Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Дем'янова Артема Олексійовича

на здобуття ступеня вищої освіти Бакалавра

Система виявлення атак на вузли в корпоративній мережі підприємства

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

Шифр КРБКБ.2101115.21.01.06 ПЗ

Виконав студент 4 курсу група КБ-21-1 Артем ДЕМ'ЯНОВ

Керівник к.т.н., доцент Юрій КЛЬОЦ

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

3 06 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дем'янову Артему Олексійовичу

1 Тема роботи Система виявлення атак на вузли в корпоративній мережі підприємства

Керівник роботи к.т.н., доцент Юрій Кльоц

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 2.06.2025

3 Вихідні дані до роботи Вибір системи, здатну виявляти різноманітні кіберзагрози на пристроях та мережевому рівні. Потрібно здійснити аналіз можливих загроз. Обрати відповідні інструменти. Спроєктувати архітектуру рішення. Реалізувати систему виявлення атак у віртуальному середовищі. Провести налаштування компонентів, оцінити ефективність виявлення і реагування системи на ці загрози.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз предметної області. Класифікація та характеристики атак. Параметри вибору систем виявлення атак. Огляд популярних систем виявлення атак. Вибір, алгоритм роботи та впровадження систем виявлення атак. Інтеграція систем виявлення атак з іншими засобами безпеки, Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Процес виявлення та реагування на атаку в корпоративній мережі. Схема корпоративної мережі з засобами виявлення атак. Взаємозв'язок між загрозами та компонентами системи виявлення атак.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Впровадження IDS	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент _____ Артем ДЕМ'ЯНОВ

Керівник кваліфікаційної роботи _____ Юрій КЛЬОЦ

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система виявлення атак на вузли в корпоративній мережі підприємства.

Автор роботи: Дем'янов Артем Олексійович.

Керівник роботи: Кльоц Юрій Павлович.

Пояснювальна записка: 67 с., 3 додатки, 26 рисунків, 3 таблиці, 40 джерел.

Графічна частина: 11 презентаційних слайдів.

СИСТЕМА ВИЯВЛЕННЯ АТАК, КОРПОРАТИВНА МЕРЕЖА, ВУЗЛИ МЕРЕЖІ, СИСТЕМА МОНИТОРИНГУ, PFSENSE, PFBLOCKERNG, SURICATA, WAZUH, SIEM, МОДЕЛЬ ЗАГРОЗ.

Кваліфікаційна робота бакалавра присвячена розробці комплексної системи виявлення та протидії атакам (IDS/IPS) для вузлів корпоративної мережі підприємства.

У роботі проаналізовано стан захищеності вузлів корпоративної мережі, визначено потенційні загрози та розроблено перелік заходів для їхнього виявлення і нейтралізації. Запропоновано архітектуру системи, що включає мережевий рівень захисту (pfSense із pfBlockerNG і Suricata) та хостовий рівень (Wazuh агенти), із централізованим аналізом подій. Розроблена система передбачає інтеграцію Wazuh із SIEM для збору, кореляції та аналізу безпекових подій у реальному часі. Впроваджено автоматизовані механізми реагування, такі як блокування підозрілих IP-адрес, детекція аномальної поведінки користувачів та контроль доступу до критичних ресурсів. Запропоноване рішення дозволяє забезпечити багаторівневий захист вузлів корпоративної мережі, знизити ризики компрометації систем та підвищити загальний рівень кібербезпеки підприємства.

28.05.2025 р.

ABSTRACT

Subject of qualification work: A system for detecting attacks on nodes in a corporate network of an enterprise.

Author: Demianov Artem Oleksiiovych.

Head of work: Klets Yurii Pavlovych.

Explanatory note: 67 p., 3 appendices, 26 figures, 3 tables, 40 sources

Graphic part: 11 presentation slides.

ATTACK DETECTION SYSTEM, CORPORATE NETWORK, NETWORK NODES, MONITORING SYSTEM, PFSENSE, PFBLOCKERNG, SURICATA, WAZUH, SIEM, THREAT MODEL.

The bachelor's thesis is devoted to the development of a comprehensive system for detecting and counteracting attacks (IDS/IPS) for the nodes of an enterprise corporate network.

The work analyses the security state of corporate network nodes, identifies potential threats and develops a list of measures to detect and neutralise them. A system architecture is proposed that includes a network layer of protection (pfSense with pfBlockerNG and Suricata) and a host layer (Wazuh agents) with centralised event analysis. The developed system provides for the integration of Wazuh with SIEM to collect, correlate and analyse security events in real time. Automated response mechanisms have been implemented, such as blocking suspicious IP addresses, detecting abnormal user behaviour and controlling access to critical resources. The proposed solution provides multi-level protection of corporate network nodes, reduces the risk of system compromise and increases the overall level of cybersecurity of the enterprise.

28.05.2025

ЗМІСТ

ВСТУП

Захист вузлів корпоративних мереж від атак є одним із ключових завдань у сфері інформаційної безпеки, адже сучасні технології та широке використання інтернету відкривають нові можливості для зловмисників. Неавторизоване проникнення до серверів, робочих станцій чи хмарних вузлів може призвести до значних фінансових втрат, погіршення репутації компанії та витоку конфіденційних даних. У зв'язку з цим створення надійних механізмів виявлення та запобігання загрозам для вузлів мережі стає критично важливим завданням.

Одним із найефективніших інструментів захисту є системи виявлення атак (IDS), які моніторять мережевий трафік і локальні події на вузлах, дозволяючи оперативно виявляти підозрілу активність. Такі рішення дають змогу своєчасно реагувати на загрози, мінімізуючи ризики або повністю нейтралізуючи їхній вплив на корпоративну інфраструктуру.

Важливим аспектом є розуміння різноманітних типів атак, спрямованих на вузли мережі, таких як мережеві загрози (DDoS, експлойти), локальні вразливості (шкідливе ПЗ, руткіти) чи комбіновані атаки, що вражають як інфраструктуру, так і окремі пристрої. Усвідомлення природи цих загроз і методів їхнього виявлення лежить в основі побудови ефективної системи захисту вузлів.

Метою цієї роботи є аналіз методів і технологій виявлення атак на вузли корпоративних мереж, а також вибір і обґрунтування оптимальних рішень, що відповідають сучасним вимогам кібербезпеки. У дослідженні розглядаються основні типи загроз для вузлів, принципи роботи систем моніторингу (мережевих і хостових), а також процеси їхнього впровадження в корпоративному середовищі. У роботі представлено рекомендації щодо налаштування та тестування системи виявлення атак, яка включає інтеграцію мережевого моніторингу (Suricata), хостового аналізу (Wazuh) і управління логами (Elastic Stack), для підвищення ефективності захисту від потенційних загроз.

1 ТЕОРЕТИЧНІ ОСНОВИ ВИЯВЛЕННЯ АТАК НА ВУЗЛИ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Основи безпеки вузлів корпоративної мережі

Інформаційна безпека вузлів корпоративної мережі – це комплекс заходів, спрямованих на захист серверів, робочих станцій та інших мережевих пристроїв від несанкціонованого доступу, атак, витоку або компрометації даних [1].

Мережева безпека використовує багатошаровий підхід до захисту, який охоплює як зовнішній периметр мережі, так і її внутрішні сегменти. Кожен шар безпеки впроваджує політику та контроль, що дозволяє авторизованим користувачам отримувати доступ до мережевих ресурсів, водночас блокуючи зловмисників від здійснення атак і загроз. Завдяки мережевій безпеці організації можуть захистити свої мережі від кібератак і забезпечити захист конфіденційної інформації, що допомагає зберігати репутацію та відповідати вимогам цифрової епохи.

Ключові поняття та принципи мережевої безпеки охоплюють основи забезпечення захисту інформаційних систем від несанкціонованого доступу, атак і порушень конфіденційності. Одним із основних принципів є ідентифікація та управління мережевими активами, що дозволяє знижувати ризик проникнення через незахищені або непідконтрольні пристрої. Важливим є також модель управління загрозами, яка дозволяє визначити потенційні ризики та розробити відповідні методи захисту від них [2].

Контроль доступу до мережевих ресурсів ґрунтується на принципі «найменших привілеїв», який передбачає обмеження прав користувачів і систем до мінімального рівня, необхідного для виконання їхніх завдань. Для захисту даних використовуються різні механізми автентифікації, такі як паролі, PIN-коди та багатофакторна автентифікація (MFA), що забезпечують додатковий рівень захисту. Крім того, важливо впроваджувати принципи безпечного проектування мереж, зокрема сегментацію мережі та архітектуру «нульового довіри», яка передбачає постійну перевірку всіх запитів на доступ. Такий підхід дозволяє

підвищити безпеку мережі та захистити конфіденційну інформацію від несанкціонованого доступу [2].

Основні принципи інформаційної безпеки вузлів включають [3]:

– конфіденційність;

– цілісність;

– доступність;

– автентифікація;

– авторизація;

– моніторинг.

Конфіденційність зосереджена на тому, щоб важлива інформація була доступна лише тим, кому це дозволено. У мережевому середовищі, де багато користувачів і пристроїв, необхідно захищати дані від стороннього втручання. Для цього застосовують шифрування, контроль доступу та поділ мережі на ізольовані частини.

Цілісність гарантує, що дані залишаються точними й не піддаються змінам без дозволу. Це особливо важливо для організацій, які покладаються на достовірність інформації у своїй роботі. Щоб досягти цього, використовують хешування, цифрові підписи та контрольні суми.

Доступність забезпечує безперебійну роботу мережі, щоб користувачі могли користуватися ресурсами тоді, коли їм це потрібно. Цього досягають через резервні системи, розподіл навантаження та регулярне оновлення обладнання й програм.

Аутентифікація перевіряє, хто саме намагається увійти в мережу, щоб тримати сторонніх подалі. Без цього захисту будь-хто міг би отримати доступ до системи. Для підтвердження особи застосовують паролі, біометрію та багатофакторну перевірку.

Авторизація визначає, що дозволено робити в мережі після входу. Вона встановлює межі для кожного користувача залежно від його прав і обов’язків. Для цього використовують рольовий контроль, списки доступу та правила на основі атрибутів.

Моніторинг відстежує дії користувачів у мережі, щоб завжди знати, що відбувається. Це потрібно для виявлення загроз і розуміння причин інцидентів. Досягають цього через ведення журналів, системи виявлення вторгнень і аналіз поведінки.

Для забезпечення кібербезпеки слід застосовувати комплексний підхід, який включає не лише технічні засоби захисту, але й організаційні заходи та постійну адаптацію до нових загроз.

Першим кроком є визначення та ідентифікація основних ризиків, з якими може зіткнутися організація. Використання підходу на основі ризиків дозволяє зосередитися на найбільш критичних елементах інфраструктури, які вимагають посиленого захисту. Такий підхід дозволяє застосовувати більш ефективні заходи, зосереджуючи ресурси на боротьбі з тими методами атак, що є найбільш ймовірними для конкретної організації. Це дозволяє оптимізувати використання ресурсів та підвищити ефективність захисту від кіберзагроз.

Відомі стандарти, такі як NCSC, ISO/IEC 27002, надають перелік заходів захисту, які зарекомендували себе як ефективні. Серед них застосування антивірусних програм, використання шифрування, встановлення файрволів і систем виявлення вторгнень, а також впровадження політик безпеки на рівні організації.

Принцип «defense in depth» базується на використанні кількох захисних рівнів. Це означає, що навіть у разі прориву одного бар’єру інші продовжать охороняти важливі дані та ресурси. Наприклад, комбінація мережевих файрволів, систем виявлення атак, антивірусних програм і механізмів контролю доступу створює багатошаровий захист, суттєво зменшує ймовірність успішної атаки [4].

Кіберзагрози постійно еволюціонують, тому необхідно регулярно оцінювати дієвість наявних захисних заходів. Проведення аудиту безпеки, перевірка відповідності сучасним стандартам і тестування на проникнення, які відтворюють реальні атаки, дозволяють визначити, наскільки організація готова до них реагувати. Такий підхід допомагає виявляти вразливості та вчасно їх усувати.

Внутрішні загрози можуть становити не меншу небезпеку, ніж зовнішні атаки. Вони виникають не лише через навмисні дії співробітників, а й через їхні випадкові помилки чи недбалість. Для запобігання цьому варто застосовувати контроль доступу, зокрема обмежуючи права користувачів до конфіденційної інформації. Крім того, регулярний моніторинг активності користувачів і ведення журналу їхніх дій допомагають оперативно виявляти підозрілу чи шкідливу поведінку та мінімізувати її наслідки [5].

Моделі безпеки створені, щоб визначити ключові принципи управління доступом, забезпечення приватності, збереження цілісності даних і гарантування їхньої доступності. Вони сприяють побудові компаніями надійних систем захисту, встановлюючи правила доступу до інформації та запобігаючи можливим загрозам. Системи виявлення атак (IDS) у корпоративних мережах потребують чіткого визначення прав доступу та принципів безпеки, які базуються на різних моделях. Одним із підходів є використання матриці контролю доступу, яка у табличній формі визначає користувачів, ресурси та дозволені операції (читання, запис, виконання тощо). Це дозволяє IDS ефективно моніторити та аналізувати активність, виявляючи спроби порушення встановлених політик доступу [6].

Модель Белла-ЛаПадули, орієнтована на конфіденційність, застосовується в системах із високими вимогами до захисту даних, наприклад, у державних установах. Її принципи «No Read Up» (заборона читання даних із вищого рівня безпеки) та «No Write Down» (заборона запису на нижчий рівень) допомагають IDS ідентифікувати спроби несанкціонованого доступу до конфіденційної інформації, що є критичним для захисту корпоративних мереж.

Модель Біба, навпаки, зосереджена на цілісності даних і використовує принципи «No Read Down» (заборона читання з нижчих рівнів) та «No Write Up» (заборона запису на вищий рівень). У контексті IDS ця модель сприяє виявленню змін або підробки даних, що можуть свідчити про атаку, наприклад, через введення шкідливого коду чи маніпуляцію інформацією [7].

Модель Кларка-Вілсона, популярна в комерційних системах (зокрема банківських), підходить для IDS, які контролюють цілісність транзакцій. Вона

використовує дозволені операції та проміжне програмне забезпечення для перевірки дій, що дозволяє системам виявлення атак оперативно реагувати на несанкціоновані модифікації даних у реальному часі.

Контроль доступу на основі ролей (RBAC) є ефективним для великих корпоративних мереж. Призначаючи права відповідно до ролей «Адміністратор», «Користувач», «Бухгалтер», RBAC спрощує інтеграцію з IDS, дозволяючи системі відстежувати відхилення від типової поведінки для кожної ролі. Наприклад, якщо користувач із роллю «Бухгалтер» намагається отримати доступ до системного файлу, IDS може розпізнати це як аномалію.

Модель Брюера-Неша «Chinese Wall» застосовується у фінансових і юридичних організаціях для запобігання конфлікту інтересів. У поєднанні з IDS вона допомагає виявляти спроби доступу до даних конкуруючих структур, що може свідчити про внутрішню загрозу або шпигунство.

Модель Take-Grant дозволяє аналізувати передачу прав доступу в системі. У корпоративних мережах IDS може використовувати цю модель для оцінки ризиків, пов’язаних із надмірними привілеями, виявляючи потенційні точки вразливості, через які зловмисники можуть отримати доступ до ресурсів [8].

Отже, вибір моделі безпеки для корпоративної мережі впливає на ефективність систем виявлення атак. Модель Белла-ЛаПадули підходить для захисту конфіденційності, Біба – для забезпечення цілісності, Кларка-Вілсона – для моніторингу транзакцій, а RBAC – для спрощення управління доступом і виявлення аномалій у великих організаціях.

1.2 Системи виявлення атак на вузлах

Система виявлення вторгнень (IDS) – це інструмент мережевої безпеки, який відстежує трафік та пристрої в мережі з метою виявлення відомої шкідливої активності, підозрілих дій або порушень політик безпеки (рисунок 1.1).

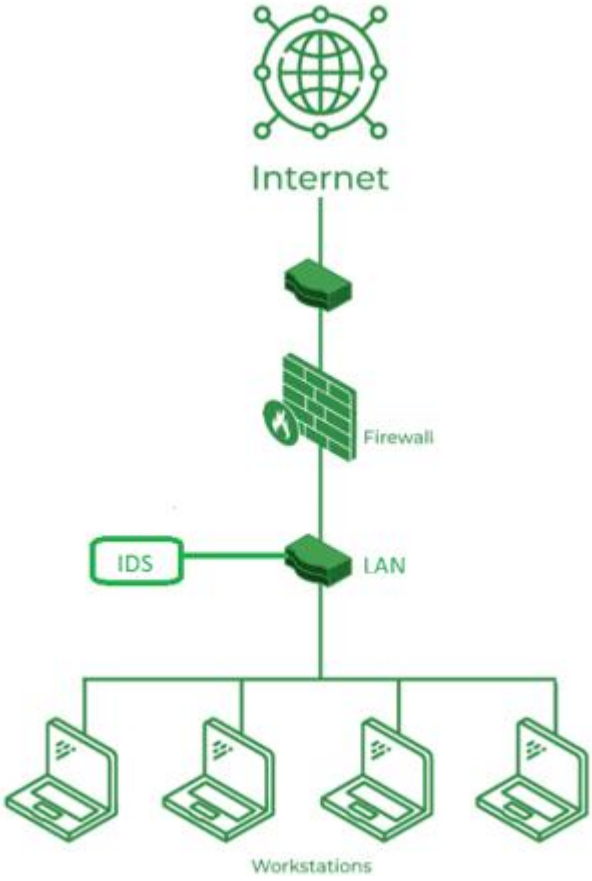


Рисунок 1.1 – Мережева інфраструктура з інтегрованою IDS

IDS дозволяє автоматизувати процес виявлення загроз, надсилаючи сповіщення адміністраторам безпеки про потенційні або виявлені атаки. Також система може передавати ці сповіщення до централізованих засобів безпеки, таких як SIEM (Security Information and Event Management), що об'єднує дані з різних джерел для точнішого аналізу та швидкого реагування на кіберзагрози, які можуть залишитися непоміченими іншими засобами захисту. Крім того, IDS допомагає організаціям виконувати вимоги нормативних актів, зокрема стандарту

PCI-DSS (Payment Card Industry Data Security Standard), який зобов'язує компанії використовувати механізми виявлення вторгнень.

IDS самостійно не може запобігати атакам. Тому сучасні системи IDS часто інтегруються з системами запобігання вторгнень (IPS), які не лише виявляють загрози, але й можуть автоматично вживати заходів для їхньої нейтралізації [9].

Основне завдання системи виявлення вторгнень (IDS) – це виявлення аномалій у мережевому трафіку до того, як зловмисники зможуть завдати шкоди мережі та підключеним пристроям. Для цього IDS використовує базу даних відомих сигнатур атак або аналізує відхилення від нормальної мережевої активності.

Після виявлення підозрілої активності система передає цю інформацію на аналіз як на рівні додатків, так і на мережевому рівні. Внутрішня робота IDS керується трьома основними компонентами [10]:

– сенсори;

– консоль;

– детектор.

Сенсори аналізують мережевий трафік і активність для виявлення загроз та ініціювання заходів безпеки.

Консоль відстежує події, надсилає сповіщення, керує відповіддю на загрози та формує звіти.

Детектор реєструє всі події безпеки, збереження сповіщень та відповідних дій у спеціальній базі даних.

Існує п'ять основних типів систем виявлення вторгнень (IDS): мережеві (NIDS), хостові (HIDS), протокольні (PIDS), на основі прикладних протоколів (APIDS) та гібридні. Найпоширенішими є мережеві та хостові IDS.

Мережева система виявлення вторгнень (Network-based IDS, NIDS) контролює всю мережеву інфраструктуру, відстежуючи трафік, що надходить до пристроїв і виходить із них. Вона розгортається у стратегічно важливих точках мережі, таких як найбільш вразливі підмережі. Система аналізує вміст мережевих пакетів і метадані, що дозволяє виявляти підозрілу активність.

Хостова система виявлення вторгнень (Host-based IDS, HIDS) HIDS встановлюється на окремі пристрої (хости) та контролює трафік, що проходить через них. Вона аналізує внутрішні та зовнішні загрози, веде журнали шкідливої активності та сповіщає відповідальних осіб про можливі загрози.

Протокольна система виявлення вторгнень (Protocol-based IDS, PIDS) встановлюється на веб-сервери та контролює взаємодію між користувачем або пристроєм і сервером. Вона аналізує специфічні мережеві протоколи та відстежує їхній стан і поведінку для виявлення відхилень від нормальних стандартів.

Система виявлення вторгнень на основі прикладних протоколів (Application Protocol-based IDS, APIDS) APIDS розташовується на рівні прикладних протоколів і контролює взаємодію між додатками. Наприклад, така система може відстежувати SQL-запити до бази даних або комунікацію між веб-сервером і програмним забезпеченням.

Hybrid IDS поєднує характеристики двох або більше підходів (наприклад, NIDS та HIDS) для забезпечення комплексного захисту. Ця система збирає та аналізує дані як із мережевих джерел, так і з окремих пристроїв, забезпечуючи ширший і точніший огляд загроз.

Гібридні системи вважаються найбільш ефективними, оскільки забезпечують комплексний моніторинг як мережевого трафіку, так і активності на окремих пристроях [11].

Системи виявлення вторгнень (IDS) можуть бути як програмними застосунками, встановленими на кінцевих пристроях, так і спеціалізованими апаратними рішеннями, що підключені до мережі. Деякі IDS також доступні у вигляді хмарних сервісів.

IDS використовують два основні методи виявлення загроз:

– сигнатурний аналіз;

– аномалійний аналіз.

Сигнатурний аналіз передбачає перевірку мережевого трафіку на наявність специфічних атак, що мають характерні ознаки або унікальні поведінкові

шаблони. Наприклад, певний фрагмент коду, який зустрічається у відомому шкідливому програмному забезпеченні, може бути сигнатурою загрози.

IDS із сигнатурним аналізом використовує базу даних атак для порівняння мережевих пакетів з відомими зразками загроз. Якщо виявлено збіг, система позначає підозрілу активність. Для ефективного функціонування така система потребує регулярного оновлення бази сигнатур, оскільки хакери постійно розробляють нові атаки, що можуть залишитися непоміченими застарілим сигнатурним аналізом.

Аномалійний аналіз використовує машинне навчання для створення базової моделі нормальної мережевої активності. Далі IDS порівнює поточний трафік з цією моделлю та виявляє відхилення, наприклад, нетипове споживання пропускної здатності або відкриття незвичайних портів.

На відміну від сигнатурного аналізу, такий метод дозволяє виявляти навіть нові та невідомі загрози, зокрема атаки нульового дня. Проте аномалійний аналіз може давати більше хибних спрацювань, оскільки навіть звичайна поведінка користувача (наприклад, перший доступ до конфіденційного ресурсу) може бути розцінена як загроза.

Менш поширені методи аналізу є:

– репутаційний аналіз;

– аналіз протоколів.

Репутаційний аналіз блокує трафік із IP-адрес або доменів, що асоціюються з небезпечною діяльністю.

Аналіз протоколів досліджує поведінку мережевих протоколів, наприклад, може виявити атаку типу DoS (Denial-of-Service), якщо одна IP-адреса одночасно відкриває надто багато з’єднань.

Незалежно від методу аналізу, коли IDS виявляє потенційну загрозу чи порушення політики безпеки, вона надсилає сповіщення команді реагування на інциденти. Крім того, система веде журнали безпеки, які можуть використовуватися для вдосконалення IDS, наприклад, шляхом оновлення сигнатур або модифікації моделі нормальної поведінки мережі [12].

Системи виявлення вторгнень ефективно виявляють аномалії та підозрілу активність, але не можуть самостійно усунути загрози. Для підвищення рівня кібербезпеки в IDS необхідно інтегрувати з іншими системами контролю, такими як система управління інформаційною безпекою та подіями (SIEM). Вона допомагає агрегувати дані, координувати їхню обробку та визначати подальші дії після виявлення нестандартної активності.

Її інтеграція з IDS, міжмережевими екранами та іншими інструментами кібербезпеки дозволяє значно прискорити реагування на загрози. Взаємодія IDS і SIEM сприяє покращенню журналювання подій, порівнянню даних і загальній узгодженості захисту середовища [13].

1.3 Класифікація атак на вузли

Мережева безпека стикається з низкою загроз, які можуть порушити стабільну роботу корпоративних систем, викрасти або знищити конфіденційні дані. Серед найпоширеніших загроз можна виділити зломи, перехоплення трафіку та DDoS-атаки.

Кіберзагрози – це дії, спрямовані на несанкціонований доступ, викрадення даних, порушення роботи інформаційних систем або завдання шкоди. Зловмисники можуть використовувати різні методи атак, серед яких шкідливе програмне забезпечення, соціальна інженерія, атаки «людина посередині» (MitM), атаки на відмову в обслуговуванні (DoS) та ін'єкційні атаки [14].

Система виявлення вторгнень (IDS) може ідентифікувати різні типи кібератак, аналізуючи трафік мережі або активність системи на наявність підозрілих патернів. Основні види атак, які виявляє IDS [15]:

- сканування;
- атаки на відмову в обслуговуванні (dos);
- атаки соціальної інженерії;
- шкідливе програмне забезпечення;

– експлойти;

– підвищення привілеїв;

– внутрішні загрози.

IDS допомагає протидіяти різним типам атак, моніторить мережевий трафік і може виявити незвично високий обсяг запитів, характерний для DDoS-атак.

Використовуючи сигнатури відомих атак або поведінковий аналіз, IDS може ідентифікувати специфічні шаблони, притаманні DDoS-атакам, такі як SYN-flood або UDP-flood.

IDS перевіряє вхідні дані на наявність шкідливих SQL-кодів, які можуть бути вставлені у форми введення або URL-запити. Система може розпізнати спроби маніпуляції з базою даних через нетипові запити або команди, що не відповідають нормальній поведінці користувачів.

IDS відстежує встановлені з'єднання та може виявити несанкціоновані перехоплення або зміни в трафіку між двома сторонами.

Система ідентифікує використання підроблених сертифікатів, спроби зниження рівня шифрування, що часто використовуються в MitM-атаках [16].

Системи виявлення вторгнень допомагають виявляти загрози, аналізуючи мережевий трафік, лог-файли та поведінкові аномалії, що дозволяє швидко реагувати на потенційні інциденти та мінімізувати їхній вплив (таблиця 1.1).

Таблиця 1.1 – Класифікація атак та їхнім зв’язком із IDS

Класифікація атак	Приклад атак	Механізм виявлення	Тип IDS
1	2	3	4
Мережеві атаки	DDoS, Man-in-the-Middle, ARP Spoofing	Аналіз трафіку, виявлення аномалій	NIDS (мережевий)
Атаки на рівні додатків	SQL Injection, XSS, CSRF	Аналіз логів, сигнатурний аналіз	HIDS (хостовий)

Кінець таблиці 1.1

1	2	3	4
Атаки на автентифікацію	Brute Force, Credential Stuffing	Виявлення підозрілих спроб входу	HIDS / NIDS
Шкідливе ПЗ (Malware)	Ransomware, Trojan, Rootkit	Моніторинг змін у файлах, евристичний аналіз	HIDS
Соціальна інженерія	Phishing, Pretexting	Аналіз вмісту електронної пошти, поведінковий аналіз	NIDS / HIDS
Експлуатація вразливостей	Buffer Overflow, Zero-day Exploits	Моніторинг аномальних процесів	NIDS / HIDS

На основі проведеної класифікації (таблиця 1.1). Сучасні кіберзагрози охоплюють широкий спектр атак, кожна з яких потребує специфічного підходу до виявлення та відповідного типу IDS. Мережеві атаки, такі як DDoS чи ARP Spoofing, ефективно відстежуються мережевими системами виявлення (NIDS) через аналіз трафіку, аномалій. Атаки на рівні додатків, наприклад SQL Injection або XSS, краще розпізнаються хостовими IDS (HIDS) завдяки аналізу логів і сигнатур. Для атак на автентифікацію, як Brute Force, підходять обидва типи систем, залежно від точки моніторингу, а боротьба зі шкідливим ПЗ, таким як ransomware чи rootkits, покладається на HIDS із евристичним аналізом і контролем змін у файлах. Соціальна інженерія, зокрема фішинг, вимагає комбінованого підходу з аналізом вмісту та поведінки, а для експлуатації вразливостей, як Zero-day Exploits, ключовим є моніторинг аномальних процесів. вибір типу IDS і

механізму виявлення залежить від природи загрози, що підкреслює важливість комплексного підходу до захисту корпоративних мереж.

1.4 Огляд систем виявлення атак

Системи виявлення та запобігання атак IDS IPS відіграють ключову роль у забезпеченні безпеки корпоративних мереж. Вони дозволяють виявляти підозрілу активність, фіксувати спроби вторгнення та в окремих випадках - автоматично реагувати на загрози. Залежно від місця встановлення та підходу до аналізу, розрізняють хостові HIDS, мережеві NIDS та комбіновані рішення. Сучасні IDS/IPS підтримують як сигнатурний, так і поведінковий методи аналізу.

Suricata позиціонується як альтернатива Snort, зберігаючи сумісність із його форматами файлів, правилами та іншими елементами, при цьому будучи безкоштовним рішенням. Вона пропонує розширені можливості, недоступні в Snort, зокрема аналіз мережевого трафіку на прикладному рівні, що дозволяє виявляти шкідливий вміст, розподілений між кількома пакетами. Розробник Zeek також пропонує пристрій, який об’єднує функціонал Suricata та Zeek в єдиному рішенні [17].

Suricata прослуховує або перехоплює мережевий трафік через вказаний мережевий інтерфейс, дозволяючи збирати дані незалежно від того, який пристрій є кінцевим одержувачем цього трафіку. Зібраний трафік у вигляді необроблених пакетів передається на синтаксичний аналіз. Suricata розбиває ці пакети на окремі компоненти: заголовки, корисне навантаження та інші специфічні для кожного протоколу дані. Suricata використовує набір правил і базу даних сигнатур для визначення шаблонів, які відповідають певним типам мережевої активності, пов'язаним з відомими загрозами. Для цього застосовуються методи зіставлення шаблонів з даними, отриманими з мережевих пакетів. Suricata може бути налаштована для глибокої перевірки пакетів. Це дозволяє аналізувати не тільки заголовки пакетів, але й вивчати їх корисне навантаження, що дозволяє виявляти

приховані загрози і збирати важливу інформацію для моніторингу мережевої безпеки. Коли Suricata виявляє загрозу або аномалію, вона виконує заздалегідь визначені дії згідно з конфігурацією. Це може бути запис події для подальшого аналізу, сповіщення персоналу служби безпеки або навіть блокування трафіку, якщо Suricata працює в режимі IPS [18].

Snort - це популярна система запобігання вторгненням (IPS) з відкритим вихідним кодом, яка використовує набір правил для виявлення шкідливої мережевої активності. Вона аналізує мережеві пакети, шукаючи відповідність заданим шаблонам, і генерує сповіщення про загрози. Snort може працювати в різних режимах: як сніфер пакетів для моніторингу трафіку, як логгер для налагодження мережевих з'єднань, або як повноцінна система IPS, що здатна блокувати загрози в реальному часі. Цю систему можна налаштувати для особистого чи корпоративного використання [19].

Декодувальник пакетів відповідає за перехоплення мережевого трафіку з заданого інтерфейсу. Він розпізнає типи протоколів, наприклад IP, TCP, UDP, ICMP, і передає ці пакети для подальшої обробки. Декодувальник є першою ланкою в обробці даних у Snort. На цьому етапі Snort використовує набір модулів для попередньої обробки трафіку. Попередні обробники можуть виконувати дефрагментацію IP-пакетів, відновлення TCP-потоків, виявлення аномалій у протоколах, а також нормалізацію даних для унеможливлення обходу сигнатур. Двигун правил - це ядро системи Snort. Саме тут застосовуються правила до попередньо обробленого трафіку. Snort порівнює вміст пакетів з базою сигнатур і визначає, чи є мережевий трафік потенційно шкідливим. Двигун підтримує як прості сигнатури, так і складні логічні умови [20].

Snort дозволяє створювати користувацькі правила, які визначають, яку мережеву активність слід вважати підозрілою або шкідливою, а також які дії слід виконувати у відповідь, наприклад, генерувати сповіщення, блокувати трафік або фіксувати подію в логах. Це дає адміністраторам можливість адаптувати систему до потреб своєї мережі, створювати правила для виявлення бекдорів, пошуку певного вмісту в пакетах, моніторингу ділянок мережі. Завдяки гнучкій системі

правил Snort може ефективно розрізняти нормальну інтернет-активність і потенційно небезпечні дії, реагуючи на загрози в режимі реального часу [20].

Wazuh - це потужна платформа з відкритим кодом для моніторингу безпеки, виявлення загроз, відповідності нормативам та реагування на інциденти. Вона поєднує в собі функціональність системи виявлення атак на хостах (HIDS), централізованого журналювання подій та засобів аналізу безпеки. Wazuh підтримує масштабування, інтеграцію з Elastic Stack (Elasticsearch, Logstash, Kibana) і пропонує агентську та безагентську архітектуру для гнучкого розгортання в корпоративних середовищах.

Wazuh Агент установлюється на кінцеві вузли (сервери, робочі станції) та відповідає за збір даних про безпеку: журнали, зміни у файлах, спроби входу, активність користувачів, тощо. Агент постійно моніторить систему та надсилає зібрану інформацію на сервер Wazuh. Сервер - центральний компонент, який отримує дані від агентів, аналізує їх за допомогою правил, кореляцій, декодування та генерує сповіщення про інциденти. Також виконує управління конфігурацією агентів. Wazuh інтегрується з Elasticsearch для зберігання та пошуку журналів безпеки, а Kibana використовується для візуалізації, створення дашбордів, пошуку інцидентів та аналітики [21].

Wazuh функціонує як хостова система виявлення вторгнень (HIDS), що дозволяє здійснювати глибокий моніторинг активності всередині операційної системи. Вона аналізує журнали подій, системні повідомлення, спроби автентифікації, а також зміни у файлах конфігурації та поведінці процесів. Завдяки використанню наборів правил і кореляції подій, Wazuh здатна розпізнати підозрілу активність, яка може свідчити про шкідливу поведінку, порушення політики безпеки чи спроби експлуатації вразливостей. Функція контролю цілісності файлів (File Integrity Monitoring) дозволяє Wazuh відслідковувати всі зміни в критично важливих системних і конфігураційних файлах. Коли файл створюється, змінюється або видаляється, система фіксує це і негайно повідомляє адміністратора. Це особливо корисно для виявлення спроб підміни файлів, що може свідчити про компрометацію системи, наприклад при встановленні бекдорів

або зміні правил доступу. Wazuh виконує збір і обробку системних логів, логів застосунків та інших джерел подій безпеки. Вона розпізнає тисячі різних форматів логів, декодує їх у структуровану форму та застосовує політики для аналізу на предмет підозрілої поведінки або відомих шаблонів атак. Це дозволяє оперативно виявляти проблеми, такі як невдалі спроби входу, використання нестандартних портів або помилки служб. Wazuh має вбудовані механізми для виявлення шкідливого програмного забезпечення, зокрема rootkit-утиліт, які намагаються приховати свою присутність у системі. Вона сканує системні каталоги, активні процеси, модулі ядра та інші критичні ділянки операційної системи, щоб виявити приховану активність. Виявлення rootkit'ів є важливою функцією, оскільки такі загрози можуть повністю контролювати заражену машину. Wazuh інтегрується з публічними базами даних вразливостей, такими як NVD (National Vulnerability Database), щоб визначати наявність відомих вразливостей у встановленому програмному забезпеченні. Вона виконує інвентаризацію програмного забезпечення, аналізує версії, та порівнює їх із відомими проблемами безпеки. Це дозволяє адміністраторам своєчасно оновлювати небезпечні пакети або змінювати конфігурації для усунення ризиків [22].

OSSEC (Open Source HIDS) - це безкоштовна система виявлення вторгнень із відкритим кодом, яка працює на рівні хосту (HIDS). Вона забезпечує захист і моніторинг систем шляхом аналізу журналів, контролю цілісності файлів, спостереження за реєстром Windows, виявлення руткітів, надає сповіщення в реальному часі та можливість автоматичного реагування на загрози. OSSEC сумісна з багатьма операційними системами, зокрема Linux, Windows, macOS, Solaris, FreeBSD та OpenBSD, і широко використовується завдяки своїй гнучкості та розвиненому функціоналу [23].

OSSEC збирає та аналізує журнали з різних систем і пристроїв, включно з Linux, Windows, macOS, а також мережевими пристроями. Він шукає шаблони, які можуть свідчити про вторгнення або підозрілу активність, і генерує попередження для адміністратора. Система регулярно перевіряє критичні файли на зміни, щоб виявити потенційні спроби несанкціонованого доступу або втручання у

конфігурації. OSSEC має механізми для виявлення rootkit-компонентів, які можуть приховувати шкідливу активність на сервері або робочій станції. Система дозволяє створювати дії у відповідь (active response) наприклад, автоматично блокувати IP-адресу, яка здійснила атаку, змінити налаштування фаєрволу, або надіслати оповіщення на електронну пошту. Структура OSSEC базується на архітектурі клієнт-сервер, що складається з кількох ключових компонентів: менеджера, агентів, правил аналізу, системи реагування та інтерфейсів сповіщення. Центральним елементом є менеджер OSSEC, який приймає дані з агентів, встановлених на хостах, і здійснює аналіз подій. Агенти відповідають за збір логів, перевірку цілісності файлів, виявлення rootkit та інші перевірки безпеки. Менеджер застосовує набір правил для виявлення підозрілої активності й ініціює відповідні дії через систему активного реагування (наприклад, блокування IP). Всі сповіщення можуть бути направлені адміністратору через консоль, email або інтегровану SIEM-платформу. Така структура дозволяє масштабовано та ефективно контролювати безпеку як окремих серверів, так і великих мереж [24].

Zeek - це платформа для моніторингу мережевого трафіку з відкритим кодом, яка орієнтована не лише на виявлення атак, а й на глибокий аналіз мережевої поведінки. На відміну від традиційних IDS-систем, що здебільшого покладаються на сигнатури, Zeek працює як аналітична система, яка розуміє контекст мережевих подій [25].

Структура та принцип роботи Zeek побудовані на модульному підході, що дозволяє йому детально аналізувати мережевий трафік, створювати лог-файли, виявляти аномалії та загрози, а також взаємодіяти з іншими компонентами інфраструктури безпеки.

Zeek працює на мережевому інтерфейсі в режимі моніторингу (promiscuous mode), використовуючи бібліотеки на зразок libpcap, щоб захоплювати весь вхідний і вихідний трафік. Він бачить не лише трафік, адресований безпосередньо хосту, на якому запущений, а й увесь потік, який проходить через дзеркальний порт або SPAN-порт. Після захоплення трафік проходить через шар обробки

пакетів, де Zeek фільтрує непотрібні дані й проводить збирання TCP-сесій. Це дозволяє йому бачити повну картину взаємодії двох вузлів (наприклад, повний HTTP-запит/відповідь). Zeek трансформує мережеву активність у події високого рівня (events), наприклад http_request, dns_request, ssh_connection тощо. Ці події передаються в скриптовий рушій для подальшої обробки. Саме ця особливість робота з подіями замість лише сірих пакетів робить Zeek потужним інструментом глибокого аналізу. У скрипті обробляються події за допомогою вбудованої мови програмування Zeek. Наприклад, можна написати скрипт, який при кожному HTTP-запиті перевіряє User-Agent або аналізує DNS-імена на предмет підозрілої активності. Це дозволяє кастомізувати поведінку системи під конкретні потреби. Zeek автоматично створює журнали (логи) для різних типів трафіку: http.log, dns.log, conn.log, ssl.log, notice.log тощо. Ці журнали структуровані у форматі TSV або JSON і легко інтегруються з іншими SIEM-рішеннями (наприклад, ELK/Elastic Stack, Splunk тощо). Також Zeek має інтегрований фреймворк інтелекту загроз (Intel Framework), який дозволяє підвантажувати зовнішні списки IOC (Indicators of Compromise) і автоматично реагувати на підозрілі з'єднання. Notice Framework - це компонент, який відповідає за створення сповіщень. Якщо скрипти визначають небажану чи підозрілу активність (наприклад, надмірну кількість запитів до DNS або передачу паролів у відкритому вигляді), вони можуть створювати повідомлення, які потрапляють у notice.log або навіть ініціювати зовнішні дії [26].

Security Onion - це безкоштовна та з відкритим кодом операційна система, спеціально розроблена для моніторингу безпеки, виявлення загроз та реагування на інциденти. Вона базується на Linux і об'єднує в собі набір популярних інструментів для аналізу мережевого трафіку, журналів та подій безпеки в єдине, готове до використання рішення [27].

Security Onion забезпечує глибоку мережеву та хостову видимість, об'єднуючи системи виявлення вторгнень, збір метаданих, повне перехоплення пакетів, аналіз файлів і використання «медових горщиків» для симуляції атак. Виявлення вторгнень (IDS) здійснюється за допомогою Suricata, яка аналізує

мережевий трафік, шукаючи сигнатури, що відповідають відомим шкідливим або підозрілим діям. Це схоже на антивірус для мережі, але гнучкіше й точніше. Мережеві метадані, які можна отримати через Zeek або Suricata, дозволяють бачити активність за основними протоколами (DNS, HTTP, FTP тощо), що створює повний контекст подій у мережі, замість лише сповіщень про загрози. Захоплення повних пакетів (Full Packet Capture) дозволяє відтворити повну картину атаки, що саме передавалося мережею, які файли, листи чи дані були переміщені. Цей процес реалізується через Stenographer або Suricata та дає змогу мати надійний «запис злочину». Аналіз файлів проводиться за допомогою Zeek і Suricata, які вміють вилучати файли з трафіку для подальшого аналізу, наприклад через інструмент Strelka, що додає до них метадані. Інструмент "медовий горщик" (Honeypot) дозволяє створити вразливий віртуальний вузол, що імітує сервіси. Будь-які спроби підключення до нього генерують сповіщення, що дозволяє відстежити спроби вторгнення. Видимість хостів реалізована через Elastic Agent, який збирає дані з кінцевих пристроїв, дозволяє робити запити в реальному часі (через osquery) і управляється централізовано через Elastic Fleet. Для пристроїв без агентів (наприклад, маршрутизаторів) підтримується збір логів через Syslog. Аналітичні інструменти включають в себе Security Onion Console (SOC) основний веб-інтерфейс платформи, де можна переглядати всі сигнали та сповіщення, згенеровані системою Suricata та іншими компонентами [28].

Системи виявлення атак є ключовим елементом забезпечення кібербезпеки, оскільки дозволяють виявляти несанкціоновану активність у мережі та на хостах. Вони аналізують мережевий трафік, журнали подій, зміни у файлах і поведінку систем, щоб вчасно ідентифікувати потенційні загрози. Такі рішення можуть працювати як на рівні мережі, так і на рівні окремих пристроїв, забезпечуючи багаторівневий захист. Вони також здатні генерувати сповіщення про підозрілу активність, блокувати атаки в реальному часі, а в деяких випадках імітувати вразливі сервіси для виявлення зловмисників. У поєднанні з інструментами аналізу та централізованим моніторингом такі системи значно підвищують рівень безпеки в корпоративному середовищі [29].

1.5 Постановка задачі

Ця робота спрямована на розробку та впровадження системи виявлення кібератак у корпоративних мережах із застосуванням інструментів системи виявлення атак, моніторингу й аналізу безпеки. Система має забезпечувати захист від загроз на мережевому та хостовому рівнях, а також безперебійну інтеграцію з інфраструктурою безпеки.

Завданням даної роботи є:

– проаналізувати актуальні загрози інформаційній безпеці;

– ознайомитися з системами виявлення атак та їхніми можливостями;

– сформувати модель загроз;

– спроєктувати архітектуру системи безпеки, яка поєднує Wazuh з Elastic Stack, pfSense, pfBlockerNG, Suricata;

– реалізувати систему виявлення атак у віртуальному середовищі з відповідними налаштуваннями всіх компонентів;

– провести тестування системи;

– оцінити ефективність виявлення загроз;

– зробити висновки щодо доцільності застосування обраної конфігурації в корпоративному середовищі.

2 ОЦІНКА ТА ВИБІР СИСТЕМ ВИЯВЛЕННЯ АТАК ДЛЯ КОРПОРАТИВНИХ МЕРЕЖ

2.1 Порівняння систем виявлення атак

Таблиця 2.1 - Порівняльна характеристика систем виявлення атак

Назва	Тип	Переваги	Недоліки	Операційна система
1	2	3	4	5
Snort	NIDS, NIPS.	Відкритий вихідний код, потужні можливості аналізу трафіку, велика бібліотека готових правил виявлення, велика спільнота, підтримка сигнатур та користувацьких правил, гнучкість налаштувань, підтримується Cisco.	Потребує високої кваліфікації для налаштування та обслуговування, обмежена продуктивність на високих швидкостях трафіку, вразлива до атак нульового дня, менш ефективна без додаткових модулів або siem-систем.	Linux, FreeBSD, Windows, macOS.
Suricata	NIDS, NIPS.	Підтримка багатопоточності дозволяє ефективно обробляти великий обсяг трафіку, підтримка різних протоколів, сумісність з правилами Snort,	Suricata потребує більше CPU та RAM, особливо при глибокому аналізі, конфігурація та оптимізація можуть бути складними, потреба у підтримці правил,	Linux, FreeBSD, Windows, macOS.

Продовження таблиці 2.1

1	2	3	4	5
		вбудоване журналювання, можливість оффлайн аналізу, активна розробка та підтримка.	може не виявити нові типи атак.	
Wazuh	HIDS.	Об’єднує hids, fim, аналіз журналів, виявлення rootkit, контроль політик, вразливостей в одному інструменті, безкоштовно з відкритим кодом, підтримує тисячі агентів з можливістю централізованого керування, інтеграція з elastic stack, підтримка хмар та контейнерів, автоматизація реакцій на інциденти.	Високе навантаження на ресурси, агенти можуть конфліктувати з антивірусами особливо в windows середовищах.	Linux, Windows, macOS, FreeBSD, Solaris, AIX, HP-UX.
Ossec	HIDS.	Безкоштовно та з відкритим кодом, підтримка великої кількості платформ	Вбудований GUI мінімальний, для зручної візуалізації потрібно інтегрувати з іншими платформами,	Linux, Windows, macOS, FreeBSD.

Продовження таблиці 2.1

1	2	3	4	5
		інтегрований лог-аналіз, моніторинг цілісності файлів, здатний обробляти журнали різних сервісів, ssh, apache, тощо, має базові механізми пошуку rootkit, інтеграція з siem.	механізм реакцій є, але не настільки гнучкий або потужний, як у Wazuh.	
Zeek	NIDS.	Працює на рівні мережі аналізує пакети, але не виконує фільтрацію або блокування, замість сигнатур, виявляє аномалії, нестандартну поведінку, порушення логіки, пише детальні логи HTTP, DNS, SSL/TLS, FTP, SSH, IRC, розбирає високорівневі протоколи, фіксує детальну інформацію про з’єднання,	Zeek не блокує трафік, а лише моніторить і логує тому, потрібна інтеграція з іншими системами для реакції, при обробці великого трафіку потребує потужного апаратного забезпечення, обмежена підтримка Windows.	Linux, FreeBSD, macOS.

Кінець таблиці 2.1

1	2	3	4	5
		власна мова сценаріїв дозволяє створювати складні політики виявлення загроз, пасивний режим роботи, генерує структуровані логи про кожну сесію, протокол, аномалію, підтримує експорт логів у Elastic Stack.		
Security Onion	NIDS, HIDS.	Встановлення одного дистрибутива надає повноцінну систему моніторингу безпеки, Об’єднує Zeek, Suricata, Wazuh, Kibana, Fleet, TheHive, CyberChef та інші, контролює як трафік у мережі, так і події на хостах, підтримує архітектури з кількома сенсорами, серверами, Активна спільнота і документація.	Через велику кількість інтегрованих компонентів потрібне потужне обладнання, переважно орієнтовано на Linux.	Linux.

У сучасній кібербезпеці існують різні типи систем виявлення атак: мережеві IDS (NIDS), хостові IDS (HIDS) та комплексні рішення. У таблиці 2.1 розглянуто шість популярних відкритих систем: Wazuh, Suricata, Zeek, OSSEC, Security Onion і Snort, їхній тип, функції, переваги, недоліки та підтримку ОС.

Snort (NIDS/IPS). Класичний вибір для мережевого моніторингу та запобігання вторгнень. Snort добре підходить для середнього навантаження і має гнучкість правил. Його доцільно використовувати там, де є знайомий із ним персонал і досвід адаптації правил. Snort часто комбінують з Wazuh або OSSEC. Так Snort забезпечує мережевий захист, а Wazuh хостовий. Альтернативно Suricata, може замінити Snort у багатьох випадках завдяки кращій продуктивності, але Snort залишається «стандартом» [30].

Wazuh (HIDS/SIEM). Рекомендується для середовищ, де потрібен детальний хостовий моніторинг, та централізований збір логів. Підходить для організацій, які вже користуються ELK або потребують відповідності стандартам (PCI, NIST тощо). Wazuh ідеально комбінується з мережею мережевими сенсорами – наприклад, Suricata чи Snort. Як рекомендують користувачі, «Wazuh – перший вибір для HIDS на Linux, а Snort/Suricata для NIDS». Тобто варто використовувати Wazuh разом з Suricata для повноцінного охоплення (Wazuh+Suricata доволі поширений і налаштовується підготовленими прикладами) [31].

Suricata (NIDS/IPS). Рекомендується у середовищах з високошвидкісним трафіком, де необхідно виявляти складні мережеві загрози. Через багатопотоковість і підтримку сучасних протоколів вона добре масштабується для великих мереж. Suricata можна комбінувати з хостовим моніторингом (Wazuh або OSSEC) для комплексного захисту. Її часто використовують разом з Zeek, Suricata фіксує сигнатури і метадані, а Zeek глибокі події протоколів. Security Onion є прикладом поєднання Suricata Zeek Wazuh у межах однієї системи.

Zeek (мережева NSM). Рекомендується, коли потрібен детальний аналіз мережі й кореляція подій. Підходить для побудови центру аналізу інцидентів, SOC, де важлива видимість на рівні додатків. Разом із Suricata (який ловить сигнатури) Zeek забезпечить повну картину трафіку, таку комбінацію часто

використовують у Security Onion. Водночас Zeek не є самостійним засобом блокування, йому доповнюють реальний захист правилами.

OSSEC (HIDS). Рекомендується малим та середнім організаціям, які потребують базового захисту кінцевих точок без великих витрат ресурсів. OSSEC легше розгорнути, ніж складні SIEM, саме тому менші компанії віддають перевагу OSSEC чи Wazuh через простоту використання та менші системні вимоги. OSSEC ефективний для центрального аналізу логів та перевірки цілісності на серверах. Проте для великих комплексних середовищ можливостей може не вистачити [32].

Security Onion (NSM-платформа). Варто обирати, коли потрібне комплексне рішення з підключенням багатьох інструментів. Це оптимальний вибір для великих підприємств і SOC, які готові інвестувати у підготовку персоналу. Security Onion дозволяє централізовано відслідковувати і корелювати події мережі та хостів; він підходить для середовищ з великим трафіком і складною інфраструктурою [33].

Найефективніші рішення зазвичай поєднують HIDS і NIDS. Наприклад, зв’язка Wazuh та Suricata поєднує збирання логів з хостів і аналіз мережі. Wazuh і Zeek забезпечить глибокий аналіз мережі на додачу до безпеки пристроїв. Security Onion фактично вже є поєднанням інструментів (Snort,Suricata, Zeek, Wazuh та ін.), тому його можна розглядати як вбудований багатокомпонентний набір. У маленькій інфраструктурі можна почати з одного-двох інструментів, а зростаючи додавати решту. Для невеликої компанії найчастіше достатньо розгорнути HIDS на критичних серверах і, можливо, легкий NIDS на межі мережі. За оцінками експертів, OSSEC,Wazuh - найпростіші у підтримці та вимогливіші до ресурсів. Для великого підприємства оптимально встановити централізовану платформу SIEM/HIDS, по всій мережі декілька сенсорів і повний доступ до збережених пакетів. У такому випадку поєднуються механізми на пристрої та в мережі для глибокого аналізу [34].

Таблиця 2.2 Порівняння ключових можливостей систем виявлення атак

Назва IDS	Snort	Suricata	Zeek	Wazuh	OSSEC	Security Onion
NIDS	+	+	+	-	+	+
HIDS	-	-	-	+	+	+
Виявлення по сигнатурам	+	+	-	+	+	+
Виявлення по поведінці	-	+	+	+	+	+
Контроль цілісності файлів	-	-	-	+	+	+
Аналіз журналів	-	-	+	+	+	+
Підтримка Honeypot	-	-	-	-	-	+
Аналіз трафіку	+	+	+	-	-	+
Повне захоплення пакетів	+	+	+	-	-	+
Веб інтерфейс	-	-	-	+	-	+

Відповідно до таблиці 2.2 кожна система виявлення вторгнень має власні унікальні особливості та переваги, які роблять її більш ефективною в певних умовах. Порівняння таких інструментів за різними критеріями, функціональними можливостями, гнучкістю налаштувань, інтеграцією з іншими системами та рівнем автоматизації, дозволяє обрати рішення для конкретного середовища або

організації. Такий аналіз допомагає краще зрозуміти сильні та слабкі сторони кожного з інструментів.

2.2 Вибір та обґрунтування системи для реалізації

Для побудови системи виявлення та запобігання атак у корпоративній мережі було прийнято рішення використати комбінацію інструментів Suricata та Wazuh. Такий вибір обумовлений необхідністю забезпечення як глибокого аналізу мережевого трафіку, так і комплексного моніторингу хостів.

Suricata підтримує розширений аналіз мережевого трафіку в реальному часі. На відміну від деяких інших рішень, вона дозволяє здійснювати не лише сигнатурне виявлення атак, а й аналіз потоків, HTTP-запитів, DNS, TLS і навіть витяг файлів із трафіку. Suricata також підтримує багатопоточність, що робить її придатною для високонавантажених мереж. Вона сумісна з сигнатурами Snort, а це значить, що її можна гнучко налаштовувати під конкретні потреби організації.

Wazuh доповнює Suricata, виконуючи роль хостової IDS. Це рішення дозволяє аналізувати журнали систем, контролювати цілісність файлів, виявляти rootkit, здійснювати моніторинг конфігурацій, керувати вразливостями та реалізовувати відповідні політики безпеки. Wazuh має потужну інтеграцію з Elastic Stack, що дозволяє зручно візуалізувати події та аналітику, а також реалізовувати централізоване управління з агентами на віддалених пристроях.

Комбінування Suricata (мережевий рівень) і Wazuh (хостовий рівень) забезпечує багаторівневий захист:

Suricata дозволяє виявити спроби проникнення або підозрілу активність у трафіку до того, як вона досягне хостів.

Wazuh, у свою чергу, моніторить уже внутрішню активність систем, включаючи модифікацію файлів, спроби ескалації прав, несанкціоновані доступи.

PfSense - це відкрите, вільнодоступне мережеве програмне забезпечення на базі FreeBSD, яке функціонує як повноцінний фаєрвол та маршрутизатор, а також

пропонує широкий набір можливостей для забезпечення мережевої безпеки. Його можна встановити як на фізичний сервер, так і віртуальне середовище, а зручний веб-інтерфейс адміністрування дозволяє керувати всіма функціями без необхідності роботи в командному рядку [35].

Серед основних можливостей pfSense [36]:

– фільтрація трафіку;
– NAT (мережева адресація);
– VPN (OpenVPN, IPsec, WireGuard);
– підтримка VLAN;
– моніторинг та журналювання трафіку;
– інтеграція з IDS/IPS-системами, такими як Suricata або Snort;
– підтримка багатьох плагінів через систему пакетів.

Таке поєднання дозволяє не лише оперативно реагувати на інциденти, а й здійснювати глибоку кореляцію подій, що підвищує ефективність виявлення загроз і зменшує кількість хибнопозитивних спрацювань. Однією з важливих переваг pfSense є те, що вона дозволяє безпосередньо інтегрувати такі IDS/IPS, як Suricata, у сам фаєрвол через систему пакетів. Це означає, що Suricata може бути встановлена і сконфігурована як розширення pfSense, забезпечуючи повноцінне виявлення атак безпосередньо на рівні шлюзу. Таким чином, з одного пристрою можна керувати як фільтрацією, так і аналізом трафіку. PfSense виконує роль першої лінії оборони - фільтрує трафік відповідно до правил доступу, контролює з'єднання, дозволяє обмеження на підставі IP-адрес, портів, протоколів тощо. Це забезпечує базовий рівень захисту ще до того, як трафік потрапить до систем IDS або кінцевих точок. PfSense може бути налаштований для дзеркалювання трафіку (наприклад, через порт span або через NetFlow), що дозволяє дублювати трафік для подальшого аналізу засобами Wazuh або Zeek. Це критично важливо для повного аналізу подій без втручання в реальний трафік [36].

У поєднанні з Suricata та Wazuh, pfSense створює багаторівневу архітектуру захисту, де кожен рівень посилює інший, забезпечуючи як фільтрацію на мережевому рівні, так і детальне виявлення атак, а також моніторинг хостів.

Розширення pfBlockerNG для pfSense, додає функції блокування IP-адрес та DNS, фільтрації контенту, геолокаційної фільтрації та захисту від шкідливого трафіку. Його основна мета запобігти взаємодії з потенційно шкідливими, небажаними або невідомими ресурсами ще на рівні мережевого шлюзу. pfBlockerNG дозволяє імпортувати великі списки IP-адрес з відкритих джерел, таких як Spamhaus, Emerging Threats, DShield, тощо. Ці списки можна використовувати для автоматичного блокування відомих джерел атак, ботнетів, спам-серверів та інших небезпечних хостів. Інтерфейс pfBlockerNG дозволяє переглядати лог-файли, статистику заблокованих IP та DNS-запитів, а також генерувати звіти для аналізу. DNSBL (DNS Blacklist) дозволяє створити локальний DNS-сервер, який блокує доступ до доменів, що потрапили до чорного списку (рекламні, трекери, шкідливі домени тощо). Якщо клієнт намагається звернутися до такого домену, запит просто не виконується або перенаправляється на порожню сторінку [37].

Переваги використання pfBlockerNG [37]:

– ще до досягнення пристроїв в мережі, підозрілий трафік буде заблоковано;
– зниження ризику інфікування;
– зменшення небажаного контенту;
– гнучкість налаштування;
– зручність інтеграції з існуючою інфраструктурою pfSense.

pfBlockerNG забезпечує проактивну фільтрацію на рівні шлюзу, знижує ризики атак і дозволяє керувати мережевим трафіком.

Elastic Stack використовується як основна платформа для зберігання та аналізу подій, які генерують інструменти моніторингу, зокрема Wazuh.

Основним компонентом є розподілена пошукова та аналітична система, яка виступає в ролі бази даних. Вона зберігає структуровані події, отримані від агентів безпеки, з можливістю здійснювати швидкий пошук, фільтрацію та аналітику. Elasticsearch підтримує масштабування, високу доступність і ефективно обробляє великі обсяги даних.

Для передачі логів у систему використовується Filebeat легкий агент із сімейства Beats. Він зчитує події з лог-файлів (наприклад, alerts.json від Wazuh) і передає їх у Elasticsearch. Filebeat простий у налаштуванні та підтримує шифрування трафіку, забезпечуючи захист даних під час передачі.

Kibana дозволяє переглядати, аналізувати та створювати дашборди на основі даних з Elasticsearch. Завдяки офіційному плагіну від Wazuh, користувачі отримують зручні панелі з інформацією про безпекові події, попередження, журнали агентів, а також інтеграцію з MITRE ATT&CK.

Загалом, Elastic Stack забезпечує повноцінну SIEM-платформу централізований аналіз подій безпеки з гнучкою фільтрацією, ефективною індексацією та широкими можливостями візуалізації, що робить його незамінним інструментом у сучасних корпоративних мережах.

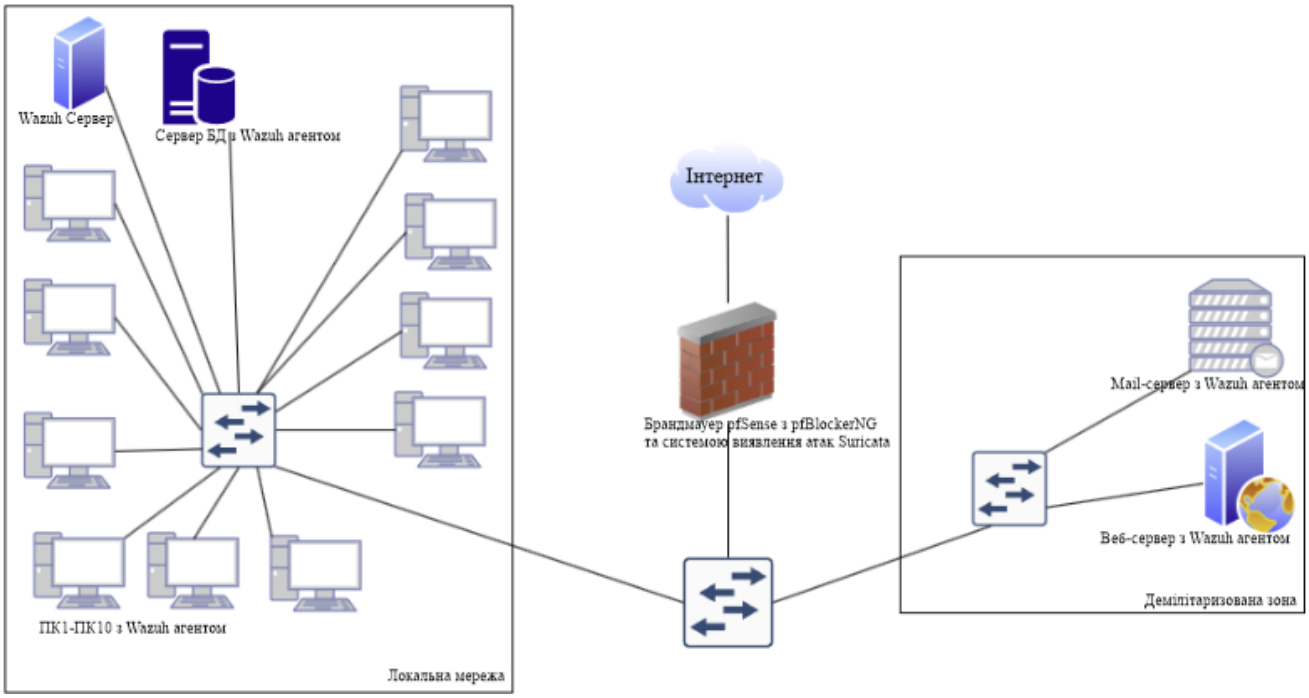


Рисунок 2.1 – Схема корпоративної мережі

На рисунку 2.1 зображено архітектуру інтегрованої системи захисту мережі, яка поєднує брандмауер, систему виявлення атак та систему централізованого моніторингу подій безпеки. Основні компоненти включають агенти Wazuh на кінцевих пристроях, централізований сервер Wazuh зі сховищем даних,

мережевий шлюз з pfSense, а також ізольовану демілітаризовану зону (DMZ) із зовнішніми серверами. Демілітаризована зона слугує додатковим рівнем безпеки, у якому розташовуються публічні веб і поштові сервери, ізольовані від внутрішньої мережі, завдяки такому підходу зовнішні користувачі можуть спілкуватися тільки з ресурсами у DMZ, а внутрішня LAN лишається недоступною для прямих атак.

У внутрішній мережі підприємства на кожному кінцевому комп'ютері встановлено Wazuh-агент, що виконує роль системи виявлення вторгнень на рівні пристроїв (HIDS). Агенти Wazuh збирають і відсилають на сервер події безпеки: системні журнали, повідомлення про входи користувачів, зміни у конфігураціях та цілісності файлів тощо. Цей механізм походить від розробки OSSEC – відомої HIDS, яка забезпечує аналіз логів, перевірку цілісності та генерацію тривожних повідомлень у реальному часі. Отже, агенти Wazuh виконують моніторинг подій на кінцевих точках і передають їх до центральної системи для подальшого аналізу.

Центральний сервер Wazuh отримує дані від агентів через захищене з'єднання і виконує їхню обробку. На сервері працює аналітичний рушій, що декодує отримані події та перевіряє їх за заздалегідь визначеними правилами виявлення. Якщо подія задовольняє умови правила, генерується тривожний сигнал із зазначенням ідентифікатору правила та опису інциденту. Усі події надходять до серверних логів. Незалежно від спрацювання правила, вони зберігаються в архівних журналах, а події із високим пріоритетом у файлі тривог. Для збереження та індексації великих обсягів даних передбачено окремий сервер бази даних (індексатор). Wazuh-сервер передає відібрані повідомлення у сховище даних (ElasticSearch, OpenSearch), використовуючи компонент Filebeat із шифруванням TLS. Цей розподіл ролей (менеджер і індексатор на різних хостах) забезпечує масштабованість і швидкий пошук у накопичених даних

На кордоні внутрішньої мережі розташовано маршрутизатор з відкритим брандмауером pfSense. pfSense реалізує функції маршрутизації та фільтрації трафіку. Він контролює потоки між Інтернетом, DMZ та локальною мережею, виконує NAT і додаткові мережеві сервіси. На цьому шлюзі встановлено пакет

pfBlockerNG модуль для автоматичного застосування списків блокування. pfBlockerNG регулярно оновлює чорні списки доменів і IP-адрес, що є шкідливими або небажаними, та додає відповідні правила до фільтра pfSense. Це дозволяє відсікати трафік із відомих джерел загроз ще на рівні мережевого екрану, зменшуючи навантаження на систему виявлення загроз. Поряд із цим на pfSense запущено Suricata систему мережевого виявлення та запобігання вторгненням (IDS/IPS). Suricata аналізує весь пакетний трафік, що проходить через інтерфейси шлюзу, перевіряючи його за наборами сигнатур і правил. У разі виявлення підозрілих патернів (сканування портів, DoS-атаки тощо) Suricata генерує відповідні події в логах.

Взаємодія компонентів організована за принципом централізованого збору і аналізу даних. Кожен Wazuh-агент на локальних ПК і серверах встановлює постійне з'єднання з центральним сервером і відправляє туди зібрані події. Сервер Wazuh, у свою чергу, декодує ці повідомлення та оцінює їх проти вбудованих правил виявлення. У разі спрацьовування правила інформація про інцидент зберігається в тривожних логах, а також передається через Filebeat до індексатора бази даних. Накопичені події у базі даних ElasticSearch, OpenSearch можуть аналізуються в режимі реального часу, за допомогою Wazuh Dashboard і корелюватися для побудови загальної картини стану безпеки.

Прикладом обробки мережевих подій є робота Suricata, якщо система IDS зафіксувала підозрілу активність, вона генерує лог-повідомлення у спеціальному файлі. Агент Wazuh зчитує цей файл і надсилає події до Wazuh-сервера, де вони аналізуються разом з іншими подіями. Таким чином, інформація від Suricata потрапляє до загальної SIEM системи. Одночасно pfBlockerNG блокує небажані підключення ще на рівні шлюзу за списками репутації, тому частина загроз блокуються до появи будь-яких подій. Система забезпечує комбіноване виявлення на рівні хостів агенти Wazuh, мережевих шлюзів Suricata та фільтрації доступу, даючи можливість оперативно реагувати на інциденти в будь-якій зоні мережі. Отже, така архітектура забезпечує централізоване збереження та аналіз журналів подій з усіх компонентів, а також швидке на отримані сповіщення.

2.3 Висновки

У рамках дослідження було здійснено огляд різних рішень у сфері систем виявлення атак IDS IPS, включаючи як мережеві, так і хостові інструменти. Аналіз охоплював ключові характеристики систем, такі як методи виявлення загроз (сигнатурний, аномальний, гібридний), інтеграції, адміністрування.

Було проведено детальне порівняння систем за функціональними ознаками, такими як обробка подій у реальному часі, підтримка журналювання, можливості фільтрації трафіку, аналітика, централізоване управління, виявлення по сигнатурам та поведінці, контроль цілісності файлів, аналіз журналів, підтримка honeypot, аналіз трафіку, захоплення пакетів, веб інтерфейс. Це дозволило виявити найбільш ефективні рішення для побудови сучасної та надійної системи кіберзахисту.

На основі зібраної інформації та порівняння було обґрунтовано вибір наступних інструментів:

- системи виявлення атак Suricata;
- платформи Wazuh для моніторингу безпеки хостів, кореляції подій;
- брандмауера pfSense з підтримкою додаткових модулів;
- платформа Elastic Stack для збору, зберігання, аналізу та візуалізації логів.

Система забезпечує виявлення, реагування та аналіз інцидентів безпеки, дозволяє обробляти великі обсяги інформації. Це створює основу для побудови ефективного комплексу захисту, здатного своєчасно виявляти загрози, блокувати підозрілу активність.

3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ СИСТЕМ ВИЯВЛЕННЯ АТАК В КОРПОРАТИВНИХ МЕРЕЖАХ

3.1 Алгоритм роботи системи виявлення атак

Для системи виявлення атак у корпоративній мережі обрано комбінацію з кількох компонентів. В якості міжмережевого екрану використано pfSense, як систему мережевого виявлення атак Suricata, для хостового моніторингу Wazuh, а для збору, обробки і візуалізації логів Elastic Stack.

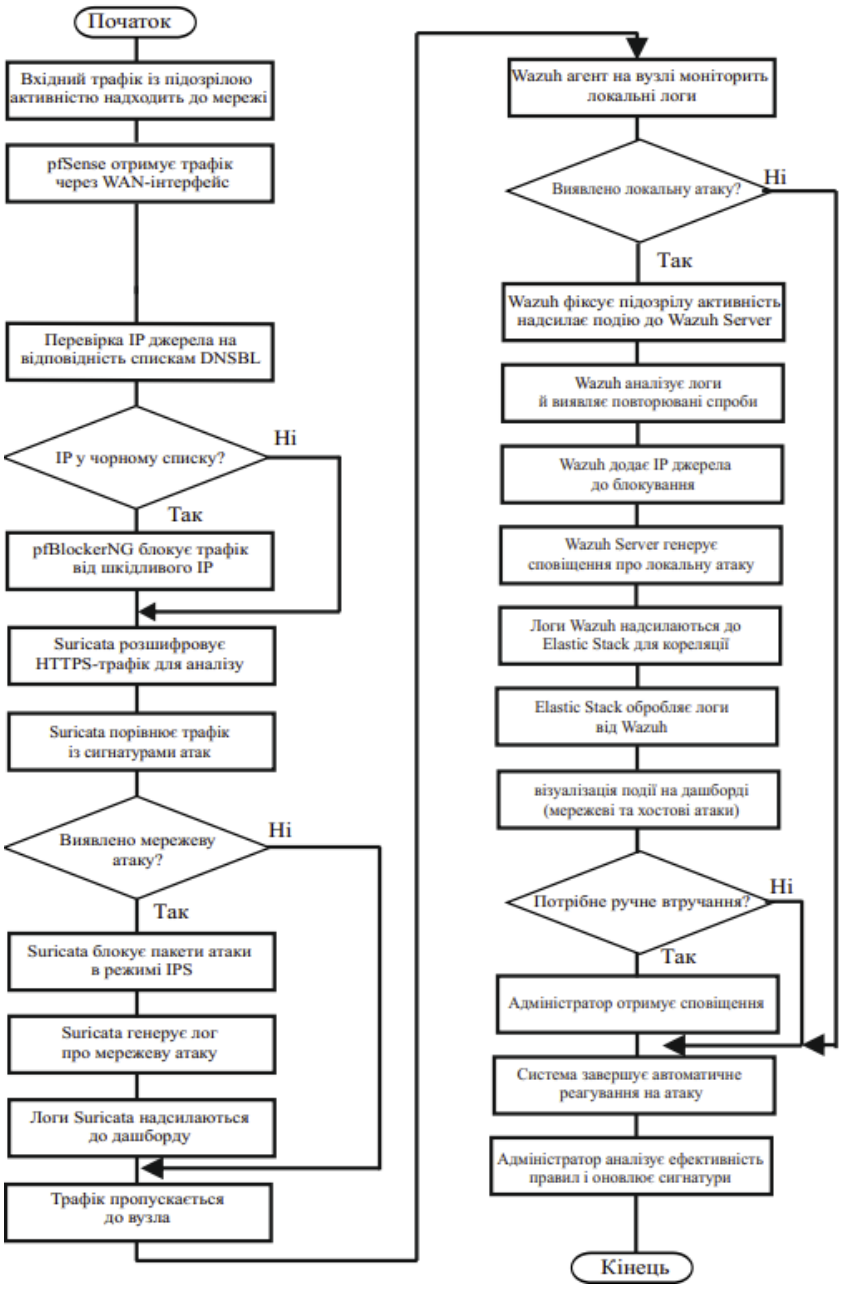


Рисунок 3.1 – Алгоритм роботи системи виявлення атак

На рисунку 3.1 система починається з того, що вхідний трафік надходить на мережевий шлюз pfSense через WAN-інтерфейс. За допомогою пакета pfBlockerNG у pfSense здійснюється перевірка IP-адреси джерела на наявність у чорних списках (DNSBL). pfBlockerNG використовує групи блокувальних списків (IP- та DNS-блок-листи), які містять відомі зловмисні адреси, шкідливі домени, боти та інші загрози. Якщо IP знаходиться у одному з DNSBL-списків, то pfBlockerNG негайно блокує весь трафік від цього джерела. Мережевий трафік фільтрується за відомими адресами та запобігає небажаним з'єднанням. Якщо джерело не було заблоковане на цьому етапі, трафік передається далі для детальнішої перевірки.

Наступний етап - аналіз трафіку в режимі IDS/IPS за допомогою Suricata, яка у реальному часі інспектує пакети, розшифровує трафік та порівнює їх із базою сигнатур відомих атак. Після декодування Suricata перевіряє зміст пакетів проти налаштованих правил. Якщо правилами виявлено зловмисну активність, Suricata в режимі IPS блокує ці пакети та фіксує подію атаки. Лог про виявлену мережеву атаку генерується і передається в систему зберігання подій. Якщо атакуючий трафік виявлено, Suricata негайно блокує подальші пакети цього з'єднання, відсилає подію до логів і лише потім пропускає безпечний трафік до внутрішньої мережі.

Паралельно з аналізом мережевого трафіку на вузлах мережі працює Wazuh хостова система виявлення вторгнень. На кожному сервері чи робочій станції встановлено Wazuh-агент, який стежить за локальними логами і пересилає їх на центральний Wazuh-сервер. Агент негайно реагує на підозрілі події. Наприклад, багаторазові невдалі спроби входу або інші сигнали атаки і відправляє відповідні повідомлення до центральної системи. Якщо Wazuh-агент виявляє локальну атаку, він фіксує цю підозрілу активність і формує подію для Wazuh-сервера. Там вона аналізується з використанням настроєних правил та кореляцій. При виявленні повторюваних спроб вторгнення Wazuh може автоматично запускати модуль «Active Response» – наприклад, виконує скрипт firewall-drop, який додає IP-адресу зловмисника до локального брандмауеру (iptables) для тимчасового

блокування. Таким чином система блокує локальне джерело атаки на рівні хоста. Крім того, Wazuh-сервер генерує оповіщення про виявлену локальну атаку і реєструє її у своїх логах.

Логи з Wazuh збираються та надходять у Elastic Stack. Suricata зазвичай записує свої JSON логи у файл, який може бути переданий в Elastic. Аналогічно, Wazuh надсилає свої зібрані події до центрального сховища. Обидва типи подій індексуються в Elasticsearch. Elastic Stack корелює мережеві і хостові сповіщення, дозволяючи на панелі візуалізувати локальні інциденти з Wazuh. Візуалізація даних дає можливість аналізувати тренди, кількість спроб атак, геолокацію джерел та інші метрики. Wazuh постачає плагін для Kibana, який забезпечує готові дашборди для моніторингу статусу агента, запитів і візуалізації сповіщень. Після того, як система виконала попереднє реагування, Elastic Stack виводить інформацію про інциденти на дашборд. Якщо спрацьовує правило, яке вимагає ручного втручання або якщо подія класифікується як критична, адміністратор отримує сповіщення. Адміністратор оцінює подію, вирішує, чи потрібно продовжити автоматичну обробку, і при необхідності змінює правила. На цьому етапі система завершує автоматичні дії і очікує на коригування. Саме адміністратор аналізує ефективність правил безпеки і вдосконалює їх. Він може змінити або створити власні сигнатури і правила для виключення хибних спрацьовувань або підвищення чутливості до нових векторів атак. Wazuh дозволяє додавати й налаштовувати кастомні правила та декодери під конкретне середовище.

Задача адміністратора полягає в постійному аналізі інцидентів, оновленні сигнатур та оптимізації списків блокування. Це забезпечує адаптивність системи й підвищує рівень захисту на основі реального досвіду і нових загроз.

3.2 Конфігурація системи Wazuh

У цьому розділі розглядається конфігурація системи Wazuh, її основні компоненти, принципи роботи, роль у підвищенні захищеності корпоративної мережі.

Система Wazuh складається з Wazuh Manager, агентів, модуля моніторингу цілісності файлів, системи збору логів, механізмів активного реагування та інтеграції з Elastic Stack. Wazuh Manager є центральним вузлом, який отримує та аналізує дані від агентів, що встановлюються на кінцеві пристрої, такі як сервери та робочі станції. Агенти Wazuh збирають логи, моніторять активність системи, зміну файлів та передають цю інформацію на менеджер. Компонент моніторингу цілісності файлів дозволяє відстежувати зміни у важливих системних файлах, що є важливим для виявлення атак або змін, зроблених вручну або зловмисниками. Зібрані дані можуть автоматично передаватися в Elasticsearch, де зберігаються та візуалізуються через Kibana, що дає змогу швидко аналізувати події безпеки.

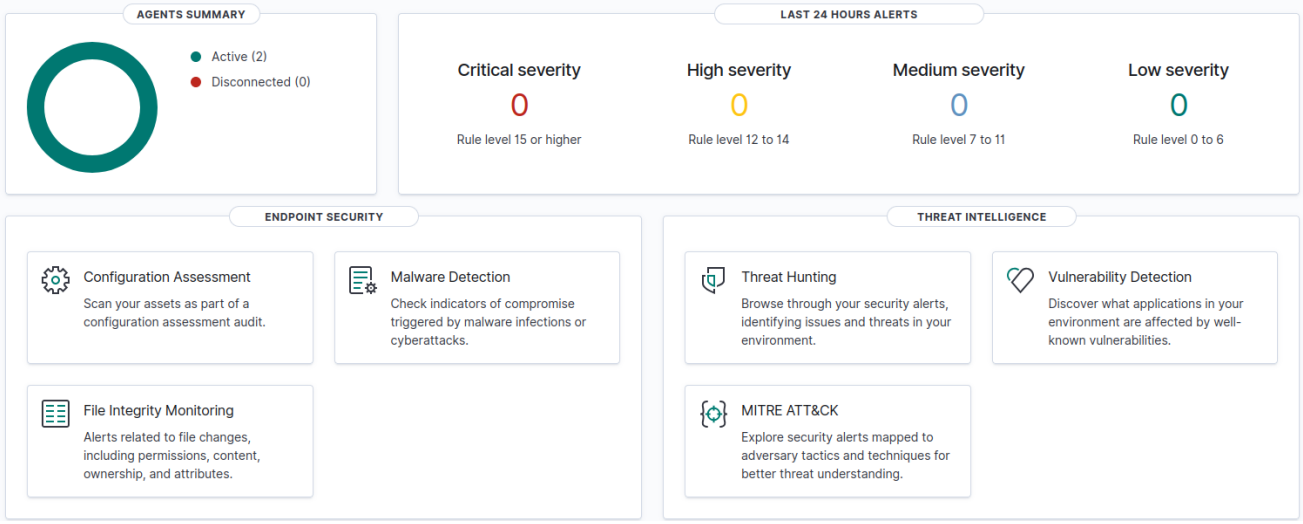


Рисунок 3.2 – Панель моніторингу системи Wazuh

На рисунку 3.2 представлено головну панель моніторингу системи Wazuh, яка відображає загальний стан агентів та безпекову інформацію за останні 24 години.

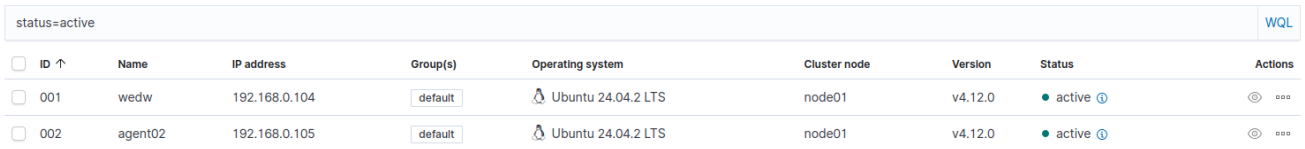


Рисунок 3.3 – Список агентів системи Wazuh

На рисунку 3.3 показано список активних агентів у системі Wazuh. Відображено два агенти з іменами wedw та agent02, які працюють на ОС Ubuntu 24.04 LTS, мають IP-адреси 192.168.0.104 та 192.168.0.105. Обидва належать до групи default, входять до вузла node01 кластера.

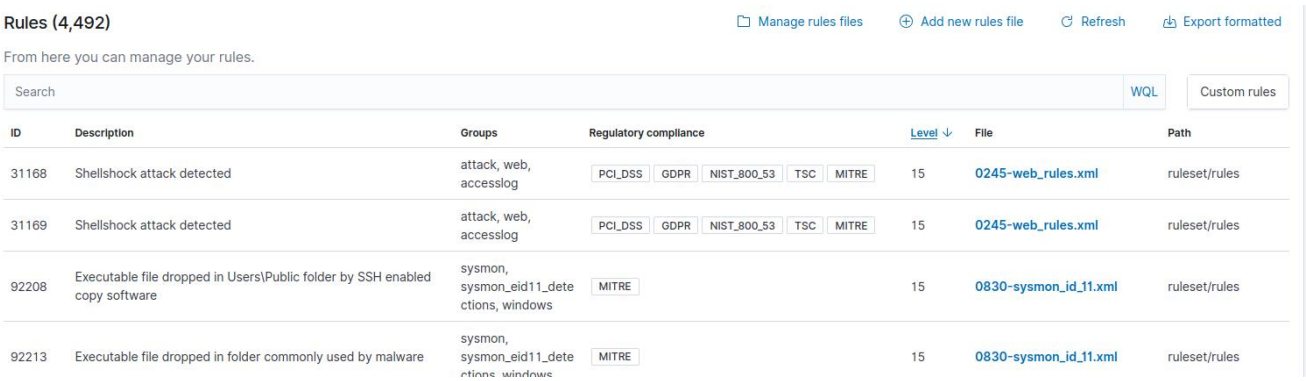


Рисунок 3.4 – Список правил системи Wazuh

Рисунок 3.4 демонструє розділ правил, де перелічені 4492 активні правила, що застосовуються для аналізу подій.

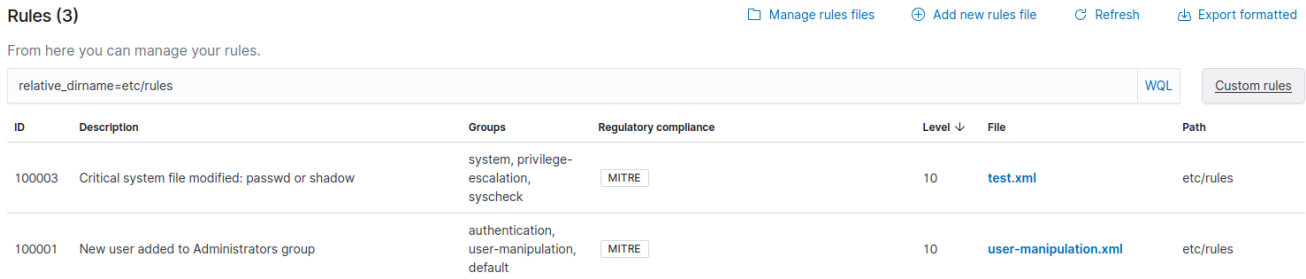


Рисунок 3.5 – Список користувацьких правил Wazuh

На рисунку 3.5 зображено розділ правил Wazuh, який показує користувацькі правила безпеки, розміщені у директорії etc/rules.

Перше правило фіксує зміну критичних системних файлів, зокрема passwd або shadow, що потенційно свідчить про ескалацію привілеїв. Відноситься до груп system, privilege-escalation і syscheck. Зберігається у файлі test.xml.

Друге правило спрацьовує при додаванні нового користувача до групи адміністраторів, що також може бути ознакою несанкціонованого втручання. Входить до груп authentication, user-manipulation і default, зберігається у файлі user-manipulation.xml.

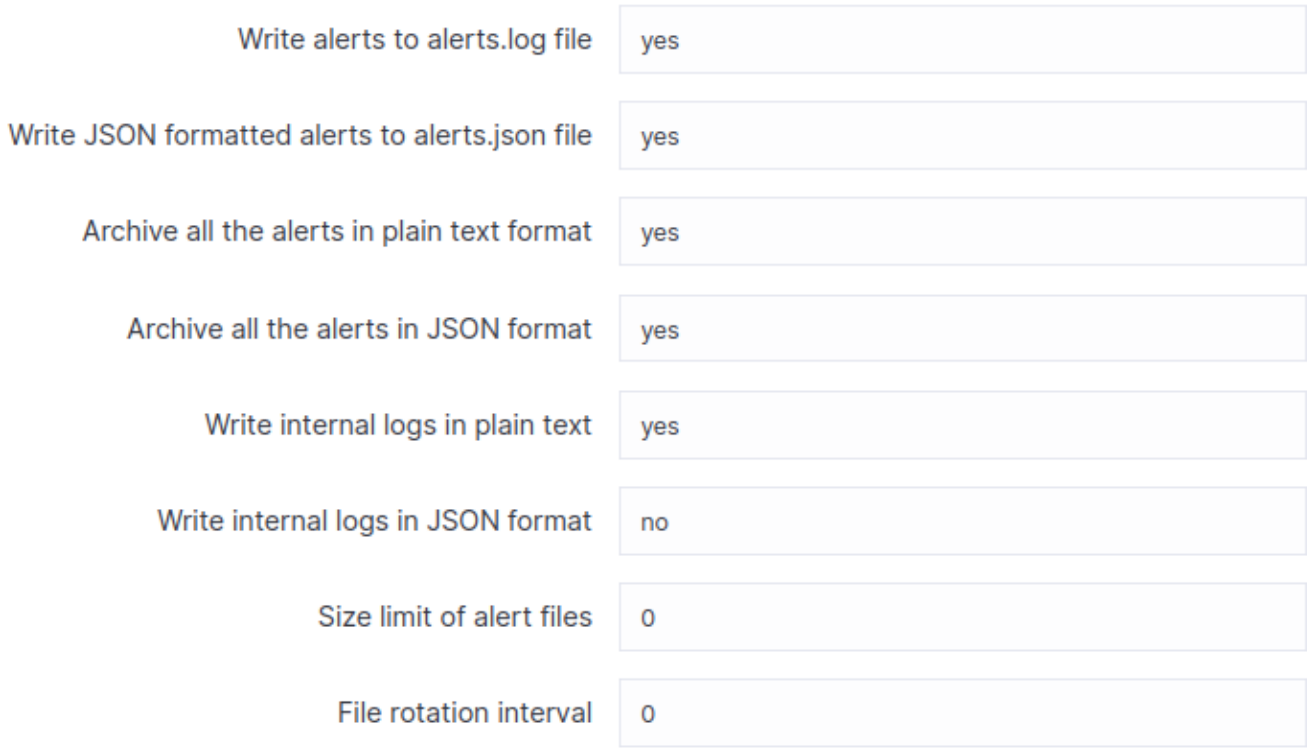


Рисунок 3.6 – Налаштування оповіщень у системі Wazuh

Усі оповіщення записуються у файл alerts.log у звичайному текстовому форматі, та у форматі JSON у файл alerts.json. Увімкнено архівацію всіх оповіщень як у текстовому, так і в JSON форматах. Внутрішні логи системи зберігаються лише у звичайному текстовому вигляді, без формату JSON рисунок 3.6.

Рисунок 3.7 – Налаштування політики моніторингу у Wazuh

Цей рисунок 3.7 містить налаштування політики моніторингу системи. У ньому активовано службу моніторингу політик, яка виконує сканування кожні 43200 секунд. Увімкнено перевірку директорії /dev, системних файлів, мережевих інтерфейсів, ідентифікаторів процесів (PID), мережевих портів, аномальних системних об'єктів та троянів. Перевірка UNIX-аудиту відключена, а мережеві диски CIFS та NFS виключено з процесу сканування. Для виявлення загроз використовуються бази даних, розміщені за шляхами etc/rootcheck/rootkit_files.txt для rootkit-файлів і etc/rootcheck/rootkit_trojans.txt для троянів. Загалом налаштування забезпечують досить детальне сканування ключових компонентів системи.

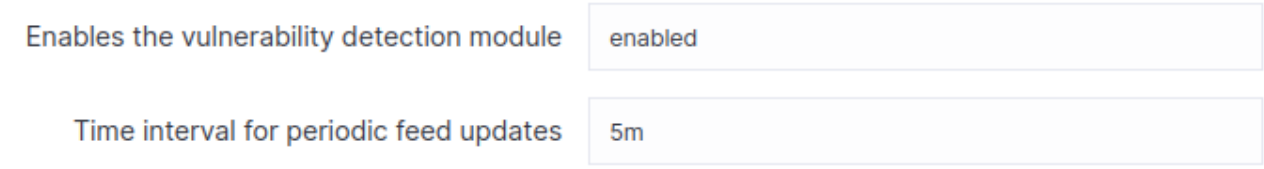


Рисунок 3.8 – Налаштування модуля виявлення вразливостей у Wazuh

На рисунку 3.8 зображено налаштування модуля виявлення вразливостей у системі. Модуль виявлення вразливостей увімкнено, що означає активний моніторинг системи на наявність відомих вразливостей. Встановлено інтервал оновлення інформації про вразливості кожні 5 хвилин. Це дозволяє системі своєчасно отримувати оновлення з баз даних вразливостей, забезпечуючи актуальність аналізу безпеки.

3.3 Налаштування компонентів pfSense, Suricata

У цьому розділі описано налаштування обох систем, починаючи з pfSense, додавання правил фільтрації через pfBlockerNG, до інтеграції Suricata для моніторингу та блокування шкідливого трафіку в режимі IPS.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/67 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
✓	0/0 B	IPv4 UDP	*	*	*	*	*	none		UDP Standart	
✓	0/0 B	IPv4 TCP	*	*	*	*	*	none		TCP Standart	
✓	5/36 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
✓	0/0 B	IPv4 ICMP	*	*	*	*	*	none		ICMP Allowed Autbound	

Рисунок 3.9 – Список правил брандмауера pfSense

На рисунку 3.9 правила брандмауера в pfSense визначають, який мережевий трафік дозволено або заборонено в межах локальної мережі та за її межами. Вони впливають на ефективність та роботу системи виявлення атак Suricata.

Перше правило гарантує, що адміністратор не втратить доступ до веб-інтерфейсу pfSense навіть у разі помилки в налаштуваннях. Це важливо для постійного контролю над системою безпеки. Друге та третє правила дозволяють стандартні TCP та UDP з'єднання з локальної мережі до зовнішніх ресурсів. Це потрібно для нормального функціонування клієнтських пристроїв, однак також означає, що система виявлення атак має ретельно перевіряти вихідний трафік на предмет аномалій або витоку даних. Четверте правило дозволяє ICMP трафік, який часто використовується для діагностики, але також може використовуватися зловмисниками для визначення доступності вузлів. Suricata повинна моніторити та логувати такий трафік при необхідності. П’яте правило виконує функцію "запобіжника": воно блокує будь-який інший IPv4-трафік, не дозволений попередніми правилами. Це дає змогу обмежити небажаний трафік, який міг би бути використаний для атак.

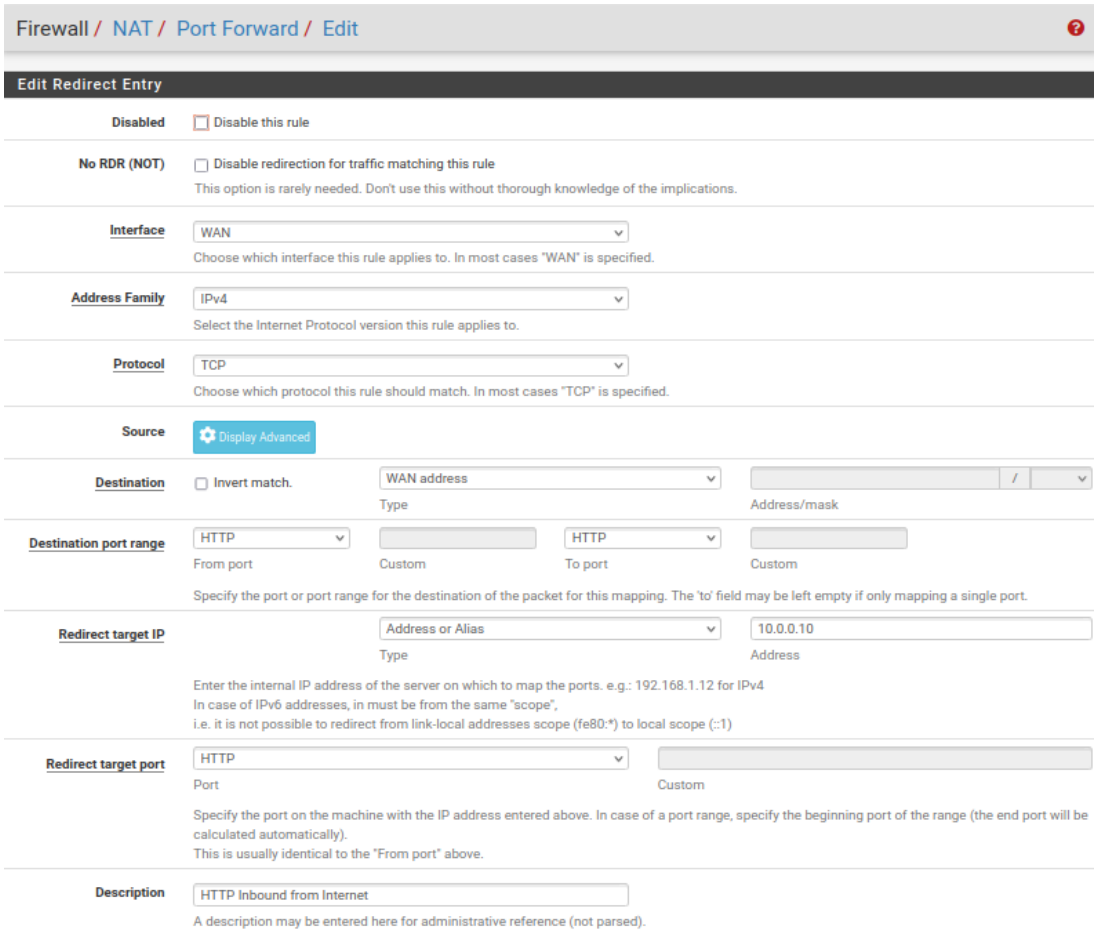


Рисунок 3.10 – Перенаправлення портів через NAT

Правило NAT на рисунку 3.10 перенаправляє вхідний HTTP-трафік з інтерфейсу WAN на внутрішній сервер з IP-адресою 10.0.0.10. Це дозволяє зовнішнім користувачам доступ до веб-сервера у локальній мережі. Коли хтось іззовні вводить домен, пов'язаний із ним, у веб-браузері, цей трафік надходить на WAN-інтерфейс pfSense.

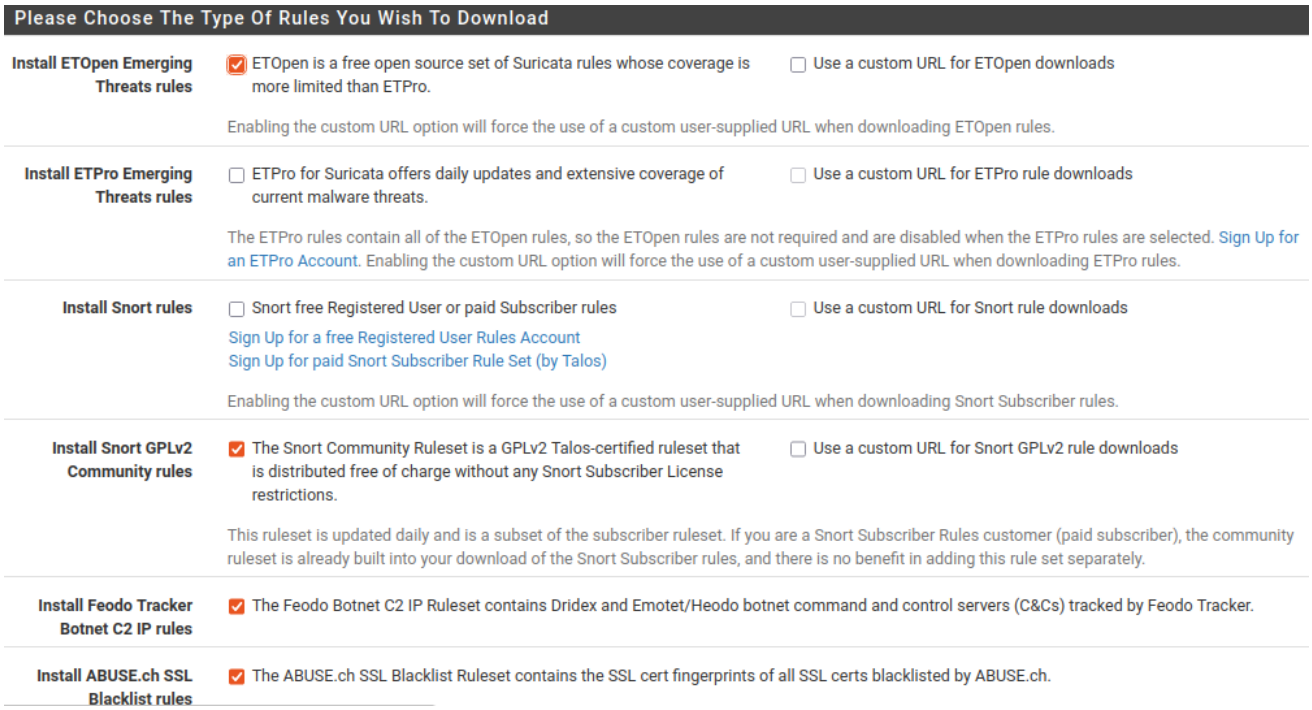


Рисунок 3.11 – Вибір типів правил безпеки для завантаження в системі

На рисунку 3.11 показано вибір типів правил безпеки для завантаження в системі, що, використовується для систем виявлення та запобігання вторгнень Suricata.

Вибрані правила безпеки відповідно до рисунку 3.11:

– безкоштовний набір правил Suricata ETOpen Emerging Threats rules з обмеженим охопленням порівняно з платною версією ETPro;

– правила Snort;

– набір IP-адрес командних серверів (C&C) ботнетів Dridex і Emotet від Feodo Tracker;

– чорний список SSL сертифікатів, відомих своєю участю в зловмисній активності від ABUSE.ch.

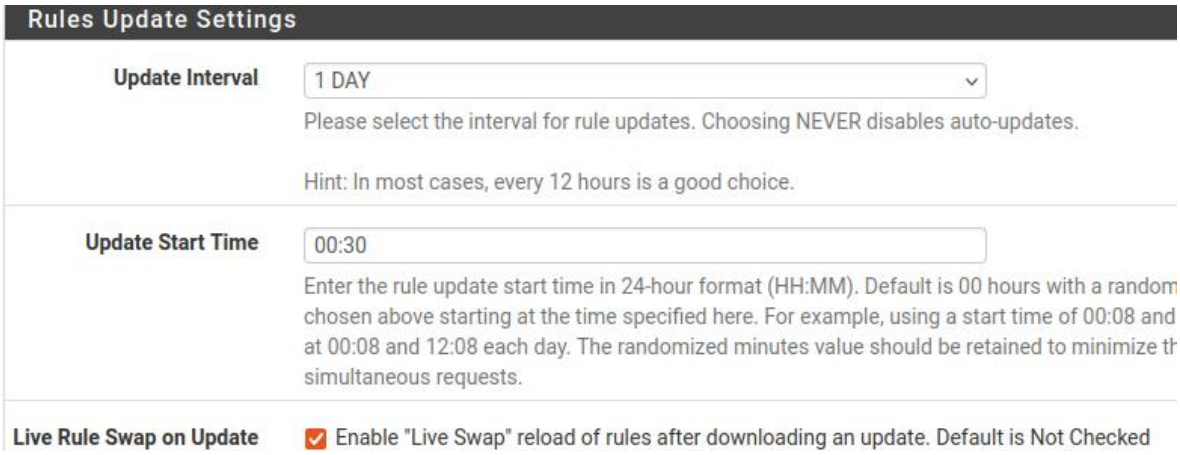


Рисунок 3.12 – Налаштування оновлення правил

Було обрано, що правила будуть оновлюватися щодня. Час початку оновлення розпочнеться о 00:30 за 24-годинним форматом. Увімкнено автоматичне перезавантажування правила після оновлення без перезапуску служби рисунок 3.12.

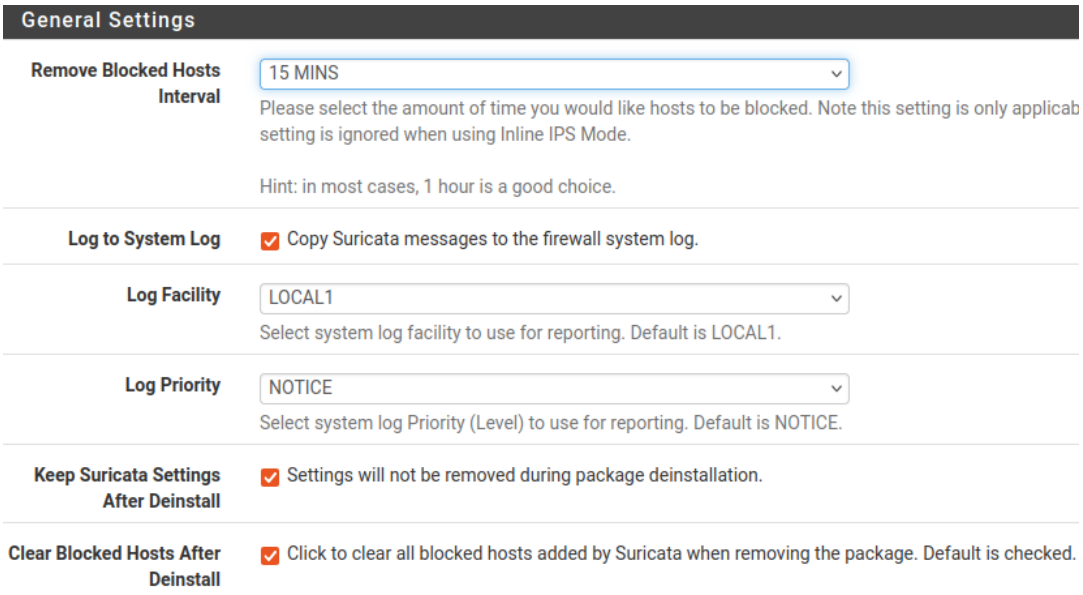


Рисунок 3.13 – Налаштування оновлення правил

На рисунку 3.13 заблоковані хости будуть розблоковуватися через 15 хвилин. Увімкнено повідомлення Suricata, які записуються до журналу фаєрволу. Обрано LOCAL1, як канал для системного журналу. Пріоритет логів «NOTICE» означає важливі події.

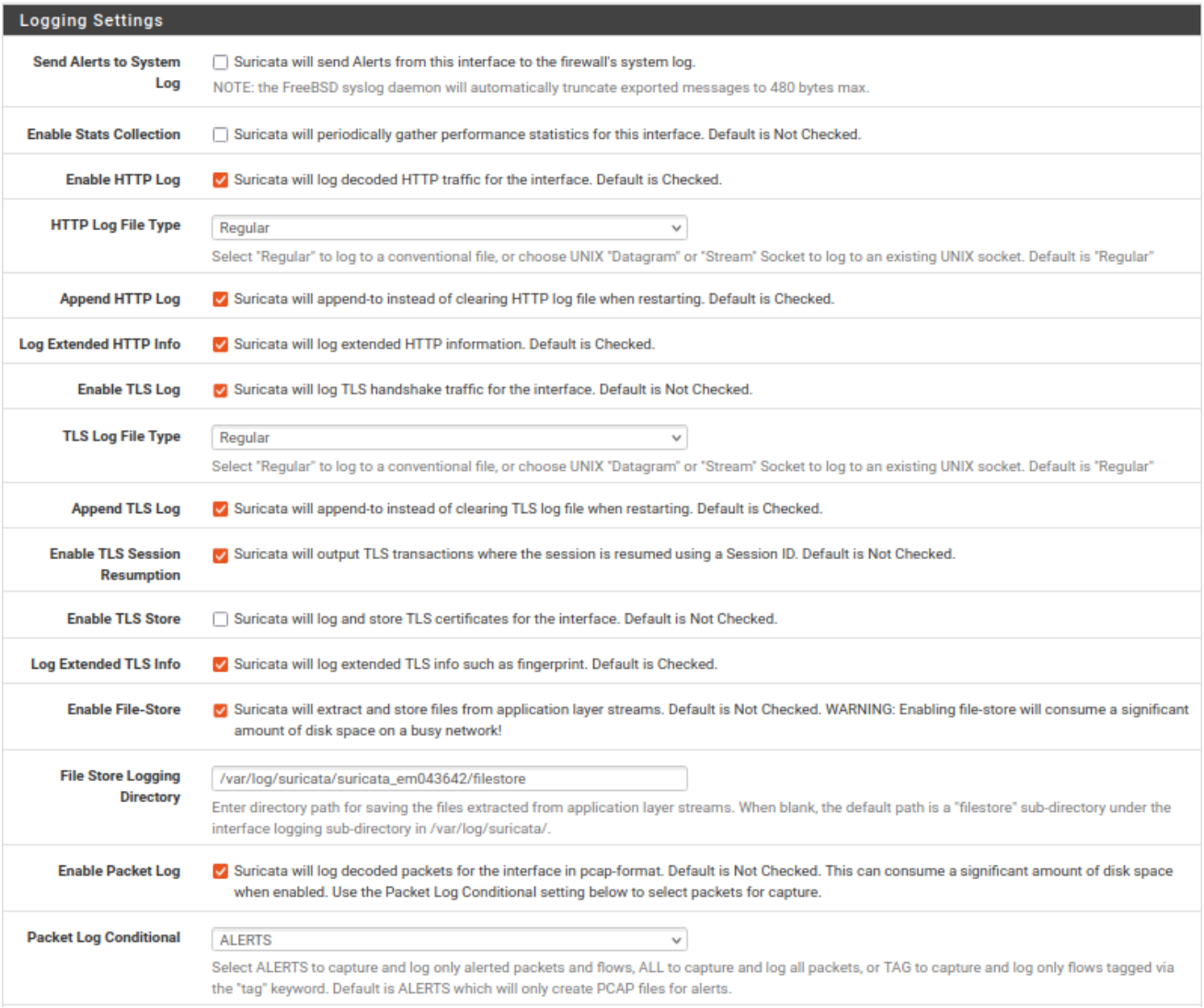


Рисунок 3.14 – Налаштування журналювання

Рисунок 3.14 демонструє налаштування журналювання для Suricata. Кожен пункт дозволяє детально контролювати, яка інформація буде зберігатися і в якому вигляді. Ця конфігурація журналювання Suricata забезпечує розширене логування HTTP-трафіку з додатковою інформацією та збереженням лише тих пакетів, які спричиняють тривоги, у форматі pcap. Увімкнене логування HTTP-трафіку з додаванням до файлів і розширена інформація дозволяє отримати повну картину активності, логування TLS-трафіку, рукостискань і сертифікатів, вимкнене для зменшення навантаження. Збір статистики, логування у системний журнал, збереження файлів та TLS-сесій також вимкнені, що дозволяє економити ресурси. Такий підхід дозволяє зосередитися на аналізі критичної інформації, мінімізуючи використання дискового простору.

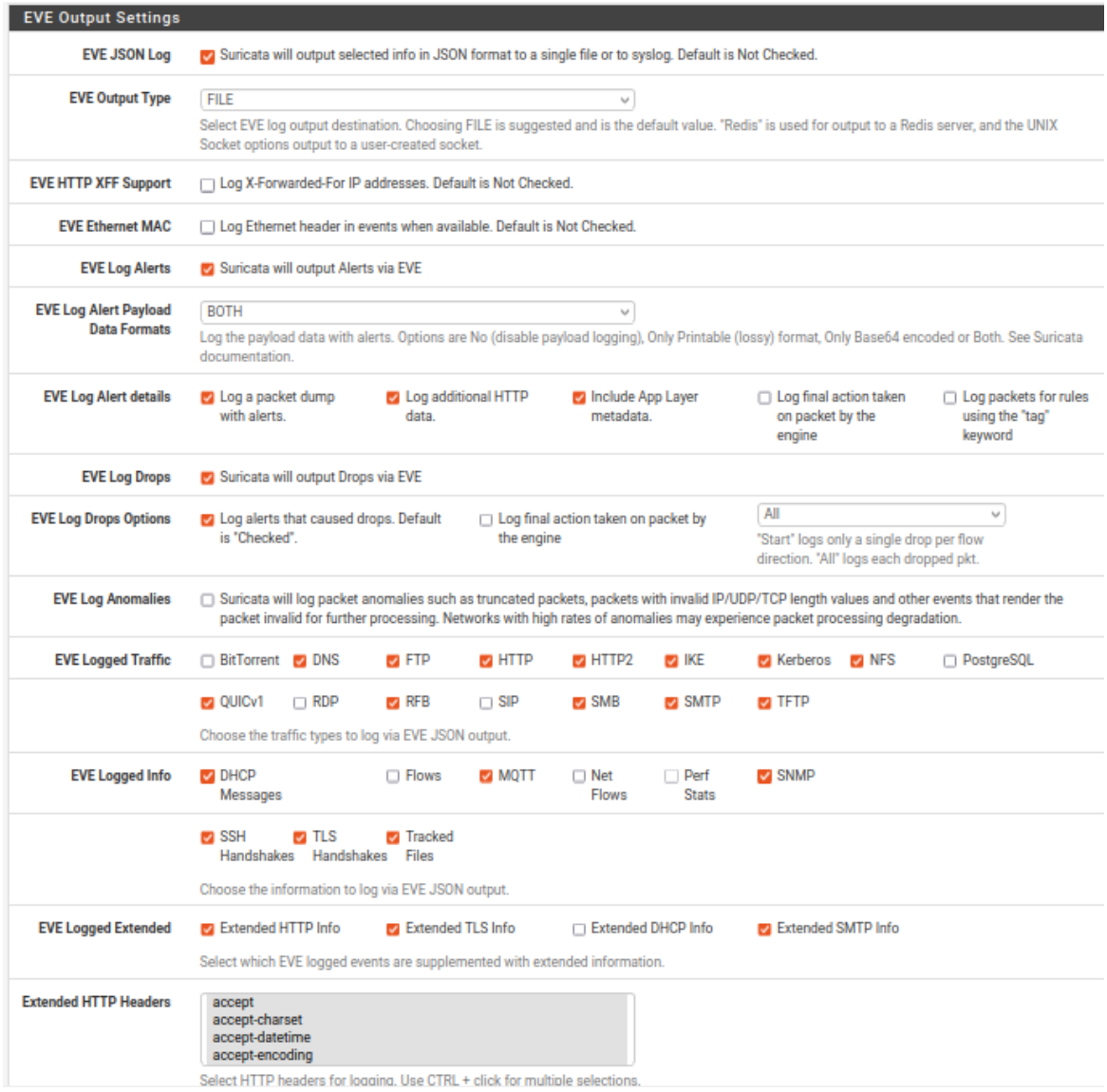


Рисунок 3.15 – Налаштування виводу EVE JSON логів

На рисунку 3.15 відображається розширене налаштування системи Suricata для виведення логів у форматі EVE JSON універсального формату для збору інформації про мережевий трафік, спрацювання сигнатур, аномалії та інші події. Вивід логів здійснюється у файл, що є рекомендованим варіантом для подальшого аналізу або інтеграції з системами SIEM. Увімкнено логування спрацювань, включно з детальним дампом пакетів, додатковими HTTP-даними, метаданими прикладного рівня, кінцевою обробкою пакета, а також збереженням пов’язаних пакетів за тегами правил. Payload дані логуються як у printable, так і в base64-форматі. Активовано логування подій, коли пакет було відкинуто, включаючи лише ті, що пов’язані з alert. Також увімкнено журналювання аномалій,

наприклад, пошкоджених або неправильно сформованих пакетів, що можуть свідчити про сканування або мережеві атаки. Вибрано логування широкого спектру мережевих протоколів, серед яких HTTP, FTP, DNS, SMB, SMTP, SIP, RDP, PostgreSQL, Kerberos, TFTP, BitTorrent та інші. Окрім цього, фіксуються типи даних, такі як DHCP-повідомлення, потоки (flows), Net Flows, MQTT, SNMP, TLS-рукостискання, Tracked Files тощо.

Загалом, така конфігурація забезпечує максимально повне логування всіх критичних аспектів мережевого трафіку й подій безпеки та дозволяє ефективно виявляти загрози, а також проводити післяінцидентний аналіз.

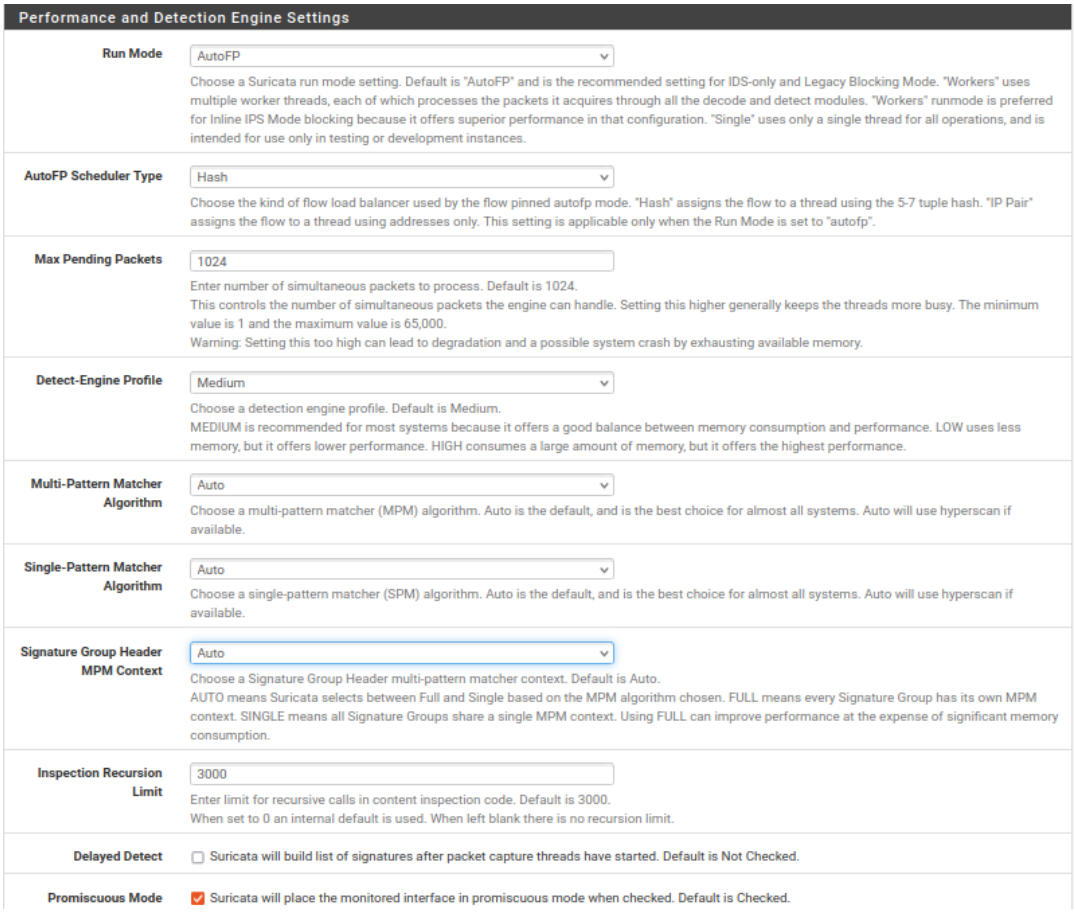


Рисунок 3.16 – Налаштування продуктивності та виявлення

Рисунок 3.16 демонструє налаштування продуктивності та виявлення в системі Suricata. Встановлено режим роботи AutoFP, який оптимально балансує навантаження між потоками на основі мережевих флоу, а планувальник потоків обрано як Hash, що розподіляє пакети за хешем мережевих атрибутів. Кількість

одночасно оброблюваних пакетів встановлена на 1024. Профіль виявлення встановлено на середній, що забезпечує хороший баланс між споживанням пам’яті та продуктивністю. Алгоритми пошуку багатьох і одиночних шаблонів залишено в режимі Auto, що дозволяє системі автоматично вибрати найоптимальніший варіант, включаючи використання Hyperscan. Контекст MPM для груп сигнатур встановлено на Auto, дозволяючи Suricata вибирати між спільним і окремим контекстом для кращої продуктивності. Межа рекурсивної перевірки визначена як 3000, що обмежує глибину вкладеного аналізу при декодуванні трафіку. Увімкнено promiscuous mode, що дозволяє інтерфейсу захоплювати весь трафік незалежно від адресата, що є необхідним для повноцінного моніторингу мережі. Опція Delayed Detect вимкнена, отже списки сигнатур формуються одразу, а не після запуску потоків. Така конфігурація забезпечує стабільну та ефективну роботу системи в умовах інтенсивного трафіку.

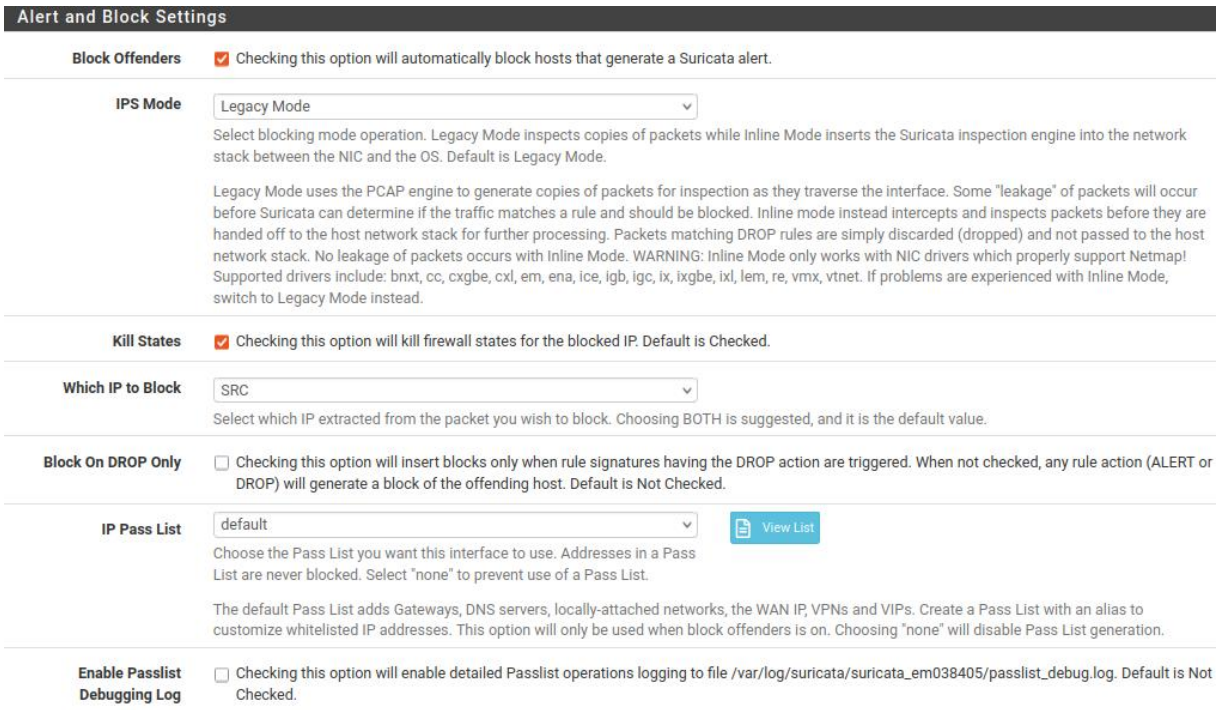


Рисунок 3.17 – Налаштування блокування

На рисунку 3.17, розділ конфігурації Suricata відповідає за спрацювання тривог та блокування хостів у разі виявлення підозрілої активності. Активовано опцію Block Offenders, що означає блокування IP-адрес джерел, які генерують

спрацювання правил Suricata. Для реалізації блокування використовується Legacy Mode, де трафік дублюється за допомогою PCAP до того, як потрапить у стек операційної системи. Це дозволяє аналізувати пакети і блокувати лише ті, що відповідають певним правилам, тоді як решта проходить далі. Додатково увімкнена опція Kill States, яка миттєво знищує всі активні з'єднання брандмауера, пов’язані з заблокованою IP-адресою, забезпечуючи ефективне припинення небажаної активності. Адреса, яка підлягає блокуванню, визначається як SRC, тобто джерело пакету, що є типовим вибором для знешкодження атакувального хоста. Опція Block on DROP Only вимкнена, тож блокування може ініціюватися будь-яким правилом, незалежно від того, має воно дію DROP чи лише ALERT, що підвищує загальну чутливість системи. Для запобігання помилковому блокуванню критичних ресурсів використовується Pass List, встановлений у значення default, який включає шлюзи, DNS-сервери, локальні мережі, IP VPN і VIP-адреси, що ніколи не блокуються. Опція ведення журналу для Passlist наразі вимкнена, що означає, що діагностика роботи білого списку не записується у лог-файли. Така конфігурація забезпечує агресивне, але контрольоване блокування загроз із збереженням доступу до важливих сервісів.

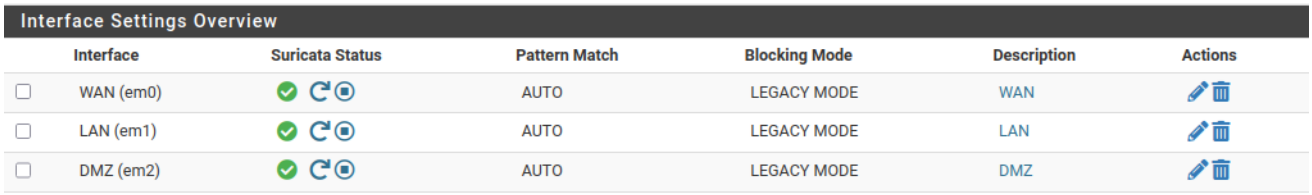


Рисунок 3.18 – Інтерфейс налаштувань Suricata

На рисунку 3.18 представлено інтерфейс налаштувань системи виявлення та запобігання вторгненням Suricata. У таблиці наведені три мережеві інтерфейси: WAN (em0), LAN (em1) та DMZ (em2). Усі вони мають активний статус Suricata, а також автоматичне виявлення шаблонів для аналізу трафіку. Для WAN, LAN та DMZ використовується режим блокування LEGACY MODE, який дозволяє Suricata активно блокувати підозрілий трафік у реальному часі.

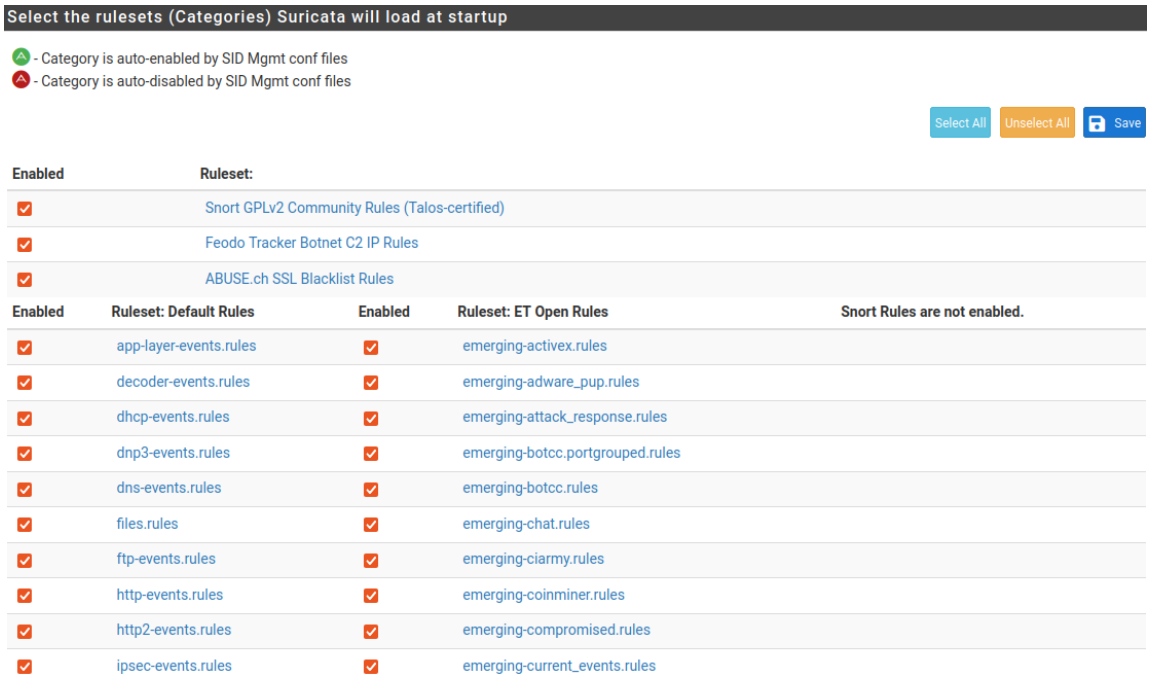


Рисунок 3.19 – Інтерфейс правил Suricata

Цей рисунок 3.19 показує інтерфейс вибраних правил, системи Suricata. Увімкнено Snort GPLv2 Community Rules, Feodo Tracker Botnet C2 IP Rules та ABUSE.ch SSL Blacklist Rules. У блоці "Default Rules" активовано базові правила, зокрема для FTP, HTTP, DNS, DHCP, IPsec тощо. У блоці "ET Open Rules" також активовано численні правила, пов’язані з атаками, ботнетами, шкідливим ПЗ, чатами, та іншими загрозами.

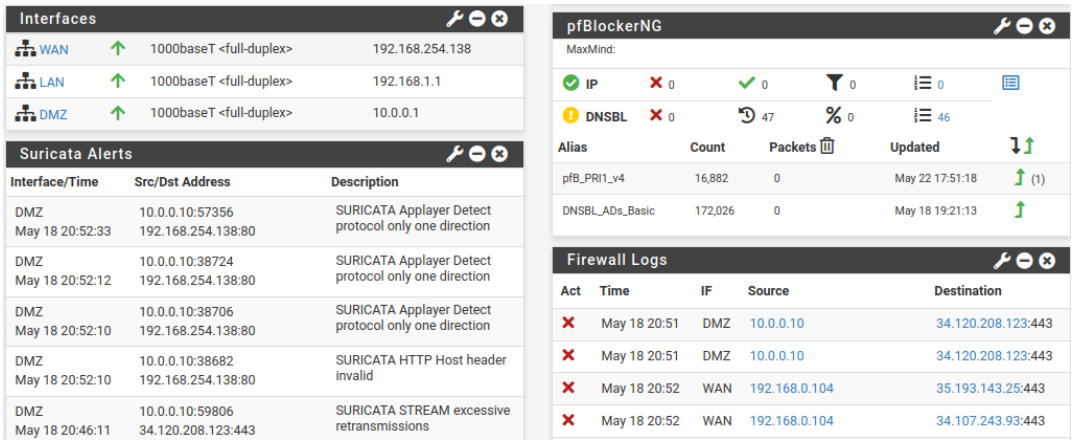


Рисунок 3.20 – Моніторинг мережевої безпеки

На рисунку 3.20 представлено інтерфейс моніторингу мережевої безпеки на базі pfSense із встановленими модулями Suricata та pfBlockerNG. Вкладка Interfaces відображає активні мережеві інтерфейси WAN, LAN та DMZ із відповідними IP-адресами. Модуль Suricata Alerts показує сповіщення про виявлені загрози, виявлені типи атак та підозрілу мережеву активність у режимі реального часу. Розділ pfBlockerNG демонструє фільтрацію за IP-адресами та DNS, активні блокувальні списки DNSBL. Firewall Logs фіксують спроби мережевих з'єднань, які були заблоковані між зонами, включаючи спроби з DMZ до зовнішніх IP-адрес по порту HTTPS.

3.4 Тестування системи виявлення атак

У рамках даної роботи було проведено тестування розгорнутої системи виявлення атак, яка включає компоненти Suricata, Wazuh, pfSense та pfBlockerNG. Метою тестування є перевірка здатності системи виявляти та реєструвати різноманітні види атак у контрольованому середовищі. Результати тестування наведено у вигляді узагальненого рисунку відповідності між конкретними загрозами, компонентами системи безпеки та їх функціональними можливостями.

File	Last modified	User	User ID	Group	Group ID	Size
/usr/bin/testfile	May 19, 2025 @ 23:22:29.000	root	0	root	0	13
/usr/bin/testff	May 19, 2025 @ 23:21:55.000	root	0	root	0	0
/usr/bin/testfile.txt	May 19, 2025 @ 23:21:52.000	root	0	root	0	0
/etc/work.txt	May 19, 2025 @ 23:18:38.000	root	0	root	0	31
/etc/testfile2.txt	May 19, 2025 @ 23:11:36.000	root	0	root	0	0
/etc/testfile	May 19, 2025 @ 23:11:13.000	root	0	root	0	0
/etc/group	May 19, 2025 @ 23:07:01.000	root	0	root	0	1107
/etc/test.txt	May 19, 2025 @ 23:06:29.000	root	0	root	0	0

Рисунок 3.21 – Моніторингу змін у файловій системі

На рисунку 3.21 у модулі File Integrity Monitoring (FIM) було автоматично зафіксовано всі створення тестових файлів та важливих змін файлів.

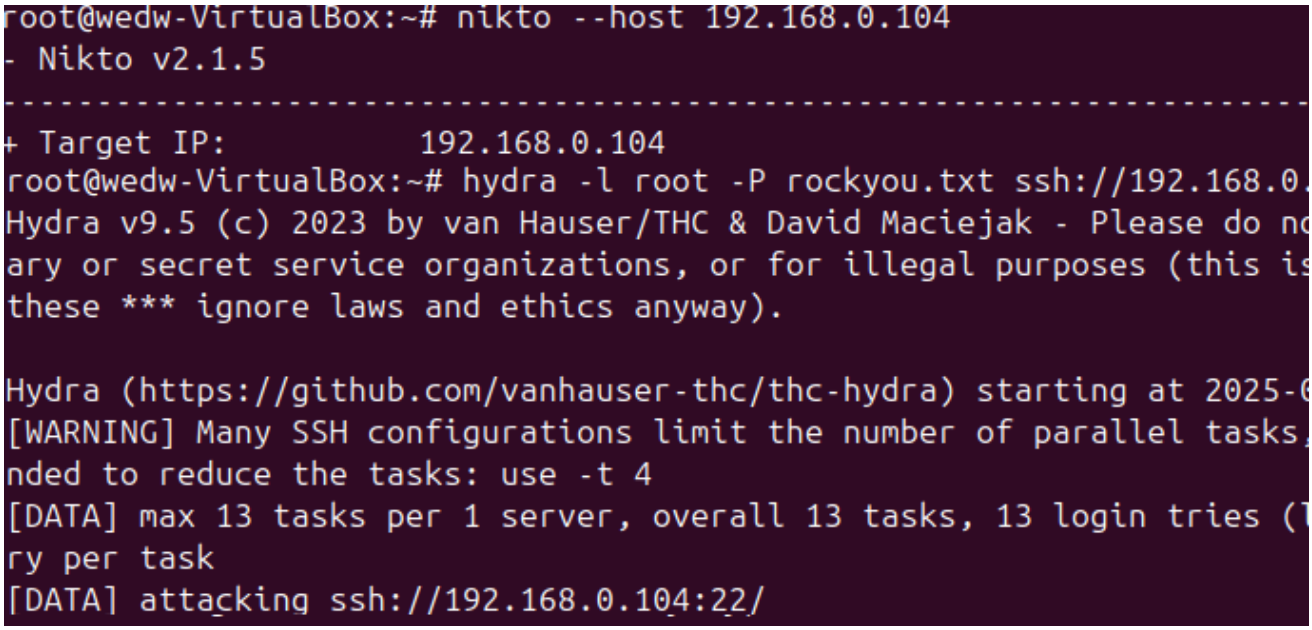


Рисунок 3.22 – Тестування з інструментами Nikto та Hydra

На рисунку 3.22 було проведено тестування безпеки, де за допомогою Nikto і Hydra проводилась оцінка вразливостей на IP-адресі 192.168.0.104.

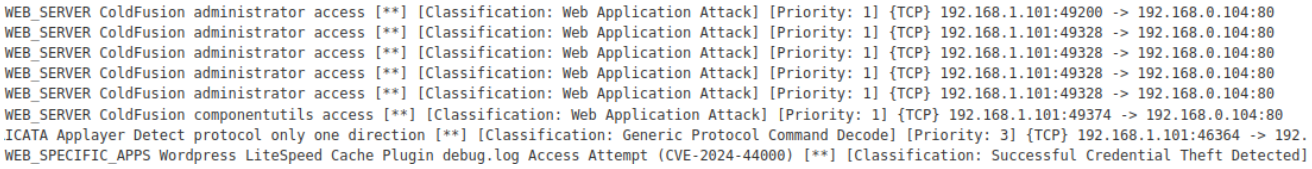


Рисунок 3.23 – Результат спрацювання системи виявлення вторгнень

Цей рисунок 3.23 є результатом спрацювання системи виявлення вторгнень (IDS) Suricata у відповідь на тестові атаки, виконані за допомогою Nikto та Hydra.

Було здійснено автоматизоване сканування за допомогою інструменту Nikto, у результаті чого IDS Suricata зафіксувала численні спроби доступу до адміністративної панелі та компонентів ColdFusion. Ці дії були класифіковані як атаки на веб-додатки з високим рівнем пріоритету. Джерелом сканування виступала машина з IP 192.168.1.101. Додатково з цього ж хоста за допомогою Hydra була здійснена брутфорс-атака на SSH, що викликало спрацювання Suricata щодо аномального одностороннього трафіку, характерного для автоматизованих зломів.

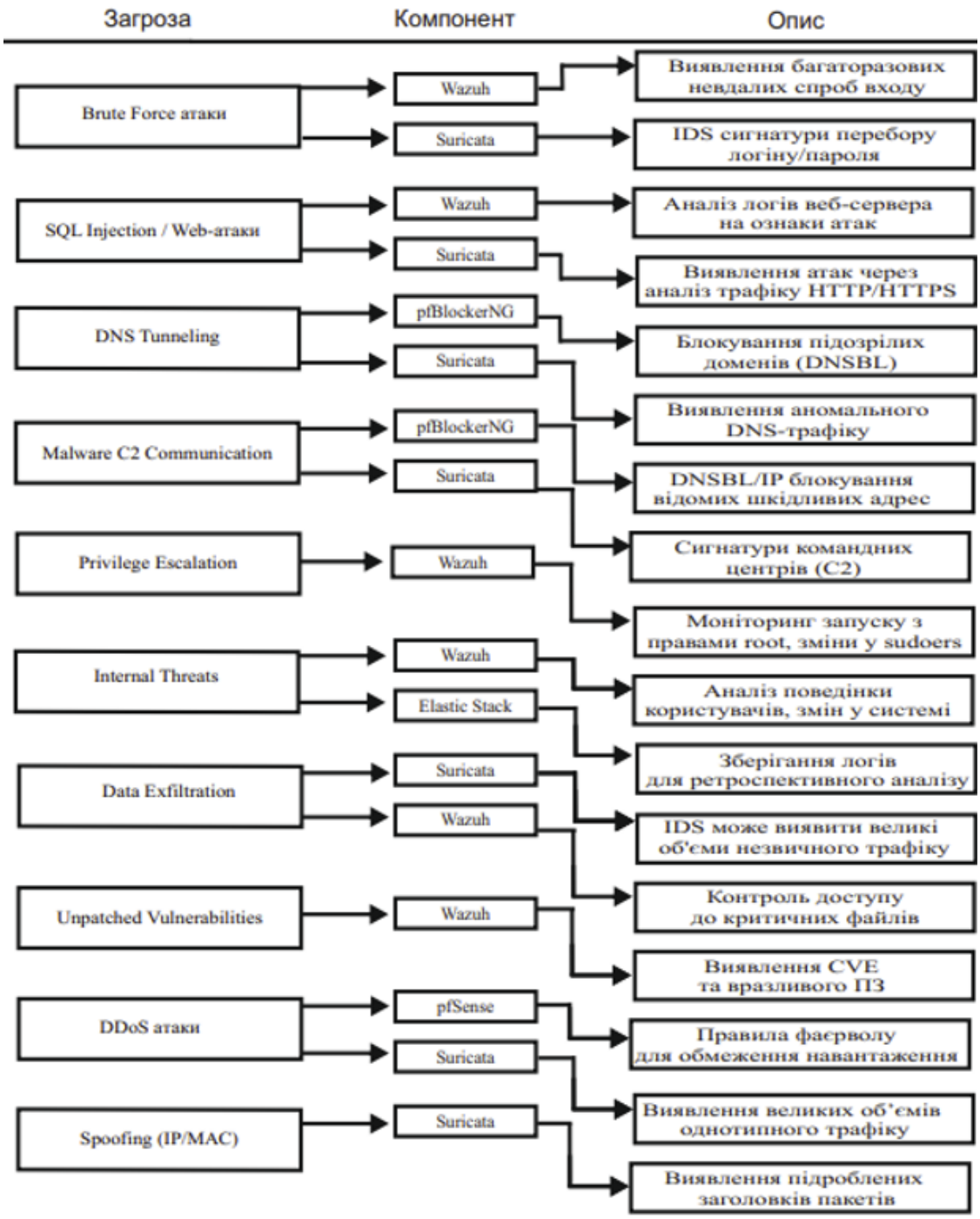


Рисунок 3.24 – Загрози між компонентами системи виявдення атак

У ході тестування на рисунку 3.24 було змодельовано різні типи загроз, що можуть виникати у корпоративній мережі, з метою перевірки ефективності обраної системи виявлення атак. Результати тестування наведено у вигляді узагальненої таблиці відповідності між конкретними загрозами, компонентами системи безпеки та їх функціональними можливостями.

3.5 Висновки

Було проаналізовано алгоритм функціонування системи виявлення атак. Було визначено, що інтеграція таких компонентів, як Wazuh, Suricata, pfSense та Elastic Stack, дозволяє забезпечити багаторівневий підхід до захисту інформаційної інфраструктури. Кожен з компонентів виконує свою функцію - моніторинг подій, аналіз мережевого трафіку, фільтрацію шкідливих запитів та візуалізацію даних.

В процесі налаштування Wazuh була реалізована централізована система збору та аналізу подій з агентів. Налаштовано модулі контролю цілісності файлів, виявлення ознак підвищення привілеїв, а також виявлення підозрілої поведінки користувачів. Wazuh також було інтегровано з Kibana, що дозволило зручно переглядати та аналізувати події системи безпеки.

Налаштування pfSense включало створення фаєрвол правил, реалізацію модулів блокування DNS-запитів через pfBlockerNG, а також базовий контроль доступу до мережевих ресурсів.

Suricata була налаштована як система глибокого аналізу мережевого трафіку. Було завантажено актуальні сигнатури атак, налаштовано інтерфейси мережі. Suricata дозволяє виявляти численні типи атак, такі як Brute Force, DDoS, SQL Injection, Port Scan, DNS Tunneling. Її використання дозволяє оперативно фіксувати шкідливу активність та приймати рішення щодо подальших дій блокування, сповіщення або аналізу.

У ході тестування було змодельовано типові сценарії атак, серед яких спроби підбору паролів, SQL-ін’єкції, спроби ексфільтрації даних, привілейований доступ, тунелювання DNS-запитів та внутрішні загрози. Усі ці події були успішно зафіксовані відповідними компонентами системи: Wazuh реєстрував зміни у критичних файлах, Suricata виявляла аномалії у мережевому трафіку, pfSense блокував DNS-запити до шкідливих доменів.

ВИСНОВКИ

У ході виконання роботи було проведено огляд сучасних систем виявлення атак, зокрема їх переваг, недоліків та доцільності використання в корпоративному середовищі. Було порівняно різні підходи до виявлення вторгнень, обґрунтовано вибір рішень для побудови комплексної системи виявлення атак.

Основою побудови системи стала відкрита платформа pfSense, яка виконує роль міжмережевого екрану, контролюючи вхідний та вихідний трафік. На цьому рівні було впроваджено механізм виявлення атак Suricata, що здійснює інспекцію пакетів і реагує на відомі загрози за допомогою сигнатурного аналізу.

Для централізованого моніторингу безпекових подій було впроваджено рішення Wazuh, систему збору, аналізу та кореляції подій з усіх компонентів мережі, включаючи кінцеві пристрої, сервери та сервіси. Wazuh здійснює виявлення змін у файлах, підозрілих процесів, активностей користувачів, атак типу brute-force, експлуатацій вразливостей.

Така комбінація дозволяє:

– маршрутизування та контроль трафіку через фаєрвол;

– блокувати небажані IP-адреси та домени за допомогою списків DNSBL/IP;

– виявляти атаки на рівні мережі завдяки механізмам IDS/IPS та генерації сигнатурних попереджень;

– проводити моніторинг подій безпеки та агентський контроль на вузлах;

– збирати, зберігати й візуалізувати логи та попередження системи.

Результати показали високу точність виявлення атак, зручність аналізу інцидентів, ефективність у блокуванні потенційних загроз у реальному часі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Corporate Network Security: How to Detect & Prevent Attacks [Електроний ресурс] – Режим доступу – URL: https://www.netmaker.io/resources/network-security (дата звернення: 20.02.2025).

2. Network security fundamentals. How to design, use, and maintain secure networks. [Електроний ресурс] – Режим доступу – URL: https://www.ncsc.gov.uk/guidance/network-security-fundamentals (дата звернення: 20.02.2025).

3. Principles of Network Security. Understand essential principles of network security, covering risk management, encryption, firewalls, and security policies to protect data. [Електроний ресурс] – Режим доступу – URL: https://digitdefence.com/blog/principles-of-network-security (дата звернення: 20.02.2025).

4. What is defense in depth? | Layered security. [Електроний ресурс] – Режим доступу – URL: https://www.cloudflare.com/learning/security/glossary/what-is-defense-in-depth (дата звернення: 20.02.2025).

5. Implementing effective cyber security measures. [Електроний ресурс] – Режим доступу – URL: https://www.ncsc.gov.uk/collection/board-toolkit/implementing-effective-cyber-security-measures (дата звернення: 20.02.2025).

6. What is a Security Model in Information Security? [Електроний ресурс] – Режим доступу – URL: https://medium.com/@Infosec-Train/what-is-a-security-model-in-information-security-ba362f7787ac (дата звернення: 20.02.2025).

7. Introduction To Classic Security Models. [Електроний ресурс] – Режим доступу – URL: https://www.geeksforgeeks.org/introduction-to-classic-security-models (дата звернення: 20.02.2025).

8. Security Models in Network Security. [Електроний ресурс] – Режим доступу – URL: https://ms.codes/blogs/internet-security/security-models-in-network-security (дата звернення: 20.02.2025).

9. What is an intrusion detection system (IDS)? [Електроний ресурс] – Режим доступу – URL: https://www.ibm.com/think/topics/intrusion-detection-system (дата звернення: 20.02.2025).

10. How Does an Intrusion Detection System Work? [Електроний ресурс] – Режим доступу – URL: https://www.packetlabs.net/posts/intrusion-detection-system (дата звернення: 20.02.2025).

11. Intrusion Detection System (IDS). [Електроний ресурс] – Режим доступу – URL: https://www.geeksforgeeks.org/intrusion-detection-system-ids (дата звернення: 20.02.2025).

12. Guide to Intrusion Detection and Prevention Systems (IDPS). [Електроний ресурс] – Режим доступу – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (дата звернення: 20.02.2025).

13. Intrusion Detection Systems (IDS): Pros and Cons. [Електроний ресурс] – Режим доступу – URL: https://www.otorio.com/blog/intrusion-detection-systems-ids (дата звернення: 20.02.2025).

14. Cybersecurity Threats. [Електроний ресурс] – Режим доступу – URL: https://www.imperva.com/learn/application-security/cyber-security-threats (дата звернення: 20.02.2025).

15. What are the Types of Computer Attacks Detected by IDS? [Електроний ресурс] – Режим доступу – URL: https://www.stamus-networks.com/blog/what-are-the-types-of-computer-attacks-detected-by-ids (дата звернення: 20.02.2025).

16. Different Types of Network Attacks & How to Mitigate Them. [Електроний ресурс] – Режим доступу – URL: https://www.netmaker.io/resources/network-attacks (дата звернення: 20.02.2025).

17. What is Suricata. [Електроний ресурс] – Режим доступу – URL: https://docs.suricata.io/en/latest/what-is-suricata.html (дата звернення: 20.03.2025).

18. Suricata Rules. [Електроний ресурс] – Режим доступу – URL: https://www.stamus-networks.com/suricata-rules (дата звернення: 20.03.2025).

19. What is Snort? [Електроний ресурс] – Режим доступу – URL: https://www.snort.org (дата звернення: 20.03.2025).

20. SNORT Definition. [Електроний ресурс] – Режим доступу – URL: https://www.fortinet.com/resources/cyberglossary/snort (дата звернення: 20.03.2025).

21. Wazuh overview. [Електроний ресурс] – Режим доступу – URL: https://wazuh.com/platform/overview/ (дата звернення: 20.03.2025).

22. Understanding Wazuh. [Електроний ресурс] – Режим доступу – URL: https://osintph.medium.com/understanding-wazuh-the-free-open-source-security-platform-for-xdr-siem-48b3c3dfba9d (дата звернення: 20.03.2025).

23. OSSEC overview. [Електроний ресурс] – Режим доступу – URL: https://www.ossec.net/docs/docs/manual/non-technical-overview.html (дата звернення: 20.03.2025).

24. OSSEC Architecture. [Електроний ресурс] – Режим доступу – URL: https://www.ossec.net/docs/docs/manual/ossec-architecture.html (дата звернення: 20.03.2025).

25. Zeek Frequently Asked Questions. [Електроний ресурс] – Режим доступу – URL: https://zeek.org/faq (дата звернення: 20.03.2025).

26. The Basics – Book of Zeek. [Електроний ресурс] – Режим доступу – URL: https://docs.zeek.org/en/master/scripting/basics.html (дата звернення: 20.03.2025).

27. About Security Onion. [Електроний ресурс] – Режим доступу – URL: https://docs.securityonion.net/en/2.4/about.html#documentation (дата звернення: 20.03.2025).

28. Introduction Security Onion. [Електроний ресурс] – Режим доступу – URL: https://docs.securityonion.net/en/2.4/introduction.html (дата звернення: 20.03.2025).

29. 25 Best Intrusion Detection Software In 2025. [Електроний ресурс] – Режим доступу – URL: https://thectoclub.com/tools/best-intrusion-detection-software/ (дата звернення: 20.03.2025).

30. Open Source IDS Tools. [Електроний ресурс] – Режим доступу – URL: https://levelblue.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview (дата звернення: 20.03.2025).

31. Building a Next-Generation Detection and Correlation Lab with Suricata and Wazuh. [Електроний ресурс] – Режим доступу – URL: https://medium.com/@kh.shabana1499/building-a-next-generation-detection-and-correlation-lab-with-suricata-and-wazuh-a-hands-on-guide-0a3b21ef89a7 (дата звернення: 20.03.2025).

32. Top 5 Open Source SIEM Tools for Security Monitoring. [Електроний ресурс] – Режим доступу – URL: https://last9.io/blog/open-source-siem-tools (дата звернення: 21.03.2025).

33. Peeling the onion Security onion OS. [Електроний ресурс] – Режим доступу – URL: https://www.infosecinstitute.com/resources/general-security/peeling-the-onion-security-onion-os (дата звернення: 21.03.2025).

34. Best HIDS Tools. [Електроний ресурс] – Режим доступу – URL: https://www.dnsstuff.com/host-based-intrusion-detection-systems (дата звернення: 21.04.2025).

35. Introduction pfSense. [Електроний ресурс] – Режим доступу – URL: https://docs.netgate.com/pfsense/en/latest/general/index.html (дата звернення: 22.04.2025).

36. Installing and Configuring pfSense. [Електроний ресурс] – Режим доступу – URL: https://servercore.com/blog/articles/installing-and-configuring-pfsense (дата звернення: 22.04.2025).

37. pfBlockerNG Guide. [Електроний ресурс] – Режим доступу – URL: https://www.zenarmor.com/docs/network-security-tutorials/pfblockerng (дата звернення: 22.04.2025).

38. An overview of the Elastic Stack. [Електроний ресурс] – Режим доступу – URL: https://www.elastic.co/docs/get-started/the-stack (дата звернення: 22.03.2025).

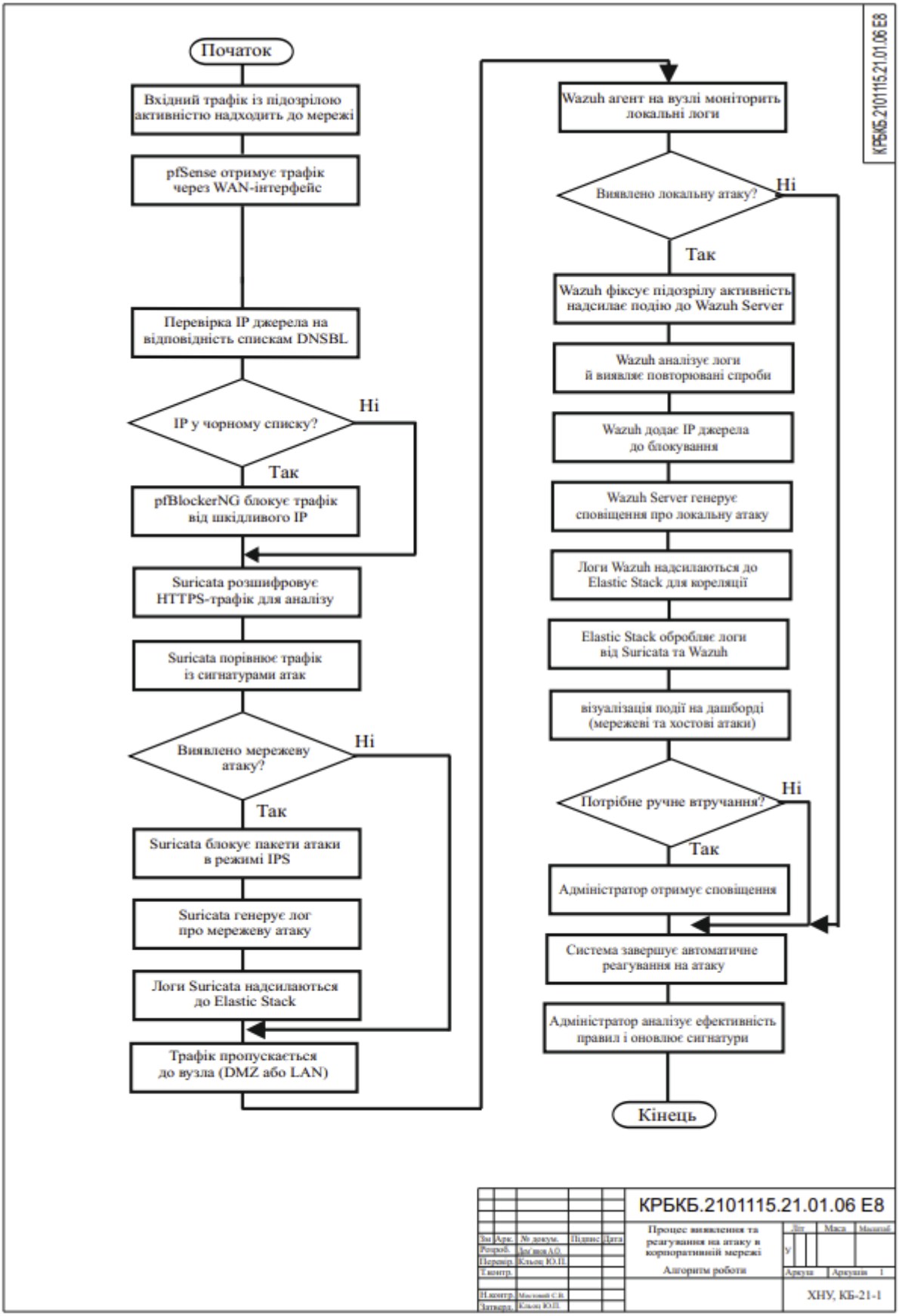
39. Understanding Suricata Signatures. [Електроний ресурс] – Режим доступу – URL: https://www.digitalocean.com/community/tutorials/understanding-suricata-signatures (дата звернення: 22.04.2025).

40. Configuration for monitoring log files. [Електроний ресурс] – Режим доступу – URL: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/monitoring-log-files.html (дата звернення: 25.04.2025).

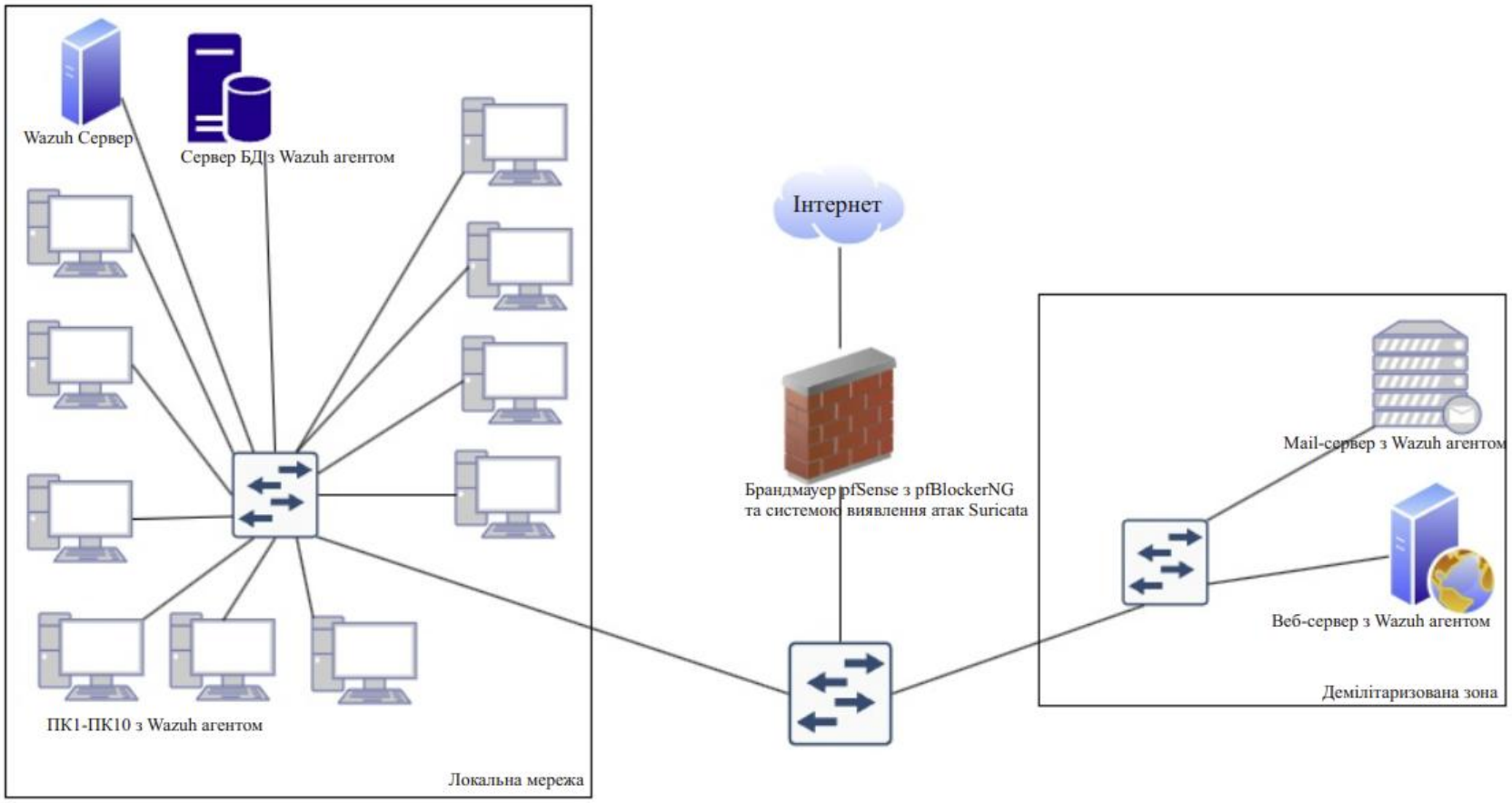
ДОДАТОК А

(обов’язковий)

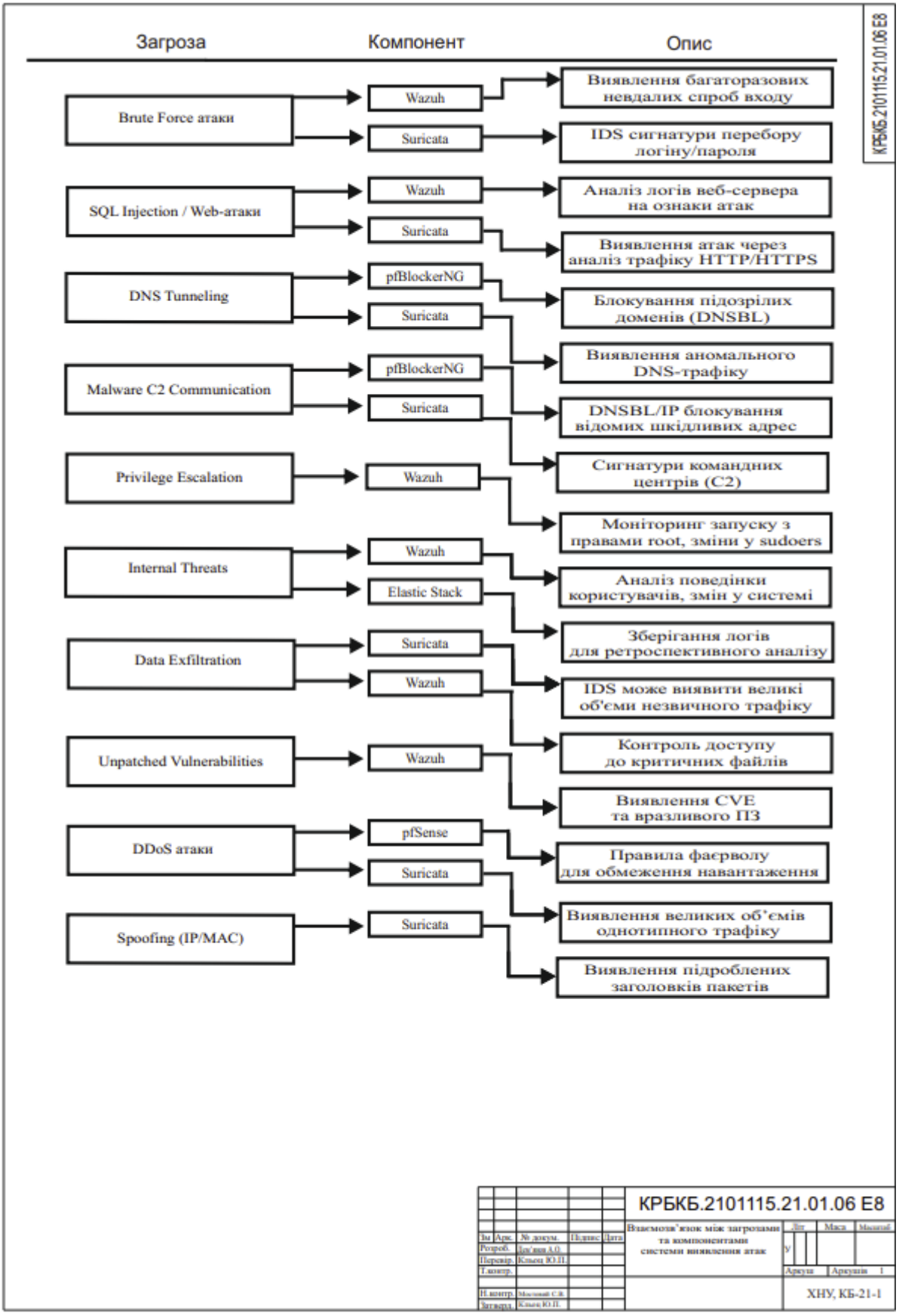
Копія графічної частин



КРБКБ.2101115.21.01.06 Е8



					КРБКБ.2101115.21.01.06 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Дем'янов А.О.			Корпоративна мережа з засобами виявлення атак	Літ.	Маса / Масштаб
Перевір.		Кльоц Ю.П.				У	
Т.контр.					Схема архітектури мережі	Аркуш	Аркушів 1
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-1	
Затверд.		Кльоц Ю.П.					


КРБКБ.2101115.21.01.06 Е8
Загроза
Компонент
Опис
Brute Force атаки
Wazuh
Виявлення багаторазових невдалих спроб входу
Suricata
IDS сигнатури перебору логіну/пароля
SQL Injection / Web-атаки
Wazuh
Аналіз логів веб-сервера на ознаки атак
Suricata
Виявлення атак через аналіз трафіку HTTP/HTTPS
DNS Tunneling
pfBlockerNG
Блокування підозрілих доменів (DNSBL)
Suricata
Виявлення аномального DNS-трафіку
Malware C2 Communication
pfBlockerNG
DNSBL/IP блокування відомих шкідливих адрес
Suricata
Сигнатури командних центрів (C2)
Privilege Escalation
Wazuh
Моніторинг запуску з правами root, зміни у sudoers
Internal Threats
Wazuh
Аналіз поведінки користувачів, змін у системі
Elastic Stack
Зберігання логів для ретроспективного аналізу
Data Exfiltration
Suricata
IDS може виявити великі об'єми незвичного трафіку
Wazuh
Контроль доступу до критичних файлів
Unpatched Vulnerabilities
Wazuh
Виявлення CVE та вразливого ПЗ
DDoS атаки
pfSense
Правила фаєрволу для обмеження навантаження
Suricata
Виявлення великих об'ємів однотипного трафіку
Spoofing (IP/MAC)
Suricata
Виявлення підроблених заголовків пакетів
КРБКБ.2101115.21.01.06 Е8
Взаємозв'язок між загрозами та компонентами системи виявлення атак
ХНУ, КБ-21-1

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Дем'янова Артема Олексійовича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

28.05.2025
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Дем'янов Артем Олексійович

Співавтор:

Назва: Система виявлення атак на вузли в корпоративній мережі підприємства

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.8%

Коефіцієнт подібності 2:0.3%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-05-29 22:37:41.0

Після аналізу Звіту подібності констатую наступне:

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

30.05.2025р. СМ

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 15%**

	Document		Sum coincidence on the DB	
ID: 242467 Title: Система виявлення атак на вузли в корпоративній мережі підприємства Added in a DB: 2025-05-29 Authors: Дем'янов Артем Олексійович Heads: Кльоц Ю.П. Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	77780	612	412 (1%)	4 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система виявлення атак на вузли в корпоративній мережі підприємства

Автор: Дем'янов Артем Олексійович

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Науковий керівник:Юрій КЛЬОЦ, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98,2%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Юрій Кльоц

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Дем'янов Артем Олексійович

Тема Система виявлення атак на вузли в корпоративній мережі підприємства

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 67.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розроблено систему виявлення атак на вузли корпоративної мережі із використанням pfSense, pfBlockerNG, Suricata, Wazuh, що забезпечує багаторівневий захист: мережевий (фільтрація трафіку, аналіз зашифрованих даних) і хостовий (моніторинг подій, блокування брутфорсу). Проаналізовано загрози (DDoS, брутфорс, SQL-ін'єкції, шкідливе ПЗ, MITM), створено модель мережі й проведено тестування підтвердивши ефективність системи для захисту вузлів.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі повністю виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі виконано детальний аналіз теоретичних основ виявлення атак, де розглянуто сучасні класифікації загроз та методи захисту, такі як аналіз зашифрованого трафіку (SSL Inspection) і поведінковий аналіз. Другий розділ присвячено порівнянню систем виявлення атак, та обґрунтування вибору Suricata, Wazuh та pfSense з модулем pfBlockerNG. У третьому розділі реалізовано практичне впровадження та налаштування з використанням Suricata для аналізу HTTPS-трафіку та Wazuh для моніторингу хостів, а також оцінити ефективність виявлення загроз.

4. Позитивні сторони роботи Робота має практичну цінність, оскільки пропонує комплексний підхід до захисту вузлів корпоративної мережі, поєднуючи мережеві та хостові механізми безпеки. Використання сучасних рішень, таких як pfSense, Suricata, Wazuh та Elastic Stack, забезпечує ефективний моніторинг і реагування на інциденти. Проведене тестування підтверджує дієвість запропонованих заходів, а розроблені рекомендації можуть бути впроваджені у реальних корпоративних середовищах для підвищення рівня кібербезпеки.

5. Негативні сторони роботи Залежність від регулярних оновлень сигнатур і правил. Несвоєчасність оновлень може знизити ефективність системи виявлення атак і пропуску нових загроз.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень у проєктуванні та супроводі розробленої комплексної системи захисту інформації.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні сторони кваліфікаційної роботи, а також негативні сторони, які не зменшують практичну цінність отриманих результатів і загальну якість роботи, рекомендованою оцінкою є "відмінно"

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Бойко Юлій Миколайович, професор кафедри ТМІТ, доктор, технічних наук, професор

« 04 » червня 2025. _____ (підпис)