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 систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: **Методи і засоби виявлення вторгнень та інформаційних атак на комп'ютерну систему**

Виконав: студент(ка) 6 курсу, групи СІм-61
спеціальності 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

(підпис) Ковтун Н.М. (прізвище та ініціали)

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

Нормоконтроль (підпис) Луцик Н.С. (прізвище та ініціали)

Завідувач кафедри (підпис) Осухівська Г.М. (прізвище та ініціали)

Рецензент (підпис) Гладьо Ю.Б. (прізвище та ініціали)

Тернопіль
2023

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 систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
« » 2023 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Ковтуну Назару Максимовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Методи і засоби виявлення вторгнень та інформаційних атак на комп'ютерну систему*

Керівник роботи *Жаровський Руслан Олегович, к.т.н.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*01*» *грудня* *2023* року № *4/7-1132*
2. Термін подання студентом завершеної роботи *27.12.2023 р.*
3. Вихідні дані до роботи *Моделі і засоби виявлення аномального трафіку в КС*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ 1 Аналіз методів і засобів виявлення вторгнень вкомп'ютерних системах
2 Аналіз алгоритмів. моделювання системи виявлення вторгнень
3 Тестування системи виявлення вторгнень
4 Охорона праці та безпека в надзвичайних ситуаціях
Висновки
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Актуальність і мета дослідження.
2. Задачі дослідження, об'єкт і предмет, наукова новизна і практична цінність дослідження.
3. Архітектура системи виявлення вторгнень
4. Вибір оптимального місця розташування IDS
5. Загальна схема роботи пропонованої IDS
6. Діаграма варіантів використання системи виявлення вторгнень
7. Результати експериментального дослідження.
8. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основи охорони праці	*Осухівська Г. М., зав. кафедри КС*		
Безпека в надзвичайних ситуаціях	*Стадник І. Я., професор кафедри ОХ*		

7. Дата видачі завдання 20.11.2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Аналіз сучасних методів і засобів виявлення вторгнень*	*01.12.2023*	*Виконано*
2.	*Аналіз методів проведення комплексного тестування комп'ютерної інформаційної системи*	*03.12.2023*	*Виконано*
3.	*Аналіз і моделювання роботи алгоритмів систем виявлення вторгнень*	*10.12.2023*	*Виконано*
4.	*Апробація тестування запропонованої збірки системи виявлення вторгнень*	*16.12.2023*	*Виконано*
5.	*Охорона праці та безпека в надзвичайних ситуаціях*	*18.12.2023*	*Виконано*
6.	*Оформлення пояснювальної записки і графічного матеріалу*	*19.12.2023*	*Виконано*
7.	*Попередній захист кваліфікаційної роботи магістра*	*20.12.2023*	*Виконано*
8.	*Захист кваліфікаційної роботи магістра*	*27.12.2023*	*Виконано*

Студент _____ *Ковтун Назар Максимович*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Жаровський Руслан Олегович*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи і засоби виявлення вторгнень та інформаційних атак на комп’ютерну систему // Кваліфікаційна робота магістра // Ковтун Назар Максимович // ТНТУ, Комп’ютерна інженерія, група СІм-61 // Тернопіль, 2023 // с. – 83, рис. – 24, табл. – 0, бібліогр. – 35.

Ключові слова: IDS, комп’ютерна система, алгоритм .

У кваліфікаційній роботі магістра проведено аналіз літератури та наукових джерел і визначені критерії оцінки захищеної інформації, визначено ключові інструменти захисту та сформульовано завдання, які вирішують системи виявлення вторгнень.

Розглянуті алгоритми, використовувані в системах виявлення вторгнень, включаючи як класичні сигнатурні методи, так і сучасні методи поведінкового та інтелектуального аналізу даних. Розроблено схему архітектури системи виявлення вторгнень.

Здійснено обчислювальний експеримент, який підтвердив перевагу комбінації алгоритмів ALAD+LERAD для виявлення атак у віртуальному середовищі, з використанням Suricata як основи системи виявлення вторгнень.

Проведено налаштування IDS Suricata для використання сторонніх алгоритмів, а також адаптацію правил Snort для взаємодії з системою виявлення вторгнень Suricata. Забезпечено підтримку пакетів готових сигнатур та розроблено можливості створення власних сигнатурних правил аналізу трафіку.

Отримані практичні висновки вказують на переваги використання Suricata, зокрема, її ефективність з використанням апаратного прискорення, швидкість роботи із сторонніми алгоритмами поведінкового аналізу та ефективність методу сигнатурного аналізу.

ABSTRACT

Methods and tools for detecting intrusions and information attacks on a computer system // Master graduation thesis // Kovtun Nazar Maksymovych // TNTU, computer engineering, group СІм-61 // Ternopil, 2023 // p. – 83, fig. – 24, tab. - 0, bibliography. - 35.

Keywords: IDS, computer system, algorithm.

In the master's qualification work, an analysis of literature and scientific sources was carried out and criteria for evaluating protected information were determined, key protection tools were defined, and the tasks that intrusion detection systems were to be solved were formulated.

Algorithms used in intrusion detection systems are considered, including both classical signature methods and modern methods of behavioral and intelligent data analysis. The scheme of the architecture of the intrusion detection system has been developed.

A computational experiment was conducted that confirmed the superiority of the combination of ALAD+LERAD algorithms for detecting attacks in a virtual environment, using Suricata as the basis of an intrusion detection system.

Configured IDS Suricata to use third-party algorithms, as well as adapted Snort rules to interact with Suricata's intrusion detection system. Support for packages of ready-made signatures is provided, and the possibility of creating your own signature rules for traffic analysis is developed.

The obtained practical conclusions indicate the advantages of using Suricata, in particular, its efficiency with the use of hardware acceleration, the speed of work with third-party behavioral analysis algorithms, and the effectiveness of the signature analysis method.

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ 8

ВСТУП 9

РОЗДІЛ 1 АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ ВКОМП'ЮТЕРНИХ СИСТЕМАХ..... 13

1.1. Роль IDS у технічному захисті інформації..... 13

1.2. Ефективність IDS в протидії поширеним мережевим атакам..... 17

1.3. Розміщення IDS у периметрі мережі 20

1.4. Порівняльний аналіз систем виявлення вторгнень 23

РОЗДІЛ 2 АНАЛІЗ АЛГОРИТМІВ І МОДЕЛЮВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ 30

2.1. Аналіз алгоритмів, що використовуються в IDS 30

2.2. Опис процесів системи виявлення вторгнень..... 36

2.3. Логічне взаємодія з компонентами системи 40

2.4. Фізична модель системи виявлення вторгнень..... 42

РОЗДІЛ 3 ТЕСТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ 46

3.1. Тестування алгоитмів системах виявлення вторгнень..... 46

3.2. Налаштування IDS Suricata для роботи зі сторонніми алгоритмами 48

3.3. Дзеркало трафіку на IDS 53

3.4. Динамічна генерація правил та тестування отриманої системи 56

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 60

4.1. Охорона праці..... 60

4.2. Безпека в надзвичайних ситуаціях 62

4.2.1. Інженерний захист персоналу об'єкту та населення. Правила застосування. 62

4.2.2. Особливості роботи та розлади здоров’я користувачів комп’ютерів, що формується під впливом роботи за комп’ютером..... 64
ВИСНОВКИ..... 67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 69
Додаток А. Тези конференцій..... 73
Додаток Б. Скрипт автоматичного запуску Suricata..... 80

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ

IDS (англ. Intrusion Detection System) система виявлення вторгнень

DLP (англ. Data Leak Prevention, DLP) — технології запобігання витоку конфіденційної інформації з інформаційної системи назовні

DoS(DDoS) (англ. DoS attack, DDoS attack, (distributed) denial-of-service attac) напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена

SSL/TLS (англ. Secure Sockets Layer/Transport Level Security) рівень захищених сокетів/ захист на транспортному рівні

SSH (англ. Secure Shell) безпечна оболонка

S/MIME (англ. Secure/Multipurpose Internet Mail Extensions) — стандарт для шифрування і підпису в електронній пошті за допомогою відкритого ключа

LAN (англ. local area network) Лока́льна комп'ю́терна мере́жа

КС комп’ютерна система

ОС операційна система

ПЗ програмне забезпечення

ВСТУП

Актуальність роботи. У питанні захисту комп’ютерних систем дуже велике значення для запобігання несанкціонованому доступу мають системи виявлення та запобігання атакам (IDS/IPS-системи або системи виявлення вторгнень).

Такі системи в реальному часі відстежують аномальну активність на підставі потоків даних, що одержуються з інформаційних систем, мережевого обладнання, антивірусних додатків, систем запобігання витоку даних та багатьох інших джерел. Системи виявлення вторгнень можуть моніторити весь трафік мережі, що дозволяє їм виявляти підозрілі активності, навіть якщо вона відбувається всередині захищеної мережі.

Системи виявлення вторгнень можуть бути масштабовані для роботи у великих мережах та системах, що робить їх більш універсальними та гнучкими в порівнянні з іншими методами захисту.

Найчастіше аналіз інформації щодо аномальної поведінки є комбінацію статистичних і сигнатурних методик виявлення. IDS-система порівнює аналізовані дані з наявним набором заздалегідь визначених правил і сигнатур, при необхідності також спираючись на дані джерела за більш тривалий період. Такий підхід дозволяє захищати комп’ютерну систему від загроз, поведінка яких заздалегідь відома чи легко прогнозована.

Однак, способи та методики мережевих вторгнень постійно змінюються та модернізуються зловмисниками. Розтягування атаки в часі або одночасна робота кількох зловмисників ускладнюють виявлення вторгнення. У таких динамічних умовах необхідний перегляд алгоритмів, що використовуються в роботі системи виявлення вторгнень, для надійної роботи системи.

Нові алгоритми роботи повинні спиратися не тільки на сигнатури відомих інструментів та методів, але й адаптуватись до нових загроз.

Аномальна поведінка в контексті комп'ютерних атак – це явища, невластиві певному мережевому вузлу чи інформаційній системі. До таких явищ можна віднести: різко збільшений обсяг вихідного або вхідного трафіку вузла, зловживання

вузлом відправки широкомовних пакетів, багаторазові невдалі спроби авторизації облікового запису, використання привілейованих системних облікових записів для створення нових облікових записів та багато іншого.

Для вирішення завдання щодо вдосконалення систем виявлення та запобігання атак дослідники виділяють кілька основних напрямків:

–вдосконалення сигнатурного та статистичного аналізу даних;

–обробка нечітких онтологій на підставі попередньо затвердженої безпекової політики;

–використання нейромереж для постійного навчання IDS-системи та протидії складнопрогнозованим атакам.

Варіант удосконалення вже наявних сигнатур є доповненням існуючих правил і алгоритмів поведінки системи виявлення вторгнень. Мінуси такого методу полягають у тому, що IDS-система не може ефективно протидіяти новим програмним методам або атакам які реалізуються з використанням вразливостей апаратного або програмного забезпечення, про які може бути відомо зловмисникам.

Використання попередньо затвердженої політики безпеки – метод, який поєднує у собі плюси використання статистичного та сигнатурного аналізу, та самостійного навчання системи виявлення вторгнень.

Безсумнівно, така IDS-система також вимагає присутності оператора для реагування на помилкові спрацьовування та додаткової оцінки ризиків, проте використання нечітких онтологій дозволяє досягти більшого охоплення загроз, ніж при використанні традиційного сигнатурного аналізу.

Проблеми та питання, пов'язані з розвитком алгоритмів роботи системи виявлення вторгнень, знайшли відображення у наукових працях вітчизняних та зарубіжних вчених та практиків, які послужили основою при виявленні критеріїв та розробці концептуальної моделі системи виявлення вторгнень та запобігання атакам. Більш детально системи IPS та IDS розглядаються такими авторами: Казієнко П., Аксельссон С., Робук К., Лант Т., П'єтро Р., Мовахеді М., Ескін Е., Коліас С.

Таким чином, актуальність дослідження обумовлена в першу чергу тим, що класичні алгоритми роботи системи виявлення вторгнень засновані на сигнатурному та поведінковому аналізі, не забезпечують достатній ступінь безпеки комп’ютерної системи та не можуть запобігти динамічній атакі на ці системи.

Метою кваліфікаційної роботи проведення дослідження існуючих алгоритмів роботи IDS-систем, оптимізації їх під конкретні комп’ютерні системи та мережеву топологію, та розробку моделі системи виявлення вторгнень.

Задачі кваліфікаційної роботи:

– дати оцінку існуючим підходам та рішенням на основі аналізу літератури, наукових та аналітичних статей у галузі виявлення вторгнень та запобігання комп'ютерним атакам;

– виявити основні засади роботи системи виявлення вторгнень, сучасні концепції та підходи до аналізу потоків даних;

– вибрати алгоритми, які застосовуються в кожній конкретній ситуації, використовувані системи виявлення вторгнень під час обробки даних;

– розробити модель системи виявлення вторгнень, що використовує оптимізовані алгоритми для вирішення завдань запобігання атакам в комп’ютерних системах.

Відповідно до цілей та завдань кваліфікаційної роботи визначено її об'єкт та предмет.

Об’єкт дослідження: системи виявлення вторгнень в комп’ютерну систему.

Предмет дослідження: методи і алгоритми роботи систем виявлення вторгнень.

Методи дослідження: Метод моделювання, який використовується для побудови моделі та аналізу його властивостей на основі побудованої моделі. Метод абстрагування, який дозволяє виключити з розгляду незначні властивості об'єкта та приділити увагу найбільш значущим характеристикам об'єкта. Метод візуалізації даних, що використовується для побудови графіків і схем, що дозволяє наочно представляти отримані результати дослідження.

Наукова новизна дослідження полягає у розробці нового алгоритму виявлення вторгнень, що дозволить скоротити кількість помилкових спрацьовувань системи, підвищить загальну безпеку мережевої структури комп’ютерної системи та мінімізує збитки, завдані комп'ютерними атаками..

Теоретична значущість полягає у описі методу використання систем виявлення вторгнень, що використовують додаткові алгоритми, що можуть бути автоматично створені або розроблені вручну. Результати дослідження ефективності протоколів виявлення вторгнень дозволяє використовувати ці результати у подальших наукових дослідженнях.

Практичне значення результатів кваліфікаційної роботи полягає у можливості використання розробленої системи виявлення вторгнень для захисту комп’ютерних систем від несанкціонованого доступу та комп'ютерних атак.

Публікації. Результати дослідження апробовано на XI науково-технічній конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології», XII міжнародній науково-технічній конференція молодих учених та студентів «Актуальні задачі сучасних технологій», у вигляді тез конференцій.

1. Ковтун Н., Жаровський Р. Алгоритмічне забезпечення систем виявлення вторгнень. Матеріали XI науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі системи та технології» (13-14 грудня 2023 року). Тернопіль: ТНТУ. 2023. С.156

2. Ковтун Н., Жаровський Р. Аналіз засобів протидії вторгненням і атакам на комп’ютерні системи. Матеріали XII Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» (6-7 грудня 2023 року). Тернопіль: ТНТУ. 2023. С. 453-454.

Структура роботи. До складу кваліфікаційної роботи магістра входить розрахунково-пояснювальна записка та графічний матеріал. Розрахунково-пояснювальна записка містить вступ, 4 розділи, загальні висновки, список використаної літератури і додатки. Обсяг роботи: розрахунково-пояснювальна записка – 83 арк. формату А4, графічна частина – 8 аркушів формату А1.

РОЗДІЛ 1
АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ ВКОМП'ЮТЕРНИХ СИСТЕМАХ

1.1. Роль IDS у технічному захисті інформації

Під безпекою інформації розуміють здатність системи її обробки забезпечити в певний проміжок часу можливість виконання визначених вимог з врахуванням ймовірності настання подій витоку, модифікації або втрати інформації, яка представляє певну цінність для її власника.

Для оцінки захищеності інформації визначено критерії, серед яких основні параметри такі:

–важливість інформації: Це узагальнений показник, який характеризує значущість інформації в контексті її призначення та умов обробки;

–повнота інформації: Визначає, чи достатньо інформації для вирішення конкретних завдань;

–адекватність інформації: Ступінь відповідності інформації дійсному стану речей, які вона відображає;

–релевантність інформації: Ступінь відповідності інформації потребам завдання;

–толерантність інформації: Зручність сприйняття та використання інформації під час вирішення задачі;

Після оцінки інформації, що потребує захисту, важливо вибрати технічні та організаційні заходи для забезпечення її безпеки. Для цього використовуються як оцінка самої інформації, так і оцінка можливих способів несанкціонованого доступу до неї. Зазвичай для аналізу дій зловмисника використовуються методики, розроблені державними органами, що регулюють захист інформації, такі як матриця технік та тактик MITRE ATT&CK, розроблена американською некомерційною організацією Mitre [1].

Типові програмні та апаратні інструменти безпеки комп’ютерних систем включають [2]:

–системи антивірусного захисту. Вони визначають та нейтралізують шкідливе програмне забезпечення, таке як віруси і трояни;

–комплексні системи захисту від несанкціонованого доступу. Ці системи об'єднують кілька підсистем в одному програмному продукті, включаючи системи управління доступом, системи реєстрації та обліку, криптографічний захист інформації, а також підсистему забезпечення цілісності;

–системи міжмережевого екранування (firewall). Вони забезпечують контроль та фільтрацію мережевих пакетів для захисту від несанкціонованого доступу;

–системи резервного копіювання інформації. Ці системи забезпечують відновлення інформації після порушення її цілісності зловмисником або внаслідок технічних та програмних збоїв;

–системи запобігання витоку даних (DLP-системи). Вони відстежують дії користувачів та формують аналітичні звіти про їх діяльність, а також запобігають можливим витокам службової інформації;

–системи виявлення (запобігання) вторгнень (IDS/IPS). Ці програмні комплекси аналізують інформацію з різних джерел, сигналізуючи про будь-яку аномальну активність або вживаючи заходів для її припинення.

Системи виявлення вторгнень у сфері інформаційної безпеки комп'ютерних систем є програмними чи апаратними засобами, які дозволяють автоматично відстежувати та аналізувати активність в мережі чи комп'ютері з метою виявлення спроб несанкціонованого доступу або використання ресурсів [3, 4]. Системи виявлення вторгнень можуть працювати як на рівні операційної системи, так і на рівні додатків комп'ютерної системи. Їх завданням є своєчасне визначення та реагування на підозрілу активність, наприклад, сканування портів, впровадження шкідливих програм, спроби перехоплення трафіку та інші загрози інформаційній безпеці [12]. Системи виявлення вторгнень відіграють важливу роль у захисті інформації та забезпеченні безпеки комп'ютерних систем [7].

Принцип роботи систем виявлення вторгнень заснований на аналізі мережної чи системної активності та пошуку відхилень від нормальної поведінки. Для цього системи виявлення вторгнень використовують моделі поведінки, які можуть бути створені на основі статистичних даних про те, як повинен проходити обмін даними всередині системи. Ці моделі можуть бути попередньо навчені та налаштовані на підставі знань про типові патерни поведінки та загрози інформаційній безпеці.

Системи виявлення вторгнень можуть працювати в режимі реального часу, постійно переглядаючи та аналізуючи дані, або виконуватись за розкладом, скануючи систему у певні моменти часу. У разі виявлення потенційно небезпечної активності, такої як сканування портів, перехоплення трафіку або спроби злому, системи виявлення вторгнень можуть сигналізувати про це адміністратору системи через різні канали зв'язку, наприклад, електронну пошту або SMS-повідомлення.

Системи виявлення вторгнень можуть використовувати різні методи для виявлення загроз, включаючи сигнатурне (signature-based) виявлення, яке шукає відповідності між зразком заздалегідь відомої загрози та зразками активності на мережі або комп'ютері, та аномалійне (anomaly-based) виявлення, яке шукає відхилення від нормальної поведінки системи. Також можуть застосовуватись гібридні методи, що поєднують різні підходи для найбільш ефективного виявлення загроз [4].

Таким чином, система виявлення вторгнень вирішує конкретне завдання інформаційної безпеки – запобігання несанкціонованому доступу до тих чи інших інформаційних ресурсів та вузлів мережі [8].

Системи виявлення вторгнень класифікуються за кількома параметрами: за місцем встановлення, за принципом дії (використовуваних алгоритмів), за методами отримання даних.

Системи виявлення вторгнень класифікуються за кількома параметрами розглянемо:

–за місцем встановлення: Мережеві системи виявлення вторгнень (NIDS), якірозташовані на стратегічно важливих ділянках мережі. Аналізують вхідний/вихідний трафік всіх пристроїв мережі на рівні канального та додаткового

рівнів. Недолік - велике споживання апаратних ресурсів. Хостові системи виявлення вторгнень (HIDS), які розташовані на окремому вузлі чи групі вузлів усередині мережі. Вони мають можливість аналізувати вхідні та вихідні пакети трафіку для визначеної групи вузлів. Існують масштабовані хостові IDS/IPS системи, які працюють за принципом клієнт-сервера;

–за алгоритмами розрізняють сигнатурні системи виявлення вторгнень: використовують заздалегідь визначений набір правил для ідентифікації відомих загроз. системи виявлення вторгнень на основі аномалій: характеризується "періодом навчання", коли система накопичує шаблони даних про "нормальну" роботу мережі. комбіновані системи виявлення вторгнень: використовують як відомі сигнатури типових атак, так і принципи самонавчання системи;

–за методами отримання даних поділяють на пасивні системи виявлення вторгнень які моніторять і аналізують дані без втручання в трафік чи системні операції. Активні системи виявлення вторгнень,які активно проводять тестування та аналізують системні чи мережеві елементи. Змішані системи виявлення вторгнень, які використовують обидва вищевказані підходи.

Ця класифікація дозволяє враховувати різноманітні характеристики систем виявлення вторгнень, допомагаючи вибрати ті, які найбільше відповідають конкретним потребам та умовам застосування.

Системи виявлення вторгнень мають суттєві переваги над іншими системами інформаційної безпеки [23].

По-перше, системи виявлення вторгнень здатна виявляти нові загрози та атаки, які до цього не були відомі. Це можливо завдяки використанню механізмів виявлення аномалій у поведінці користувачів чи трафіку у мережі. Таким чином, системи виявлення вторгнень дозволяє оперативно реагувати на нові види загроз, що особливо важливо в умовах постійного змінного загрозливого середовища.

По-друге, системи виявлення вторгнень працює в режимі безперервного моніторингу трафіку і може оперативно реагувати на інциденти в реальному часі. Це дозволяє своєчасно помічати та реагувати на підозрілу активність у мережі, що знижує ризик витоку конфіденційної інформації та інших негативних наслідків.

По-третє, системи виявлення вторгнень може автоматично реагувати на загрози без участі людини, що прискорює процес реакції на інциденти та дозволяє скоротити час простою системи.

По-четверте, системи виявлення вторгнень може бути масштабована в залежності від розміру мережі, що захищається, і обсягу трафіку. Це означає, що вона може бути використана як у невеликих компаніях, так і у великих корпораціях та державних установах.

По-п'яте, системи виявлення вторгнень здатна мінімізувати помилки людського чинника, пов'язані з неуважністю, недосвідченістю чи іншими чинниками. Це досягається автоматичним виявленням та реагуванням на загрози без участі людини.

І, нарешті, система виявлення вторгнень може бути розширена для виявлення нових типів загроз і атак. Це робить її ефективною у захисті мережі при появі нових загроз та допомагає запобігати можливим атакам у майбутньому.

Розглянемо докладніше, для яких мережевих атак на комп’ютерну систему найефективніші системи IDS.

1.2. Ефективність IDS в протидії поширеним мережевим атакам

Загалом системи виявлення вторгнень можуть виявляти різні типи атак, але найкраще вони справляються з наступними категоріями.

Атаки відмови в обслуговуванні (Denial of Service або DoS) та їх розподілений варіант (Distributed Denial of Service або DDoS) представляють собою кібератаки, спрямовані на виведення з ладу систем та сервісів в Інтернеті. Ці атаки досягаються шляхом блокування доступу до ресурсів або зниження їх продуктивності [25].

Основна мета DDoS-атак полягає в перевантаженні сервера чи мережі великою кількістю запитів, таким чином, щоб не залишалося ресурсів для обробки легітимних запитів [24]. Атакуючі використовують ботнети – мережу заражених комп'ютерів, які вдало контролюються зловмисниками. Ці комп'ютери можуть бути

заражені вірусами або троянськими програмами, що дають можливість зловмиснику віддалено керувати ними.

DDoS-атаки можуть приймати різні форми та обсяги. Вони можуть бути запущені з одного комп'ютера або складатися з тисяч комп'ютерів, які одночасно атакують [24]. Також атакуючі можуть використовувати різні методи для маскування своїх дій, таких як зміна IP-адрес відправника чи використання "ботів-зомбі" (заражених вузлів ботнета), які можуть обходити системи захисту.

В результаті DDoS-атак доступ до сайту або додатку може бути блокований на кілька хвилин або годин, що, у свою чергу, може призвести до серйозних фінансових втрат для компанії, таких як втрати клієнтів та доходів через недоступність сайту [24].

Системи виявлення вторгнень (IDS) можуть виявляти подібні атаки через аналіз характерного об'ємного потоку трафіку з одного чи декількох IP-адрес або MAC-адрес. Наприклад, випадки атак типу SYN-flooding всередині мережі, де багато клієнтських пристроїв намагаються ініціювати TCP-сесію з цільовим хостом, можуть бути виявлені IDS за адресою призначення пакетів. У разі використання IPS-систем реакцією на виявлену DoS(DDoS)-атаку може бути тимчасове блокування окремих портів цільового хоста або обрив всіх нових сесій до нього.

Атаки сканування (Scanning Attacks) представляють собою один з типів мережевих атак, під час якого зловмисник проводить сканування мережі чи системи для виявлення можливих уразливостей. Цей вид атак може служити першим кроком перед більш серйозними атаками на систему [26].

Процес сканування включає відправлення запитів на різні порти та протоколи для пошуку слабких місць у мережі. Зловмисники можуть використовувати різноманітні інструменти для цього, такі як Nmap. Залежно від мети атакуючого, сканування може бути спрямоване на пошук конкретних уразливостей у певних пристроях або виконуватися загально для виявлення можливих слабких точок.

Приклади атак сканування включають:

– Ping Sweep: метод сканування, під час якого зловмисник відправляє ICMP-запити на всі адреси підмережі для виявлення активних пристроїв у мережі;

– Port Scanning: метод сканування, під час якого зловмисник відправляє запити на відкриті порти пристроїв у мережі для визначення, які сервіси запущені та які можуть бути використані для атак;

– Vulnerability Scanning: метод сканування, під час якого зловмисник відправляє запити на відомі уразливості у мережі чи конкретних пристроях для виявлення можливостей атаки.

Системи виявлення вторгнень (IDS) виявляють атаки сканування шляхом визначення невдалих спроб підключення до портів цільового хоста. Якщо система IPS зафіксує певну кількість таких невдалих спроб, вона може автоматично заблокувати вузол, з якого ведеться атака. Крім того, система може генерувати сповіщення про невідомі IP- та MAC-адреси в мережі, з яких відбувається активне розсилання пакетів.

Атаки на протоколи представляють собою методи, в яких зловмисники використовують уразливості під час передачі даних між комп'ютерами чи мережами. Ці атаки можуть мати різноманітні цілі, від крадіжки особистих даних до отримання контролю над системою [27]. Існує багато різновидів атак на протоколи, серед яких деякі включають:

– атаки на протоколи безпеки: ці атаки спрямовані на використання вразливостей в захисті протоколу для отримання доступу до системи або інформації, що передається між пристроями [27]. Протоколи безпеки, такі як SSL/TLS, SSH, S/MIME та інші, широко використовуються для забезпечення конфіденційності, цілісності та доступності даних;

– атаки на протоколи маршрутизації: ці атаки спрямовані на зміну маршруту передачі даних між пристроями, часто з метою створення каналу витоку конфіденційної інформації з локальної мережі. Серед таких атак варто відзначити DNS-redirecting, де зловмисник стає DNS-сервером, щоб підмінювати DNS-адреси інформаційних ресурсів, а також Routing Table Poisoning, коли зловмисник змінює таблиці маршрутів на маршрути, які контролюються ним;

– атаки на протоколи авторизації: ці атаки спрямовані на отримання доступу до системи, використовуючи вкрадені облікові дані чи атакуючи процес авторизації.

Такі атаки, як SQL або XSS-ін'єкції, можуть дозволити зловмиснику отримати несанкціонований доступ до бази даних та обійти механізм авторизації системи [12].

Системи виявлення вторгнень (IDS) виявляють атаки на протоколи за допомогою сигнатурного аналізу пакетів, що передаються в протоколах. Уразливості протоколів часто відомі, і способи їх використання легко визначаються за допомогою баз сигнатур [10]. Системи захисту від вторгнень (IPS) можуть автоматично додавати хости, що використовують уразливості протоколів, до списку ненадійних джерел і блокувати їм доступ до внутрішніх ресурсів мережі. Складніші атаки на авторизацію, такі як Kerberoasting, виявляються за допомогою поведінкового аналізу [13].

1.3. Розміщення IDS у периметрі мережі

Розглянемо важливий аспект ефективності систем виявлення та запобігання вторгнень (IDS/IPS) - їхнє місце в периметрі мережі, особливо враховуючи наявність міжмережевого екрана (фаєрвола). Вибір оптимального місця розташування визначає як навантаження на систему виявлення вторгнень, так і ефективність фільтрації трафіку [28].

Міжмережевий екран, працюючи на рівні мережного з'єднання, приймає рішення про дозвіл або блокування пакетів, аналізуючи вхідний та вихідний трафік. Він використовує набір правил для обробки кожного пакета, враховуючи параметри, такі як IP-адреса, номери портів та тип протоколу [28]. IDS, натомість, аналізує вміст пакетів на предмет загроз на рівні програми.

Ефективний захист може бути досягнутий за умови інтеграції IDS та фаєрвола, які взаємодіють для аналізу та блокування потенційно небезпечного трафіку. Наприклад, фаєрвол може блокувати доступ до певних портів або протоколів, а IDS - аналізувати дозволений трафік на предмет загроз .

Також може бути використаний режим "внутрішнього" міжмережевого екрану, коли IDS виконує функції контролю та блокування трафіку на основі

правил. Це дозволяє IDS запобігати внутрішнім загрозам, запобігаючи їх поширенню усередині мережі.

Щодо розміщення IDS перед фаєрволом, це характерно для протокольних IDS, які аналізують трафік перед його фільтрацією всередині мережі. Цей підхід, хоча збільшує навантаження на систему виявлення вторгнень, дозволяє фіксувати атаки не лише на внутрішню мережу, а й на зовнішні ресурси веб-сервера, таким чином захищаючи від DoS та DDoS-атак [27].

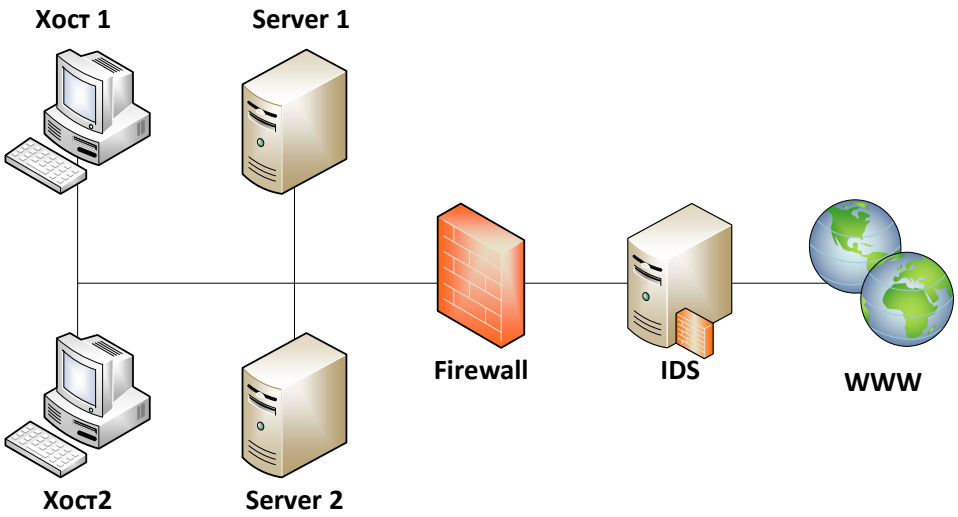

Рис. 1.1 Розташування IDS-системи поза мережею

Альтернативний і широко використовуваний метод розміщення системи виявлення вторгнень полягає в розташуванні її безпосередньо за міжмережевим екраном (фаєрволом), де весь вхідний та вихідний трафік пройшовши фільтрацію, подається на сервер системи виявлення вторгнень. Тут він аналізується, і при необхідності блокується, після чого дозволені пакети спрямовуються безпосередньо на цільовий хост (рис. 1.2). Такий підхід суттєво зменшує навантаження на IDS, проте вимагає використання додаткових заходів безпеки для захисту веб-серверів з відкритими зовнішніми інтерфейсами, таких як інтернет-сайти та відкриті для зовнішніх підключень веб-додатки.

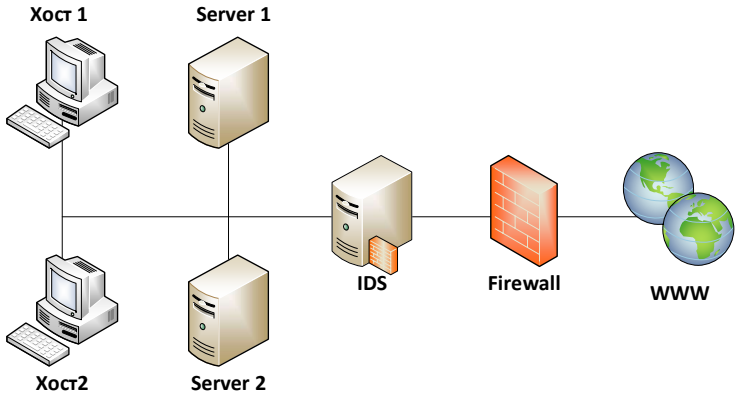

Рис. 1.2. Розташування IDS-системи у периметрі внутрішньої мережі

Третій сценарій розташування передбачає внутрішнє розташування системи виявлення вторгнень (IDS) всередині мережі (рис. 1.3), проте паралельно до хостів. Цей варіант є більш актуальним для IDS-систем, оскільки він не перешкоджає проходженню трафіку до цільових хостів і не може безпосередньо блокувати підозрілі пакети. Однак, він суттєво знижує навантаження на модуль аналізу трафіку і дозволяє ефективно масштабувати систему, додаючи будь-яку кількість окремих серверів IDS для збільшення продуктивності.

Важливо відзначити, що це рішення може не бути оптимальним для всіх алгоритмів, використовуваних в IDS, але воно ідеально вписується в модель, розглянуту в даному дослідженні, де використовується комбінація декількох алгоритмів аналізу та центрального модуля прийняття рішень, який надає інформацію оператору IDS про підозрілу поведінку всередині мережі.

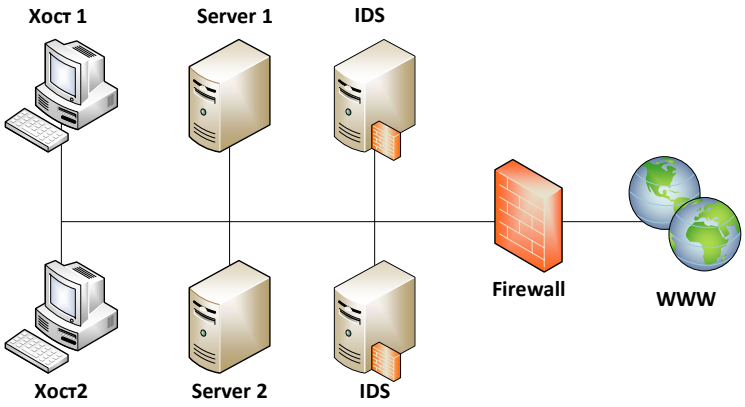

Рис. 1.3. Розташування кількох паралельних нод IDS-системи всередині мережі

Надалі в роботі роботі буде розглядатися саме такий метод розташування системи виявлення вторгнень всередині мережі. Одна з важливих переваг це можливість масштабування системи та розподілу її на кілька цільових серверів. Такий підхід дозволить досягти вищого рівня безпеки для системи виявлення вторгнень, забезпечить стійкість до відмов, оптимально розподілить серверні ресурси, зокрема у випадку розміщення системи виявлення вторгнень на віртуальних машинах. Крім того, цей метод сприятиме впровадженню окремих модулів та сенсорів не лише на основні мережеві магістралі, але і на кожен великий вузол, включаючи розташування їх в кожній локальній підмережі, що полегшить подальше розширення системи.

1.4. Порівняльний аналіз систем виявлення вторгнень

Однією з систем виявлення вторгнень є Snort, яка широко використовується для моніторингу та аналізу мережевого трафіку з метою виявлення можливих атак та вторгнень в комп'ютерні системи. Структурно Snort складається з наступних елементів (рис. 1.4):

- сніфер пакетів – забезпечує перехоплення та дублювання пакетів мережевого трафіку для подальшої передачі в обробку;
- декодер пакетів – визначає заголовки пакетів трафіку, аналізує їх прапори, відсікає пакети, які містять істотної інформації. На цьому етапі виявляються аномалії канального та мережевого рівнів;
- препроцесори. На цьому етапі відбувається детальний аналіз кожного з протоколів, зокрема прикладного рівня, таких як HTTP, SMTP, SSH і т.д. Препроцесори нормалізують та реконструюють потоки для подальшого пошуку аномалій за сигнатурами чи правилами;
- модуль виявлення атак – ядро системи, саме він здійснює аналіз підготовлених даних на відповідність або невідповідність відомим сигнатурам і правилам, приймає рішення про подальше пересилання пакетів та відображення інформації в модулі виведення;

- модуль виведення – способи інформування оператора у разі виявлення атак. Snort підтримує всі найбільш популярні формати ведення логів та виведення – файлові відображення, syslog, PCAP, ASCII тощо.

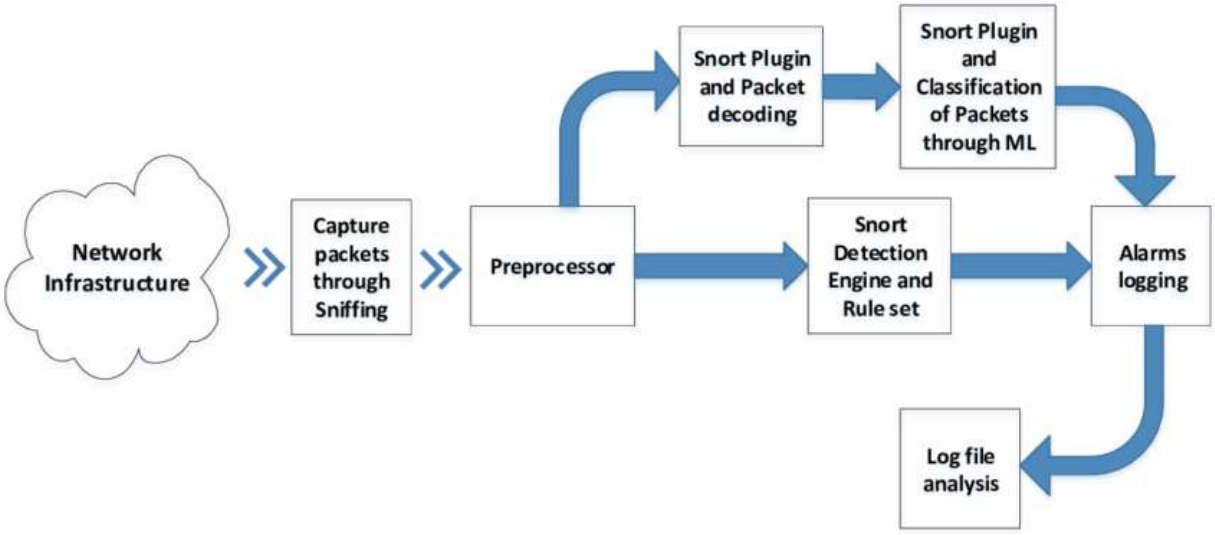

Рис. 1.4. Архітектура Snort

Snort представляє інтерес у першу чергу, тому що завдяки модульності та підтримці сторонніх систем аналізу є можливим порівняння роботи кожного окремого модуля аналізу трафіку. У комерційних IDS такі модулі є інтегрованими та невідключними.

Найбільш близька до Snort є вільно поширювана IDS Suricata (рис.1.5.).

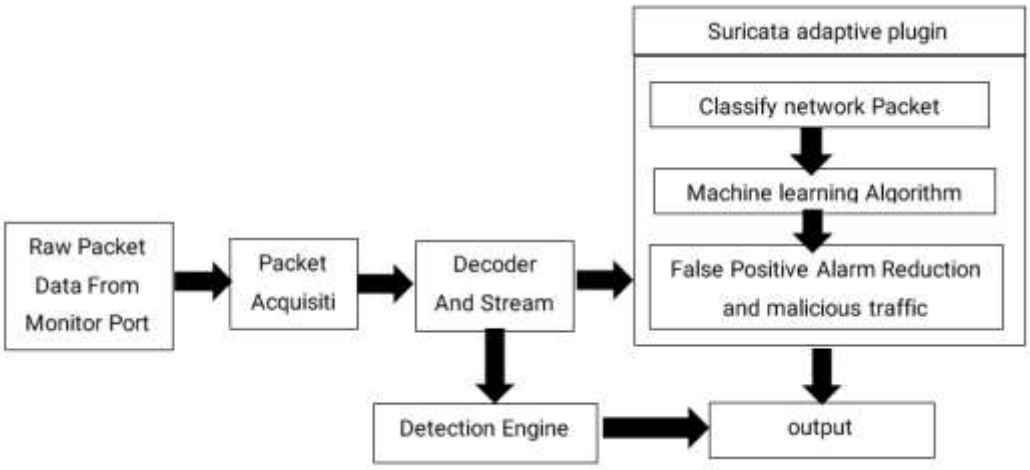

Рис.1.5 Архітектура обробки пакетів в Suricata

Однак, незважаючи на аналогічну архітектуру, вона має кілька ключових особливостей, серед яких:

- початкова робота з упором на багатопоточність. IDS оптимізована під багатопроцесорні системи, що дозволяє досягати стабільного приросту продуктивності рахунок збільшення фізичних ресурсів;
- апаратне прискорення. Suricata підтримує обчислення на графічному процесорі (за рахунок використання технологій CUDA та OpenCL), що дозволяє використовувати як ефективний сервер звичайний ПК з дискретною відеокартою;
- широкі можливості конфігурації. Наприклад, у Snort весь трафік через сніффер до декодера проходить одним потоком. У Suricata можна гнучко налаштувати поведінку потоків трафіку відразу після їхнього захоплення;
- режим IDS штатними засобами. Suricata можна налаштувати не тільки на оповіщення оператора, але й на виконання заздалегідь запрограмованих дій у разі виявлення атак;
- підтримка IPv6. На жаль, Snort підтримує лише адресацію IPv4, що накладає обмеження роботи в сучасних мережах, в яких активно здійснюється перехід на нову модель адресації.
- підтримка надбудов Snort. Ключова особливість Suricata – повна підтримка всіх напрацювань Snort, починаючи від наборів правил та сигнатур, закінчуючи логуванням ключів та сертифікатів SSL-з'єднань.

Однією з ключових особливостей Suricata є її здатність працювати в режимі реального часу та швидко обробляти великі обсяги трафіку. Завдяки цьому вона може використовуватися у великих мережах, де необхідно перевіряти трафік на наявність загроз без затримок та втрат продуктивності.

У сукупності ці фактори роблять із Suricata серйозного конкурента для Snort, а за рахунок гнучких налаштувань потоків даних та оптимізації програмного забезпечення для багатопотокових процесорів та GPU можна забезпечити суттєве прискорення роботи алгоритмів обробки інформації.

Zeek (до 2018 року відома як BroIDS) позиціонується як фреймворк, ніж класична IDS. Zeek має свою власну скриптову мову і вимагає більшого

попереднього налаштування, ніж Snort або Suricata, проте забезпечує сканування більшого обсягу даних за рахунок гнучкого семантичного аналізу. Zeek має модульну архітектуру, яка складається з наступних рівнів (рис.1.6.):

- модуль захвату пакетів. У Zeek використовується libpcap, аналогічна бібліотека використовується, наприклад, Wireshark для захоплення трафіку. Використання libpcap дозволяє системі не залежати від платформи розміщення та мережного рівня;
- ядро подій. Цей модуль формує окремих пакетів ланцюжка подій для подальшого аналізу. Ланцюжки формуються з урахуванням відомих методів обміну даними і протоколів. На даному етапі не приймаються жодних рішень щодо того, чи є подія підозрілою чи ні;
- інтерпретатор подій. Цей модуль – головна відмінність Zeek від аналогів. Оброблювач для кожного ланцюжка подій, що очікують реакції, вибирає найбільш підходящий скрипт і ставить події у чергу. Скриптом визначається набір дій для виявлення підозрілої активності подій та приймається рішення про подальше пересилання пакетів.

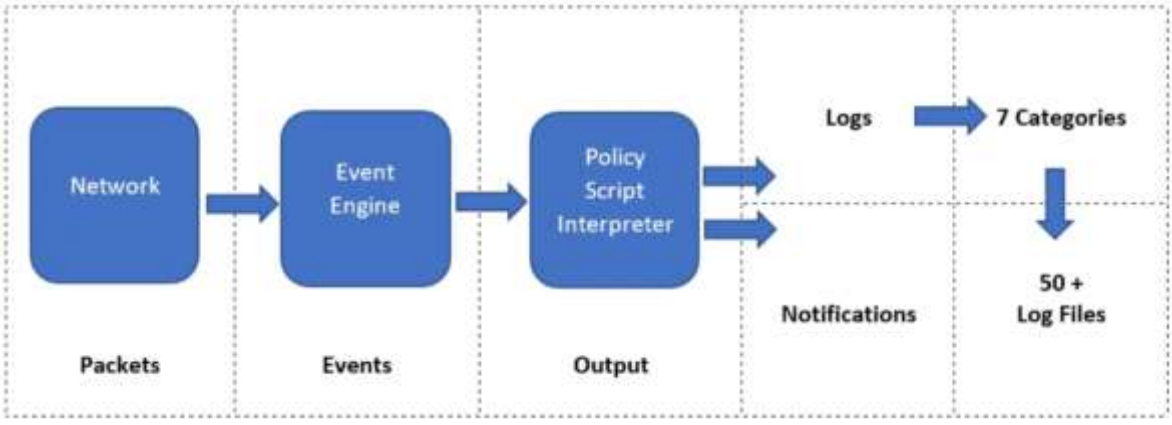

Рис.1.6. Архітектура Zeek

Архітектура системи побудована таким чином, що у разі перевищення передбачуваного навантаження на сервер, частина пакетів трафіку відкидається. Відповідно, при масштабних флуд-атаках, Zeek працюватиме менш стабільно, але не гальмуватиме мережу, як Snort або Suricata.

Можливостей виведення даних у Zeek менше, ніж у конкурентів – є підтримка файлового виведення та підтримка ElasticSearch.

При всіх своїх можливостях у Zeek є один серйозний недолік - дуже високий поріг входження. Щоб побудувати за допомогою Zeek повноцінно функціонуючу IDS необхідно досконально розбиратися в протоколах низького рівня, вивчити мовну скриптову платформу, розробити регулярні вирази для роботи скриптів і використовувати кластерне розміщення Zeek всередині мережі для вирішення проблеми відкидання пакетів.

OSSEC (Open Source Security) – це безкоштовна система виявлення вторгнень (IDS/IPS), яка була розроблена з урахуванням потреб малих та середніх підприємств (рис.1.7.). Вона може працювати на операційних системах Linux, MacOS та Windows.

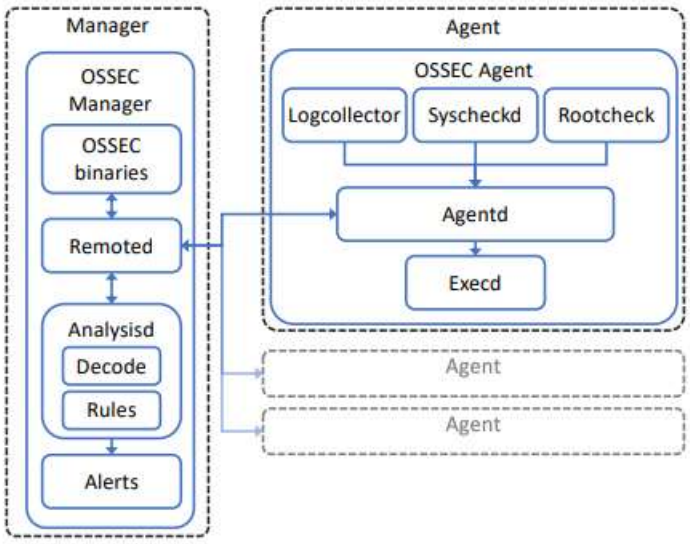

Рис.1.7. Open Source Host-based Intrusion Detection System (OSSEC) компоненти

Основними особливостями OSSEC є:

- централізоване управління журналами: OSSEC може збирати та зберігати журнали подій з кількох серверів у централізованому репозиторії, що забезпечує зручний доступ до інформації про безпеку;

- моніторинг цілісності файлів: OSSEC може відслідковувати зміни у системних файлах та інших критичних файлах та сповіщати адміністратора, якщо вони були модифіковані. Це допомагає запобігти атакам на цілісність даних;
- підтримка багатьох платформ: OSSEC підтримує широкий спектр операційних систем, у тому числі Linux, MacOS, Windows, Solaris, FreeBSD та інші;
- гнучка настройка: OSSEC має гнучку конфігурацію, яка дозволяє настроювати систему відповідно до конкретних потреб та вимог безпеки;
- безкоштовність та відкритий вихідний код: OSSEC є безкоштовною та має відкритий вихідний код, що дозволяє користувачам вільно використовувати та змінювати систему відповідно до їхніх потреб;
- активна спільнота: OSSEC має велику спільноту користувачів та розробників, які забезпечують активну підтримку та розвиток проекту.

Однак зазначена платформа не позбавлена недоліків. Серед основних проблем можна відзначити низьку швидкість обробки даних через постійний контроль цілісності файлів, високе споживання апаратних ресурсів та відсутність графічного інтерфейсу, що заважає інтерпретації результатів роботи.

OpenWIPS-ng – це безкоштовна система виявлення вторгнень (IDS) для бездротових мереж. Вона призначена для аналізу трафіку Wi-Fi, виявлення загроз безпеки та надання захисту від них.

Основні особливості OpenWIPS-ng:

- моніторинг трафіку Wi-Fi: OpenWIPS-ng може моніторити трафік Wi-Fi та аналізувати його, щоб виявляти потенційні загрози безпеці;
- гнучка конфігурація: OpenWIPS-ng має гнучку конфігурацію, яка дозволяє настроювати систему відповідно до конкретних потреб та вимог безпеки;
- підтримка різних режимів роботи: OpenWIPS-ng підтримує кілька режимів роботи, включаючи режим "монітор", "деаутентифікація" та "захист";
- підтримка різних інтерфейсів: OpenWIPS-ng може працювати на різних операційних системах, включаючи Linux, macOS та Windows, та підтримує різні інтерфейси, такі як Ethernet, Wi-Fi та інші.

Проблема використання OpenWIPS-ng у її вузькій спеціалізації – система підходить для бездротових мереж, але немає підтримки більшості протоколів L2-L3 рівнів LAN.

Таким чином, для вирішення проблеми оптимізації роботи алгоритмів найбільш відповідною IDS є Suricata, оскільки вона надає більше можливостей для апаратної оптимізації, ніж Snort.

Висновки до розділу 1

На основі аналізу наукових та аналітичних матеріалів, присвячених удосконаленню систем виявлення вторгнень і запобіганню комп'ютерним атакам, були визначені критерії оцінки захищеної інформації, визначено основні засоби її захисту та сформульовано завдання, що розв'язуються такими системами.

У ході роботи було проведено класифікацію IDS/IPS-систем, виокремлено методи їх розташування, аналізовано алгоритми та методи отримання даних. Сильні та слабкі сторони кожного класу були визначені для подальшого порівняння.

Розглянуті алгоритми систем виявлення вторгнень охоплюють як класичні сигнатурні методи, так і сучасні підходи поведінкового та інтелектуального аналізу даних. Описана архітектура системи виявлення вторгнень дозволяє отримати уявлення про її функціонал та організацію.

За результатами аналізу зроблено висновок про необхідність використання комбінації алгоритмів аналізу трафіку на різних рівнях мережевої моделі OSI та для різних видів мережевої активності.

Вивчені методи виявлення атак в системах виявлення вторгнень були узагальнені в загальний алгоритм роботи, використовуючи комбінацію модулів аналізу, що обіцяє найбільшу ефективність у виявленні атак.

Для оптимізації роботи системи виявлення вторгнень запропоновано замінити основну IDS Snort на більш ефективний аналог.

Проведено порівняльний аналіз альтернатив, таких як IDS Suricata та Zeek, і визначено Suricata як найбільш підходящий варіант, зокрема через його кращу апаратну оптимізацію та сумісність з надбудовами Snort.

РОЗДІЛ 2
АНАЛІЗ АЛГОРИТМІВ. МОДЕЛЮВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

2.1. Аналіз алгоритмів, що використовуються в IDS

Принцип роботи сигнатурних IDS досить простий і багато в чому ідентичний антивірусним системам: в основі системи є інформація про певні шаблони пакетів, характерних для проведення тих чи інших атак. Більшість атак не є унікальними і їх процедури досить добре досліджені, щоб виділити моменти, що характеризують кожну атаку. До того ж, бази сигнатур регулярно оновлюються і поповнюються новими записами, збільшуючи спектр застосування IDS.

Такі системи виявлення вторгнень характеризуються високою швидкістю роботи рахунок відомих алгоритмів атаки [3]. Сигнатурні системи виявлення вторгнень простіше в початковому налаштуванні, оскільки для своєї роботи використовують фіксовані бази сигнатур, які просто підключаються до системи [3].

Однак, через велику кількість сигнатур такі системи схильні до частих помилкових спрацьовувань [6]. Система генерує сигнал підозрілої активності на всі прояви підозрілої активності, хоча більшість трафіку може виявитися в результаті нормальним для цієї мережі, а підозріла активність обумовлена специфікою роботи всередині організації. Наприклад, IDS розглядатиме як підозрілі дії роботу стандартних систем моніторингу мережі, оскільки ті мають високу мережну активність опитування цільових хостів. У великій мережі система моніторингу здатна породжувати тисячі сигналів тривоги на годину, залишаючись легальним регламентним засобом стеження мережевими вузлами [10]. Такої проблеми можна уникнути, якщо попередньо прописати в IDS правила, що ігнорують активність IP-адрес систем моніторингу. Іншим яскравим прикладом помилкового спрацьовування тривоги є висока активність привілейованих користувачів у базах даних.

У теорії, в експлуатованій базі даних не має спостерігатися постійна адміністративна активність, але у реальності найчастіше модифікації баз даних відбуваються одночасно з їх роботою, тому система виявлення вторгнень сприймає таку активність як аномальну.

Тому найбільш пріоритетним етапом розгортання системи виявлення вторгнень є саме конфігурація системи з метою мінімізації хибних спрацьовувань та необхідних ресурсів. Більшість системи виявлення вторгнень групують сигнали тривоги за категоріями, і якщо, наприклад, у мережі відсутні UNIX-хости, можна сміливо відключити спрацювання всіх сигнатур UNIX-платформ [14].

Також сигнатурні системи виявлення вторгнень неефективні при виявленні нових типів загроз, сигнатури яких ще не були занесені до баз. До таких загроз належать уразливості «нульового дня» програмного забезпечення та операційних систем, бекдори та закладки від несумлінних розробників ПЗ.

Для системи виявлення вторгнень, побудованих на поведінковому аналізі, характерними є інші особливості:

–роботі системи обов'язково передує збір трафіку, характерний для нормальної роботи контрольованої ділянки мережі;

–система безперервно перевіряє трафік, що проходить через неї з наявним «еталоном»;

–у разі прояву аномальної активності посилає відповідний сигнал.

Як правило, комерційні IDS поєднують у собі як сигнатурні методи, так і поведінковий аналіз, що збільшує загальний рівень безпеки системи, але також підвищує кількість помилкових спрацьовувань. Також система може включати в себе модуль прийняття рішень та модуль реагування, що забезпечує можливість реагувати на вторгнення та запобігати атакам. Загальна схема архітектури системи виявлення вторгнень зазначена рис. 2.1.

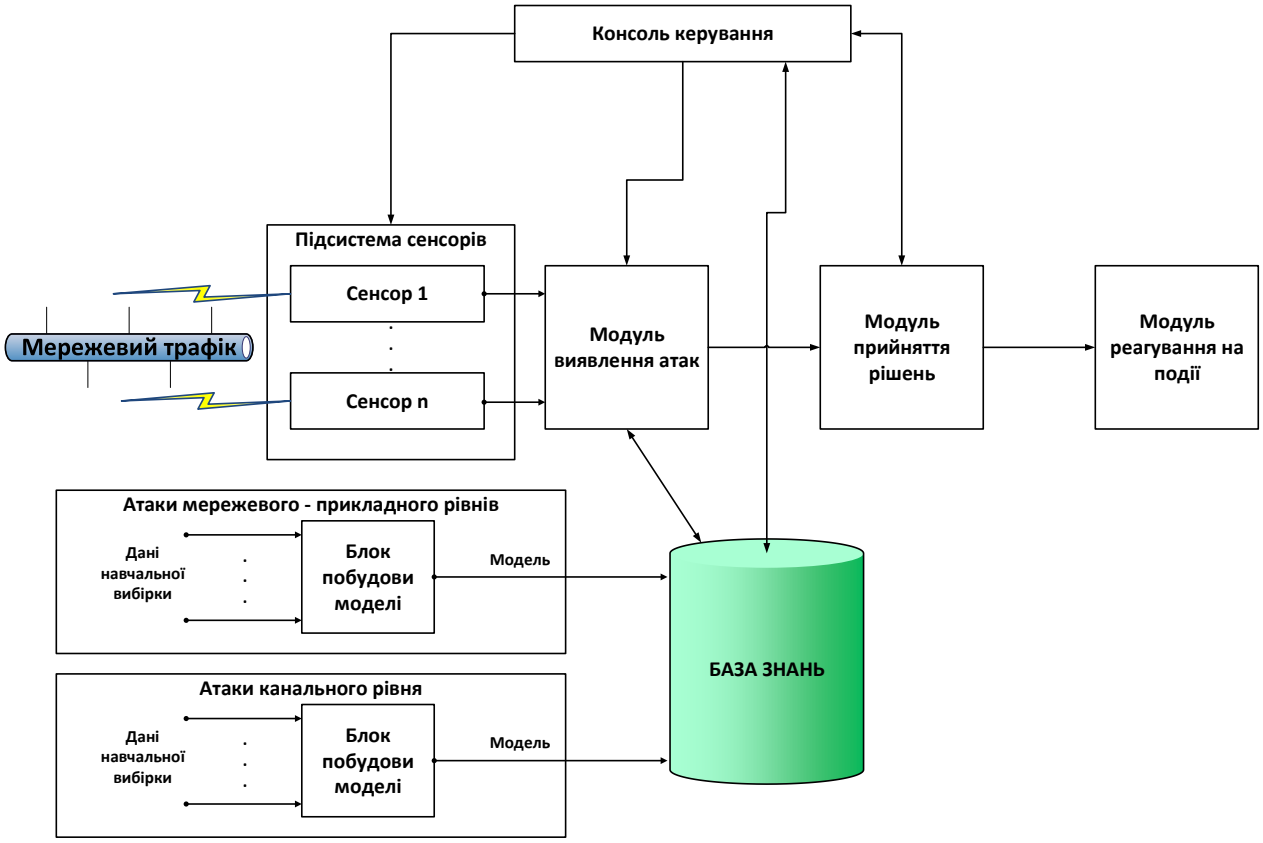

Рис. 2.1. Архітектура системи виявлення вторгнень

На представленій схемі архітектура системи виявлення вторгнень складається з трьох основних модулів та системи контролю мережевого трафіку.

Модуль виявлення атак призначений для аналізу стану мережі та фіксування фактів підозрілої активності чи комп'ютерних атак.

Модуль прийняття рішень отримує інформацію про здійснення атаки від модуля виявлення атак і на підставі різних параметрів (критичність інциденту, масштаб атаки в рамках мережі, ймовірність ескалації інциденту тощо) відправляє на модуль реагування відповідні команди.

У числі реакцій на атаку можуть бути: блокування певної IP або MAC адреси пристрою, введення тимчасових або постійних правил для міжмережевих екранів мережного обладнання, блокування або позбавлення привілеїв певних облікових записів систем (в тому числі доменних), інформування оператора системи виявлення вторгнень або системного адміністратора і т.д. Атаки мережного, прикладного та канального рівнів проходять через фільтрацію бази знань.

Мережевий трафік контролюється підсистемою сенсорів, які в реальному часі фільтрують за заздалегідь визначеними правилами пакети, характерні для найбільш поширених атак (наприклад, DDoS-атаки), копіюють інші пакети та направляють копії модулю виявлення атак, а також у сховище, за необхідності дозволяючи проводити аналіз трафіку. Сенсори спираються на сигнатурний метод аналізу трафіку, отримуючи інформацію про шаблони проведення атак із бази знань. Також у базі знань містяться шаблони реагування на інциденти, які допомагають модулю прийняття рішень (і оператору системи виявлення вторгнень, у разі потреби) вибрати найбільш підходящий спосіб реагування.

Модулі системи виявлення вторгнень контролюються оператором через консоль керування. Все це дозволяє системи виявлення вторгнень контролювати та діагностувати стан мережі та інформаційних систем усередині неї.

Сучасні дослідники також розглядають можливість використання технологій нейронних мереж та інтелектуального аналізу даних для роботи IDS-систем. Наукові праці [29, 30] демонструють перевагу деяких методів над іншими у певних групах атак. Так, наприклад, метод опорних векторів перевершує нейронні мережі у виявленні атак канального рівня, але поступається у виявленні атак прикладного рівня методу дерева прийняття рішень.

Згідно з вищезазначеним дослідженням, найбільш оптимальним з точки зору безпеки є комбінація кількох алгоритмів виявлення атак за участю програмного арбітра, який визначає рівень моделі OSI (Open Systems Interconnection) та тип мережної активності для вибору подальшого алгоритму аналізу трафіку.

Розглянемо докладніше існуючі алгоритми, які у системах виявлення вторгнень. IDS виявляють атаки шляхом використання різних методів аналізу вихідних даних. У цій дослідницькій роботі торкнемося наступні методи виявлення атак:

- packet header anomaly detection (PHAD) – аналіз заголовків пакетів трафіку;
- network traffic anomaly detection (NETAD) – аналіз вмісту кадрів мережного трафіку;
- application layer anomaly detection (ALAD) – аналіз роботи додатків;

- learning rules for anomaly detection (LERAD) – умовні правила виявлення аномалій у вихідних даних пакетів (наприклад, ланцюжки handshake, що передаються в рамках TCP-сесії).

Кожен метод виявлення атак показує найбільшу ефективність проти певних видів атак. Наприклад, аналіз заголовків ефективний виявлення атак типу DNS-spoofing чи SYN-flood, але з здатний виявити використання SQL-ін'єкцій, яке, своєю чергою, легко виявляється з допомогою аналізу роботи додатків [12].

Тому в більшості системи виявлення вторгнень використовуються комбінації різних методів виявлення атак разом з попередньо налаштованими правилами та/або технологіями машинного навчання для забезпечення найбільшої безпеки системи, що захищається, і мінімізації можливої шкоди [17].

Незважаючи на те, що методи виявлення аномалій удосконалюються з кожним роком, першим етапом роботи будь-якого IDS є сигнатурний аналіз. Він дозволяє максимально швидко виявити найпоширеніші атаки без залучення основних ресурсів системи, що економить час та обчислювальні потужності серверів.

З такої точки зору системи виявлення вторгнень виглядає так (рис. 2.2).

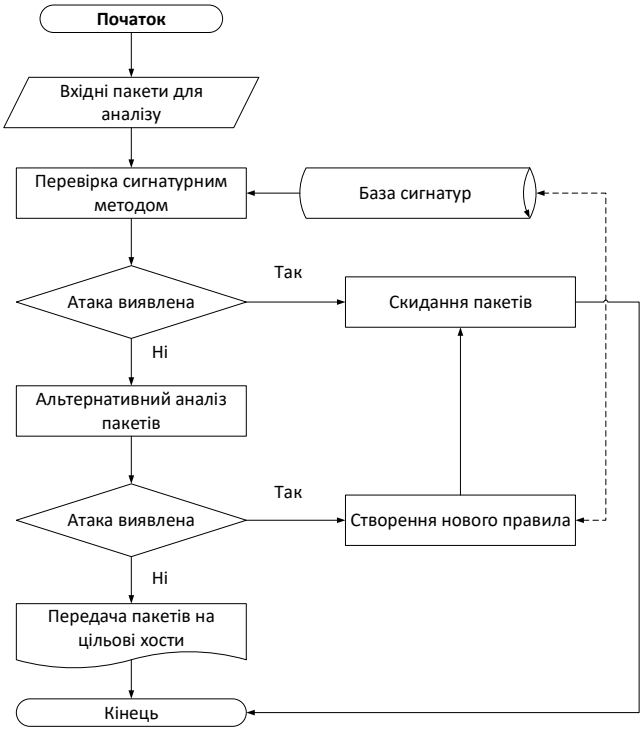

Рис. 2.2. Загальний алгоритм роботи IDS

Основні небезпеки відкидаються на початковому етапі шляхом перевірки сигнатур. Це дозволяє мінімізувати навантаження на апаратні можливості системи, оскільки в такому разі не потрібна глибока інспекція трафіку. Якщо система виявлення вторгнень виявляє загрозу щодо сигнатур, подальші перевірки трафіку недоцільні, оскільки пакет відкидається в будь-якому випадку.

Особливу увагу у схемі роботи варто звернути на пункт «Альтернативний аналіз пакетів». Саме цьому етапі можна застосовувати вищевказані методи аналізу (PHAD, NETAD, ALAD і LERAD).

Ефективність роботи алгоритмів визначається наступним рядом параметрів:

–швидкість обчислень (час обробки вихідних даних);

–точність визначення атак (достовірність визначення факту атаки та її правильна класифікація);

–частота помилкових спрацьовувань системи.

Для порівняння відносної ефективності алгоритмів ми спиратимемося на дослідження вчених GV Nadiammai та M. Hemalatha [31].

В якості базової системи IDS використаємо Suricata, оскільки вона надає більше можливостей для апаратної оптимізації, ніж Snort, але при цьому підтримує алгоритми глибокого аналізу пакетів ALAD + LERAD, розроблені як надбудови для Snort. Тоді цільова система піддаватиме кожен пакет трафіку двом видам аналізу (рис. 2.3): початковий аналіз відповідність сигнатурам здійснюється рахунок баз сигнатур і правил Suricata, а подальший глибокий аналіз виконується модулями ALAD + LERAD.

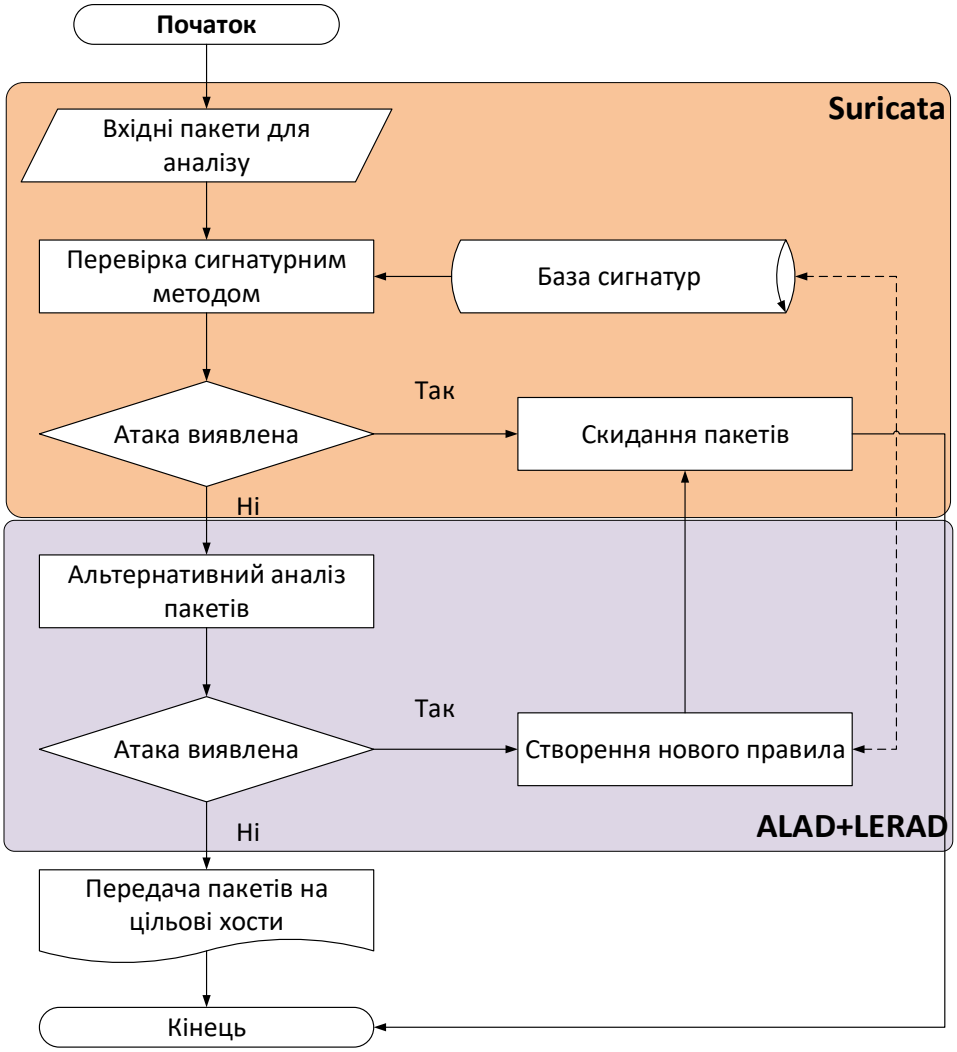

Рис. 2.3. Загальна схема роботи пропонованої IDS

В подальшому наведемо результати тестування обраних протоколів для підтвердежння гіпотези щодо їх ефективності і швидкодії.

2.2. Опис процесів системи виявлення вторгнень

Щоб сформувати логічну модель системи виявлення вторгнень, необхідно описати процес виявлення атак та реагування на них. Для цього скористаємось нотацією BPMN, за допомогою якої можна описати як організаційні, так і технічні елементи бізнес-процесів.

BPMN (Business Process Model and Notation) – це стандартна графічна нотація, яка використовується для моделювання бізнес-процесів та діаграм потоків роботи.

Вона була розроблена групою експертів із різних галузей бізнесу з метою створення загальної та зрозумілої моделі процесів для всіх учасників бізнес-процесу.

Нотація BPMN дозволяє описувати бізнес-процеси у вигляді діаграми, що складається з набору символів та позначень. BPMN використовується для моделювання бізнес-процесів, щоб допомогти компаніям краще розуміти, як працюють їхні процеси, та оптимізувати їх виконання. Це може включати:

- покращення ефективності процесів: BPMN може допомогти ідентифікувати вузькі місця у процесах та визначити, де можна зробити поліпшення для підвищення ефективності;
- зниження витрат: завдяки оптимізації процесів, можна знизити витрати виконання завдань і поліпшити якість роботи;
- покращення взаємодії: BPMN дозволяє різним співробітникам департаментам розуміти, як працює бізнес-процес, що сприяє кращій взаємодії між ними та покращує комунікацію;
- створення єдиної системи для роботи з процесами: BPMN створює стандартну нотацію, яка може бути використана всіма учасниками процесу, що полегшує розуміння та взаємодію;
- автоматизація процесів: BPMN може бути основою для автоматизації бізнес-процесів, що дозволяє скоротити час виконання завдань та підвищити точність;
- розуміння складних процесів: BPMN дозволяє розбивати складні процеси більш прості, що полегшує розуміння їх структури і потоків.

В цілому, BPMN є потужним інструментом для моделювання та оптимізації бізнес-процесів, який може допомогти компаніям покращити свою ефективність та конкурентоспроможність. Нотація BPMN забезпечує єдину інтерпретацію процесів на всіх рівнях організації та знижує ймовірність нерозуміння та помилок у процесах. Вона застосовується у багатьох галузях, включаючи виробництво, фінанси, охорону здоров'я тощо.

Процеси в нотації BPMN розбиваються на простіші компоненти для кращого розуміння та управління. Ці компоненти включають такі елементи:

- події (Events): це події, які починають або закінчують процес чи його частину. Вони можуть бути стартовими (початковими), проміжними та кінцевими;
- завдання (Tasks): це елементи, які представляють виконання певної роботи. Вони можуть бути автоматичними або користувальницькими;
- шлюзи (Gateways): це елементи, які керують потоком виконання завдань у процесі. Вони можуть визначати, які завдання виконуватимуться, залежно від певних умов;
- артефакти (Artifacts): це додаткові елементи, які використовуються для опису процесу чи його частин. Вони можуть включати коментарі, інструкції або документацію;
- сполучні об'єкти (Connecting Objects): це стрілки, які пов'язують різні елементи процесу визначають порядок виконання завдань.

Кожен процес може складатися з декількох підпроцесів, які можуть бути розбиті на більш прості компоненти. Такий підхід до моделювання процесів допомагає зробити їх більш зрозумілими, керованими та оптимізованими.

Для розуміння логіки роботи системи виявлення вторгнень складемо спрощену модель процесу виявлення вторгнень в організації (рис. 2.4.).

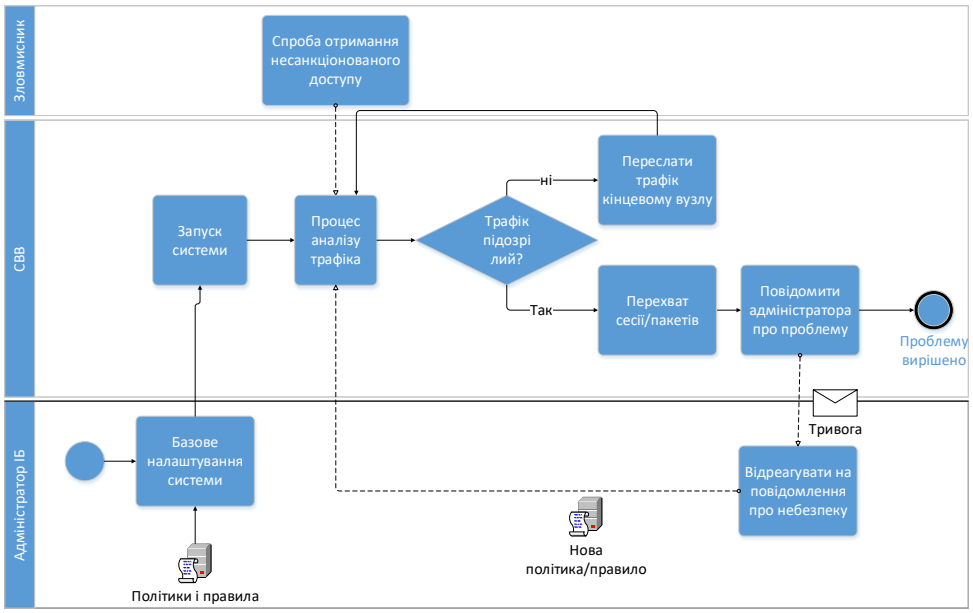

Рис. 2.4. Спрощена модель процесу роботи системи виявлення вторгнень у нотації BPMN

З діаграми можна зрозуміти, що адміністратор ІБ займається не тільки первісним настроюванням системи виявлення вторгнень, але й бере участь у перевірці загроз, що надходять за результатами аналізу трафіку. На підставі отриманої інформації адміністратор формує нові правила та політики, які завантажує у систему виявлення вторгнень для автоматизації реагування на подібні інциденти надалі. Однак, кількість подій і атак може обчислюватися десятками за хвилину, і в такому разі організації доведеться збільшувати навантаження на адміністратора ІБ аж до розширення штату, що спричиняє додаткові витрати. У запропонованій моделі взаємодії (рис. 2.5) процес додавання політик автоматизується рахунок самонавчання системи з урахуванням алгоритмів інтелектуального аналізу пакетів.

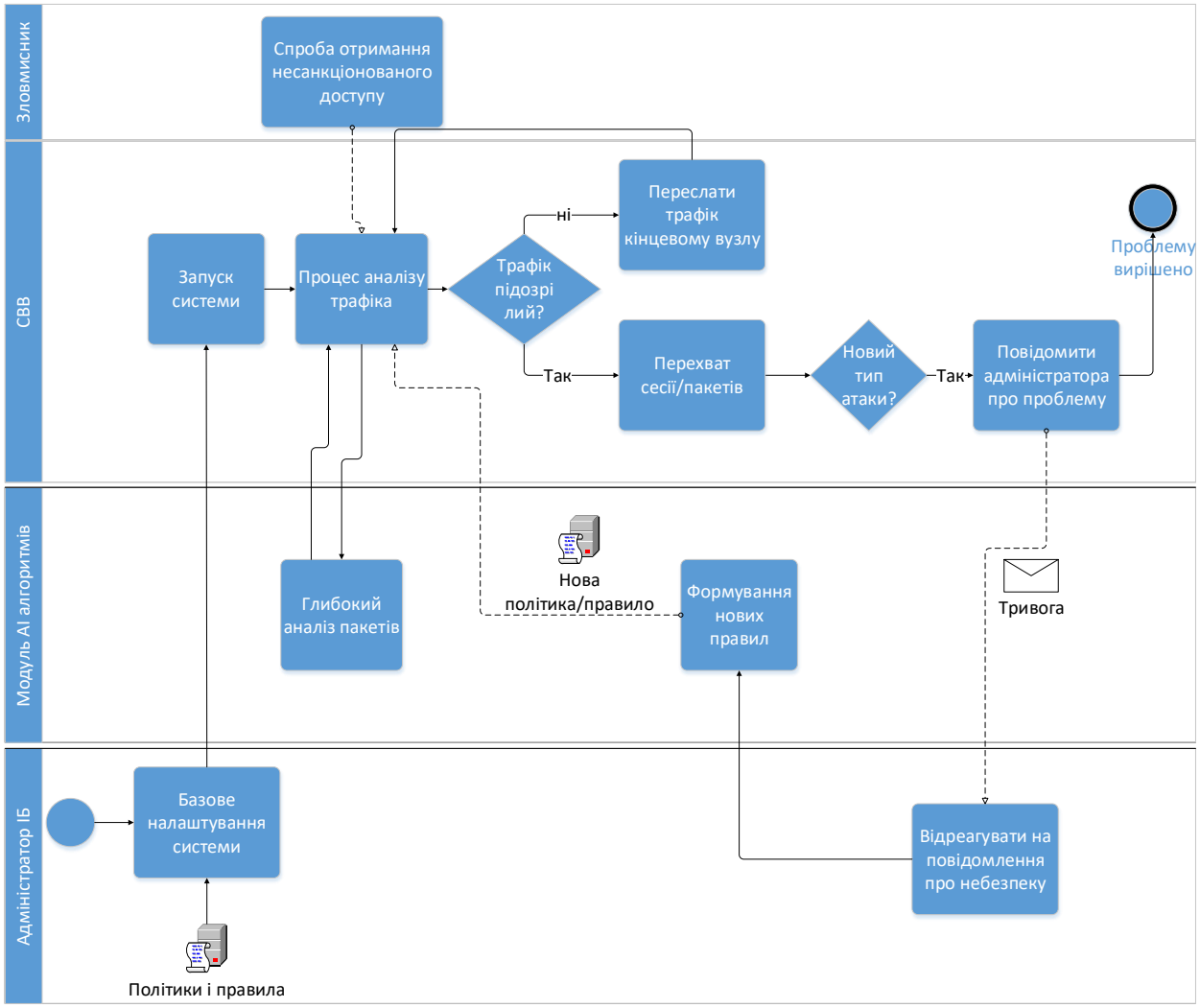

Рис. 2.5. Спрощена модель роботи системи виявлення вторгнень

Таким чином, для однотипних інцидентів з різними джерелами небезпеки (IP-адреси, URL, MAC-адреси пристроїв тощо) система автоматично створюватиме правила на основі вже відомих, а при виявленні нового підозрілого інциденту – так само сповіщати адміністратора ІБ. Такий підхід дозволить точніше виявляти справді критичні інциденти та знизити трудові витрати на підтримку працездатності системи.

2.3. Логічне взаємодія з компонентами системи

Щоб описати, як користувач системи взаємодіє з її компонентами щодо забезпечення працездатності та налаштування, звернімося до нотації UML.

UML (Unified Modeling Language) представляє собою стандартну мову моделювання, яка використовується для опису проектування програмного забезпечення. Складаючись із графічних символів та правил, UML дозволяє створювати різні види діаграм, таких як діаграми класів, діаграми послідовностей, діаграми станів тощо. Головна мета UML полягає в допомозі розробникам програмного забезпечення у розумінні вимог замовника, визначенні архітектури програми та перевірці її відповідності специфікації.

Діаграми UML використовуються для візуального представлення архітектури, структури, поведінки та інших характеристик програмних систем. Вони є ефективним інструментом для розробників, дозволяючи краще розуміти вимоги до системи та ефективно її проектувати.

Наприклад, діаграма класів UML служить для опису структури об'єктно-орієнтованої програми, включаючи класи, властивості та методи. Діаграма послідовності UML застосовується для уявлення взаємодії об'єктів під час виконання завдання.

Діаграма варіантів використання (Use Case Diagram) у UML використовується для моделювання функціональних вимог до системи, представляючи різні сценарії використання. Елементи діаграми включають акторів (користувачі чи інші системи), варіанти використання (конкретні сценарії) та відносини між ними. Цей вид

діаграми сприяє уточненню вимог до системи, визначаючи її основні функції та взаємодію з користувачами, що полегшує розробку більш ефективних та зручних для використання систем.

Побудуємо діаграму варіантів використання, виходячи з наявності трьох акторів: адміністратора системи, який відповідає за її конфігурацію, оператора системи, який займається моніторингом трафіку для своєчасного реагування на інциденти, а також AI-алгоритмів, які відповідають за самонавчання системи (рис. 2.6).

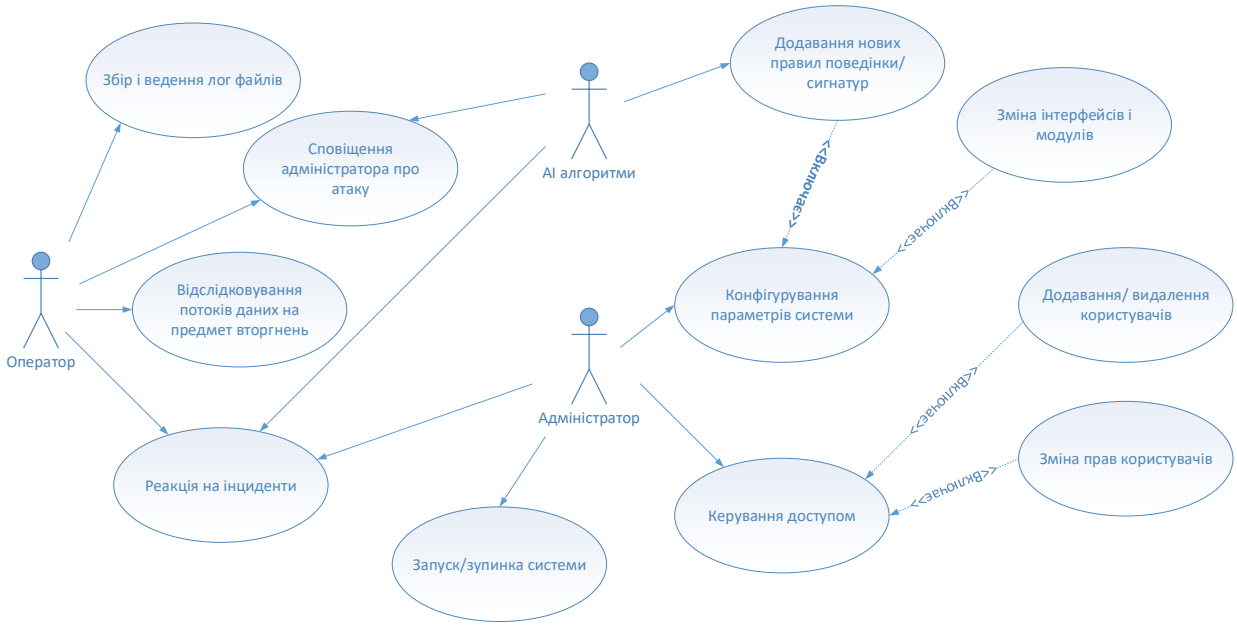

Рис. 2.6. Діаграма варіантів використання системи виявлення вторгнень

Таким чином, в проектованій системі обмежуються функції оператора. Конфігурування системи виявлення вторгнень, її загальної працездатності та зміни правил поведінки дозволено лиш адміністратору системи. Оператор займається безпосередньо моніторингом оброблених даних та за необхідності сповіщає адміністратора про проблеми. Алгоритми інтелектуального аналізу полегшують роботу як оператора, і адміністратора, рахунок автоматизації процесів реагування на інциденти, оповіщення і додавання нових сигнатур і правил.

Логічна модель системи та принцип обробки даних визначені, тепер необхідно розробити фізичну модель системи та взаємодії її компонентів.

2.4. Фізична модель системи виявлення вторгнень

Фізична модель інформаційної системи – це опис апаратного та програмного забезпечення, що використовується в системі, вона допомагає розробникам та адміністраторам системи зрозуміти, які компоненти необхідні для створення та підтримки системи, а також які зміни можуть бути внесені до системи у майбутньому. Вона може включати:

–системні компоненти: опис серверів, мереж, сховищ даних та ін;

–програмне забезпечення: опис використовуваних програмних компонентів, бібліотек, операційних систем та баз даних;

–структуру даних: опис даних, що використовуються в системі, та їх зберігання;

–опис вузлів та з'єднань: вказівка з'єднань між компонентами вузлами системи;

–Опис структури інтерфейсів: Опис інтерфейсів між різними компонентами інформаційної системи.

Фізична модель інформаційної системи є необхідним кроком у процесі її створення, оскільки вона є конкретним планом фізичної реалізації даної системи.

В рамках цього підходу розробляються детальні специфікації апаратного та програмного забезпечення, включаючи операційні системи, бази даних, мережну інфраструктуру та інші компоненти, які необхідні забезпечення повноцінного функціонування системи.

Фізична модель інформаційної системи має низку переваг, таких як:

- створення більш повної та точної візуалізації системи, яка легко зрозуміла як технічним, так і не технічним фахівцям;
- можливість уникнути помилок під час встановлення системи;
- створення складніших систем з урахуванням вже розробленої, що дозволяє підвищити ефективність процесу розробки;
- забезпечення оптимальної роботи обчислювального середовища;
- захист від можливих загроз безпеці.

Цей підхід є важливим елементом розробки інформаційних систем і використовується для більш ефективну і точну роботу системи в майбутньому.

Система виявлення вторгнень може пропускати трафік безпосередньо через свій вузол, так і сканувати дзеркальний трафік з інтерфейсів інших мережевих пристроїв. Це визначає можливість реагування на інциденти та заборону подальшої передачі трафіку – у разі наскрізного підключення СВР може автоматично скидати з'єднання, але такий підхід збільшить загальну затримку трафіку.

На етапі тестування системи ми розглянемо паралельне підключення системи виявлення вторгнень з подальшою перспективою наскрізного підключення. У схемі мережі це буде виглядати так (рис. 2.7).

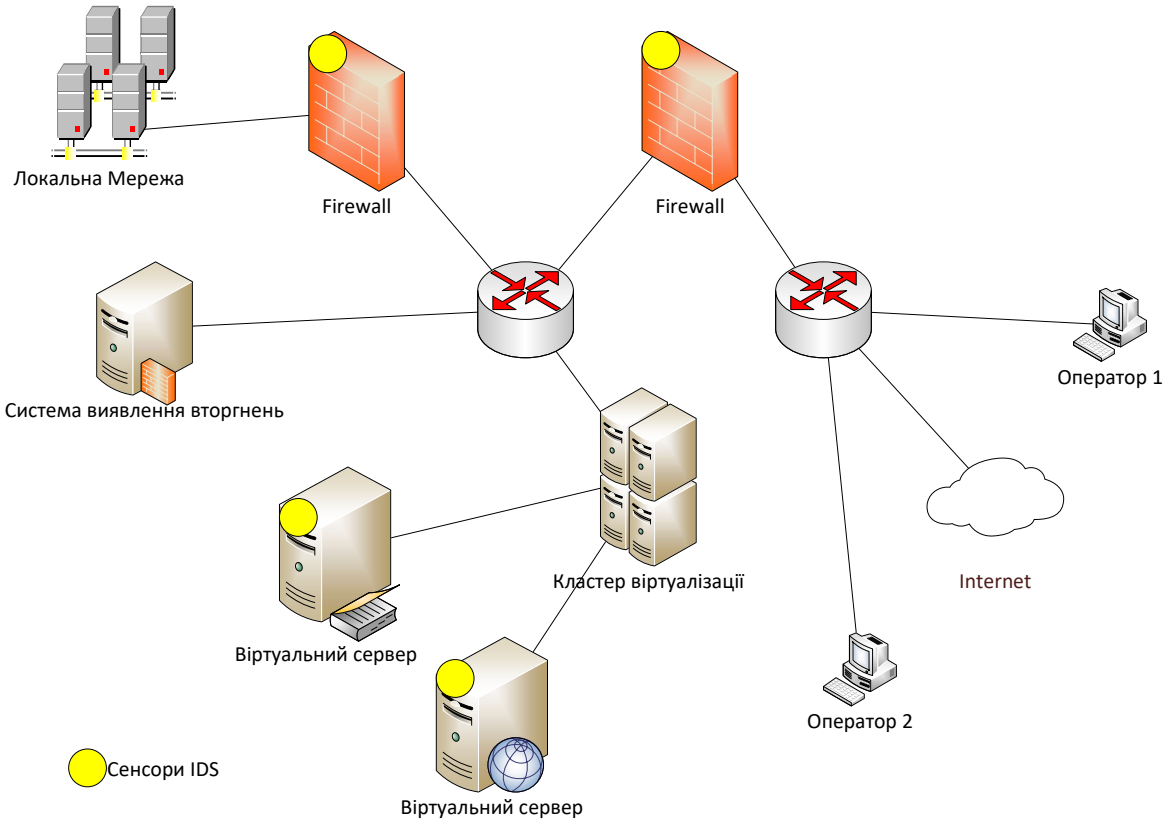

Рис. 2.7. Фізичне розміщення системи виявлення вторгнень у типовій мережі

Основний функціонал системи виявлення вторгнень – аналіз трафіку – досягається за рахунок дзеркалювання всього внутрішнього та зовнішнього трафіку зі стеку комутаторів мережі. Також можливе розміщення додаткових сенсорів на мережевих вузлах та передача окремих потоків трафіку з кожного сенсора. Тоді

можна налаштувати керування системою виявлення вторгнень окремо для кожної групи вузлів та задавати відповідні правила реагування. Такий функціонал підходить для подальшого розвитку системи при впровадженні її в наявну мережеву інфраструктуру, тому на етапі тестування ми використовуємо лише сканування трафіку.

Фізично система виявлення вторгнень представляє собою сервер (контролер) із встановленим програмним забезпеченням. Ядром нашої системи є Suricata, а плагінами, які відповідають за самонавчання системи – алгоритми ALAD + LERAD.

Висновок до другого розділу.

На основі Suricata запропоновано алгоритм оптимізованої IDS, який об'єднує сигнатурний аналіз, попередній перегляд заголовків пакетів та глибокий аналіз трафіку за допомогою модулів ALAD і LERAD. Рекомендується розробити та протестувати нову модель системи виявлення вторгнень в умовах, що наближаються до реальних.

Була розроблена логічна модель запропонованої системи виявлення вторгнень, з якої стало зрозуміло, які саме процеси зачіпаються в результаті її роботи, а також які аспекти покращують впровадження алгоритмів штучного інтелекту.

У новій моделі процес додавання політик автоматизується рахунок самонавчання системи з урахуванням алгоритмів інтелектуального аналізу пакетів.

У діаграмі варіантів використання було показано, за які аспекти інформаційної системи, що розробляється, відповідають люди (адміністратор і оператор системи), а за які – штучний інтелект (AI-алгоритми). UML діаграма варіантів використання допоможе розробникам визначити, як система має взаємодіяти з користувачем та як користувачі використовуватимуть систему.

В результаті можна зробити висновок, що алгоритми глибокого аналізу дозволяють заощадити час реагування на інциденти, що витрачається оператором та адміністратором у процесі роботи системи.

Фізична схема системи визначає розташування системи виявлення вторгнень у периметрі мережі, а також як саме система взаємодіє з трафіком та вразливими вузлами.

Такий варіант розташування системи забезпечує більш гнучкий та масштабований підхід до захисту мереж та ресурсів, зручність управління, більш високу ефективність використання ресурсів, збільшення безпеки та покращення продуктивності.

Таким чином, розробивши модель проектованої системи виявлення вторгнень можна переходити до етапу практичного тестування.

РОЗДІЛ 3
ТЕСТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

3.1. Тестування алгоитмів системах виявлення вторгнень

Для підтвердження гіпотези щодо ефективності обраних алгоритмів, ми провели попередній експеримент. В якості вихідних даних ми використовували добовий дамп трафіку вузла з запущеним інструментарієм Blue Team Training Toolkit (BT3), який імітує роботу зловмисника. Дамп включає кілька ітерацій сканування портів, атак типу Kerberoasting, man-in-the-middle атак, атак на вразливості операційної системи та багато інших. Загалом дамп містить 1,93 ГБ даних про 274 атаки.

Для тестування як цільового хоста використовується віртуальна машина на базі CentOS 8.2.2004 з характеристиками: процесор AMD Ryzen 5 3350G 3.6 GHz (4 ядра, 8 потоків), оперативна пам'ять DDR4 2993 MHz (8 ГБ) та обсяг виділеного місця на SSD – 120 ГБ.

На сервері були запущені по черзі Snort та різні комбінації модулів-надбудов. За допомогою Wireshark була проведена імітація обміну трафіку з сервером, під час якої визначалися час роботи алгоритмів та точність виявлення атак. Результати експерименту представлені на рис. 3.1.

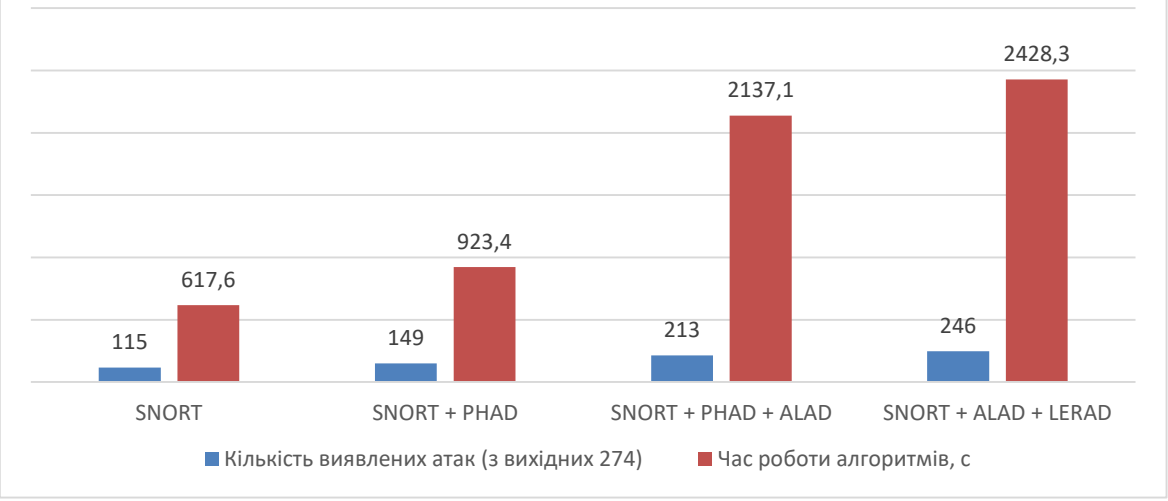

Рис 3.1. Ефективність алгоритмів в експерименті (час роботи)

На основі отриманих значень можна зробити висновок, що найбільшу точність визначення атак продемонструвало поєднання модулів ALAD + LERAD, яке було застосовано поверх роботи Snort.

Для порівняння ефективності методів також був проведений експеримент з використанням Snort з кожним модулем на фіксованих дампах трафіку, в яких було виявлено 180 характерних ознак атак. Результати експерименту щодо області точності визначення атак представлені на рис. 3.2.

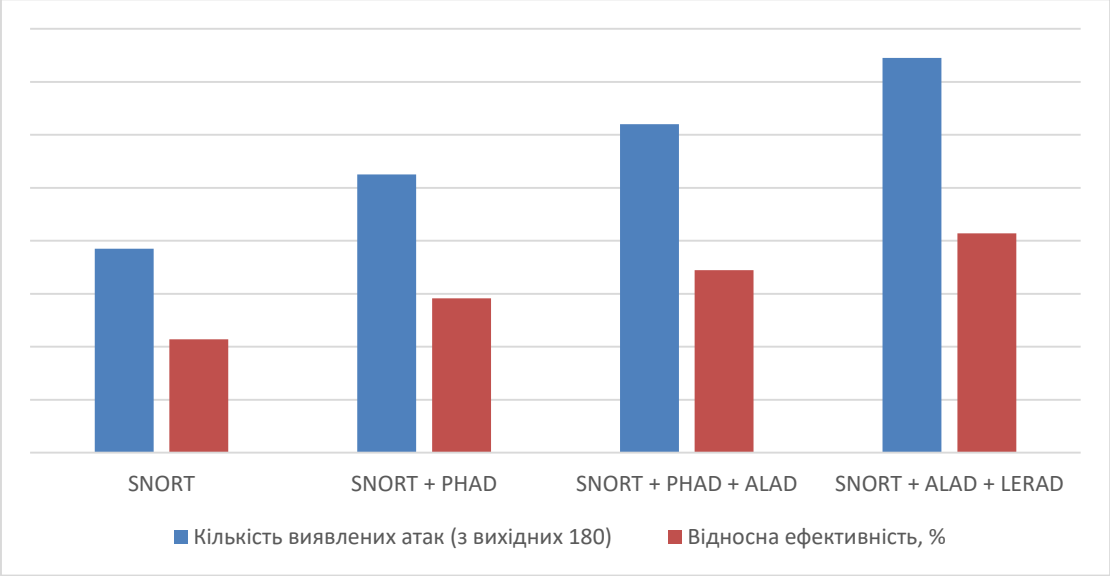

Рис 3.2. Відносна ефективність алгоритмів згідно з дослідженням

При підключенні модуля докладного аналізу пакетів помітно суттєве збільшення часу роботи IDS, але також значно підвищується точність визначення атак.

Для оцінки загальної ефективності роботи алгоритмів візьмемо швидкість роботи Snort без модулів 100%. Порівнявши швидкість роботи алгоритмів та точність визначення атак, сформуємо наступний графік ефективності (рис. 3.3).

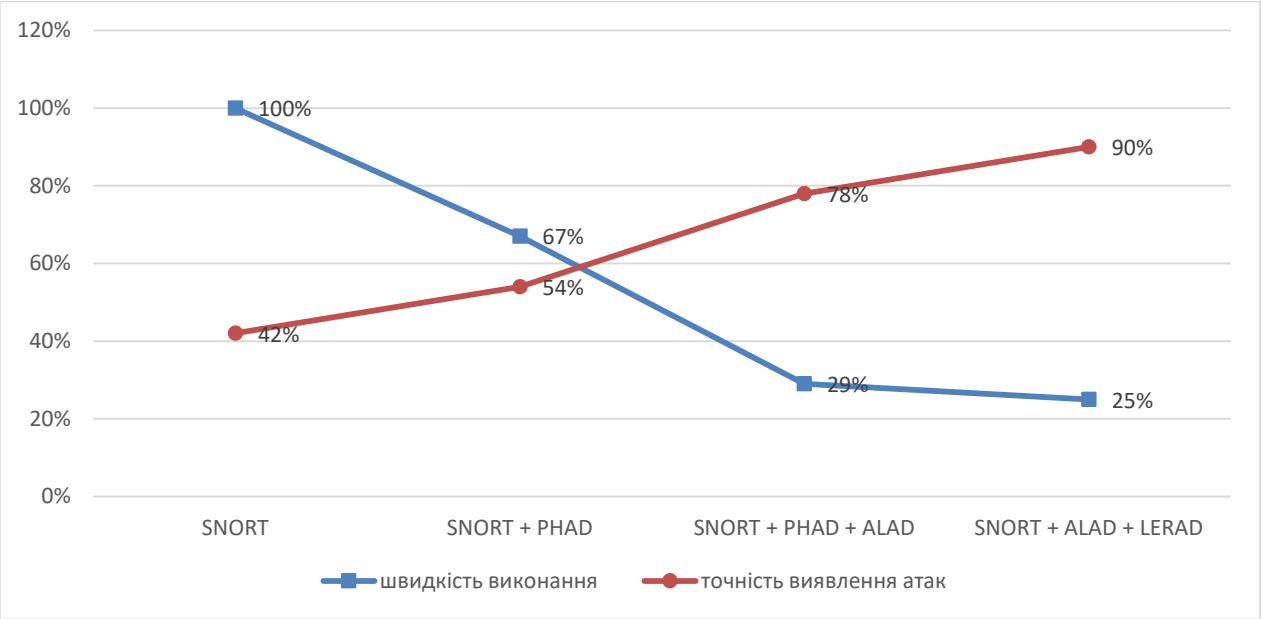

Рис. 3.3. Ефективність роботи алгоритмів

Отже, щодо точності визначення атак в порівнянні з часом роботи алгоритмів, найвищу ефективність представляють сигнатурний аналіз Snort спільно з аналізом заголовків PHAD. Такий підхід, однак, пропускає майже половину можливих атак і є придатним лише для первинного етапу виявлення атак. У важливих аспектах безпеки інформаційних ресурсів можливе знехтування чотириразовим збільшенням часу обробки, якщо це призводить до подвоєння точності визначення атак.

Таким чином, у подальших дослідженнях також буде акцентовано на комбінації ALAD + LERAD, оскільки цей підхід надає найбільш повне визначення атак. Однак, використання Snort як основного IDS може бути піддане сумнівам через виявлене високе навантаження на систему в експериментах.

Як було зазначено в першому розділі, головною системою для подальших досліджень буде Suricata.

3.2. Налаштування IDS Suricata для роботи зі сторонніми алгоритмами

Suricata – вільно розповсюджуване ПЗ, тому установка його можлива двома шляхами – з вихідних джерел або з репозиторіїв. Репозиторії містять налаштовані

стандартні складання програмного комплексу, тому для використання додаткових функцій необхідне використання програм з відкритих джерел.

Після завантаження вихідного коду необхідно встановити пакети залежностей: libcap, libnet, pkg-config та інші, повний перелік наведено в документації проекту. Також важливим моментом при встановленні Suricata є встановлення правильного часу системи і часового поясу. Для синхронізації часу ми будемо використовувати утиліту chrony. Ця утиліта забезпечує своєчасне оновлення системного часу через протокол NTP (Network Time Protocol) і запобігає помилкам Suricata, пов'язаним з некоректними відмітками часу пакетів трафіку.

Для конфігурації Suricata у режимі IDS необхідно встановити такі параметри збірки:

--prefix=/usr/ – визначає місце встановлення бінарних файлів у /usr/bin;

--sysconfdir=/etc/ – визначає розташування конфігураційних файлів у /etc/suricata/ замість /usr/local/etc/ за умовчанням;

--localstatedir=/var/ – визначає зберігання журналів подій Suricata в /var/log/suricata/ замість /usr/local/var/log/suricata/ за умовчанням;

--enable-lua – включає підтримку lua-скриптів для виявлення атак та виведення даних.

Зазначені установки необхідні зниження можливих конфліктів з наборами правил, до яких входять правила, генеровані алгоритмами ALAD і LERAD.

Потім командою make необхідно зібрати налаштований пакет Suricata і встановити його за допомогою make install.

Для автоматичного запуску Suricata використовується bash-скрипт (Додаток Б). Цей скрипт забезпечує запуск IDS під час старту системи, а також автоматичне перезавантаження при збоях. Використання даного скрипту дозволяє змінювати особливості роботи Suricata шляхом редагування конфігураційного файлу без повної переустановки системи виявлення вторгнень.

Далі необхідно визначити мережний інтерфейс, пакети з якого піддаватимуться моніторингу. За замовчуванням Suricata відстежує мережний інтерфейс eth0, але у разі використання віртуальних машин чи нестандартних

дистрибутивів Linux робочий інтерфейс може відрізнятися. Знайти необхідний мережний інтерфейс можна за допомогою команди ifconfig з прапором -a (рис. 3.4) або за допомогою команди ip link show.

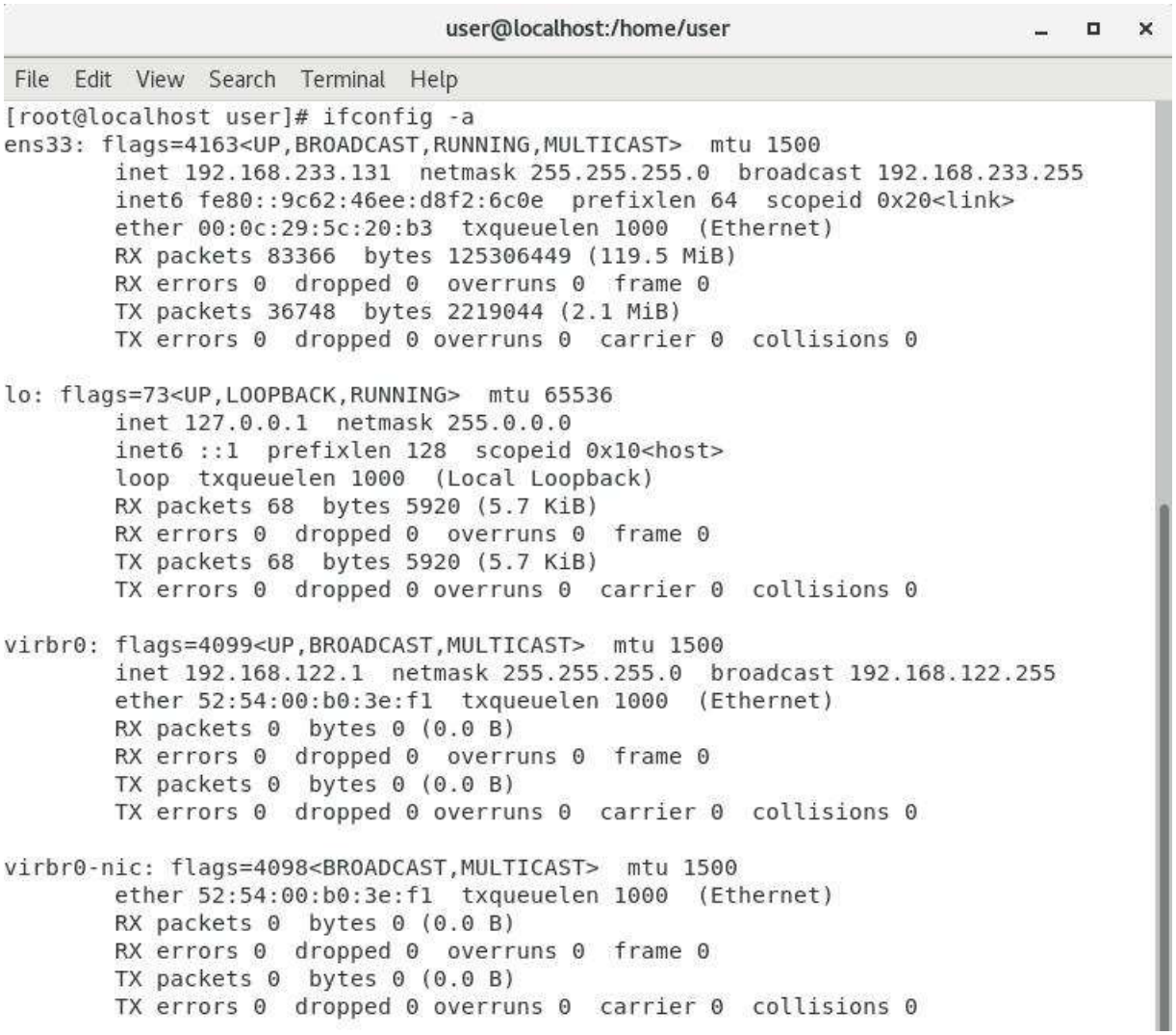

Рис. 3.4. Відображення мережевих інтерфейсів системи

Як видно зі скріншота, основним мережевим інтерфейсом нашої віртуальної машини є ens33, тому саме його необхідно записати d конфігураційний файл Suricata. Вибраний інтерфейс необхідно вказати в двох місцях: у налаштуваннях Suricata за замовчуванням (/etc/default/suricata) прописується рядок IFACE=ens33, далі в установках (/etc/suricata/suricata.yaml) прописуються інтерфейси для служб af-packet, pcap, pfring.

Після визначення інтерфейсу для роботи Suricata можна приступити до додавання правил обробки пакетів. Правила додаються за допомогою suricata-update інструменту. Для початку з'ясуємо, які правила використовує Suricata за замовчуванням за допомогою команди suricata-update list-sources (рис. 3.5.).

```
Name: sslbl/ja3-fingerprints
  Vendor: Abuse.ch
  Summary: Abuse.ch Suricata JA3 Fingerprint Ruleset
  License: Non-Commercial
Name: tgreen/hunting
  Vendor: tgreen
  Summary: Threat hunting rules
  License: GPLv3
Name: sslbl/ssl-fp-blacklist
  Vendor: Abuse.ch
  Summary: Abuse.ch SSL Blacklist
  License: Non-Commercial
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: ptresearch/attackdetection
  Vendor: Positive Technologies
  Summary: Positive Technologies Attack Detection Team ruleset
  License: Custom
Name: scwx/security
  Vendor: Secureworks
  Summary: Secureworks suricata-security ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: scwx/malware
  Vendor: Secureworks
  Summary: Secureworks suricata-malware ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: etnetera/aggressive
  Vendor: Etnetera a.s.
  Summary: Etnetera aggressive IP blacklist
  License: MIT
[root@localhost user]#
```

Рис. 3.5. Списки правил Suricata за замовчуванням

Для успішного додавання правил вони повинні відповідати наступному формату:

- дія, яка описує, що має статися при виявленні загрози;
- заголовок, що описує протокол, IP-адресу або порт правила, а також куди слід перенаправити пакет;

- опції правила, що деталізують його роботу.

До доступних дій входять такі:

- alert – виводить попередження;
- pass – зупиняє подальше вивчення пакета;
- drop – відкидає пакет та виводить попередження;
- reject – повертає відправнику пакета помилку destination_unreachable за протоколом RST/ICMP;
- rejectdst – надсилає вищезгадану помилку одержувачу пакета;
- rejectboth – відправляє помилку обом сторонам обміну даними.

Заголовки протоколів у правилах Suricata доступні у загальному вигляді: tcp для tcp-трафіку, udp для udp-трафіку, icmp для технічної інформації та ip для всіх протоколів. Крім цього, можлива ідентифікація пакетів, що використовують протоколи рівня додатків: http, ftp, tls (включаючи ssl), smb, dns, dhcp, ssh, smtp, sip та інші.

Для вказівки IP-адрес та портів можна використовувати оператори ../.. – діапазон адрес (в нотації CIDR), ! – виняток, а також [.., ..] – групування.

Наприклад, якщо необхідно визначити правило, що реагує на всі пакети з діапазону адрес 192.168.0.0/24, крім 192.168.0.10, запис буде виглядати так: [192.168.0.0/24, !192.168.0.10]. Аналогічні оператори діють задля вказання портів адрес.

Опції – це найчастіше найоб'ємніший елемент правила. Вони вказуються в дужках і поділяються крапкою з комою. Опціями визначається, які саме дані пакеті необхідно враховувати для спрацьовування правила.

Для адаптації правил Snort під використання у системі Suricata необхідно визначити основні відмінності.

Перша відмінність - дії Snort відрізняються від можливих дій Suricata за рахунок динамічних правил Snort. Тому всі правила Snort, що містять ключові слова dynamic і activate, необхідно розбити на окремі правила.

Друга відмінність – Snort вимагає явної вказівки протоколу трафіку та порту передачі для роботи передпроцесора, а Suricata вміє автоматично визначати

більшість прикладних протоколів та порти. Відповідно, правила Snort, спрямовані на виявлення однотипних атак з різних портів можна згрупувати, прибравши прив'язку до досліджуваних мережних портів ключовим словом any. Третя важлива відмінність у роботі правил – правила Suricata поширюються на потік трафіку, тоді як Snort досліджує кожен пакет окремо. Корекція правил на дослідження потоків вимагатиме практично повної їх переробки, тому у зазначеному контексті правила Snort не змінюватимуться. Однак варто враховувати, що Suricata може генерувати два оповіщення на один пакет трафіку у випадках, коли пакет перевіряється сам по собі та у складі потоку. Інші відмінності правил Snort і Suricata відносяться до використання конкретних методів та ключових слів, тому докладно розглядати їх у цій роботі немає сенсу.

Підготувавши правила роботи з трафіком, необхідно забезпечити IDS наскрізну передачу пакетів з інших вузлів, щоб розпочати практичну частину експерименту.

3.3. Дзеркало трафіку на IDS

Передача трафіку на IDS може здійснюватись як на рівні комутатора, так і безпосередньо з одного вузла на інший. На комутатор для дублювання трафіку з одного порту на інший використовується механізм SPAN (Switch Port Analyzer). Для його використання необхідно вказати джерело трафіку та одержувача трафіку. Як джерело можуть виступати окремі порти комутатора, чи групи портів (VLAN). Як одержувача вказується один із портів комутатора. Принцип дії SPAN вказаний рис. 3.6.

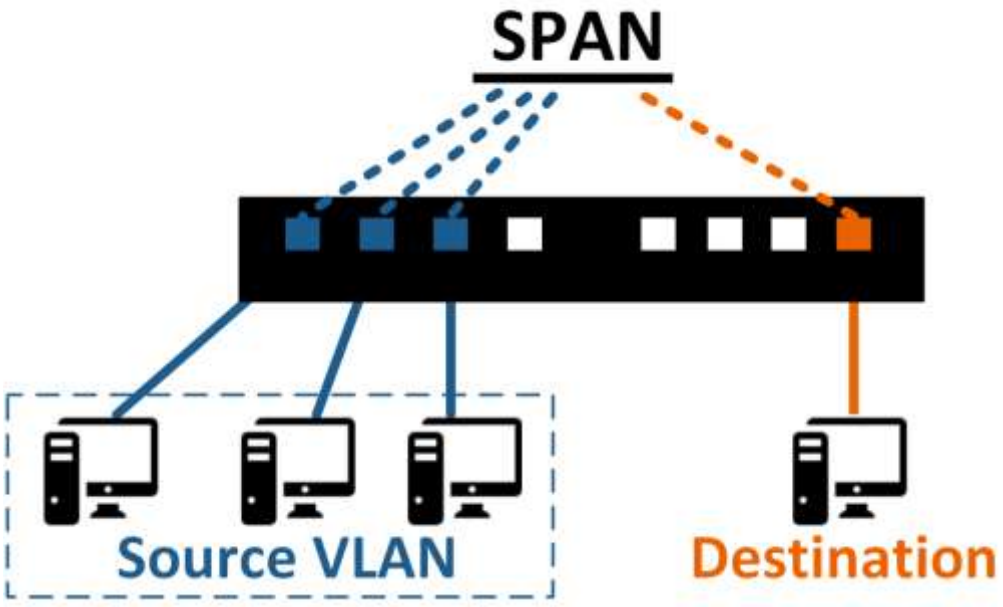

Рис. 3.6. Принцип дзеркалювання SPAN

Очевидно, такий спосіб передачі трафіку спрацює тільки в тому випадку, якщо IDS буде знаходитися на тому ж комутаторі, що й досліджувані вузли. У масштабних мережах таке можливо далеко не завжди, тому є альтернативні способи передачі трафіку.

Для мереж комутаторів найчастіше застосовується метод RSPAN (Remote SPAN). У разі використання створюється спеціальна RSPAN-сесія, куди входять порти-джерела, trunk-порти, що з'єднують комутатори, і навіть порт призначення (рис. 16).

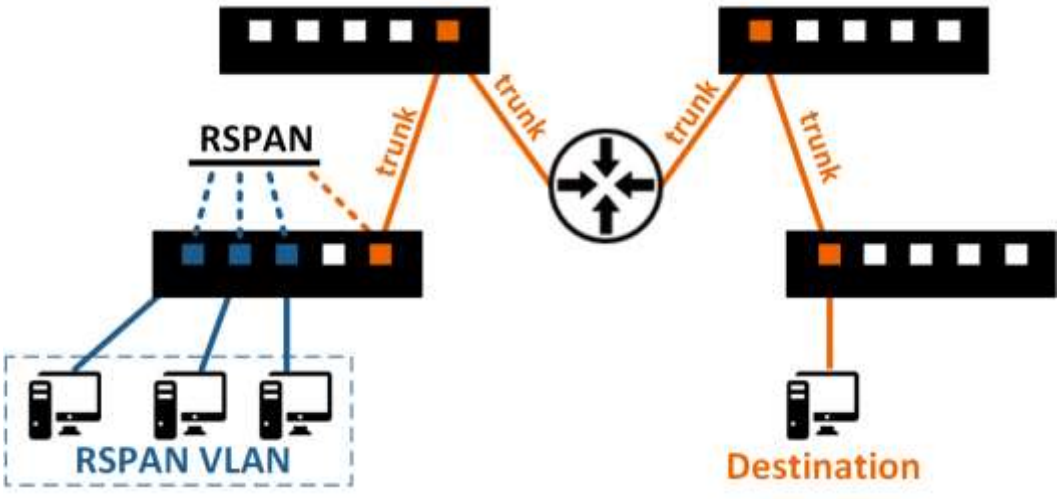

Рис. 3.7. Принцип дзеркалювання RSPAN

Необхідно врахувати, що з оголошенні порту одержувачем, порт зможе лише приймати дубльований трафік, інші можливості порту блокуються.

Пряма передача трафіку між двома хостами здійснюється за допомогою сторонніх програмних засобів і доцільна за неможливості використання комутаторів для дзеркалювання, наприклад, у випадках значної фізичної віддаленості вузлів та відсутності загальної мережі. У нашому випадку для дублювання трафіку буде достатньо RSPAN.

Для перевірки коректності роботи Suricata та сесії RSPAN створимо мережну активність на вихідному вузлі. Логи та попередження Suricata записуються у файл /var/log/suricata/eve.json. Відкриваємо його за допомогою команди tail з прапором –f та спостерігаємо постійне оновлення файлу при активній передачі пакетів вихідного вузла (рис. 3.8).

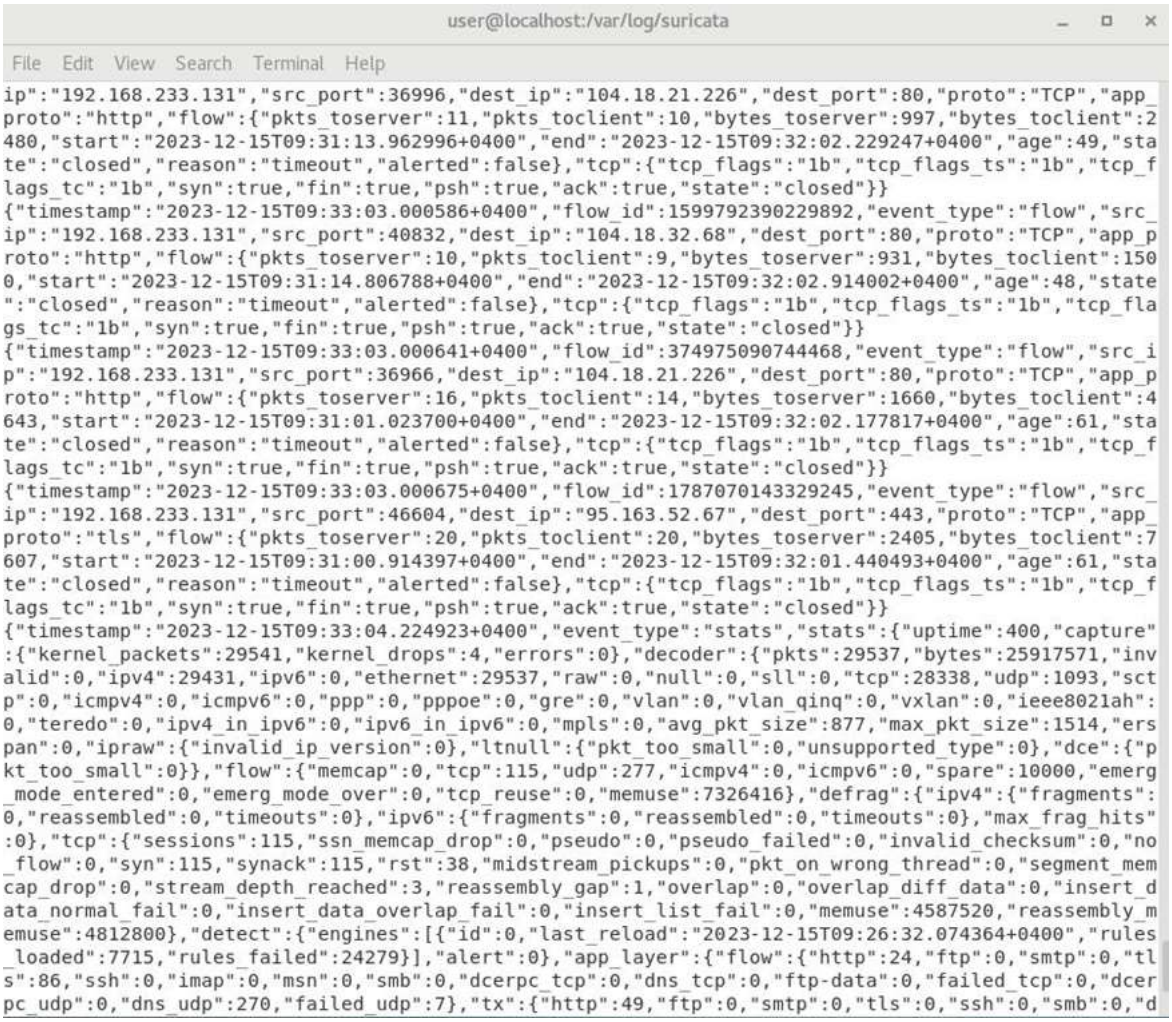

Рис. 3.8. Перелік попереджень та подій Suricata

Виділення потрібних подій здійснюється за допомогою утиліт grep, як і в першому обчислювальному експерименті. Для перевірки системи та динамічних алгоритмів необхідне проведення експерименту, аналогічного попереднім.

3.4. Динамічна генерація правил та тестування отриманої системи

Для пересилання пакетів, оброблених правилами Suricata, для подальшої обробки алгоритмами ALAD та LERAD необхідно змінити конфігураційні файли, вказавши сервіс отримання пакетів відповідно до способу автозапуску (etc/default/suricata).

У разі Snort доповнення правил зазначеними алгоритмами розширює стандартний список правил, а у випадку Suricata рекомендується створити окремий список правил для виключення конфліктів у роботі IDS через можливу несумісність ключових слів та методів.

Початкове тестування отриманої системи проведемо аналогічно до попереднього експерименту. Для цього використовується той же дамп пакетів об'ємом 1,93 ГБ, що містить 274 атаки. Передача пакетів здійснюється за допомогою Wireshark на мережевий інтерфейс lo (локальна петля). Для тестування використовуються різні конфігурації віртуальної машини з метою оцінки впливу багатопоточного режиму обробки Suricata і алгоритмів ALAD і LERAD на швидкість аналізу трафіку. Процесор для всіх ітерацій використовується той самий (AMD Ryzen 5 3350G 4.05 GHz), оперативна пам'ять DDR4 частотою 2400 MHz, обсяг дискового простору не змінюється. Фіксація часу виконання здійснюється порівнянням штампів часу першого та останнього пакетів у логах Suricata, а також вбудованим профайлером Linux time для алгоритмів ALAD та LERAD. Результати експерименту наведено на рис. 3.9.

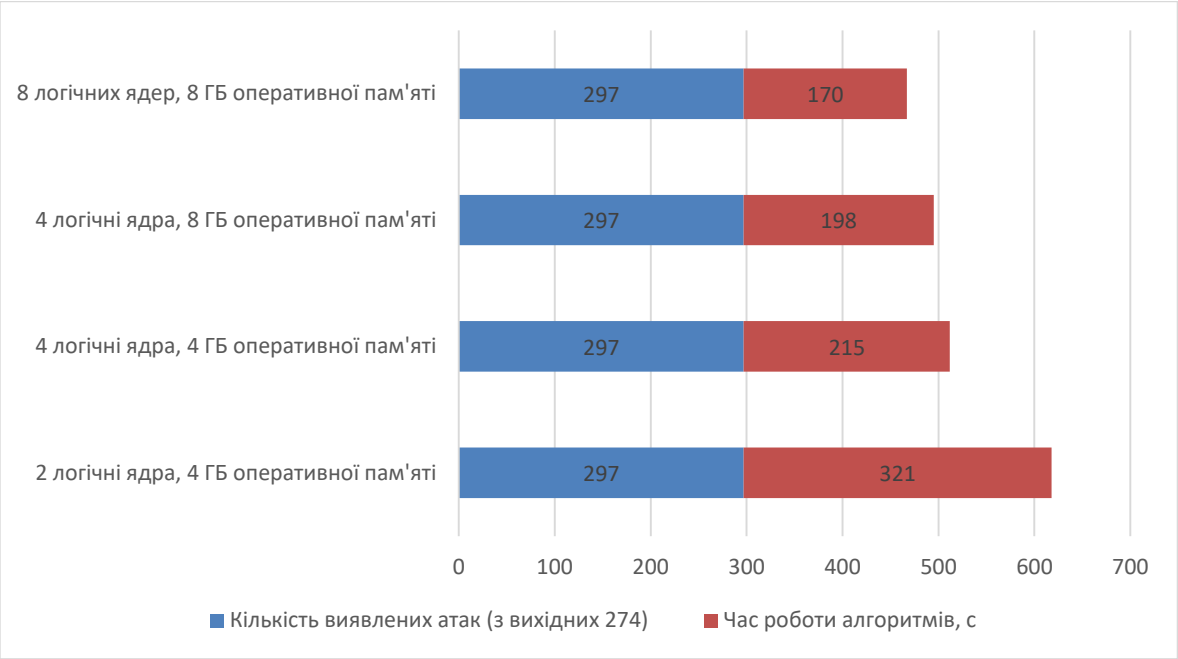

Рис.3.9. Ефективність роботи IDS Suricata з алгоритмами ALAD+LERAD

За наявності в дампі 274 атак Suricata у всіх випадках сигналізувала про 297 загроз. Аналіз логів попереджень показав, що одні й самі пакети у деяких випадках оброблялися двічі – у складі tcp-сесії і самі собою. Таким чином, деякі застереження дублюються. Suricata пропустила 8 атак, які надалі були розпізнані алгоритмами динамічного аналізу.

Також за результатами експерименту простежується залежність швидкості аналізу, залежно від характеристик системи. Найбільше впливає додавання обчислювальних ядер – Suricata набагато ефективніше працює у багатопотоковому режимі, ніж Snort. Стрибок продуктивності при додаванні двох ядер до двох вже наявних становив 33%. Подальші зміни конфігурації показують менше підвищення продуктивності, оскільки сторонні алгоритми гірше оптимізовані для систем з понад 4-х логічних ядер.

В результаті роботи алгоритмів динамічно згенерували нові правила для Suricata. Додаємо правила за допомогою suricata-update та перезапускаємо сервіс. Результат представлений рис. 3.10.

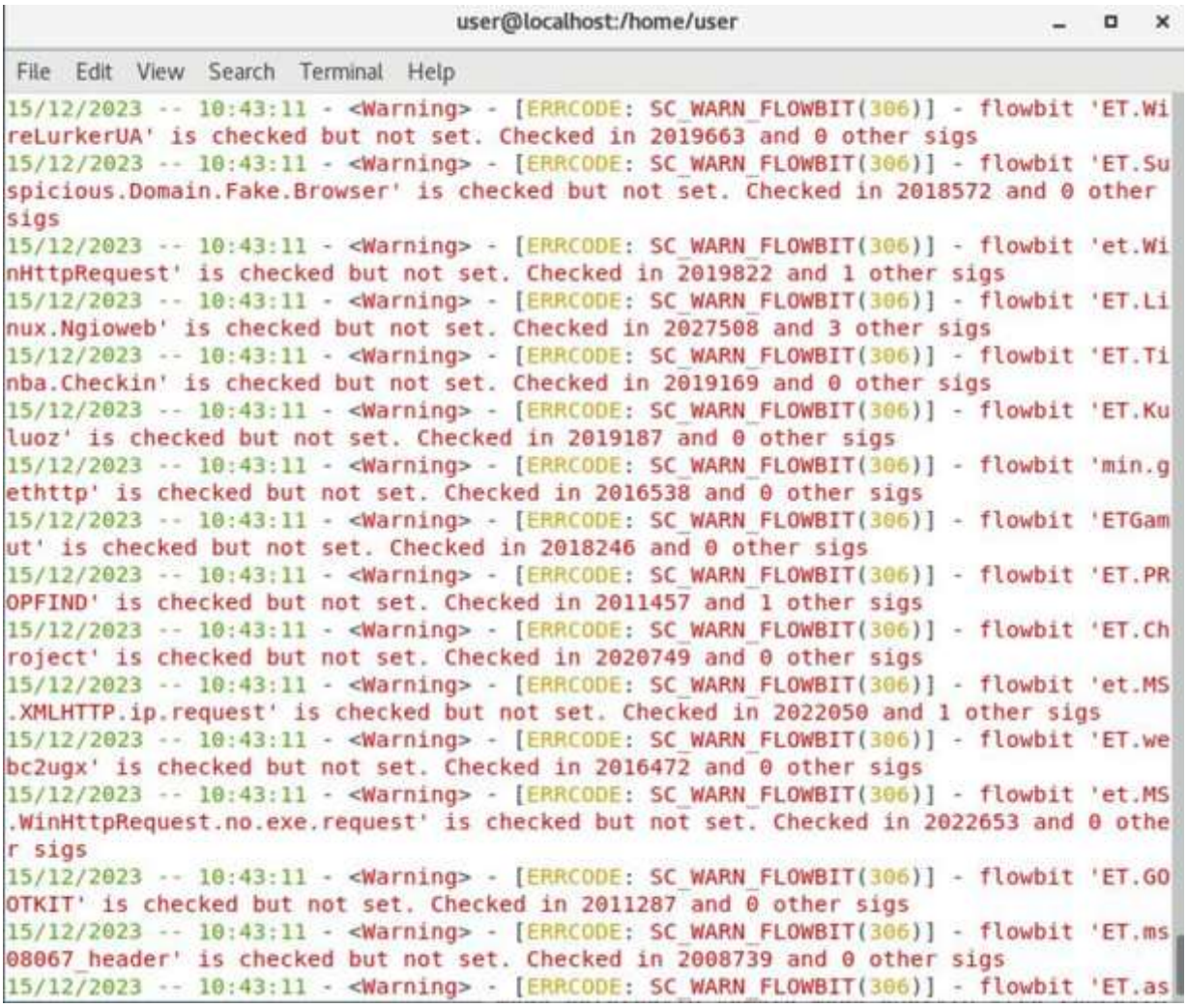

Рис. 3.10. Результат додавання нових правил

Крім помилок SC_WARN_FLOWBIT, також є помилки виду SC_ERR_RULE_KEYWORD_UNKNOWN, що говорить про те, що правила, додані за допомогою автоматичних алгоритмів, також необхідно додатково адаптувати.

Висновок до розділу 3

Для підтвердження гіпотези було проведено проміжний експеримент, який показав, що використання комбінації алгоритмів ALAD та LERAD дійсно дає найбільшу ефективність у виявленні атак.

У ході роботи було проведено конфігурацію програмного комплексу Suricata як IDS, проведено налаштування системи виявлення вторгнень для роботи у віртуальному середовищі та автоматизацію запуску IDS при збоях, а також перезавантаження.

Також у рамках роботи було описано механізми дзеркалювання трафіку та реалізація такого механізму в рамках дослідження. Далі було проведено обчислювальний експеримент із виявлення ефективності роботи системи за умов різних апаратних змін. В експерименті використовувалася система Suricata з використанням сторонніх алгоритмів ALAD та LERAD для глибокого аналізу пакетів трафіку. За результатами експерименту було зроблено такі висновки:

- Suricata ефективніше працює з багатопроцесорними системами, ніж Snort;
- деякі пакети обробляються двічі - у складі потоку та окремо від нього, що призводить до дубляжу попереджень;
- сторонні алгоритми менш ефективні в режимі багатопоточності, ніж сама Suricata і можуть гальмувати систему за високої завантаженості трафіком.

Крім цього, за результатами роботи алгоритмів були створені правила для IDS, проте генерація правил використовує принципи синтаксису Snort і вимагає подальшої модифікації відповідно до синтаксису Suricata.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Усі дослідження методів виявлення вторгнень та інформаційних атак на комп'ютерну систему проводились з дотриманням правил та норм охорони праці і вимог техніки безпеки.

При роботі за ЕОМ необхідно особливу увагу звертати на правильне освітлення. Неправильне освітлення (пряма та відбита від екранів близькість, вуалюючі відбиття, несприятливий розподіл яскравості в полі зору, невірна орієнтація робочого місця відносно світлових отворів) призводить до негативних фізіологічних впливів на користувачів ЕОМ. Погана якість символів, що представлені на екрані, також може викликати зоровий дискомфорт, бути стресовим фактором та ін.

Вимоги до освітлення для візуального сприймання користувачами інформації з двох різних носіїв (з екрана ЕОМ та паперового носія) різні. Надто низький рівень освітленості погіршує сприймання інформації при читанні документів, а надто високий призводить до зменшення контрасту зображення знаків на екрані. Відношення яскравості екрана ЕОМ до яскравості оточуючих його поверхонь не перевищує у робочій зоні 3:1.

Наближено можна вважати, що при 10%-ному зменшенні освітленості працездатність знижується на 1%. Коли за характером роботи вимагається комбінація цих двох носіїв інформації, освітленість можна варіювати від 300 до 700 лк, причому чим рідшою є зміна полів зору в процесі роботи (з екрана на документ та навпаки), тим вищим може бути рівень освітленості. 300-500 лк — оптимальна освітленість робочих приміщень для роботи з ЕОМ. Стрибки яскравості при зміні полів зору мають бути мінімальними, тобто інтенсивність освітлення поверхні, де знаходяться рукописи та документи, не повинна перевищувати яскравості екрана дисплея.

Рівень освітленості на робочому столі має бути в межах 300–500 лк ДБН В.2.5-28:2018 Природне і штучне освітлення.

Приміщення в якому виконувалась кваліфікаційна робота забезпечене природнім і штучним освітленням. При роботі за ЕОМ обрано місце, щоб в поле зору не потрапляли вікна або освітлювальні прилади. Регулювання світлових променів здійснюється за рахунок жалюзі на вікнах. Вікна приміщення орієнтовані на схід.

Штучне освітлення у приміщені реалізовано у вигляді комбінованої системи освітлення з використанням люмінесцентних джерел світла у світильниках загального освітлення, які слід розташовані над робочими поверхнями у рівномірно-прямокутному порядку. Для запобігання засвітленню екранів ЕОМ прямими світловими потоками лінії світильників розташовані з достатнім бічним зміщенням відносно робочих місць, а також паралельно до вікон.

На робочому місці забезпечена рівномірна освітленість за допомогою переважно відбитого або розсіяного світлорозподілу. Світлових відблисків з клавіатури, екрана та від інших частин ЕОМ у напрямку очей користувача немає. Дискомфорт від відбиття світла знижується при збільшенні яскравості екрана та зниженні рівня навколишнього освітлення.

Пульсація освітленості люмінесцентних ламп, що використовуються, відповідно до технічної документації 10%, що відповідає діючим вимогам.

Інформація, яку одержує користувач, генерується на екрані, а комфортність її сприймання залежить від чіткості символів. При обговоренні проблеми дискомфорту або негативних наслідків для здоров'я та ефективності роботи на ЕОМ слід враховувати ряд параметрів. Ці параметри поділені на три групи, пов'язані з

−мигтінням

−структурою

−яскравістю символів, що представляються на екрані.

Отже в даному підрозділі розглянуто вплив середовища на працездатність та здоров’я користувачів комп’ютерів. Як висновок можна сказати, що робоче місце

яке використовувалось для написання даного наукового дослідження відповідає вимогам з охорони праці.

Однак необхідно не забувати що надмірна робота з ПК може привезти до порушення роботи організму користувача. Тому необхідно дотримуватись вимог щодо планування робочого часу за ЕОМ.

4.2. Безпека в надзвичайних ситуаціях

4.2.1.Інженерний захист персоналу об’єкту та населення. Правила застосування.

Інженерний захист – це комплекс організаційних і інженерно-технічних заходів, що проводяться завчасно а також в оперативному порядку і спрямованих на запобігання або максимальне зниження втрат при виникненні надзвичайних ситуацій шляхом забезпечення укриття і життєдіяльності персоналу об'єкту та населення в захисних спорудах, запобігання, усунення або зниження до допустимого рівня негативного впливу вражаючих факторів, стихійних лих, аварій, природних і техногенних катастроф. Заходи інженерного захисту регламентуються низкою нормативних документів, основним з яких є Кодекс цивільного захисту України .[31]

Оцінка інженерного захисту працівників об’єкта полягає у визначенні показників, які характеризують здатність інженерних споруд забезпечити надійний захист людей, що можливо при виконанні наступних умов:

–загальна місткість захисних споруд дозволяє вкрити найбільшу працюючу зміну;

–захисні властивості захисних споруд відповідають потрібним;

–системи життєзабезпечення захисних споруд забезпечують життєдіяльність персоналу протягом встановленого терміну безперервного перебування їх в захисних спорудах;

–розміщення захисних споруд відносно місць роботи дозволяє людям укритися за сигналом ЦО у встановлені строки. На основі оцінки інженерного

захисту визначаються заходи, спрямовані на підвищення надійності заходу персоналу об’єкта від вражаючих факторів, а відповідно, і на підвищення стійкості функціонування об’єкта в умовах виникнення НС.[32]

До захисних споруд цивільного захисту належать:

–сховище – герметична споруда для захисту людей, в якій протягом певного часу створюються умови, що виключають вплив на них небезпечних 58 факторів, які виникають внаслідок надзвичайної ситуації, воєнних (бойових) дій та терористичних актів;

–протирадіаційне укриття – негерметична споруда для захисту людей, в якій створюються умови, що виключають вплив на них іонізуючого опромінення у разі радіоактивного забруднення місцевості;

–швидкоспоруджувана захисна споруда цивільного захисту – захисна споруда, що зводиться із спеціальних конструкцій за короткий час для захисту людей від дії засобів ураження в особливий період.

Для захисту людей від деяких факторів небезпеки, що виникають внаслідок надзвичайних ситуацій у мирний час, та дії засобів ураження в особливий період також використовуються споруди подвійного призначення та найпростіші укриття.

Для вирішення питань щодо укриття населення в захисних спорудах цивільного захисту центральні органи виконавчої влади, місцеві державні адміністрації, органи місцевого самоврядування та суб’єкти господарювання завчасно створюють фонд таких споруд. Порядок створення, утримання фонду захисних споруд цивільного захисту та ведення його обліку визначається Кабінетом Міністрів України.

Проектування, будівництво, пристосування і розміщення захисних споруд та об’єктів подвійного призначення здійснюються згідно з нормами, які розробляються відповідно до Закону України "Про будівельні норми". Вимоги щодо утримання та експлуатації захисних споруд визначаються центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту.

4.2.2.Особливості роботи та розлади здоров’я користувачів комп’ютерів, що формується під впливом роботи за комп’ютером.

У професійних операторів частіше зустрічаються порушення органів зору, опорно-рухового апарату, центральної нервової, серцево-судинної, імунної та статевої систем, захворювання шкіри. Зафіксована значна кількість скарг операторського персоналу на загальне недомагання, передчасне стомлювання, головний біль, порушення функцій органів зору, які здійснювали несприятливий психофізіологічний вплив на самопочуття та працездатність операторів [3]. Сучасна професія користувача ВДТ належить до розумової праці, яка характеризується: високою напруженістю зорових функцій; одноманітною позою; великою кількістю стереотипних висококоординованих рухів, що виконуються лише м'язами кистей рук на фоні малої загальної рухової активності; значним нервово-емоційним компонентом, особливо в умовах дефіциту часу; роботою з великими масивами інформації, що викликає активізацію уваги та інших вищих психічних функцій.

Крім того, при роботі з дисплеями на електронно-променевих трубках виникає вплив на користувача цілої низки факторів фізичної природи — електростатичні поля, радіочастотне та рентгенівське випромінювання тощо.

Розлади здоров'я користувачів, що формуються під впливом роботи за комп'ютером [34]:

–Комп’ютерний зоровий синдром (КЗС) – комплекс порушень здоров’я, який може виникати у користувачів персональних комп’ютерів (ПК). Діагноз ставлять, якщо людина, що працює за ПК протягом двох годин, висловлює хоча б дві з десяти скарг: головний біль, сльозотеча, різь, туман, двоїння, свербіж, важкість в очах, фотофобія, миготіння знаків на екрані, нудота. У користувачів ПК дуже поширені кон’юнктивіти і блефарити, патогенетично пов’язані з КЗС. Синдром розвивається при умові, що робоче місце організовано неправильно – у користувача незручне крісло, відсутні пюпітри для паперів, підставки для ніг та кистей рук, не встановлена висота і нахил монітора відносно очей, відстань від очей до екрана. За таких умов тіло людини при роботі займає вимушене положення: спина статично напружена, шия витягнута, плечі жорстко фіксовані. Напружені м’язи погіршують кровотік у

сонних артеріях, а недостатнє кровозабезпечення головного мозку веде до очманіння, появи головного болю. На фоні шийного остеохондрозу з’являється відчуття випирання очних яблук, туману в очах, мушок та райдужних кіл у полі зору. Розвитку КЗС сприяє поганий мікроклімат приміщення, значна загальна іонізація та мікробне забруднення, а також куріння.

–Перенапруження скелетно-м'язової системи. Діяльність користувачів комп'ютерів характеризується тривалою багатогодинною (8 год. і більше) працею в одноманітному напруженому сидячому положенні, малою руховою активністю при значних локальних динамічних навантаженнях, що припадають лише на кисті рук. Такий характер роботи може призвести до появи низки хворобливих симптомів, що об'єднані загальною назвою — синдром довготривалих статичних навантажень, що може проявлятись втомою, скутістю, болем, судомою, онімінням та ін., локалізуватись у різних частинах тіла (шия, спина, руки, ноги та ін.) і виникати індивідуально з різною частотою (ніколи, рідко, епізодично, щоденно). Робоче положення "сидячи" забезпечується статичною працею значної кількості м'язів, що дуже втомлює. При такому положенні тіла м'язи ніг, плечей, шиї та рук довгий час перебувають у скороченому стані. Оскільки м'язи не розслабляються, в них погіршується кровообіг.

–Ураження шкіри. Частота шкірних уражень корелюється з низькою відносною вологістю на робочих місцях операторів та частим виникненням електростатичних зарядів. Електростатичне поле, яке генерується дисплеєм комп'ютера, посилює електростатичний заряд на тілі оператора, а відтак зростає електростатичне поле біля нього. Підвищення відносної вологості повітря у приміщенні в поєднанні з вилученням килимових покриттів, в яких нагромаджуються статичні заряди, сприяли зниженню шкірних висипань на обличчі. Обладнання заземлення, встановлення сіткового екрана з металевого дроту між дисплеєм і оператором у деяких випадках знижувало частоту захворювань шкіри.

–Розлади центральної нервової системи (ЦНС). До найважливіших факторів, характерних для роботи операторів ВДТ, що впливають на погіршення стану їх ЦНС

належать: інформаційне перевантаження мозку в поєднанні з дефіцитом часу, тривожне очікування інформації, особливо тієї, що викликає необхідність прийняти рішення; велике зорове та нервово-емоційне напруження; гіподинамія; монотомія; висока відповідальність за кінцевий результат. Під впливом цих факторів виникають зміни у співвідношенні процесів збудження та гальмування в корі головного мозку. При цьому функціональна активність ЦНС знижується, а порушення рівноваги основних нервових процесів все більше спрямовано в бік гальмування. В організмі розвивається втома.

В результаті написання даного підрозділу можна дійти до висновків, що інженерний захист є обов'язковою умовою для попередження чи максимального зниження втрат та матеріальних збитків при виникненні надзвичайних ситуацій. Раціонально сплановані підготовлені та реалізовані заходи інженерного захисту забезпечують зниження можливих людських втрат та матеріальних збитків, створюють умови для успішного проведення аварійно-рятувальних та інших невідкладних робіт.

Щодо взаємодії з комп'ютерною технікою, очевидно, що це може негативно позначитися на здоров'ї та фізичному самопочутті людини. Тому, при організації та обладнанні комп’ютерних приміщень і визначенні робочого часу, обов'язково слід дотримуватися санітарних, ергономічних та гігієнічних стандартів, а також проводити спеціальні фізкультурно-оздоровчі заходи. Це сприятиме значному зменшенню негативного впливу комп'ютерної роботи на здоров'я, фізичний стан та психічний стан людини.

ВИСНОВКИ

Основні висновки та наукові результати дослідження можна узагальнити наступним чином:

1.За допомогою аналізу літератури та наукових джерел були визначені критерії оцінки захищеної інформації, визначено ключові інструменти захисту та сформульовано завдання, які вирішують системи виявлення вторгнень.

2.Проведено класифікацію IDS/IPS-систем, визначені варіанти їх розміщення, алгоритми роботи та методи отримання даних. Ретельно проаналізовано сильні та слабкі сторони кожного класу, а також розглянуто основні атаки на мережну інфраструктуру комп’ютерних систем.

3.Розглянуті алгоритми, використовувані в системах виявлення вторгнень, включаючи як класичні сигнатурні методи, так і сучасні методи поведінкового та інтелектуального аналізу даних. Розроблено схему архітектури системи виявлення вторгнень.

4.Визначено необхідність застосування комбінації алгоритмів аналізу трафіку на різних рівнях мережевої моделі OSI та для різних типів мережевої активності.

5.Здійснено обчислювальний експеримент, який підтвердив перевагу комбінації алгоритмів ALAD+LERAD для виявлення атак у віртуальному середовищі, з використанням Suricata як основи системи виявлення вторгнень.

6.На основі Suricata та обраних алгоритмів розроблено логічну модель системи виявлення вторгнень, описано схеми взаємодії компонентів та варіанти використання системи. Також побудовано фізичну модель та визначено взаємодію з іншими пристроями локальної мережі.

7.Проведено налаштування IDS Suricata для використання сторонніх алгоритмів, а також адаптацію правил Snort для взаємодії з системою виявлення вторгнень Suricata. Забезпечено підтримку пакетів готових сигнатур та розроблено можливості створення власних сигнатурних правил аналізу трафіку.

8.Проведено підключення системи виявлення вторгнень до імітаційного середовища та здійснено обчислювальний експеримент з фіксованими контрольними пакетами трафіку при різних конфігураціях віртуального середовища.

9.Отримані практичні висновки вказують на переваги використання Suricata, зокрема, її ефективність з використанням апаратного прискорення, швидкість роботи із сторонніми алгоритмами поведінкового аналізу та ефективність методу сигнатурного аналізу.

10.Визначені недоліки створеної системи включають надмірність сигналів про атаки, обробку деяких пакетів двічі, обмеженість інспектування шифрованого трафіку та необхідність доопрацювання правил відповідно до синтаксису Suricata.

Усі ці результати підтверджують поставлені гіпотезу, досягнення мети та виконання завдань дослідження. Розроблена система виявлення вторгнень є повністю функціональною і має практичне значення в контексті інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Allen J. State of the Practice of Intrusion Detection Technologies [Текст]// J. Allen, A. Christie, W. Fithen. – Carnegie Mellon University, Software Engineering Institute, 2000. – P. 17-29.

2.Nadiammai GV, Hemalatha M. Effective approach toward Intrusion Detection System using data mining techniques - Egyptian Informatics Journal, Volume 15, Issue 1, 2014. - P. 37-50.

3.String Matching Enhancement for Snort IDS, 2010, Safaa Almamory, Ali Jaddoa, Asala Abdul-Razak, Zainab Falah. URL: https://www.researchgate.net/publication/ 251990313_String_matching _enhancement _for_snort_IDS (дата звернення: 12.12.2023).

4.Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation, 2021, Gauthama Raman MR, Chuadhry Mujeeb Ahmed & Aditya Mathur. URL: https://link.springer.com/article/10.1186/s42400-021-00095-5 (дата звернення: 15.12.2023).

5.Feature selection for intrusion detection systems, 2020, Kamalov, F (Kamalov, Firuz), Moussa, S (Moussa, Sherif), Zgheib, R (Zgheib, Rita), Mashaal, O (Mashaal, Omar). URL: https://www.webofscience.com/wos/woscc/full-record /WOS:000653085400058 (дата звернення: 12.12.2023).

6.Improving Intrusion Detection Systems За допомогою Artificial Neural Networks, 2018, Jasim, YA (Jasim, Yaser A.). URL: https://www.webofscience.com/wos/woscc/full-record/WOS:000439499300005 (дата звернення: 15.12.2023).

7.Intelligent Intrusion detection systems using artificial neural networks, 2018, Shenfield, A (Shenfield, Alex), Day, D (Day, David) 2, Ayesh, A (Ayesh, Aladdin). URL: https://www.webofscience.com/wos/woscc/full-record/WOS:000435857100008 (дата звернення: 15.12.2023).

8.Network Intrusion Detection System за допомогою Deep Learning, 2021, Ashiku, L (Ashiku, Lirim), Dagli, C (Dagli, Cihan). URL:

https://www.webofscience.com/wos/woscc/full-record/WOS:000681039400028 (дата звернення: 15.12.2023).

9.A Sequential Classifiers Combination Method to Reduce False Negative for Intrusion Detection System, 2019, Phetlasy, S (Phetlasy, Sornxayya), Ohzahata, S (Ohzahata, Satoshi), Wu, C (Wu, Celimuge), Kato, T URL: https://www.webofscience.com/wos/woscc/full-record/WOS:000466289200003 (дата звернення: 15.12.2023).

10.Analysis of Intrusion Detection Systems in Industrial Ecosystems, 2017, Juan Enrique Rubio, Cristina Alcaraz, Rodrigo Roman, Javier Lopez. URL: https://www.nics.uma.es/pub/papers/1662.pdf (дата звернення: 15.12.2023).

11.A Survey of Intrusion Detection & Prevention Techniques, 2011, Usman Asghar Sandhu, Sajjad Haider, Salman Naseer, Obaid Ullah Ateeb. URL: https://www.researchgate.net/publication/340931654_A_Survey_of_Intrusion_Detect ion_Prevention_Techniques (дата звернення: 15.12.2023).

12.Survey of intrusion detection systems: techniques, datasets and challenges, 2019, Ansam Khraisat, Iqbal Gondal, Peter Vamplew & Joarder Kamruzzaman. URL: https://link.springer.com/article/10.1186/s42400-019-0038-7 (дата звернення: 15.12.2023).

13.Denial of Service Attacks: офіційний сайт організації "Texas State University". URL: https://s2.ist.psu.edu/ist451/DDoS-Chap-Gu-June-07.pdf (дата звернення: 15.12.2023).

14.Adaptation Techniques for Intrusion Detection and Intrusion Response Systems. URL: http://www.secdev.org/idsbiblio/adapt.pdf (дата звернення: 15.12.2023).

15.Чайковський А.В., Жаровський Р.О., Лещишин Ю.З Конспект лекцій з дисципліни «Дослідження і проєктування комп’ютерних систем та мереж» для студентів спеціальності 123 - Комп’ютерна інженерія. Тернопіль, 2021. 148 с.

16.Ковтун Н., Жаровський Р. Алгоритмічне забезпечення систем виявлення вторгнень. Матеріали XI науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі системи та технології» (13-14 грудня 2023 року). Тернопіль: ТНТУ. 2023. С.156.

17.Ковтун Н., Жаровський Р. Аналіз засобів протидії вторгненням і атакам на комп'ютерні системи. Матеріали XII Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» (6-7 грудня 2023 року). Тернопіль: ТНТУ. 2023. С. 453-454.

18.Enterprise Matrix URL: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 15.12.2023).

19.Жаровський, Р. О. Конспект лекцій з дисципліни Захист інформації у комп'ютерних системах. 2019. 268 с.

20.Казмірчук, Світлана Володимирівна, Анна Олександрівна Корченко, and Тарас Іванович Паращук. "Аналіз систем виявлення вторгнень." *Захист інформації* 20.4 2018. Сс.259-276.

21.Коробейнікова, Т.; Цар, О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. *Grail of Science*, 2023, 27: сс 317-325.

22.Ilyenko, Anna, et al. Практичні підходи щодо виявлення вразливостей в інформаційно-телекомунікаційних мережах. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2023, 3.19: 96-108.

23.Ahmed, M., Mahmood, N. & Hu, J. A survey of network anomaly detection techniques. J. Netw. Comput. Appl. 60. 2016. pp19–31.

24.ALI, Tariq Emad; CHONG, Yung-Wey; MANICKAM, Selvakumar. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. *Applied Sciences*, 2023, 13.5: 3183.

25.SCHWENK, Jörg. Attacks on SSL and TLS. In: *Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications*. Cham: Springer International Publishing, 2022. p. 267-328.

26.SOE, Yan Naung, et al. Machine learning-based IoT-botnet attack detection with sequential architecture. *Sensors*, 2020, 20.16: 4372.

27.MYINT OO, Myo, et al. Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN). *Journal of Computer Networks and Communications*, 2019, 2019.

28.OTOUM, Yazan; LIU, Dandan; NAYAK, Amiya. DL-IDS: a deep learning–

based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies*, 2022, 33.3: e3803.

29.CHIBA, Zouhair, et al. Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms. *computers & security*, 2019, 86: 291-317.

30.NIE, Laisen, et al. Data-driven intrusion detection for intelligent internet of vehicles: A deep convolutional neural network-based method. *IEEE Transactions on Network Science and Engineering*, 2020, 7.4: 2219-2230.

31.NADIAMMAI, G. V.; HEMALATHA, MJEIJ. Effective approach toward Intrusion Detection System using data mining techniques. *Egyptian Informatics Journal*, 2014, 15.1: 37-50.

32.Зеркалов Д.В. Охорона праці в галузі: Загальні вимоги. Навчальний посібник. К.: Основа. 2011. 551 с.

33.Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. – 2011. 215 с.

34.Вплив комп’ютера на здоров’я користувача URL: https://ukped.com /informatyka / 713-vplyv- kompyutera-na- zdorovya-korystuvacha.html (дата звернення: 13.12.2023).

35.Лупенко С.А., Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Методичні рекомендації до виконання кваліфікаційної роботи магістра для студентів спеціальності 123 «Комп’ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль. 2021. 34 с.

Додаток А.

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XII Міжнародної науково-практичної конференції молодих учених та студентів
6-7 грудня 2023 року

УКРАЇНА
ТЕРНОПІЛЬ – 2023

МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ
55. **В. В. Яцишин, О. О. Горбач** **440**
ПРОЦЕСИ РОЗРОБКИ ТА МОДЕЛІ ЖИТТЄВОГО ЦИКЛУ КОМП'ЮТЕРНИХ СИСТЕМ
56. **А. М. Луцків, Ю. Б. Мельничук** **441**
ПРИНЦИПИ ОРГАНІЗАЦІЇ ОНЛАЙН АУКЦІОНІВ З ІНТЕГРАЦІЄЮ ЕЛЕМЕНТІВ БЛОКЧЕЙН ТЕХНОЛОГІЇ І ТЕОРІЇ ІГОР
57. **Т. А. Озарків, Р. О. Жаровський** **442**
ОПТИМІЗАЦІЯ РОБОТИ ПРОТОКОЛУ EIGRP В УМОВАХ ВЕЛИКИХ МЕРЕЖ ЗІ СКЛАДНОЮ ТОПОЛОГІЄЮ
58. **М. Р. Лещук, Б. М. Зозуляк, В. М. Кравчук, Р. І. Королюк** **443**
МОДЕЛЮВАННЯ РОБОТИ СИСТЕМИ КОНТРОЛЮ НАТЯГУ ПРИ ПРОКАТУВАННІ АЛЮМІНІЮ
59. **Ю. І. Микитів, І. Я. Харів, М. Б. Горват, Р. З. Золотий** **445**
АНАЛІЗ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОМФОРТУ ТА ЕНЕРГОЕФЕКТИВНОСТІ БУДІВЕЛЬ
60. **М. С. Дзюмак, С. З. Кульчицький, І. М. Поливаний, О.С. Голотенко** **447**
ДОСЛІДЖЕННЯ СИСТЕМИ ПЛАНУВАННЯ МАРШРУТУ НА ОСНОВІ ІНТЕРВАЛЬНИХ ОБЧИСЛЕНЬ
61. **А. О. Мацюк, В. В. Дрогомирецький, Ю. О. Зеленко, А. А. Станько** **448**
РОЗРОБКА СИСТЕМИ КЕРУВАННЯ ПРОЦЕСОМ ПАКУВАННЯ КОНСЕРВНИХ ВИРОБІВ
62. **Т. В. Чомко, В. В. Панчук, В. П. Пинило, В. В. Карташов** **450**
РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ ТА УПРАВЛІННЯ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ КЕРУВАННЯ ПІДЙОМНИМ МЕХАНІЗМОМ
63. **А. М. Луцків, А. Я. Островський** **452**
ХАРАКТЕРИСТИКИ ТА СФЕРА ЗАСТОСУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ
64. **Н. М. Ковтун, Р. О. Жаровський** **453**
АНАЛІЗ ЗАСОБІВ ПРОТИДІЇ ВТОРГНЕННЯМ І АТАКАМ НА КОМП'ЮТЕРНІ СИСТЕМИ
65. **А. М. Луцків, В. В. Гладій** **455**
ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ТА КЛАСИФІКАЦІЇ РОЗПОДІЛЕНИХ СИСТЕМ ЗБЕРІГАННЯ ДАНИХ
66. **Д. Р. Карабан, Р. О. Жаровський** **456**
АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ КОРИСТУВАЧІВ ПРИ ВИКОРИСТАННІ МЕРЕЖІ ІНТЕРНЕТ
67. **А. В. Ремез, Й. Р. Кравець, І. В. Карп, Д. П. Стухляк** **457**
ДОСЛІДЖЕННЯ РУЙНІВНОГО НАПРУЖЕННЯ ПРИ ЗГИНАННІ НАПОВНЕНИХ ЕПОКСИКОМПОЗИТІВ
68. **Р. О. Іванов, Е. С. Рожко, А. В. Антонишин, І. В. Чихіра** **459**
РОЗРОБКА СИСТЕМИ АВТОМАТИЗАЦІЇ СКЛАДСЬКОГО УПРАВЛІННЯ НА БАЗІ ПЛК
69. **В. В. Яцишин, О. В.Пасіка, С. О. Куліков** **461**
КОНЦЕПТУАЛЬНА АРХІТЕКТУРА КОМП'ЮТЕРНОЇ СИСТЕМИ УПРАВЛІННЯ ПРИВАТНИМИ РЕСТОРАНАМИ

УДК 004.45
Н. М. Ковтун; Р. О. Жаровський , к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ЗАСОБІВ ПРОТИДІЇ ВТОРГНЕННЯМ І АТАКАМ НА КОМП'ЮТЕРНІ СИСТЕМИ

N. M. Kovtun; R.O. Zharovskyi, Ph.D.

ANALYSIS OF MEANS OF RESISTING INTRUSIONS AND ATTACKS ON COMPUTER SYSTEMS

У питанні захисту інформації в комп'ютерних системах дуже велике значення для запобігання несанкціонованому доступу мають системи виявлення та запобігання атакам.

Такі системи в реальному часі відстежують аномальну активність на підставі потоків даних, що одержуються з інформаційних систем, мережевого обладнання, антивірусних додатків, систем запобігання витоку даних та багатьох інших джерел. Системи виявлення вторгнень можуть моніторити весь трафік мережі, що дозволяє їм виявляти підозрілі активності, навіть якщо вона відбувається всередині захищеної мережі.

Однак, способи та методики мережевих вторгнень постійно змінюються та модернізуються зловмисниками. У таких динамічних умовах необхідний перегляд алгоритмів, що використовуються в роботі СВВ (системи виявлення вторгнень), для надійної роботи системи. Нові алгоритми роботи повинні спиратися не тільки на сигнатури відомих інструментів та методів, але й адаптуватись до нових загроз.

Для вирішення завдання щодо вдосконалення систем виявлення та запобігання атак дослідники виділяють кілька основних напрямків:

- вдосконалення сигнатурного та статистичного аналізу даних;
- обробка нечітких онтологій на підставі попередньо затвердженої безпекової політики;
- використання нейромереж для постійного навчання IDS-системи та протидії складнопрогнозованим атакам.

Принцип роботи IDS-систем заснований на аналізі мережної чи системної активності та пошуку відхилень від нормальної поведінки. Для цього IDS використовують моделі поведінки, які можуть бути створені на основі статистичних даних про те, як повинен проходити обмін даними всередині системи.

IDS можуть працювати в режимі реального часу, постійно переглядаючи та аналізуючи дані, або виконуватись за розкладом, скануючи систему у певні моменти часу.

Як правило IDS поєднують у собі як сигнатурні методи, так і поведінковий аналіз, що збільшує загальний рівень безпеки системи, але також підвищується кількість помилкових спрацьовувань. Також система може включати в себе модуль прийняття рішень та модуль реагування, що забезпечує можливість реагувати на вторгнення та запобігати атакам. Загальна схема архітектури IDS зазначена на рисунку 1.

Функціональність модуля виявлення атак спрямована на аналіз стану мережі та реєстрацію подій підозрілої активності або комп'ютерних атак. Модуль прийняття рішень отримує дані щодо здійснених атак від модуля виявлення атак і, базуючись на різних параметрах, відправляє відповідні команди модулю реагування [1]. Реакції на атаку можуть включати блокування конкретної IP- або MAC-адреси пристрою, встановлення тимчасових або постійних правил для міжмережевих екранів мережевого

обладнання, а також блокування або позбавлення привілеїв облікових записів систем, включаючи доменні. Інші можливі дії включають інформування оператора IDS або системного адміністратора тощо.

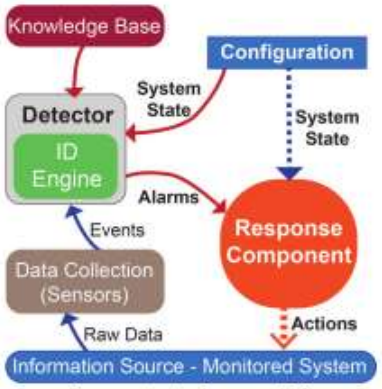

Рисунок 1. Архітектура IDS

Атаки на мережевому, прикладному та канальному рівнях проходять через фільтрацію бази знань. Мережевий трафік піддається контролю підсистемою сенсорів, які в реальному часі фільтрують пакети за заздалегідь визначеними правилами, характерними для найпоширеніших атак. Сенсори копіюють пакети і передають їх модулю виявлення атак та сховищу. Сенсори використовують сигнатурний метод аналізу трафіку, отримуючи інформацію про шаблони проведення атак із бази знань [2].

База знань також включає шаблони реагування на інциденти, які сприяють модулю прийняття рішень у виборі найбільш підходящого способу реагування. Модулі IDS керуються оператором через консоль управління, що дозволяє IDS взаємодіяти та діагностувати стан мережі та інформаційних систем всередині неї.

Сучасні дослідники також розглядають можливість використання технологій нейронних мереж та інтелектуального аналізу даних для роботи IDS-систем [3, 4,] Згідно з вищезазначеним дослідженням, найбільш оптимальним з точки зору безпеки є комбінація кількох алгоритмів виявлення атак за участю програмного арбітра, який визначає рівень моделі OSI та тип мережної активності для вибору подальшого алгоритму аналізу трафіку

Література

1 Deconstructing the Computer: Report of a Symposium / Committee on Deconstructing the Computer, Committee on Measuring and Sustaining the New Economy, Board on Science, Technology, and Economic Policy, Policy and Global Affairs, National Research Council - Washington: National Academies Press, 2005. - P. 49-50.

2 Adaptation Techniques for Intrusion Detection and Intrusion Response Systems URL: http://www.secdev.org/idsbiblio/adapt.pdf

3. Batista, L. O., de Silva, G. A., Araujo, V. S., Araujo, V. J. S., Rezende, T. S., Guimarães, A. J., Souza, P. V. D. C. Fuzzy neural networks to create an expert system for detecting attacks by sql injection. 2019 . URL: https://arxiv.org/abs/1901.02868

4. Mahdavifar, S., Ghorbani, A. A. DeNNeS: deep embedded neural network expert system for detecting cyber attacks. Neural Computing and Applications. 2020. URL: https://link.springer.com/article/10.1007/s00521-020-04830-w

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

О.А. Дичук; Р.О. Жаровський
УПРАВЛІННЯ ПОТОКОМ ЗА КРИТЕРІЯМИ ДОСТУПНОСТІ
O.A. Diachuk; R.O. Zharovskyi
FLOW CONTROL BY ACCESSIBILITY CRITERIA 151

Ю.І. Залісковий, Ю.З. Лещишин, А.В. Варавін
МЕТОДИ ПРОВЕДЕННЯ МОНІТОРИНГУ І АНАЛІЗУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ІНТЕРНЕТ ПРОВАЙДЕРАМИ
Y.I. Zaliskovyi, Y.Z. Leshchyshyn, A.V. Varavin
METHODS OF MONITORING AND ANALYSIS OF NETWORK INFRASTRUCTURE BY INTERNET PROVIDERS 152

Ю.І. Залісковий, Ю.З. Лещишин, А.В. Варавін
ВИБІР ТЕХНОЛОГІЙ РОЗРОБКИ ВЕБ-РЕСУРСУ МОНІТОРИНГУ МЕРЕЖІ ІНТЕРНЕТ ПРОВАЙДЕРАМИ
Y.I. Zaliskovyi, Y.Z. Leshchyshyn, A.V. Varavin
SELECTION OF TECHNOLOGIES FOR THE DEVELOPMENT OF A WEB RESOURCE FOR NETWORK MONITORING BY INTERNET PROVIDERS 153

І. Кардаш, Ю. Лещишин, А. Варавін
КРИТЕРІЇ ЕФЕКТИВНОСТІ РОБОТИ ДЛЯ ЗАДАЧІ МОНІТОРИНГУ ЛОКАЛЬНОЇ МЕРЕЖІ
I. Kardash, Yu. Leshchyshyn, A. Varavin
WORK EFFICIENCY CRITERIA FOR THE LOCAL NETWORK MONITORING TASK 154

І. Кардаш, Ю. Лещишин, А. Варавін
МОНІТОРИНГ ЕФЕКТИВНОСТІ РОБОТИ ЛОКАЛЬНИХ МЕРЕЖ
I. Kardash, Yu. Leshchyshyn, A. Varavin
MONITORING OF THE EFFICIENCY OF LOCAL NETWORKS 155

Н.М. Ковтун; Р.О. Жаровський
АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ
N.M. Kovtun; R.O. Zharovskyi
ALGORITHMIC PROVISION OF INTRUSION DETECTION SYSTEMS 156

Д. Козарик, Ю. Лещишин
МОДЕЛЮВАННЯ МЕТОДІВ ПОТОКОВОГО ШИФРУВАННЯ ТА ПЕРЕДАВАННЯ ФОТОГРАФІЧНИХ ЗОБРАЖЕНЬ
D. Kozaryk; Yu. Leshchyshyn
SIMULATION OF STREAM ENCRYPTION METHODS AND TRANSMISSION OF PHOTOGRAPHIC IMAGES 157

Д. Козарик; Ю. Лещишин
МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ КОМП'ЮТЕРНОЇ СИСТЕМИ ДЛЯ ПОТОКОВОГО ШИФРУВАННЯ ТА ПЕРЕДАВАННЯ ФОТОГРАФІЧНИХ ЗОБРАЖЕНЬ
D. Kozaryk; Yu. Leshchyshyn
METHODS AND MEANS FOR CONSTRUCTING A COMPUTER SYSTEM FOR STREAM ENCRYPTION AND TRANSMISSION OF PHOTOGRAPHIC IMAGES 158

Т. І. Крамар; Є. В. Тиш
СУЧАСНІ ТЕХНОЛОГІЇ РОБОТИ КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЕКСПОРТУ ЕЛЕКТРОЕНЕРГІЇ
T. Kramar; Ie. Tysh
MODERN WORK TECHNOLOGIES COMPUTERIZED ELECTRICITY EXPORT SYSTEMS 159

Т. І. Крамар; Є. В. Тиш
МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОГО ФУНКЦІОНУВАННЯ ЕЛЕКТРОМЕРЕЖ ПІД ЧАС ПОГОДНИХ АНОМАЛІЙ.
T. Kramar; Ie. Tysh
METHODS AND MEANS OF ENSURING STABLE FUNCTIONING OF ELECTRICAL NETWORKS DURING WEATHER ANOMALIES 160

УДК 004.45

Н.М. Ковтун; Р.О. Жаровський , к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

N.M. Kovtun; R.O. Zharovskyi, Ph.D.

ALGORITHMIC PROVISION OF INTRUSION DETECTION SYSTEMS

На підставі аналізу літератури, наукових та аналітичних статей з проблеми вдосконалення систем виявлення вторгнень та попередження комп'ютерних атак було виділено критерії оцінки інформації, що захищається, визначено основні інструменти її захисту, а також сформульовано завдання, яке вирішують системи виявлення вторгнень.

У ході роботи було проведено класифікацію IDS/IPS-систем, виявлено способи їх розміщення, алгоритми роботи та методи отримання даних. Визначено сильні та слабкі сторони кожного згаданого класу.

Були проаналізовані алгоритми, які у роботі системи виявлення вторгнень, як із використанням класичних сигнатурних алгоритмів, і більш сучасних методів поведінкового аналізу та інтелектуального аналізу даних. Також було визначено схему архітектури системи виявлення вторгнень.

За результатами аналізу було зроблено висновок необхідність застосування системи виявлення вторгнень комбінації алгоритмів аналізу трафіку щодо різних рівнів мережевої моделі OSI і типів мережевої активності.

Розглянемо докладніше існуючі алгоритми, які у системах виявлення вторгнень. IDS виявляють атаки шляхом використання різних методів аналізу вихідних даних. У цій дослідницькій роботі торкнемося наступні методи виявлення атак:

- packet header anomaly detection (PHAD) – аналіз заголовків пакетів трафіку;
- network traffic anomaly detection (NETAD) – аналіз вмісту кадрів мережного трафіку;
- application layer anomaly detection (ALAD) – аналіз роботи додатків;
- learning rules for anomaly detection (LERAD) – умовні правила виявлення аномалій у вихідних даних пакетів (наприклад, ланцюжки handshake, що передаються в рамках TCP-сесії).

Кожен метод виявлення атак показує найбільшу ефективність проти певних видів атак. Наприклад, аналіз заголовків ефективний виявлення атак типу DNS-spoofing чи SYN-flood, але з здатний виявити використання SQL-ін'єкцій, яке, своєю чергою, легко виявляється з допомогою аналізу роботи додатків.

Тому в більшості систем виявлення вторгнень використовуються комбінації різних методів виявлення атак разом з попередньо налаштованими правилами та/або технологіями машинного навчання для забезпечення найбільшої безпеки системи, що захищається, і мінімізації можливої шкоди.

Незважаючи на те, що методи виявлення аномалій удосконалюються з кожним роком, першим етапом роботи будь-якого IDS є сигнатурний аналіз. Він дозволяє максимально швидко виявити найпоширеніші атаки без залучення основних ресурсів системи, що економить час та обчислювальні потужності серверів.

Ефективність роботи алгоритмів визначається наступним рядом параметрів: швидкість обчислень (час обробки вихідних даних), точність визначення атак (достовірність визначення факту атаки та її правильна класифікація), частота помилкових спрацьовувань системи.

Додаток Б.

Скрипт автоматичного запуску Suricata

```
#!/bin/sh -e
#
### BEGIN INIT INFO
# Provides: suricata
#Required-Start: $time $network $local_fs $remote_fs
#Required-Stop: $remote_fs
#Default-Start: 2 3 4 5
#Default-Stop:0 1 6
#Short-Description: Next Generation IDS/IPS
# Description: Intrusion detection system that will
# capture traffic from the network cards and will
# match agast a set of known attacks.
###END INIT INFO
. /lib/lsb/init-functions
# Source function library.
if test -f /etc/default/suricata; then
. /etc/default/suricata
else
echo "/etc/default/suricata is missing... bailing out!"
fi
#We'll add up all the options above and use them NAME=suricata
DAEMON=/usr/bin/$NAME
if [-z "$RUN_AS_USER"]; then
USER_SWITCH=
else
USER_SWITCH=--user=$RUN_AS_USER
fi
#Використовуйте цей параметр, якщо Ви захочете встановити 'RUN' in
#/etc/default/
if [ "x$RUN" != "xyes" ] ; then
log_failure_msg "$NAME disabled, please adjust the configuration to
your
needs "
log_failure_msg "and then set RUN to 'yes' in /etc/default/$NAME to
enable
it."
exit 0
fi
check_root() {
if [ "$(id -u)"! = "0"]; then
log_failure_msg  "Ви повинні скористатися start, stop or restart
$NAME."
exit 4
fi
}
check_nfqueue() {
if    [!    -e    /proc/net/netfilter/nf_queue    ]    &&    [    !    -e
/proc/net/netfilter/nfnetlink_queue]; then
```

```
log_failure_msg "NFQUEUE support not found !"
log_failure_msg "Плещати налаштування nfnetlink_queue module loaded or
built in kernel"
exit 5
fi
}
check_run_dir() {
if [! -d /var/run/suricata]; then
mkdir /var/run/suricata
if [! -z "$ RUN_AS_USER"]; then
chown $RUN_AS_USER /var/run/suricata;
fi
chmod 0755 /var/run/suricata
fi
}
check_root
case "$LISTENMODE" in
nfqueue)
IDMODE="IPS (nfqueue)"
LISTEN_OPTIONS="$NFQUEUE"
check_nfqueue
;;;
custom_nfqueue)
IDMODE="IPS (custom multi-nfqueue)"
LISTEN_OPTIONS="$CUSTOM_NFQUEUE"
check_nfqueue
;;;
pcap)
IDMODE="IDS (pcap)"
LISTEN_OPTIONS="-i $IFACE"
;;;
af-packet)
IDMODE="IDS (af-packet)"
LISTEN_OPTIONS=" --af-packet"
;;;
*)
echo "Unsupported listen mode $LISTENMODE, aborting"
exit 1
;;;
esac
SURICATA_OPTIONS="-c $SURCONF --pidfile $PIDFILE $LISTEN_OPTIONS -D -
vvv $USER_SWITCH"
#See how we were called. case "$1" in
start)
if [-f $PIDFILE]; then PID1=`cat $PIDFILE`
if kill -0 "$PID1" 2>/dev/null; then
echo "$NAME is already running with PID $PID1"
exit 0
else
echo "Likely stale PID `cat $PIDFILE` з $PIDFILE exists, але процес is
not running!"
echo "Removing stale PID file $PIDFILE"
rm -f $PIDFILE
```

```
fi
fi
check_run_dir
echo -n "Start suricata in $IDMODE mode..."
$DAEMON $SURICATA_OPTIONS > /var/log/suricata/suricata-start.log
2>&1 &
echo "done."
;;;
stop)
echo -n "Stopping suricata:"
if [-f $PIDFILE]; then
PID2=`cat $PIDFILE`
else
echo "No PID file found; not running?"
exit 0;
fi
start-stop-daemon –oknodo –stop –quiet --pidfile=$PIDFILE --exec
$DAEMON
if [-n "$ PID2"]; then
kill "$PID2"
ret = $?
sleep 2
if kill -0 "$PID2" 2>/dev/null; then
ret = $?
echo-n "Waiting."
cnt=0
while kill -0 "$PID2" 2>/dev/null; do
ret = $?
cnt=`expr "$cnt" + 1`
if [ "$ cnt" -gt 10]; then
kill -9 "$PID2"
break
fi
sleep 2
echo -n". "
done
fi
fi
if [-e $PIDFILE]; then
rm $PIDFILE > /dev/null 2>&1
fi
echo "done."
;;;
status)
# Check if running...
if [-s $PIDFILE]; then
PID3=`cat $PIDFILE`
if kill -0 "$PID3" 2>/dev/null; then
echo "$NAME is running with PID $PID3"
exit 0
else
echo "PID file $PIDFILE exists, but process not running!"
fi
```

```
else
echo "$NAME not running!"
fi
;;;
restart)
$0 stop
$0 start
;;;
force-reload)
$0 stop
$0 start
;;;
*)
echo "Usage: $0 {start|stop|restart|status}"
exit 1
esac
exit 0
```