оскільки він не лише ідентифікує загрози, але й активно протидіє їм. Це дозволяє мінімізувати ризики компрометації веб-додатків та запобігати отриманню атакуючими критично важливої інформації з бази даних.

3.3 Висновки до третього розділу

В третьому розділі було проведено тестування та оцінку ефективності систем запобігання вторгненням Suricata та Snort у виявленні та блокуванні атак

SQL Injection. Було реалізовано два сценарії тестування, у яких перевірялась здатність цих систем виявляти та запобігати несанкціонованим SQL-запитам за допомогою інструменту sqlmap.

У першому сценарії тестувалася ефективність Suricata при виявленні та запобіганні SQL Injection атак на веб-додаток Mutillidae, що працює на сервері Metasploitable VM. Тестування проводилося у двох режимах: IDS та IPS. У режимі IDS Suricata змогла виявити ознаки SQL Injection, зокрема Boolean-Based, Error-Based, Time-Based та UNION-Based ін'єкції.. У режимі IPS система успішно заблокувала SQL-запити, перервавши з'єднання між атакуючим пристроєм та веб-додатком, що свідчить про ефективність Suricata у запобіганні атакам.

У другому сценарії перевірялася ефективність Snort у боротьбі з SQL Injection атаками. Тестування також відбувалося у режимах IDS та IPS. У режимі IDS Snort виявив спроби SQL Injection, зафіксувавши характерні запити, такі як SELECT USER, SELECT VERSION, INFORMATION_SCHEMA та SLEEP(). При переході в режим IPS Snort не лише ідентифікував шкідливі запити, але й заблокував їх, перериваючи з'єднання атакуючого з веб-додатком. Це унеможливило отримання будь-яких результатів щодо структури бази даних, що свідчить про ефективність системи у запобіганні SQL Injection атакам.

Оцінка ефективності показала, що обидві системи Suricata та Snort здатні виявляти та блокувати SQL Injection атаки у режимі IPS. Важливими факторами ефективності є коректне налаштування правил виявлення та режиму роботи систем. Під час тестування не було зафіксовано хибнопозитивних спрацювань, що свідчить про високу точність сигнатурного аналізу. Таким чином, результати тестування підтвердили, що використання Suricata та Snort у режимі IPS значно підвищує рівень безпеки веб-додатків, запобігаючи компрометації баз даних через SQL Injection атаки. Обидві системи забезпечують ефективний захист, дозволяючи своєчасно реагувати на спроби вторгнення та блокувати шкідливий трафік.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Забезпечення пожежної безпеки в приміщенні ЕОМ

Пожежна безпека в серверних кімнатах є важливим завдання збереження матеріальних цінностей та життя людей. Небезпечними чинниками, які впливають на людей під час пожежі, може бути відкритий вогонь чи іскри, підвищена температура повітря, предметів, токсичні продукти горіння, дим, знижена концентрація кисню. Тому пожежну безпеку вважають за невід'ємну частину охорони праці.

Пожежна безпека – це стан об'єкта, за якого із встановленою ймовірністю виключається можливість виникнення та розвитку пожежі, а також забезпечується захист матеріальних цінностей. У сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються різні елементи, дроти, комутаційні кабелі. При протіканні електричного струму відходить значна кількість теплоти, що може призвести до підвищення температури окремих вузлів до 80-100°С. З іншого боку, робоча температура силових транзисторів сягає 120°С. Все це може викликати оплавлення ізоляції з'єднувальних дротів, їх оголення і, як наслідок, коротке замикання, що супроводжується іскрінням, веде до неприпустимих температурних навантажень елементів схем, їх згоряння з виділенням диму [28].

Будівлі і ті їх частини, в яких розташовуються ЕОМ, повинні мати не нижче II ступень вогнестійкості. Приміщення для обслуговування, ремонту та налагодження ЕОМ повинні належати до категорії В за безпекою що до пожеж та вибухів, а за класом приміщення - до П за ПБЕ.

Неприпустимим є розташування приміщень категорій А і Б, а також виробництв з мокрими технологічними процесами поряд з приміщеннями, де розташовуються ЕОМ, виконується їх обслуговування, налагодження і ремонт, а також над такими приміщеннями або під ними.

Стіни кабін мають бути виготовлені з негорючих матеріалів. Дозволяється виготовляти їх зі скла та металевих конструкцій. У кабіні мусить бути оглядове

вікно (вікна). Висота оглядового вікна має бути не менше 1,5 м, а відстань від підлоги не більше 0,8 м.

Приміщення з ЕОМ повинні бути оснащені системою автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог правил пожежної безпеки в Україні. В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, в яких розміщуються великі ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до правил пожежної безпеки в Україні та вимог нормативно-технічної та експлуатаційної документації заводу-виробника [28].

Підходи до засобів пожежогасіння повинні бути вільними. Будівлі та приміщення, в яких експлуатуються ПК та виконується їх обслуговування, налагодження і ремонт, повинні відповідати вимогам пожежної безпеки об'єктів будівництва, експлуатаційної документації заводу-виробника ПК, чинним санітарним нормам у сфері охорони праці.

Не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог, в інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення, мають бути оснащені вогнегасниками.

Приміщення, в яких розміщуються робочі місця операторів великих ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння

Система вентиляції обчислювальних центрів та приміщень з ЕОМ повинна бути обладнана блокувальним пристроєм, який забезпечує її відключення на випадок пожежі.

Пожежна безпека приміщень забезпечується такими засобами:

- справність електропроводки;
- наявність засобів пожежогасіння;
- наявність пожежної сигналізації.

До первинних засобів пожежогасіння у приміщеннях з ЕОМ відносяться різні вуглекислотні, аерозольні, порошкові вогнегасники, призначені для гасіння загорянь та пожеж у початковій стадії їх розвитку.

Вуглекислотні вогнегасники (ВВ-2, ВВ-5, ВВ-8) призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники містять вуглекислоту, яка при відкритті крана розширюється та викидається через розтруб у вигляді вуглекислого снігу температурою -55°С. Тривалість роботи вогнегасників 25-40 секунд, довжина струменя, що викидається, 1,5-2 м (ВВ-2, ВВ-5).

Аерозольні вогнегасники закачувального типу містять або тільки вогнегасний засіб, або ще й додатковий (робочий) газ (наприклад, азот, хладон). Вони призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники малогабаритні, спрощені (з об'ємом заряду від 0,25 до 1,0 літра).

Порошкові вогнегасники (ВП-1, Момент, ВП-2А, ВП-10А) застосовуються для гасіння лужних металів, що горять, горючих рідин, а також обладнання з напругою до 5000 В. Дані вогнегасники містять вогнегасний порошок і балон з газом. Порошок з корпусу вогнегасника виштовхується стисненим газом (азот, повітря) приблизно за 30 секунд.

Автоматичні засоби пожежогасіння розраховані на подачу вогнегасної речовини у разі виникнення пожежі незалежно від того, перебувають у приміщенні люди або відсутні. Останнім часом знаходять широке застосування автономних автоматичних установок порошкового пожежогасіння.

Проведені дослідження в кваліфікаційній роботі вимагали взаємодії людини з серверним обладнанням. Тому важливим є забезпечити безпечні умови праці інженерів комп'ютерних систем при встановленні, налаштуванні та подальшому обслуговуванні систем захисту сервісів.

4.2 Забезпечення захисту працівників суб'єкта господарювання від іонізуючого випромінювання

Працівники, які виконують роботи з радіоактивними речовинами, повинні перебувати під постійним медичним наглядом, використовувати засоби індивідуального захисту від радіації та прилади індивідуального дозиметричного контролю (універсальні радіометри) для своєчасного виявлення і вимірювання рівня випромінювання [29].

Захищаючись від зовнішнього іонізуючого опромінювання при роботах із закритими джерелами випромінювання, тобто такими, які виключають можливість потрапляння радіоактивних речовин у навколишнє середовище, перш за все необхідно не допустити переопромінення працівників.

Основним способами захисту від цього є:

- зменшення активності джерела, з яким контактують працівники під час конкретного технологічного процесу – досягається шляхом використання речовин із меншою активністю;
- зменшення часу контакту з джерелом випромінювання – досягається шляхом вдосконалення організації робіт і технологічного виробничого процесу та проведення попередніх тренінгів працівників;
- збільшення відстані між людиною і джерелом – використовується, як правило, при контакті з точковим джерелом випромінювання шляхом використання дистанційних універсальних маніпуляторів та інших автоматизованих пристроїв;
- розташування між людиною і джерелом захисного екрану (стаціонарного, пересувного, розбірного, настільного тощо), тобто

пристрою, який зменшує інтенсивність випромінювання до безпечного рівня [29].

Для виготовлення екранів, а також для захисту працівників в стаціонарних спорудах, використовується бетон, чавун, сталь, алюміній, скло, свинець та інші матеріали. Від дії рентгенівських променів застосовують екрани зі сталевого листа товщиною 0,5-1 мм або алюмінію товщиною 3 мм, спеціальної гуми. Оглядові вікна виконують з плексигласу товщиною 30 мм або з покритого оловом скла товщиною 9 мм.

Для захисту шкіри від забруднень радіоактивними речовинами та запобігання їх попаданню всередину організму, захисту від альфа і бета-випромінювання передусім застосовуються засоби індивідуального захисту (ЗІЗ) від радіації.

Отже, засоби захисту від радіації використовуються у тих випадках, коли інші заходи недостатньо ефективні: при переході через зони збільшеної інтенсивності випромінювання, при ремонтних та налагоджувальних роботах у аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення.

З урахуванням зазначеного прогнозу на території області може виникнути складна радіаційна обстановка наслідки якої вимагатимуть від органів виконавчої влади, органів місцевого самоврядування, суб'єктів господарювання, на які покладено виконання завдань щодо захисту населення і територій від надзвичайних ситуацій, оперативного реагування та дій [29].

Місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання здійснюють для забезпечення захисту людей від впливу іонізуючих випромінювань наступні заходи:

- приймають згідно з законодавством України рішення щодо застосування на підвідомчій території заходів втручання у разі радіаційних аварій;
- організовують проведення в установленому порядку щорічні обстеження з метою оцінки стану захисту людини від впливу

іонізуючих випромінювань та ведення екологічного паспорта підвідомчої території;

- здійснюють організаційне керівництво системою обліку та контролю доз опромінення населення на підвідомчій території;
- організовують контроль за виконанням заходів щодо захисту людини від впливу радіонуклідів, що містяться у будівельних матеріалах;
- затверджують відповідні плани щодо захисту населення від радіаційних аварій та їх наслідків;
- забезпечують постійну готовність засобів оповіщення населення на підвідомчій території про виникнення радіаційної аварії;
- організовують контроль за виконанням заходів щодо захисту населення від радіаційних аварій та їх наслідків;
- забезпечують населення, в місцях його проживання, інформацією щодо рівнів опромінення людини та заходів захисту від впливу іонізуючих випромінювань, що виконуються на підвідомчій території;
- розроблюють та впроваджують програми захисту людей від впливу іонізуючих випромінювання;
- здійснюють оповіщення населення у разі виникнення радіаційної аварії та інформування про рятувальні та профілактичні заходи у зв’язку з цим.

Для виконання вищезазначених заходів залучаються органи управління, сили і засоби обласної територіальної та функціональних підсистем єдиної державної системи цивільного захисту (далі – ЄДС ЦЗ), порядок дій яких визначено Планом реагування на надзвичайні ситуації, пов'язаних з викидом радіоактивних речовин.

Режими захисту робітників і службовців на суб'єктах господарювання вводяться в дію рішенням керівників об'єктів. Незалежно від місця розміщення суб'єкту господарювання (в населеному пункті або за його межами) на його території вводиться в дію свій режим захисту з урахуванням рівнів радіації, виміряних на об'єкті, і реального ступеню захисту працівників і службовців.

При виникненні комунальної радіаційної аварії окрім термінових робіт щодо стабілізації радіаційного стану (включаючи відновлення контролю над джерелом) місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання одночасно здійснюють заходи, спрямовані на:

- зведення до мінімуму кількості осіб з населення, які зазнають аварійного опромінення;
- запобігання чи зниження індивідуальних і колективних доз опромінення населення;
- запобігання чи зниження рівнів радіоактивного забруднення продуктів харчування, питної води, сільськогосподарської сировини і сільгоспугідь, об'єктів довкілля (повітря, води, ґрунту, рослин тощо), а також будівель і споруд.

Для населення, робітників та службовців суб'єктів господарювання, які можуть потрапити в зону випадіння радіоактивних опадів, доцільно завчасно, виходячи з конкретних місцевих умов, розрахувати варіанти режимів радіаційного захисту [30].

З урахуванням вищезазначеного, режими радіаційного захисту вводяться в дію місцевими органами виконавчої влади, органами місцевого самоврядування, суб'єктами господарювання з метою захисту людей від впливу іонізуючого випромінювання у разі загрози або виникнення надзвичайних ситуацій, пов'язаних з радіаційними аваріями.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було досліджено механізми та особливості проведення однієї з найнебезпечніших для веб-додатків атак – SQL Injection, а також методи протидії їй за допомогою систем виявлення та запобігання вторгненням Snort і Suricata. У роботі було детально розглянуто різновиди SQL-ін'єкцій (Boolean-Based, Error-Based, Time-Based, UNION-Based, Out-of-Band), проаналізовано їхні наслідки для безпеки баз даних та організацій загалом. Значну увагу зосереджено на налаштуванні та роботі системи IPS на базі pfSense із використанням Snort і Suricata. Для цього було розроблено спеціалізоване віртуальне середовище в гіпервізорі VMware Workstation, що дало змогу імітувати реальну корпоративну мережу з розподілом на зовнішній (WAN) та внутрішній (LAN) сегменти. Здійснено інтеграцію Metasploitable VM із вразливим веб-додатком Mutillidae, Kali Linux як інструмента атаки та двох віртуальних маршрутизаторів pfSense – кожен із власною IPS (Snort або Suricata).

Під час тестування було зібрано та проаналізовано дані про спроби експлуатації SQL-ін'єкцій, проведені за допомогою спеціалізованого інструменту sqlmap. Перевірку ефективності Snort або Suricata виконано у двох режимах роботи кожної системи: IDS (виявлення) та IPS (запобігання). У режимі IDS Suricata й Snort успішно виявляли найрізноманітніші прийоми SQL-ін'єкцій та реєстрували їх у журналах подій безпеки, але пропускали шкідливі запити далі. Переведення в режим IPS дозволило блокувати спроби ін'єкцій на рівні мережевого трафіку та відкидати потенційно небезпечні пакети.

Результати дослідження засвідчили високу ефективність обох IPS-рішень у виявленні та блокуванні SQL-ін'єкцій під час коректного налаштування правил і сигнатур. У жодній із систем не спостерігалося помилкових спрацювань під час тестування. Це вказує на надійність сигнатур, призначених для захисту від SQL-ін'єкцій.

Отримані в межах кваліфікаційної роботи результати можуть бути корисними для спеціалістів із кібербезпеки та системних адміністраторів, які

шукають ефективне рішення для захисту веб-додатків і баз даних від SQL Injection. Практичним результатом стало розгортання й документування тестового стенду із застосуванням Snort та Suricata, а також формулювання рекомендацій щодо їхнього налаштування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is SQL injection attack? Definition & faqs | vmware. (n.d.). VMware by Broadcom - Cloud Computing for the Enterprise. https://www.vmware.com/topics/sql-injection-attack

2. What is SQL injection (sqli)? Types & examples. part 1. (n.d.). Wallarm | Advanced API Security. https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1

3. What is SQL injection (sqli) and how to prevent attacks. (n.d.). Acunetix. https://www.acunetix.com/websitesecurity/sql-injection/

4. What is SQL injection? Examples & prevention. (n.d.). SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/sql-injection/

5. 7 types of SQL injection attacks & how to prevent them? (n.d.). SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/types-of-sql-injection/

6. What is an intrusion prevention system (IPS). (n.d.). Wallarm | Advanced API Security. https://www.wallarm.com/what/intrusion-prevention-system

7. 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

8. 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.

9. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

10. 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.

11. 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.

12. What is an intrusion prevention system? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

13. What is an intrusion prevention system (IPS)? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-an-ips

14. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] - Львів, "Магнолія 2006", 2013. – 256 с.

15. Fekolkin, R. (2015). Intrusion detection & prevention system: overview of snort & suricata. Internet Security, A7011N, Lulea University of Technology, 1-4.

16. 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.

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

18. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології "Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

19. Inc, C. (2025, January 30). VMware workstation pro 17.0. TechDocs. https://techdocs.broadcom.com/us/en/vmware-cis/desktop-hypervisors/workstation-pro/17-0.html

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

21. 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.

22. SNORT users manual2.9.16. (n.d.). SNORT Users Manual2.9.16. http://manual-snort-org.s3-website-us-east-1.amazonaws.com/

23. Suricata User Guide. (n.d.). Suricata 8.0.0-dev documentation. https://docs.suricata.io/en/latest/

24. 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.

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

26. Metasploitable 2 | metasploit documentation. (n.d.). Docs @ Rapid7. https://docs.rapid7.com/metasploit/metasploitable-2/

27. Sqlmap: Automatic SQL injection and database takeover tool. (n.d.). sqlmap: automatic SQL injection and database takeover tool. https://sqlmap.org/

28. Yesin, V., Karpinski, M., Yesina, M., Vilihura, V., Kozak, R., Shevchuk, R. (2023). Technique for Searching Data in a Cryptographically Protected SQL Database. Applied Sciences, 13(20), art. no. 11525, 1-21. doi: 10.3390/app132011525.

29. Revniuk O.A., Zagorodna N.V., Kozak R.O., Karpinski M.P., Flud L.O. “The improvement of web-application SDL process to prevent Insecure Design vulnerabilities”. Applied Aspects of Information Technology. 2024; Vol. 7, No. 2: 162–174. DOI:https://doi.org/10.15276/aait.07.2024.12.

30. Основи охорони праці: навчальний посібник / М. П. Купчі та ін. Київ: Основа, 2000. 416 с.

31. Желібо Є. П., Сагайдак І. С. Безпека життєдіяльності. Навчальний посібник для аудиторної та практичної роботи. К.:ЕКОМЕН. 2011. 200 с.

32. Депутат О. П., Коваленко І. В., Мужик І. С. Цивільна оборона. Навчальний посібник. За редакцією полковника В.С. Франчука. Львів: Афіша. 2000. 336 с.